Asian Quantum Information Science Conference 2024

Abstract Booklet
TALKS

August 26-30, 2024
Venue: Hokkaido University, Sapporo, Japan

Hosted by Hokkaido University

Sponsors

JST Japan Science and Technology Agency
PRESTO
SAKIGAKE

Q-STAR

IBM Quantum

RIKEN
RIKEN QUANTUM COMPUTING

SAPPORO CONVENTION BUREAU

SCAT Support Center for Advanced Telecommunications Technology Research

Murata Science and Education Founda

THE KAJIMA FOUNDATION

2020-2024 Grant-in-Aid for Transformative Research Areas, MEXT, Japan
AFSA Algorithmic Foundations for Social Advancement
Creation and Organization of Innovative Algorithmic Foundations for Social Advancem

Preface

These proceedings contain abstracts for the talks and posters of the 24th Asian Quantum Information Science conference, AQIS'24, held from August 26th to August 30th, 2024, at Hokkaido University, Sapporo, Japan.

AQIS, the successor to the EQIS conferences held in Japan from 2001 to 2005, has been the foremost Asian conference series converging all aspects of quantum information science, the burgeoning interdisciplinary field across quantum physics, computer science, mathematics, and information technologies, which includes theoretical and experimental research in all of the following areas: quantum computation and simulation, from algorithms and complexity to circuit design; quantum programming languages and semantics; quantum information theory; quantum cryptography, communication, and more general network tasks; quantum gate design and architecture; quantum technologies and related fields such as quantum foundations, quantum metrology, many-body quantum (thermo)dynamics, and quantum space-time.

This year's program comprises 7 invited talks, 55 contributed talks (12 long and 43 regular talks), and 218 posters. In response to the Call for Papers, we received record-breaking 312 submissions for talks by the deadline of May 20th. Of these, 55 contributed talks (i.e., the acceptance rate is less than 18%) were selected via intensive reviews within a limited period of time, followed by serious discussions between all members of the Program Committee.

We would like to thank the invited speakers and all authors who submitted abstracts of papers for consideration. We would also like to thank the AQIS'24 conference chair, Prof. Akihisa Tomita; the conference Steering Committee, chaired by Prof. Jaewan Kim; and the Organizing Committee, chaired by Prof. Shigeru Yamashita. Lastly, we would like to express our deep gratitude to all the members of the Program Committee, who accomplished difficult tasks with great perseverance and dedication within such a limited period.

Eleni Diamanti (co-Chair)
Mio Murao (co-Chair)
Seiichiro Tani (Chair)
AQIS 2024 Program Committee Chairs

Conference Chair

Akihisa Tomita (Hokkaido University)

Program Committee

Koji Azuma (NTT)
Hiroo Azuma (National Institute of Informatics)
Joonwoo Bae (KAIST)
Mario Berta (RWTH Aachen University)
Mathieu Bozzio (University of Vienna)
Francesco Buscemi (Nagoya University)
Areeya Chantasri (Mahidol University)
Giulio Chiribella (The University of Hong Kong)
Michele Dall 'Arno (Toyohashi University of Technology)
Usha Devi A R (Bangalore University)
Eleni Diamanti (Sorbonne Université, **Co-Chair**)
Daoyi Dong (Australian National University)
Mile Gu (Nanyang Technological University/National University of Singapore)
Qiongyi He (Peking University)
Itay Hen (USC)
Min-Hsiu Hsieh (Foxconn)
Richard Jozsa (University of Cambridge)
Myungshik Kim (Imperial College London)
Hyukjoon Kwon (KIAS)
Changhyoup Lee (Korea Research Institute of Standards and Science)
Seung-Woo Lee (Korea Institute of Science and Technology)
Yeong-Cherng Liang (National Cheng Kung University)
Nana Liu (Shanghai Jiao Tong University (SJTU))
Xiongfeng Ma (Tsinghua University)
Kosuke Mitarai (Osaka University)
Tomoyuki Morimae (Kyoto University)
Milan Mosonyi (Budapest University of Technology)
Bill Munro (OIST)
Mio Murao (University of Tokyo, **Co-Chair**)
Yasunobu Nakamura (The University of Tokyo)
Yoshifumi Nakata (Kyoto University)
Hui Khoon Ng (NUS)
Harumichi Nishimura (Nagoya University)
Francis Paraan (University of the Philippines Diliman)
Daniel Kyungdeock Park (Yonsei University)
Marco Túlio Quintino (Sorbonne University)
Ravishankar Ramanathan (The University of Hong Kong)
Rudy Raymond (JPMC)
Junghee Ryu (Korea Institute of Science and Technology Information)

Wonmin Son (Sogang University)
Fang Song (Portland State University)
Jun Suzuki (University of Electro-Communications)
Yasunari Suzuki (NTT)
Ryuji Takagi (The University of Tokyo)
Yasuhiro Takahashi (Tsukuba University)
Masahiro Takeoka (Keio University)
Seiichiro Tani (Waseda University, **Chair**)
Xin Wang (Hong Kong University of Science and Technology)
Rebing Wu (Tsinghua University)
Guoyong Xiang (University of Science & Technology of China)
Naoki Yamamoto (Keio University)
Hayata Yamasaki (The University of Tokyo)
Penghui Yao (Nanjing University)
Xiao Yuan (Peking University)
Qi Zhao (University of Hong Kong)

Steering Committee

Charles Bennett (IBM)
Jozef Gruska (Masaryk U)
Guang-Can Guo (USTC)
Hiroshi Imai (U Tokyo, ex-Chair)
Richard Jozsa (U Cambridge)
Jaewan Kim (KIAS, Chair)
Shigeru Yamashita (Ritsumeikan U, Secretary)

Organizing Committee

Hideyuki Miyahara (Hokkaido University)
Yuta Mizuno (Hokkaido University)
Shigeru Yamashita (Ritsumeikan University, Chair)

Program

Oral Presentations

August 26, 2024 (Mon.)

[Invited Talk]

[Long talks]

[Regular Talks (Parallel Session I A)]

[Regular Talks (Parallel Session I B)]

[Invited Talk]

August 27, 2024 (Tue.)

[Invited Talk]

[Long talks]

[Regular Talks (Parallel Session II A)]

[Regular Talks (Parallel Session II B)]

[Invited Talk]

August 28, 2024 (Wed.)

[Invited Talk]

[Regular Talks (Parallel Session III A)]

[Regular Talks (Parallel Session III B)]

August 29, 2024 (Thr.)

[Invited Talk]

[Long Talks]

[Regular Talks (Parallel Session IV A)]

[Regular Talks (Parallel Session IV B)]

[Regular Talks (Parallel Session V A)]

[Regular Talks (Parallel Session V B)]

August 30, 2024 (Fri.)

[Invited Talk]

[Long Talks]

[Regular Talks (Parallel Session VI A)]

[Regular Talks (Parallel Session VI B)]

[Regular Talks (Parallel Session VII A)]

[Regular Talks (Parallel Session VII B)]

Quantum processes with indefinite input-output direction

Giulio Chiribella[1] [2] [3] *

[1] *QICI Quantum Information and Computation Initiative, The University of Hong Kong, Hong Kong, China*
[2] *Department of Computer Science, University of Oxford, Oxford, United Kingdom*
[3] *Perimeter Institute for Theoretical Physics, Waterloo, Canada*

Abstract. At the fundamental level, the dynamics of quantum particles and fields is time-symmetric: their dynamical equations are invariant under inversion of the time coordinate, possibly in conjunction with the change of other physical properties, such as charge and parity. At the operational level, the time-symmetry of the fundamental equations implies that certain quantum devices are bidirectional, meaning that the role of their inputs and outputs can be exchanged. Here we characterize the largest set of operations that can in principle be implemented on bidirectional devices, and show that this set includes operations in which the role of the input and output ports of the given devices becomes indefinite. An example of such an operation, called the "quantum time flip," achieves input-output indefiniteness by adding quantum control to the direction in which a single device is used. We show that quantum operations with indefinite input-output directions can in principle achieve information-theoretic advantages over all possible operations with definite time direction, and can lead to an extrmely strong form of indefinite causal order.

Related works:

G. Chiribella and Z. Liu, Quantum Operations with Indefinite Time Direction, Communication Physics **5**, 190 (2022).

Z. Liu, M. Yang, and G. Chiribella, Quantum communication through devices with indefinite input-output direction, New J. Phys. **25** 043017 (2023).

Y. Guo, Z. Liu, H. Tang, X.-M. Hu, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, and G. Chiribella, Experimental Demonstration of Input-Output Indefiniteness in a Single Quantum Device, Phys. Rev. Lett. **132**, 160201 (2024).

Z. Liu and G. Chiribella, Tsirelson bounds for quantum correlations with indefinite causal order, arXiv:2403.02749.

Keywords: quantum causal structures, time in quantum mechanics, indefinite input-output direction, quantum time flip

*giulio@cs.hku.hk

Color code decoder with improved scaling for correcting circuit-level noise

Seok-Hyung Lee[1] * Andrew Li[1] Stephen D. Bartlett[1]

[1] *Centre for Engineered Quantum Systems, School of Physics, The University of Sydney, Sydney, NSW 2006, Australia*

Abstract. Two-dimensional color codes are a promising candidate for fault-tolerant quantum computing, as they have high encoding rates and transversal implementation of logical Clifford gates. However, decoding color codes presents a significant challenge due to their complex structure. We introduce an efficient color-code decoder that tackles these issues by combining two matching decoders for each color, generalized to handle circuit-level noise by employing detector error models. Our simulations reveal that this decoding strategy nearly reaches the best possible scaling of logical failure ($p_{\text{fail}} \sim p^{d/2}$), where p is the physical noise strength, which significantly outperforms the best matching-based decoders.

Keywords: Quantum error correction, Color code, Decoder

1 Introduction

Two-dimensional (2D) color codes [1, 2], visualized in Fig. 1, are a family of stabilizer quantum error-correcting codes that can be realized with local interactions on a 2D plane, and provide a promising pathway for implementing fault-tolerant quantum computation. Compared to surface codes [3, 4], color codes have several noteworthy advantages: (i) They have higher encoding rates for the same code distance [5], (ii) all the Clifford gates can be implemented transversally [1], and (iii) an arbitrary pair of commuting logical Pauli product operators can be measured in parallel via lattice surgery [6]. In addition, the well-studied Steane code is a small instance of a color code, and recently a number of fault-tolerant operations including transversal logic gates and magic state injection have been demonstrated using color codes [7–11].

For these desirable features to be exploited for fault-tolerant quantum computing in practice, we need better decoders for color codes. Surface codes benefit from the many advantages of a decoding approach based on 'matching', which is a standard method to handle errors in codes that can only have *edge-like* errors (namely, elementary errors violate at most two checks). Matching-based decoders can operate both efficiently and near-optimally, and are readily adapted to handle noisy syndrome extraction circuits. In color codes, an elementary error, which is a single-qubit X or Z error, is generally involved in three checks, and so a matching decoder cannot directly be used. Moreover, considering realistic circuit-level noise makes decoding more difficult because the color code syndrome extraction circuits are more complex than for the surface code. As a result of these deficiencies, existing decoders for the color code do not perform as well as expected either in terms of error thresholds or for sub-threshold scaling of the logical failure rate.

Several approaches to decode errors in color codes have been proposed. The most widely studied methods are the projection decoder and its variants [12–16], which can achieve thresholds of around 8.7% for bit-flip noise [12] and around 0.47% for circuit-level noise [16]. However, they have a fundamental limitation that the logical failure rate p_{fail} scales like $p^{d/3}$ below threshold [14, 16, 17], not $p^{d/2}$, where p is a physical noise strength and d is the code distance. Such a drawback may significantly hinder resource efficiency of quantum computing; roughly speaking, it demands 9/4 times as many qubits than the case with an optimal decoder if other factors are the same. The Möbius decoder [17] is another matching-based decoder, which achieves a higher threshold of 9.0% under bit-flip noise and, more importantly, a better scaling of $p_{\text{fail}} \sim p^{3d/7}$. The decoder has subsequently been improved to accommodate circuit-level noise and general color-code lattices [18].

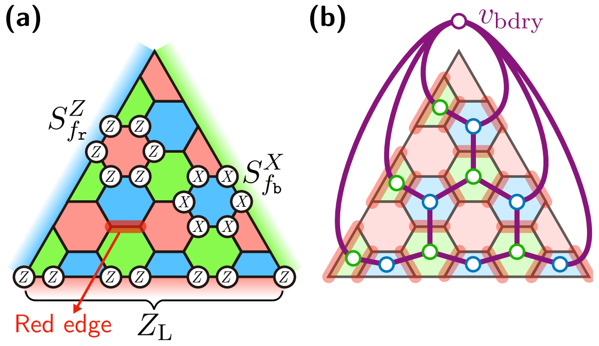


Figure 1: **(a)** Triangular 2D color code with code distance $d = 7$ based on a hexagonal lattice. Each vertex hosts a qubit and each hexagonal face is associated with a pair of Z-type and X-type checks. Logical operators X_L and Z_L are supported on one of the three boundaries. **(b)** Red-restricted lattice. Vertices and edges are shown as blue/green circles and purple lines, respectively.

In this work, we propose a matching-based color-code decoder, which we call the *concatenated minimum-weight perfect matching (MWPM) decoder*, that demonstrates exceptional sub-threshold scaling of the logical failure rate in regimes of interest for fault-tolerant quantum computing. Our decoder functions by 'concatenation' of two matching decoders per color, for a total of six

[*] seokhyung.lee@sydney.edu.au

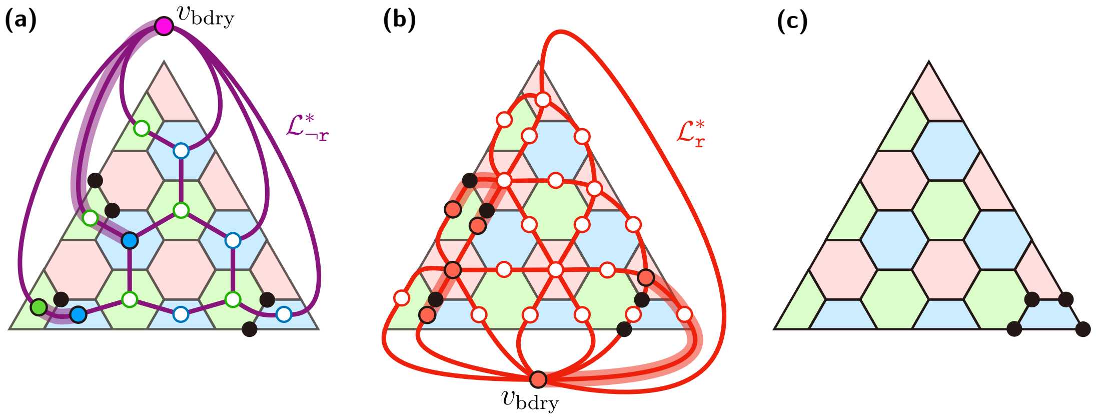

(a)
v_{bdry}
$\mathcal{L}^*_{\neg\mathtt{r}}$
(b)
$\mathcal{L}^*_{\mathtt{r}}$
v_{bdry}
(c)

Figure 2: **Example of executing the concatenated MWPM decoder on the triangular color code of distance 7.** **(a)** First-round MWPM on the red-restricted lattice $\mathcal{L}^*_{\neg\mathtt{r}}$. **(b)** Second-round MWPM on the red-only lattice $\mathcal{L}^*_{\mathtt{r}}$. **(c)** Residual errors after correcting $V^{(\mathtt{r})}_{\text{pred}}$, which is equivalent to a stabilizer.

matchings. We demonstrate that this decoder can be generalized to handle circuit-level noise by using the concept of *detector error model*. Notably, the logical failure rates of the concatenated MWPM decoder below threshold is shown to be well-described by the scaling $p_{\text{fail}} \sim p^{d/2}$ for both bit-flip and circuit-level noise models. Thanks to this improvement, its sub-threshold performance significantly surpasses the projection decoder. Compared to the Möbius decoder, our decoder has a similar scaling factor against d but achieves approximately 3–7 times lower logical failure rates for circuit-level noise when $10^{-4} \lessapprox p \lessapprox 5 \times 10^{-4}$.

Technical description of our work is presented in Ref. [19].

2 Concatenated MWPM decoder

We first describe the 2D variant of the concatenated MWPM decoder that is applicable only when every syndrome measurement is perfect. Let us consider the 2D color code on a lattice $\mathcal{L}_{\text{2D}}$, which may have boundaries. The decoder to predict X errors in a single round can be briefly depicted as follows (see Fig. 2 for an example):

1. **(First-round MWPM)** Input violated blue and green Z-type checks to the MWPM algorithm on the red-restricted lattice $\mathcal{L}^*_{\neg\mathtt{r}}$, which returns a set of edges of $\mathcal{L}^*_{\neg\mathtt{r}}$. This set corresponds to a set $E^{(\mathtt{r})}_{\text{pred}}$ of red edges of $\mathcal{L}_{\text{2D}}$, each of which is predicted to contain one X error. See Fig. 2(a).

2. **(Second-round MWPM)** Input $E^{(\mathtt{r})}_{\text{pred}}$ and violated red Z-type checks to the MWPM algorithm on the 'red-only lattice' $\mathcal{L}^*_{\mathtt{r}}$, which is constructed according to the connection structure of red edges and faces in $\mathcal{L}_{\text{2D}}$. The algorithm returns a set of edges of $\mathcal{L}^*_{\mathtt{r}}$, which correspond to a set of vertices $V^{(\mathtt{r})}_{\text{pred}}$ of $\mathcal{L}_{\text{2D}}$ that are predicted to have errors. See Fig. 2(b).

3. Repeat the above two steps (together referred to as the *red sub-decoding procedure*) while varying the color to green and blue, obtaining $V^{(\mathtt{g})}_{\text{pred}}$ and $V^{(\mathtt{b})}_{\text{pred}}$. Select the smallest one V_{pred} among $V^{(\mathtt{r})}_{\text{pred}}$, $V^{(\mathtt{g})}_{\text{pred}}$, and $V^{(\mathtt{b})}_{\text{pred}}$ as the final outcome.

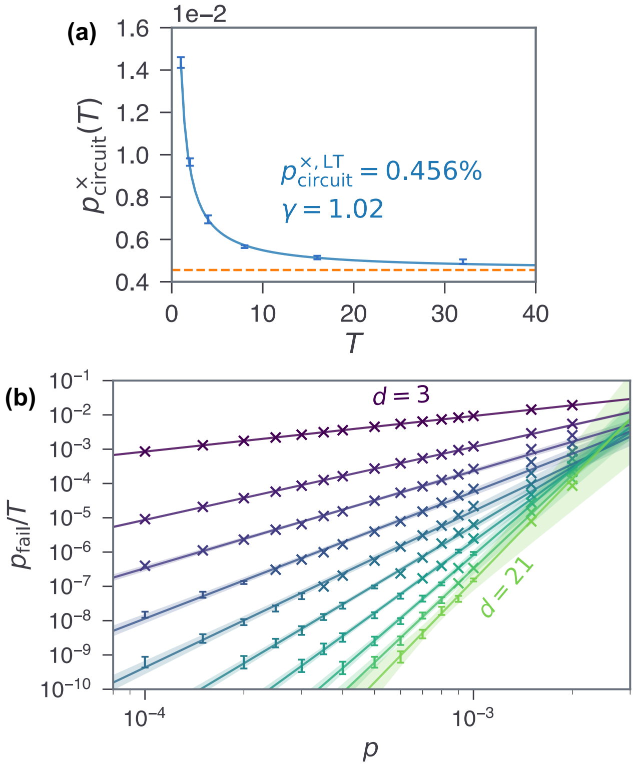


Figure 3: **Numerical analysis of the concatenated MWPM decoder under circuit-level noise.** **(a)** Noise threshold $p^{\times}_{\text{circuit}}(T)$ as a function of the number T of QEC rounds, which converges to $p^{\times,\text{LT}}_{\text{circuit}} \approx 0.456\%$. **(b)** Logical failure rate per round p_{fail}/T against p for various code distances d when p is sufficiently lower than the threshold.

Figure 2(c) presents a set of residual errors after correction, which is equivalent to a stabilizer thus does not

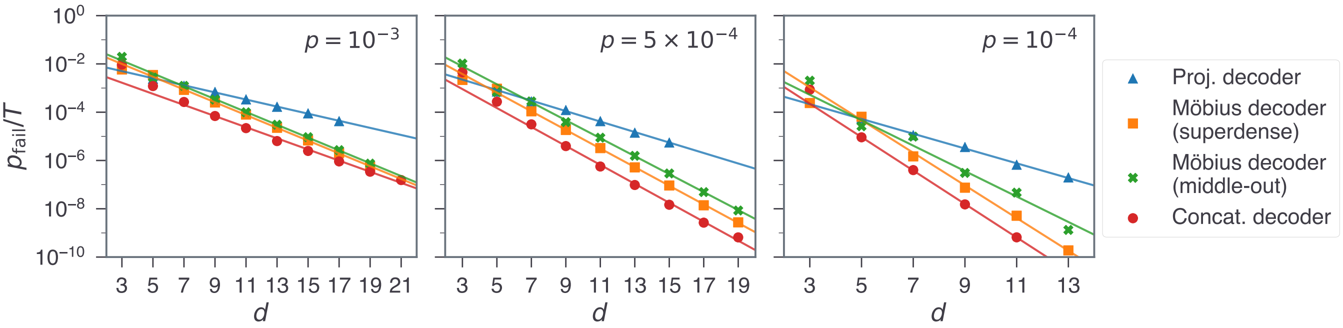


Figure 4: **Comparison of three matching-based decoders under circuit-level noise.** Logical failure rates per round p_{fail}/T are estimated by using three different decoders: projection [14], Möbius [17, 18], and concatenated MWPM decoders. The data for the projection and Möbius decoders are from Ref. [14] and [18], respectively.

cause a logical failure. Z errors can be predicted by decoding X-type check outcomes in an analogous way.

The above scheme cannot handle realistic noise (including measurement errors) that is relevant to fault-tolerant quantum computing. We thus adapt the decoder to a circuit-level noise model, where each preparation/measurement gives an orthogonal outcome with probability p and each unitary gate is followed by a depolarizing noise channel with strength p. We employ detector error models [20] for this, which are lists of independent error mechanisms specifying their probabilities and the set of detectors (i.e., products of measurement outcomes that are deterministic when noiseless) and logical observables damaged by them. We generalize the three steps of the concatenated MWPM decoder using detector error models and employ the *Stim* library [20] to implement and analyze the decoder.

3 Performance analysis

For assessing the performance of the decoder, we consider T rounds of the logical idling gate of the triangular color code with code distance d under circuit-level noise with strength p. The results are summarized in Fig. 3(a) and (b), which are respectively for near-threshold and sub-threshold regimes. From Fig. 3(a), we estimate the long-term threshold of the decoder (when $T \to \infty$) as 0.456%. From Fig. 3(b), we obtain an approximation of the logical failure rate p_{fail} as a function of T, p, and d when $p \lessapprox 0.1\%$: $p_{\mathrm{fail}} \approx (0.0093) \times (p/0.0032)^{0.50d-0.60}$.

Notably, the concatenated MWPM decoder has a significant advantage in terms of the scaling of the failure rate over d and p. Namely, $p_{\mathrm{fail}} \sim p^{0.5d}$ for our decoder within our simulation range of $d \le 31$, while it is $\sim p^{d/3}$ for the projection decoder [14] and $\sim p^{(3/7)d}$ for the Möbius decoder [17, 18]. The impact of this improvement is numerically presented in Fig. 4, which compares the performance (in terms of p_{fail}/T) of the concatenated MWPM decoder with those of these two decoders. The figure shows that the projection decoder significantly underperforms the other two due to its suboptimal scaling against d. The scaling against d is comparably similar for the other two decoders (when $p \lessapprox 5 \times 10^{-4}$); however, the concatenated MWPM decoder achieves logical failure rates that are approximately 3–7 times lower than the Möbius decoder.

More numerical results are presented in our technical description [19]. In particular, we observe that choosing an optimal CNOT schedule is very important as the logical failure rates of the best and worst schedules differ by more than twice.

4 Remarks

In this work, we introduced the concatenated MWPM decoder processed by the concatenation of two rounds of MWPM per color, which is applicable not only to simple bit-flip noise but also to realistic circuit-level noise. The decoder is based on the idea that the outcome obtained from decoding on a restricted lattice can serve as additional 'virtual syndrome data', which undergo a subsequent decoding round in conjunction with remaining syndrome data.

We numerically analyzed the performance of the decoder in various aspects: We considered both bit-flip and circuit-level noise models and investigated near-threshold and sub-threshold behaviors of the logical failure rate p_{fail}. We found that the decoder has the thresholds of 8.2% for bit-flip noise and 0.46% for circuit-level noise, which are comparable with those of previous matching-based decoders such as the projection decoder [12–16] and Möbius MWPM decoder [17, 18]. Remarkably, we verified that the decoder approaches a scaling of $p_{\mathrm{fail}} \sim p^{d/2}$, where p is the noise strength and d is the code distance, at least within our simulation range ($d \lessapprox 31$ for bit-flip noise and $d \lessapprox 21$ for circuit-level noise). As a consequence, it outperforms previous matching-based decoders in terms of their sub-threshold failure rates across both bit-flip and circuit-level noise. We therefore anticipate that our decoder enhances the practicality of employing color codes in quantum computing, which has been considered less viable than surface codes due to its logical failure rate performance despite its advantage in resource efficiency [6]. We distributed a python module implementing the decoder on Github [21] so that other researchers can use it.

References

[1] H. Bombin and M. A. Martin-Delgado. Topological quantum distillation. *Phys. Rev. Lett.*, 97(18): 180501, 2006. doi: 10.1103/PhysRevLett.97.180501.

[2] Héctor Bombín. Topological codes. In Daniel A. Lidar and Todd A. Brun, editors, *Quantum Error Correction*, chapter 19, pages 455–481. Cambridge, 2013. doi: 10.48550/arXiv.1311.0277.

[3] S. B. Bravyi and A. Yu. Kitaev. Quantum codes on a lattice with boundary. *arXiv:quant-ph/9811052*, 1998.

[4] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *J. Math. Phys.*, 43(9):4452–4505, 2002. doi: 10.1063/1.1499754.

[5] Andrew J. Landahl, Jonas T. Anderson, and Patrick R. Rice. Fault-tolerant quantum computing with color codes. *arXiv:1108.5738*, 2011.

[6] Felix Thomsen, Markus S. Kesselring, Stephen D. Bartlett, and Benjamin J. Brown. Low-overhead quantum computing with the color code. *arXiv:2201.07806*, 2022.

[7] Lukas Postler, Sascha Heuβen, Ivan Pogorelov, Manuel Rispler, Thomas Feldker, Michael Meth, Christian D. Marciniak, Roman Stricker, Martin Ringbauer, Rainer Blatt, Philipp Schindler, Markus Müller, and Thomas Monz. Demonstration of fault-tolerant universal quantum gate operations. *Nature*, 605(7911):675–680, May 2022. doi: 10.1038/s41586-022-04721-1.

[8] C. Ryan-Anderson, N. C. Brown, M. S. Allman, B. Arkin, G. Asa-Attuah, C. Baldwin, J. Berg, J. G. Bohnet, S. Braxton, N. Burdick, J. P. Campora, A. Chernoguzov, J. Esposito, B. Evans, D. Francois, J. P. Gaebler, T. M. Gatterman, J. Gerber, K. Gilmore, D. Gresh, A. Hall, A. Hankin, J. Hostetter, D. Lucchetti, K. Mayer, J. Myers, B. Neyenhuis, J. Santiago, J. Sedlacek, T. Skripka, A. Slattery, R. P. Stutz, J. Tait, R. Tobey, G. Vittorini, J. Walker, and D. Hayes. Implementing fault-tolerant entangling gates on the five-qubit code and the color code, 2022.

[9] Dolev Bluvstein, Simon J. Evered, Alexandra A. Geim, Sophie H. Li, Hengyun Zhou, Tom Manovitz, Sepehr Ebadi, Madelyn Cain, Marcin Kalinowski, Dominik Hangleiter, J. Pablo Bonilla Ataides, Nishad Maskara, Iris Cong, Xun Gao, Pedro Sales Rodriguez, Thomas Karolyshyn, Giulia Semeghini, Michael J. Gullans, Markus Greiner, Vladan Vuletić, and Mikhail D. Lukin. Logical quantum processor based on reconfigurable atom arrays. *Nature*, 626(7997):58–65, February 2024. doi: 10.1038/s41586-023-06927-3.

[10] Lukas Postler, Friederike Butt, Ivan Pogorelov, Christian D. Marciniak, Sascha Heußen, Rainer Blatt, Philipp Schindler, Manuel Rispler, Markus Müller, and Thomas Monz. Demonstration of fault-tolerant Steane quantum error correction. *arXiv:2312.09745*, 2023.

[11] Yi-Fei Wang, Yixu Wang, Yu-An Chen, Wenjun Zhang, Tao Zhang, Jiazhong Hu, Wenlan Chen, Yingfei Gu, and Zi-Wen Liu. Efficient fault-tolerant implementations of non-Clifford gates with reconfigurable atom arrays. *arXiv:2312.09111*, 2024.

[12] Nicolas Delfosse. Decoding color codes by projection onto surface codes. *Phys. Rev. A*, 89:012317, Jan 2014. doi: 10.1103/PhysRevA.89.012317.

[13] Christopher Chamberland, Aleksander Kubica, Theodore J. Yoder, and Guanyu Zhu. Triangular color codes on trivalent graphs with flag qubits. *New J. Phys.*, 22(2):023019, 2020. ISSN 1367-2630. doi: 10.1088/1367-2630/ab68fd.

[14] Michael E. Beverland, Aleksander Kubica, and Krysta M. Svore. Cost of universality: A comparative study of the overhead of state distillation and code switching with color codes. *PRX Quantum*, 2(2):020341, 2021. ISSN 2691-3399. doi: 10.1103/PRXQuantum.2.020341.

[15] Aleksander Kubica and Nicolas Delfosse. Efficient color code decoders in $d \geq 2$ dimensions from toric code decoders. *Quantum*, 7:929, February 2023. ISSN 2521-327X. doi: 10.22331/q-2023-02-21-929.

[16] Jiaxuan Zhang, Yu-Chun Wu, and Guo-Ping Guo. Facilitating practical fault-tolerant quantum computing based on color codes. *2309.05222*, 2023.

[17] Kaavya Sahay and Benjamin J. Brown. Decoder for the triangular color code by matching on a Möbius strip. *PRX Quantum*, 3:010310, Jan 2022. doi: 10.1103/PRXQuantum.3.010310.

[18] Craig Gidney and Cody Jones. New circuits and an open source decoder for the color code. *arXiv:2312.08813*, 2023.

[19] Seok-Hyung Lee, Andrew Li, and Stephen D. Bartlett. Color code decoder with improved scaling for correcting circuit-level noise. *arXiv:2404.07482*, 2024.

[20] Craig Gidney. Stim: a fast stabilizer circuit simulator. *Quantum*, 5:497, July 2021. ISSN 2521-327X. doi: 10.22331/q-2021-07-06-497.

[21] Seok-Hyung Lee. Github: color-code-stim. `https://github.com/seokhyung-lee/color-code-stim`, 2024.

Snapshotting Quantum Dynamics at Multiple Time Points

Pengfei Wang[1] [2] Hyukjoon Kwon[3] [*] Chun-Yang Luan[1] Wentao Chen[1] Mu Qiao[1]
Zinan Zhou[1] Kaizhao Wang[1] M. S. Kim,4[3] [†] Kihwan Kim,2,5,6[1] [‡]

[1] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*
[2] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[3] *Korea Institute for Advanced Study, Seoul 02455, Korea*
[4] *Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom*
[5] *Hefei National Laboratory, Hefei 230088, P. R. China*
[6] *Frontier Science Center for Quantum Information, Beijing 100084, China*

Abstract. Measurement-induced state disturbance is a main challenge in obtaining quantum statistics at multiple time points. We introduce a novel method, namely snapshotting quantum dynamics, for extracting temporal quantum statics from intermediate measurements at each time point. This allows us to extract temporal quasi-probability distributions and correlation functions for various time orderings. We experimentally demonstrate the proposed protocol using a $^{171}\mathrm{Yb}^{+}$and $^{138}\mathrm{Ba}^{+}$dual-species trapped-ion system. The nonclassicality of multi-time QPDs is observed by their negativity and complex values, which clearly indicate a contribution of quantum coherence in the dynamics.

Keywords: quantum statistics, quantum correlation function, quasi-probability, trapped-ion system

1 Introduction

A striking difference between quantum and classical mechanics arises from the understanding of measurements. In quantum mechanics, the uncertainty principle asserts that defining a joint probability distribution of statistical properties of non-commuting variables is impossible, prohibiting a description of quantum physics using classical probability theory. The same principle is applied when performing sequential measurements during the quantum state's evolution. The double-slit experiment serves as an illustration of this phenomenon: attempting to extract path information causes the final interference patterns to disappear. Consequently, one cannot attain a classical joint probability distribution that simultaneously describes both the which-path information and the particle's final position. The destructive and irreversible effect of measurements on a quantum system raises an ongoing question: Is it possible to extract the system's information throughout quantum dynamics while minimizing the impact of measurement on subsequent events? In this work, we show that dynamical quantum information can be reconstructed from intermediate measurement outcomes aided by classical post-processing, where the statistics at the latter time are not affected by the measurement at the formal time. We provide a schematic protocol for doing this, which we named snapshotting quantum dynamics.

Technical details are in the Appendix (see also [1]).

2 Snapshotting quantum dynamics

The main idea of snapshotting quantum dynamics (see Fig. 1) is to consider a joint quasi-probability distribution between time points based on the Kirkwood-Dirac (KD) distribution [2, 3]. For example, when a quantum state ρ_{t_1} at time t_1 evolves under a quantum channel $\mathcal{N}_{t_1\to t_2}$, we define the joint measurement statistics at two times t_1, t_2 with outcomes x_1, x_2 as

$$\begin{aligned} p(x_1, x_2; t_1, t_2) &= \mathrm{Tr}\left[\mathcal{N}_{t_1\to t_2}\left(\rho_{t_1}\Pi_{x_1}\right)\Pi_{x_2}\right] \\ &= \mathrm{Tr}\left[\left(\mathcal{M}_{x_2}\circ\mathcal{N}_{t_1\to t_2}\circ\mathcal{M}_{x_1}\right)\rho_{t_1}\right], \end{aligned}$$

where $\mathcal{M}_x(\rho) \equiv \rho\Pi_x$. Such a joint distribution is not a classical probability distribution as it can have negative or non-real values, often referred to as quasi-probability distribution. Nevertheless, the KD distribution preserves the marginal statistics at each time, i.e., $\sum_{x_2} p(x_1, x_2; t_1, t_2) = \mathrm{Tr}\left[\rho_{t_1}\Pi_{x_1}\right]$ and $\sum_{x_1} p(x_1, x_2; t_1, t_2) = \mathrm{Tr}\left[\mathcal{N}_{t_1\to t_2}(\rho_{t_1})\Pi_{x_2}\right] = \mathrm{Tr}\left[\rho_{t_2}\Pi_{x_2}\right]$. We can further generalize this to N-time points as

$$\begin{aligned} &p(x_1, x_2, \cdots, x_N; t_1, t_2, \cdots, t_N) \\ &= \mathrm{Tr}\left[\left(\mathcal{M}_{x_N}\circ\mathcal{N}_{t_{N-1}\to t_N}\circ\cdots\circ\mathcal{N}_{t_1\to t_2}\circ\mathcal{M}_{x_1}\right)\left(\rho_{t_1}\right)\right]. \end{aligned}$$

Our key observation is that these quasi-probability distributions can be obtained from sequential measurement at each time. This can be done by decomposing $\mathcal{M}_x(\rho)$ into a linear combination of weighted Kraus operators as

$$\mathcal{M}_x(\rho) = \sum_m \gamma_{xm} K_m \rho K_m^\dagger$$

with some complex-valued coefficients γ_{xm} (see also Fig. 2).

As Kraus operators with outcomes m can be realized by ancilla-assisted measurements, one can reconstruct the N-time quasi-probability distribution from the intermediate outcomes by averaging over them with the complex value weight as

$$p(x_1, x_2, \cdots, x_N; t_1, t_2, \cdots, t_N) = \mathbb{E}\left[\prod_{i=1}^{N}\gamma_{x_i m_i}\right].$$

[*] hjkwon@kias.re.kr
[†] m.kim@imperial.ac.uk
[‡] kimkihwan@mail.tsinghua.edu.cn

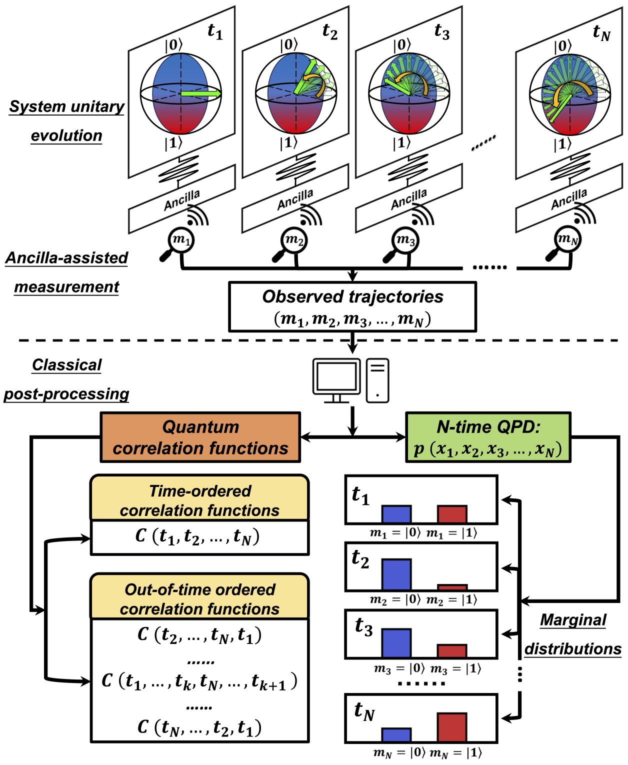

System unitary evolution
t_1
t_2
t_3
t_N
$|0\rangle$
$|1\rangle$
Ancilla
m_1
m_2
m_3
m_N
Ancilla-assisted measurement
Observed trajectories $(m_1, m_2, m_3, \ldots, m_N)$
Classical post-processing
Quantum correlation functions
N-time QPD: $p\,(x_1, x_2, x_3, \ldots, x_N)$
Time-ordered correlation functions
$C\,(t_1, t_2, \ldots, t_N)$
Out-of-time ordered correlation functions
$C\,(t_2, \ldots, t_N, t_1)$
$C\,(t_1, \ldots, t_k, t_N, \ldots, t_{k+1})$
$C\,(t_N, \ldots, t_2, t_1)$
$m_1 = |0\rangle$ $m_1 = |1\rangle$
$m_2 = |0\rangle$ $m_2 = |1\rangle$
$m_3 = |0\rangle$ $m_3 = |1\rangle$
$m_N = |0\rangle$ $m_N = |1\rangle$
Marginal distributions

Figure 1: Schematic procedure for snapshotting quantum dynamics. Various types of information on quantum dynamics are obtained simultaneously through classical post-processing of the intermediate measurement outcomes. These include the multi-time QPD with the correct marginal probabilities at the respective time points, as well as both time-ordered and out-of-time-ordered correlation functions.

Here, $\mathbb{E}[\cdot]$ denotes averaging over all possible sequential measurement outcomes $(m_1, \cdots, m_N)$, which can be understood as the observed trajectories of the quantum dynamics, following the distribution $p^{\mathcal{K}}(m_1, \cdots, m_N) = \mathrm{Tr}[(\mathcal{K}_{m_N} \circ \mathcal{N}_{t_{N-1} \to t_N} \circ \cdots \circ \mathcal{N}_{t_1 \to t_2} \circ \mathcal{K}_{m_1})(\rho_{t_1})]$.

An important consequence of the proposed protocol is that the quasi-probability contains the information of both time- ordered and out-of-time-ordered quantum correlations. In other words, one can obtain the multi-time correlation functions,

$$C(t_1, t_2, \cdots, t_N) = \langle A(t_1) A(t_2) \cdots A(t_N) \rangle,$$

even for the cases where the time-ordering $t_1 \leq t_2 \leq \cdots \leq t_N$ is not satisfied.

As a special case, our approach offers a novel scheme to obtain the out-of-time-ordered correlator (OTOC) throughout quantum dynamics, which has been widely adopted as a quantifier of quantum information scrambling throughout complex quantum dynamics [4]. The OTOC of a quantum system under unitary dynamics U_τ is defined as the absolute square of the commutator between two operators V and W,

$$C_{\mathrm{OTOC}} \equiv \langle [W(\tau), V(0)]^\dagger [W(\tau), V(0)] \rangle, \tag{1}$$

where $V(0) = V$ and $W(\tau) = U_\tau^\dagger W U_\tau$. We note that the OTOC is essentially a linear sum of four-point functions

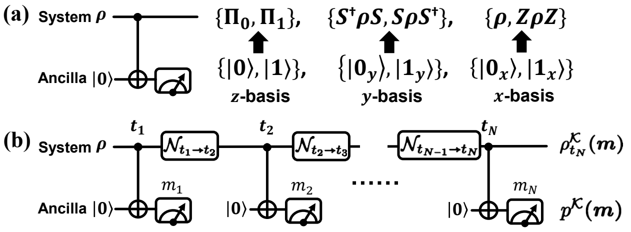

(a) System ρ
Ancilla $|0\rangle$
$\{\Pi_0, \Pi_1\}$,
$\{S^\dagger \rho S, S\rho S^\dagger\}$,
$\{\rho, Z\rho Z\}$
$\{|0\rangle, |1\rangle\}$,
z-basis
$\{|0_y\rangle, |1_y\rangle\}$,
y-basis
$\{|0_x\rangle, |1_x\rangle\}$
x-basis
(b) System ρ
t_1
t_2
t_N
$\mathcal{N}_{t_1 \to t_2}$
$\mathcal{N}_{t_2 \to t_3}$
$\mathcal{N}_{t_{N-1} \to t_N}$
$\rho^{\mathcal{K}}_{t_N}(\boldsymbol{m})$
Ancilla $|0\rangle$
m_1
$|0\rangle$
m_2
$|0\rangle$
m_N
$p^{\mathcal{K}}(\boldsymbol{m})$

Figure 2: (a) Ancilla-assisted measurement for realizing Kraus operators. By performing z-, y- and x-basis measurements on the ancilla, the system state is updated depending on the measurement outcome. (b) The quantum circuit to obtain the QPD $p(x_1, \cdots, x_N)$ for a qubit system. $\mathcal{N}_{t_{N-1} \to t_N}$ describes the dynamics of the system from t_{N-1} to t_N. The ancilla-assisted measurement is performed at each time t_i with the outcome m_i. The system state is updated to $\rho^{\mathcal{K}}_{t_N}(m_1, \cdots, m_N)$ when the measurement outcomes read $(m_1, \cdots, m_N)$, which happens with probability $p^{\mathcal{K}}(m_1, \cdots, m_N)$.

containing both time-ordered and out-of-time-ordered correlation functions. Even though C_{OTOC} in Eq. (1) contains terms with reversed time ordering, C_{OTOC} can be obtained from the sequential measurement outcomes (m_1, m_2, m_3) at three-time points (t_1, t_2, t_3) under the unitary dynamics $U_{t_1 \to t_2} = U_\tau$ and $U_{t_2 \to t_3} = U_\tau^\dagger$ as

$$C_{\mathrm{OTOC}} = \mathbb{E}\left[\prod_{i=1}^{3} \gamma_{m_i}^{\mathrm{OTOC}}\right], \tag{2}$$

with some complex coefficients $\gamma_{m_i}^{\mathrm{OTOC}}$.

Compared to interference-based schemes for obtaining the OTOC [5, 6], our scheme offers the advantage that an ancilla state is required to remain coherent only for a short time during each ancilla-assisted measurement. We highlight that the time-reversal unitary is applied only once in our scheme. This can be contrasted with the weak measurement-based schemes [7, 8], which possess the same advantage as our scheme in ancilla coherence time but require two time-reversals [7, 8].

3 Experimental demonstration

We experimentally demonstrate the proposed scheme using dual-species trapped-ion system. $^{171}\mathrm{Yb}^+$and $^{138}\mathrm{Ba}^+$ions are used as the system qubit and the ancillary qubit for measurement, respectively. We apply two different rotations to the system qubit for two different time intervals (see also Fig. 3). We successfully reconstructed the three-time quasi-probability distribution of the dynamics, whose negative and non-real values indicate the non-classical contributions of coherence. From the quasi-probability distribution, two- and three-point correlation functions for the Pauli Z operator are evaluated, which nicely match the theoretical predictions (see Fig. 3). We also verify that the classical post-processing of our protocol successfully cancels out the impact of measurement when compared to the projective measurement case (see Fig. 4).

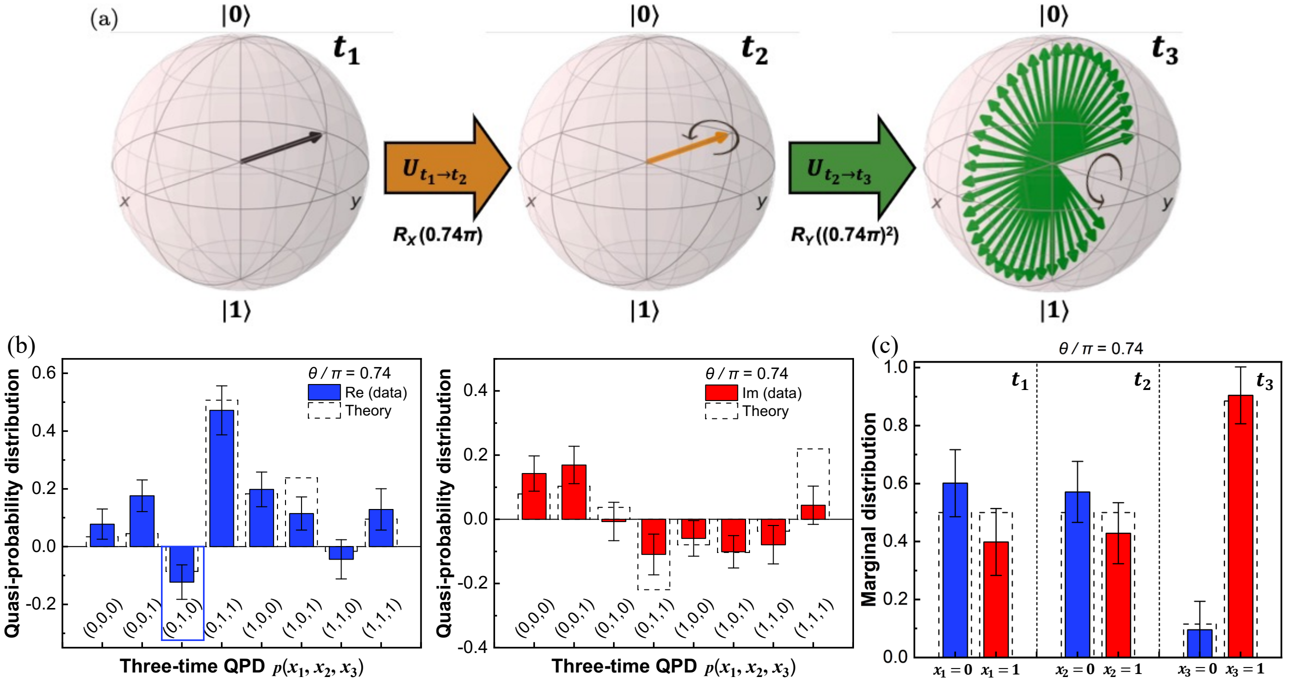


Figure 3: (a) The unitary evolution of the system qubit: the operator $U_{t_1\to t_2} = R_X(\theta)$ rotates the initial state around the x-axis, and the operator $U_{t_2\to t_3} = R_Y(\theta^2)$ further rotates the system state around the y-axis. (b) The three-time QPD $p(x_1, x_2, x_3)$ reconstructed from the observed trajectories by classical postprocessing. The negativity of the real QPD is verified for $p(x_1 = 0, x_2 = 1, x_3 = 0)$ (in blue-dashed-line boxes). (c) The marginal distributions for t_1, t_2, and t_3 under the unitary dynamics show the snapshotting of the state evolution.

4 Remarks

Our protocol provides a systematic approach to extracting quantum statistics from intermediate measurement outcomes aided by classical post-processing. Our method is applicable to any quantum system and dynamics, serving as a valuable experimental tool for exploring the quantum statistics of both open and closed quantum systems. The potential applications include obtaining various critical quantities based on correlation functions, such as OTOC, in quantum many-body systems.

References

[1] P. Wang *et al.*, arXiv:2207.06106.

[2] J. G. Kirkwood, Phys. Rev. **44**, 31 (1933).

[3] P. A. M. Dirac, Rev. Mod. Phys. **17**, 195 (1945).

[4] K. A. Landsman *et al.*, Nature **567**, 61 (2019).

[5] B. Swingle *et al.*, Phys. Rev. A **94**, 040302 (2016).

[6] N. Yunger Halpern, B. Swingle, and J. Dressel, Phys. Rev. A **97**, 042105 (2018).

[7] J. Dressel *et al.*, Phys. Rev. A **98**, 012132 (2018).

[8] R. Mohseninia, J. Raúl G. Alonso, and J. Dressel, Phys. Rev. A **100**, 062336 (2019).

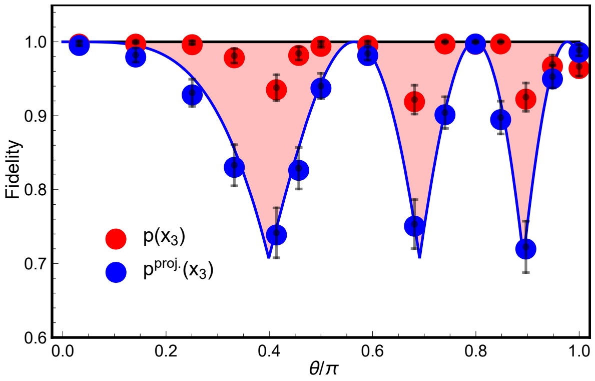


Figure 4: Fidelity between the distributions for the z-basis measurement at time t_3. Red dots refer to the fidelity between the marginal distribution from theory ($p(x_3)$) and the experimentally obtained three-time QPD ($p_{\text{exp.}}(x_3) = \sum_{x_1,x_2} p_{\text{exp.}}(x_1, x_2, x_3)$). The black line refers to the fidelity of 1 when the two distributions are equal. The blue line refers to the theoretical fidelity between $p(x_3)$ and $p^{\text{proj.}}(x_3)$ when projective measurements are performed at times t_1 and t_2. The blue dots refer to the corresponding experimental result.

Snapshotting Quantum Dynamics at Multiple Time Points

Pengfei Wang,[1, 2, *] Hyukjoon Kwon,[3, †] Chun-Yang Luan,[2, *] Wentao Chen,[2] Mu Qiao,[2] Zinan Zhou,[2] Kaizhao Wang,[2] M. S. Kim,[3, 4, ‡] and Kihwan Kim[1, 2, 5, 6, §]

[1]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2]*State Key Laboratory of Low Dimensional Quantum Physics,*
Department of Physics, Tsinghua University, Beijing 100084, China
[3]*Korea Institute for Advanced Study, Seoul 02455, Korea*
[4]*Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom*
[5]*Hefei National Laboratory, Hefei 230088, P. R. China*
[6]*Frontier Science Center for Quantum Information, Beijing 100084, China*

Measurement-induced state disturbance is a major challenge in obtaining quantum statistics at multiple time points. We propose a method to extract dynamic information from a quantum system at intermediate time points, namely snapshotting quantum dynamics. To this end, we apply classical post-processing after performing the ancilla-assisted measurements to cancel out the impact of the measurements at each time point. Based on this, we reconstruct a multi-time quasi-probability distribution (QPD) that correctly recovers the probability distributions at the respective time points. Our approach can also be applied to simultaneously extract exponentially many correlation functions with various time-orderings. We provide a proof-of-principle experimental demonstration of the proposed protocol using a dual-species trapped-ion system by employing $^{171}\mathrm{Yb}^{+}$ and $^{138}\mathrm{Ba}^{+}$ ions as the system and the ancilla, respectively. Multi-time measurements are performed by repeated initialization and detection of the ancilla state without directly measuring the system state. The two- and three-time QPDs and correlation functions are reconstructed reliably from the experiment, negativity and complex values in the QPDs clearly indicate a contribution of the quantum coherence throughout dynamics.

INTRODUCTION

A striking difference between quantum mechanics and classical mechanics arises from understanding the measurements. In quantum mechanics, the uncertainty principle asserts that it is impossible to define a joint probability distribution of statistical properties of non-commuting variables, thus prohibiting a description of quantum physics using classical probability theory. This leads to the introduction of quasi-probability distributions (QPDs), a prototypical example of which is the Wigner function [1] describing quantum phase space. Another important class of QPDs is the Kirkwood-Dirac (KD) distribution [2, 3], which can be applied to any two incompatible sets of measurement operators. The non-classical features in these QPDs, characterized by negative [1, 4] or even non-real values [2, 3], have been investigated within the realms of quantum foundations [5, 6], closely connected to quantum contextuality [7–12], and recently recognized as a resource in quantum computing [13–18] and quantum metrology [19–22].

The same principle is applied when performing sequential measurements during the evolution of a quantum state. The double-slit experiment serves as an illustration of this phenomenon: attempting to extract path information causes the final interference patterns to disappear. Consequently, one cannot obtain a classical joint probability distribution that simultaneously describes both the which-path information and the final position of the particle. The absence of the classical probability description of quantum mechanical processes gives rise to the nonclassicality of temporal correlation described by the Leggett-Garg inequality [6] and the no-go theorem for defining work observables in quantum thermodynamics [23]. Meanwhile, with recent advances in quantum information science, there has been an increasing demand to study multi-time quantum statistics to explore exotic features of quantum dynamics, such as information spreading throughout quantum dynamics [24, 25]. Recently, it has also been shown that monitoring the dynamics of a quantum system at multiple time points can witness entanglement [26].

On the other hand, a major challenge arises when attempting to access these quantum correlations over time in experiments. As observed from the double-slit experiment, direct measurements performed on a quantum state wash out quantum coherences so that they can no longer contribute to the subsequent dynamics. The destructive and irreversible effect of measurements on a quantum system raises an ongoing question: Is it possible to extract information of the system at intermediate points in time throughout quantum dynamics while minimizing the impact of the measurement on subsequent events? The most widely adopted method is the use of weak measurements [27–32] (see Refs. [33–38] for experimental realizations) to gain little information with little disturbance of the system [39–41]. Over the years, various quantum measurement schemes [30, 31, 42] beyond weak measurement have been proposed to extract temporal quantum correlation functions. Alternative approaches have also been explored, including those utilizing long-time entanglement between the system and the ancilla [43–46], as well as methods involving multiple copies of quantum states for each trial [23, 47, 48].

In this work, we propose a novel method to extract dynamical information from a quantum system through ancilla-assisted measurements at intermediate time points, which we term *snapshotting* quantum dynamics. After collecting the ancilla measurement outcomes, they are properly weighted to cancel out the impact of the measurements at each time point, enabling us to obtain multi-time QPDs with correct marginal probabilities at the respective time points.

Our method shares an advantage with sequential weak measurements [31, 36–38], requiring a short interaction time between the system and the ancilla. However, the main difference lies in the ability of our protocol to completely cancel out the measurement effect through classical post-processing, without approximating the system state in the weakly interacting regime.

Another important feature of the proposed protocol is that exponentially many quantum correlation functions can be obtained simultaneously from the N-time ancilla measurement outcomes. This provides a useful methodology for obtaining multiple temporal quantum statistics without changing the experimental settings. In particular, the obtainable correlation functions include the out-of-time-ordered correlator (OTOC), a quantifier of quantum information scrambling [24, 25], which has also been studied in the context of QPDs [46, 49, 50].

We provide a proof-of-principle experimental demonstration of snapshotting to reconstruct multi-time QPDs. We employ a dual-species trapped-ion system consisting of $^{171}\mathrm{Yb}^{+}$ and $^{138}\mathrm{Ba}^{+}$ ions. We realize the required repeated ancilla-assisted measurements through interactions between $^{171}\mathrm{Yb}^{+}$ and $^{138}\mathrm{Ba}^{+}$ ions by performing in-circuit detection (ICD) and in-circuit initialization (ICI) [51–55]. The experimentally reconstructed QPD up to three-time points correctly reveals the marginal distribution at each time, and the correlation functions extracted from them match the quantum mechanical prediction well with the full contribution of coherence. To the best of our knowledge, this is the first direct experimental realization of a quantum mechanical temporal joint distribution beyond two-time points without process tomography.

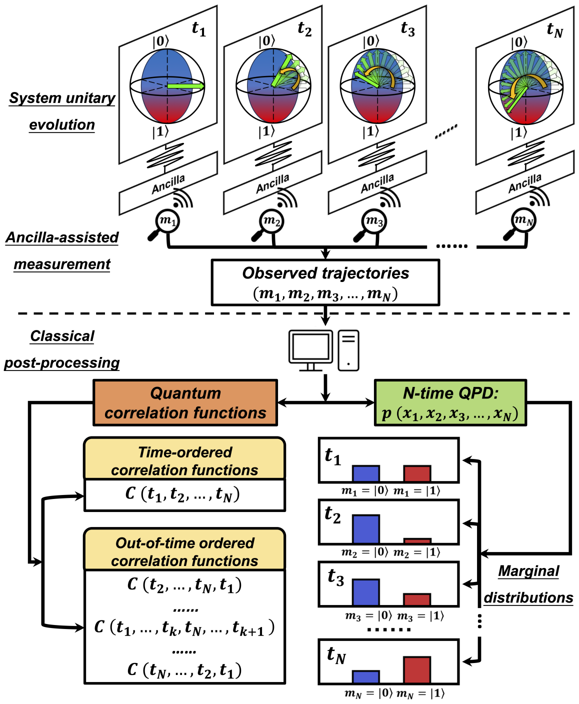

System unitary evolution
t_1
t_2
t_3
t_N
$|0\rangle$
$|1\rangle$
Ancilla
m_1
m_2
m_3
m_N
Ancilla-assisted measurement
Observed trajectories $(m_1, m_2, m_3, \ldots, m_N)$
Classical post-processing
Quantum correlation functions
N-time QPD: $p\,(x_1, x_2, x_3, \ldots, x_N)$
Time-ordered correlation functions
$C\,(t_1, t_2, \ldots, t_N)$
Out-of-time ordered correlation functions
$C\,(t_2, \ldots, t_N, t_1)$
$C\,(t_1, \ldots, t_k, t_N, \ldots, t_{k+1})$
$C\,(t_N, \ldots, t_2, t_1)$
$m_1 = |0\rangle$ $m_1 = |1\rangle$
$m_2 = |0\rangle$ $m_2 = |1\rangle$
$m_3 = |0\rangle$ $m_3 = |1\rangle$
$m_N = |0\rangle$ $m_N = |1\rangle$
Marginal distributions

FIG. 1. Schematic procedure for snapshotting quantum dynamics. Various types of information on quantum dynamics are obtained simultaneously through classical post-processing of the intermediate measurement outcomes. These include the multi-time QPD with the correct marginal probabilities at the respective time points, as well as both time-ordered and out-of-time-ordered correlation functions.

QPD FOR MULTIPLE TIME POINTS

Suppose a quantum state is ρ_{t_i} at t_i and evolves in time. The quantum state at a certain time t_j can be expressed as

$$\rho_{t_j} = \mathcal{N}_{t_i \to t_j}(\rho_{t_i}), \tag{1}$$

where $\mathcal{N}_{t_i \to t_j}$ is a completely positive trace-preserving quantum channel describing the evolution from time t_i to t_j. To obtain the information of the quantum state at time t_i, one may perform measurements given by a set of projection operators $\Pi_{x_i} = |x_i\rangle\langle x_i|$ satisfying $\sum_{x_i} \Pi_{x_i} = \mathbb{1}$, which leads to the outcome distribution of x_i at time t_i, $p(x_i; t_i) = \mathrm{Tr}[\rho_{t_i} \Pi_{x_i}]$. After the measurement is performed, the state collapses to $|x_i\rangle\langle x_i|$. Such a projective measurement incurs a critical issue when obtaining quantum statistics for more than two sequential time points. For example, the joint distribution of outcomes by performing projective measurements at times t_1 and t_2 can be written as $p^{\text{proj.}}(x_1, x_2; t_1, t_2) = p(x_1; t_1)\mathrm{Tr}[\mathcal{N}_{t_1 \to t_2}(|x_1\rangle\langle x_1|)\Pi_{x_2}]$. However, the marginal distribution at time t_2 obtained from the joint distribution $p^{\text{proj.}}(x_1, x_2; t_1, t_2)$ does not match the statistics without the measurement at time t_1, i.e., $\sum_{x_1} p^{\text{proj.}}(x_1, x_2; t_1, t_2) \neq p(x_2; t_2)$. This invokes the so-called measurement problem that the wavefunction collapse induced by the measurement cannot be explained as a direct consequence of the Schrödinger equation [56–58]. Consequently, the joint distribution of projective measurement outcomes becomes unsuitable for providing a complete description of quantum dynamics.

To address such a problem, one can introduce a two-time joint distribution,

$$\begin{aligned} p(x_1,x_2;t_1,t_2) &\equiv \mathrm{Tr}[\mathcal{N}_{t_1\to t_2}(\rho_{t_1}\Pi_{x_1})\Pi_{x_2}] \\ &= \mathrm{Tr}[(\mathcal{M}_{x_2}\circ\mathcal{N}_{t_1\to t_2}\circ\mathcal{M}_{x_1})(\rho_{t_1})], \end{aligned} \tag{2}$$

where $\mathcal{M}_x(\rho) \equiv \rho\Pi_x$. We note that $p(x_1,x_2;t_1,t_2)$ is well-normalized, $\sum_{x_1,x_2} p(x_1,x_2;t_1,t_2) = 1$, and correctly indicates the marginal distribution, $\sum_{x_1} p(x_1,x_2;t_1,t_2) = p(x_2;t_2)$. However, $p(x_1,x_2;t_1,t_2)$ can have complex values, i.e., being a QPD, and can be understood as the KD distribution [2, 3] of the two different measurement operators Π_{x_1} and $\mathcal{N}^\dagger_{t_1\to t_2}(\Pi_{x_2})$ [59]. Such a distribution has been recently rediscovered to provide a useful mathematical formalism to explore the concept of work and the fluctuation theorems in quantum thermodynamics [23, 46, 49, 59–63].

The QPD based on the KD distribution was also generalized to multiple-time points [22, 49]. In this paper, we define N-time QPD as

$$\begin{aligned} &p(x_1,x_2,\cdots,x_N;t_1,t_2,\cdots,t_N) \\ &\equiv \mathrm{Tr}[(\mathcal{M}_{x_N}\circ\mathcal{N}_{t_{N-1}\to t_N}\circ\cdots\circ\mathcal{M}_{x_2}\circ\mathcal{N}_{t_1\to t_2}\circ\mathcal{M}_{x_1})(\rho_{t_1})]. \end{aligned} \tag{3}$$

When the quantum state at each time point commutes with the measurement operator, i.e., $[\rho_{t_i},\Pi_{x_i}] = 0$ for all t_i, the distribution coincides with the classical joint distribution obtained from sequential projective measurements. Consequently, nonclassical values, i.e., negative or non-real values in the QPD capture the coherence of the system state within the measurement basis by witnessing the non-commutativity between the state and the measurement operator (see, e.g., Refs. [10–12, 64] for more detailed analysis). Throughout the manuscript, we will also use a simplified notation $p(x_1,x_2,\cdots,x_N) = p(x_1,x_2,\cdots,x_N;t_1,t_2,\cdots,t_N)$ when the time sequence is trivial from the context.

An important property of the N-time QPD is that it correctly reproduces marginal distributions, satisfying

$$\sum_{x_k} p(x_1,\cdots,x_N) = p(x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_N) \tag{4}$$

for any $k = 1,2,\cdots,N$, where $p(\cdots,x_{k-1},x_{k+1},\cdots) \equiv \mathrm{Tr}[(\cdots\circ\mathcal{M}_{x_{k+1}}\circ\mathcal{N}_{t_{k-1}\to t_{k+1}}\circ\mathcal{M}_{x_{k-1}}\circ\cdots)(\rho_{t_1})]$ is a joint QPD without performing a measurement $\mathcal{M}_{t_k}$ at time t_k. This is known as the Kolmogorov consistency condition in classical probability theory [65]. In other words, the N-time QPD incorporates all the information from the k-time QPDs $p(x_{i_1},x_{i_2},\cdots,x_{i_k};t_{i_1},t_{i_2},\cdots,t_{i_k})$ for any sub-time sequences with $1 \le i_1 < i_2 < \cdots < i_k \le N$. In particular, the marginal distribution of the QPD at a single time t_i, $p(x_i)$, becomes real and non-negative, correctly indicating the probability distribution of the measurement outcome x_i at time t_i.

We also note that the N-time QPD cannot simply be expressed as a product of two-time QPDs, since it does not obey the Markov chain property [65], i.e., $p(x_1,\cdots,x_N) \neq p(x_N|x_{N-1})\cdots p(x_2|x_1)p(x_1)$ with $p(x_k|x_{k-1}) = \frac{p(x_{k-1},x_k)}{p(x_{k-1})}$. We highlight that the quantum channel $\mathcal{N}_{t_k\to t_{k+1}}$ for each time interval is Markovian, hence the non-Markovianity arises from the effect of $\mathcal{M}_{x_k}$.

SNAPSHOTTING QUANTUM DYNAMICS

The primary challenge in dealing with QPDs is that experimental reconstruction is not straightforward due to the presence of negative or non-real values. For the N-time QPD defined in Eq. (3), this stems from the fact that $\mathcal{M}_{x_i}(\rho_{t_i}) = \rho_{t_i}\Pi_{x_i}$ at each time t_i is a non-physical process that does not yield a Hermitian matrix. Our key observation to overcome this issue is that $\mathcal{M}_x$ can be alternatively expressed as a weighted sum of $\mathcal{K}_m(\rho) \equiv K_m\rho K_m^\dagger = p^{\mathcal{K}}(m)\rho_m^{\mathcal{K}}$, which can be interpreted as the result of a generalized measurement with outcome m [66]. The probability of the outcome is given by $p^{\mathcal{K}}(m) = \mathrm{Tr}[\mathcal{K}_m(\rho)] = \mathrm{Tr}[\rho K_m^\dagger K_m]$, and the state after the measurement becomes $\rho_m^{\mathcal{K}} = \frac{K_m\rho K_m^\dagger}{p^{\mathcal{K}}(m)}$. The measurement operators compose a set of Kraus operators $\{K_m\}$, satisfying $\sum_m K_m^\dagger K_m = \mathbb{1}$.

More explicitly, we aim to prove the following expression,

$$\mathcal{M}_x(\rho) = \sum_m \gamma_{xm}\mathcal{K}_m(\rho), \tag{5}$$

with complex-valued coefficients γ_{xm}. The complex coefficients can be implemented via classical post-processing by weighting the measurement outcomes differently, which will be discussed in more detail. For example, the projection onto the computational basis of a qubit system, $\Pi_x = |x\rangle\langle x|$ with $x = 0,1$, can be decomposed into

$$\rho\Pi_x = \frac{\rho - Z\rho Z + 4\Pi_x\rho\Pi_x - i(-1)^x S\rho S^\dagger + i(-1)^x S^\dagger\rho S}{4}, \tag{6}$$

where $S = |0\rangle\langle 0| + i|1\rangle\langle 1|$ is the phase gate. We further note that any Kraus operators can be realized by ancilla-assisted measurements [66]. For the qubit case in Eq. (6), the CNOT gate between the system and the ancilla followed by the ancilla measurement in the x-, y-, and z-bases leads to the set of Kraus operators, $\{K_m\} = \left\{\frac{\Pi_0}{\sqrt{3}}, \frac{\Pi_1}{\sqrt{3}}, \frac{S^\dagger}{\sqrt{6}}, \frac{S}{\sqrt{6}}, \frac{\mathbb{1}}{\sqrt{6}}, \frac{Z}{\sqrt{6}}\right\}$ (see Fig. 2(a)).

This observation can be further generalized to any d dimensional quantum system as follows:

Theorem 1. *For any set of projectors $\{\Pi_x\}_{x=0}^{d-1}$ acting on a d-dimensional quantum state ρ, one can always construct a set of Kraus operators $\{K_m\}$ from ancilla-assisted measurement and find coefficients γ_{xm} satisfying Eq. (5). The Kraus operators are determined by the informationally complete measurement on a d-dimensional ancilla state after its interaction with the system.*

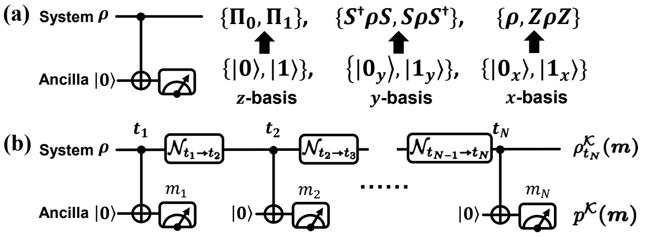

(a)
System ρ
Ancilla $|0\rangle$
$\{\Pi_0, \Pi_1\}$,
$\{S^\dagger \rho S, S\rho S^\dagger\}$,
$\{\rho, Z\rho Z\}$
$\{|0\rangle, |1\rangle\}$,
$\{|0_y\rangle, |1_y\rangle\}$,
$\{|0_x\rangle, |1_x\rangle\}$
z-basis
y-basis
x-basis
(b)
System ρ
t_1
$\mathcal{N}_{t_1\to t_2}$
t_2
$\mathcal{N}_{t_2\to t_3}$
$\mathcal{N}_{t_{N-1}\to t_N}$
t_N
$\rho^{\mathcal{K}}_{t_N}(\boldsymbol{m})$
Ancilla $|0\rangle$
m_1
$|0\rangle$
m_2
......
$|0\rangle$
m_N
$p^{\mathcal{K}}(\boldsymbol{m})$

FIG. 2. (a) Ancilla-assisted measurement for realizing Kraus operators. By performing z-, y- and x-basis measurements on the ancilla, the system state is updated depending on the measurement outcome. (b) The quantum circuit to obtain the QPD $p(x_1, \cdots, x_N)$ for a qubit system. $\mathcal{N}_{t_{N-1}\to t_N}$ describes the dynamics of the system from t_{N-1} to t_N. The ancilla-assisted measurement is performed at each time t_i with the outcome m_i. The system state is updated to $\rho^{\mathcal{K}}_{t_N}(m_1, \cdots, m_N)$ when the measurement outcomes read $(m_1, \cdots, m_N)$, which happens with probability $p^{\mathcal{K}}(m_1, \cdots, m_N)$.

The proof of Theorem 1 with more details can be found in Methods.

Now, we introduce a protocol for snapshotting quantum dynamics via intermediate measurements. As an illustrative example, we show that the two-time QPD $p(x_1, x_2; t_1, t_2)$ can be obtained by ancilla-assisted measurements at times t_1 and t_2 as follows. At time t_1, we interact the state ρ_{t_1} with the ancilla and measure the ancilla state. For the ancilla state's outcome m_1, the system state is updated to $\rho^{\mathcal{K}}_{t_1}(m_1) = \frac{\mathcal{K}_{m_1}(\rho_{t_1})}{p^{\mathcal{K}}_{t_1}(m_1)}$ with probability $p^{\mathcal{K}}_{t_1}(m_1) = \mathrm{Tr}[\mathcal{K}_{m_1}(\rho_{t_1})]$. Subsequently, the system evolves to $\rho^{\mathcal{K}}_{t_2}(m_1) = \mathcal{N}_{t_1\to t_2}\left(\rho^{\mathcal{K}}_{t_1}(m_1)\right)$ from time t_1 to t_2. We then perform the second measurement at time t_2. When the outcome is m_2, the system state is updated to $\rho^{\mathcal{K}}_{t_2}(m_1, m_2) = \frac{\mathcal{K}_{m_2}(\rho^{\mathcal{K}}_{t_2}(m_1))}{p^{\mathcal{K}}_{t_2}(m_2|m_1)}$ with conditional probability $p^{\mathcal{K}}_{t_2}(m_2|m_1) = \mathrm{Tr}[\mathcal{K}_{m_2}(\rho^{\mathcal{K}}_{t_2}(m_1))]$ for a given first measurement outcome m_1. The joint probability of the sequential measurement outcome (m_1, m_2) becomes $p^{\mathcal{K}}(m_1, m_2) = p^{\mathcal{K}}_{t_1}(m_1)p^{\mathcal{K}}_{t_2}(m_2|m_1) = \mathrm{Tr}[(\mathcal{K}_{m_2} \circ \mathcal{N}_{t_1\to t_2} \circ \mathcal{K}_{m_1})(\rho_{t_1})]$. We note that this joint probability is a classical probability distribution that can be obtained directly from the outcome statistics.

We emphasize that the QPD $p(x_1, x_2)$ and the classical joint distribution $p^{\mathcal{K}}(m_1, m_2)$ are linked through Eq. (5) in the form of $p(x_1, x_2) = \sum_{m_1, m_2} \gamma_{x_1 m_1}\gamma_{x_2 m_2} p^{\mathcal{K}}(m_1, m_2)$. Therefore once the probability distribution $p^{\mathcal{K}}(m_1, m_2)$ is obtained from the measurement outcomes, $p(x_1, x_2)$ can be reconstructed via classical post-processing by the weighted sum of these probabilities.

As shown in Fig. 2(b), it is straightforward to repeat this protocol for multiple time points, which leads to the following expression of the N-time QPD:

$$\begin{aligned} p(x_1, \cdots, x_N) &= \sum_{m_1, \cdots, m_N} p^{\mathcal{K}}(m_1, \cdots, m_N)\left[\prod_{i=1}^{N} \gamma_{x_i m_i}\right] \\ &= \mathbb{E}\left[\prod_{i=1}^{N} \gamma_{x_i m_i}\right], \end{aligned} \tag{7}$$

where $\mathbb{E}[\cdot]$ denotes averaging over all possible sequential measurement outcomes $(m_1, \cdots, m_N)$, which can be understood as the observed trajectories of the quantum dynamics, following the distribution $p^{\mathcal{K}}(m_1, \cdots, m_N) = \mathrm{Tr}[(\mathcal{K}_{m_N} \circ \mathcal{N}_{t_{N-1}\to t_N} \circ \cdots \circ \mathcal{N}_{t_1\to t_2} \circ \mathcal{K}_{m_1})(\rho_{t_1})]$.

We note that the number of observed trajectories to be collected to reconstruct quantum statistics $p(x_1, \cdots, x_N)$ is greater than that for classical statistics $p^{\mathcal{K}}(m_1, \cdots, m_N)$ with the same precision. More precisely, the number of trajectories M_{traj} to estimate $p(x_1, \cdots, x_N)$ for each time point within a fixed precision ϵ with probability $1 - \delta$ scales as $M_{\mathrm{traj}} = \frac{2(\max_{x,m}|\gamma_{xm}|)^{2N}}{\epsilon}\ln(2/\delta)$ from Hoeffding's inequality [67]. Our protocol can also be applied to local projectors of multi-qubit systems with the same sampling overhead. We also provide a systematic algorithm to find the optimal coefficient γ_{xm} to reconstruct the joint probability with the minimum number of measurement outcomes (see Methods).

The resource requirement of the proposed protocol can be compared to other schemes for obtaining the KD distribution, while explicit comparisons between these protocols are challenging due to their different natures (see also Refs. [49, 59] for an overview). Compared to the two-point measurement-based scheme [42], which requires the measurement of multiple measurement distributions to infer the KD distribution, our protocol only requires a single measurement distribution $p^{\mathcal{K}}(m_1, m_2)$. The main difference compared to the weak measurement-based schemes [30, 31] is that our protocol does not need to implement a weak coupling between the system and the ancilla to ensure that the system is undisturbed. While the schemes [68, 69] entailing strong measurements for two-time points share a similar structure with our protocol, our protocol provides a straightforward multi-time generalization. Another scheme based on characteristic function estimation [43] requires classical post-processing of the inverse Fourier transform, while our protocol has a relatively simple post-processing with pre-determined coefficients $\gamma_{x_i m_i}$. The interference-based scheme [46] requires overlapping measurement and tomography of a quantum state in some occasions, both of which are not required in our scheme. A recently proposed quantum circuit model based on the block-encoding [70] could have a lower sampling cost than our protocol, but its application is limited to unitary dynamics and requires the implementation of the inverse unitary channel.

Taking into account the physical constraints, our protocol has a short time of system-ancilla coherence during a measurement process at each time, which has an advantage over interferometric schemes [43, 46] that require a long time of system-ancilla coherence throughout the entire protocol. While applying measurements in sequential times could also be a challenging task, it has been realized on various physical platforms [36, 48, 71–74]. We also note that such intermediate measurement has been an active research area, as being an essential technique for quantum information processing, such as syndrome detection for quantum error correction [66].

In the following section, we discuss that the classical post-processing of the sequential measurement outcomes leads to a unique feature of our approach, which allows the simultaneous extraction of exponentially many correlation functions.

EXTRACTION OF MULTI-TIME CORRELATION FUNCTIONS

While the N-time QPD provides valuable information about the marginal distribution at each time, its utility can even go beyond that. We demonstrate that correlation functions with different time-orderings can be obtained simultaneously from the N-time QPD. The quantum correlation function of an observable A throughout unitary quantum dynamics given by $U_{t_i \to t_j}$ is defined as

$$C(t_1, \cdots, t_N) \equiv \langle A(t_1) \cdots A(t_N) \rangle \equiv \mathrm{Tr}[\rho_{t_0} A(t_1) \cdots A(t_N)], \tag{8}$$

where $A(t_i) = U^{\dagger}_{t_0 \to t_i} A U_{t_0 \to t_i}$ is an observable in the Heisenberg picture. If the time sequence is given in increasing order, i.e., $t_1 \le t_2 \le \cdots \le t_N$, the correlation function is called time-ordered, otherwise it is called out-of-time-ordered.

Using the eigenvalue decomposition of the observable, $A = \sum_x a_x \Pi_x$, the time-ordered correlation function can be expressed in terms of the QPD as

$$C(t_1, \cdots, t_N) = \sum_{x_1, \cdots, x_N} a_{x_1} \cdots a_{x_N} p(x_1, \cdots, x_N). \tag{9}$$

Furthermore, as the N-time QPD contains any k-time QPD with $k \le N$, all lower order correlation functions can also be obtained from $p(x_1, \cdots, x_N)$. For example, one can simultaneously obtain a complete set of time-ordered correlation functions $\{C(t_1), C(t_2), C(t_3)\}$, $C(t_1, t_2), C(t_2, t_3), C(t_1, t_3)\}$, and $C(t_1, t_2, t_3)$ from the three-time QPD $p(x_1, x_2, x_3)$.

More surprisingly, the snapshotting method can be utilized to obtain a family of out-of-time-ordered quantum correlation functions, summarized by the following observation.

Observation 1. *All correlation functions $C(t_{\mu_1}, \cdots, t_{\mu_j}, t_{\mu_{j+1}} \cdots, t_{\mu_k})$ with $\mu_1 \le \mu_2 \le \cdots \le \mu_{j-1} \le \mu_j$ and $\mu_j \ge \mu_{j+1} \ge \cdots \ge \mu_{k-1} \ge \mu_k$ for some $\mu_j \le N$ can be simultaneously deduced from the distribution of observed trajectories $p^{\mathcal{K}}(m_1, \cdots, m_N)$.*

This can be shown by expressing the correlation function as $C(t_{\mu_1}, \cdots, t_{\mu_j}, \cdots, t_{\mu_k}) = \mathrm{Tr}[A(t_{\mu_{j+1}}) \cdots A(t_{\mu_k}) \rho_{t_0} A(t_{\mu_1}) \cdots A(t_{\mu_j})]$, with two monotonically increasing sub-time sequences $t_{\mu_1} \le t_{\mu_2} \le \cdots \le t_{\mu_j}$ and $t_{\mu_k} \le t_{\mu_{k-1}} \le \cdots \le t_{\mu_{j+1}}$. The correlation function is then expressed in terms of $p^{\mathcal{K}}(m_1, \cdots, m_N)$ by noting that $\rho_{t_i} A$, $A \rho_{t_i}$, and $A \rho_{t_i} A$ can be simultaneously decomposed as a linear sum of $\mathcal{K}_{m_i}(\rho_{t_i})$ at each time t_i (see Methods for detailed discussions). We highlight that our approach allows a systematic protocol to obtain both time-ordered and out-of-time-ordered correlation functions from a single set of measurement data $p^{\mathcal{K}}(m_1, \cdots, m_N)$, without changing the setting for each correlation function. For example, in the three-time case, one can additionally access the out-of-time-ordered correlation functions $C(t_3, t_2, t_1)$, $C(t_2, t_3, t_1)$, and $C(t_1, t_3, t_2)$. The number of correlation functions that can be obtained from the N-time distribution $p^{\mathcal{K}}(m_1, \cdots, m_N)$ scales exponentially as $\approx 2^N$, since there are two choices for $A(t_i)$ to be placed either on the left or on the right sides of the quantum state ρ_{t_i} at each time t_i. The out-of-time-ordered QPDs can also be obtained in the same way by taking $A(t_i) = \Pi_{x_i}(t_i)$.

As a special case, our approach offers a novel scheme to obtain the OTOC throughout quantum dynamics, which has been widely adopted as a quantifier of quantum information scrambling throughout complex quantum dynamics [24, 25]. The OTOC of a quantum system under unitary dynamics U_τ is defined as the absolute square of the commutator between two operators V and W,

$$C_{\mathrm{OTOC}} \equiv \langle [W(\tau), V(0)]^{\dagger} [W(\tau), V(0)] \rangle, \tag{10}$$

where $V(0) = V$ and $W(\tau) = U^{\dagger}_{\tau} W U_{\tau}$. We note that the OTOC is essentially a linear sum of four-point functions containing both time-ordered and out-of-time-ordered correlation functions. For example, if both V and W are Hermitian and unitary, $C_{\mathrm{OTOC}} = 2(1 - \langle W(\tau) V(0) W(\tau) V(0) \rangle)$. Even though C_{OTOC} in Eq. (10) contains terms with reversed time ordering, $p^{\mathcal{K}}(m_1, m_2, m_3)$ obtained from the three-time snapshotting method enables us to evaluate its value described as follows (see Methods):

Observation 2. *C_{OTOC} can be obtained from the sequential measurement outcomes (m_1, m_2, m_3) at three-time points (t_1, t_2, t_3) under the unitary dynamics $U_{t_1 \to t_2} = U_\tau$ and $U_{t_2 \to t_3} = U^{\dagger}_{\tau}$ as*

$$C_{\mathrm{OTOC}} = \mathbb{E}\left[\prod_{i=1}^{3} \gamma^{\mathrm{OTOC}}_{m_i} \right], \tag{11}$$

with the Kraus operator described in Theorem 1 and some complex coefficients $\gamma^{\mathrm{OTOC}}_{m_i}$.

Compared to interference-based schemes for obtaining the OTOC [45–47, 75, 76], our scheme offers the advantage that an ancilla state is required to remain coherent only for a short time during each ancilla-assisted measurement. We highlight that the time-reversal unitary is applied only once in our scheme. This can be contrasted with the weak measurement-based schemes [46, 49, 77], which possess the same advantage as our scheme in ancilla coherence time but require two time-reversals [46, 49, 77]. On the other hand, the stability of the protocol against imperfect implementations of the time-reversal unitary [78, 79] remains open for quantitative comparison with an interference-based scheme without time reversals [46, 47]. We also note that our scheme works for any diagonalizable operators V and W, nor on the target state ρ.

EXPERIMENTAL REALIZATION

We experimentally demonstrate the proposed protocol with trapped ions. A crucial part of the protocol is the repeated measurement (ICD) and initialization (ICI) of the ancilla without influencing the system, which are also core technologies for quantum error correction. In trapped-ion systems, the ICD and ICI can be achieved by adopting ion shuttling [80–84] or multiple types of qubits [53, 85–92]. Here, we employ two different species trapped in a single trap, $^{171}\mathrm{Yb}^{+}$and $^{138}\mathrm{Ba}^{+}$ions [90, 93, 94], which are used for the system qubit and the ancilla qubit, respectively. Both trapped ions are controlled by lasers with different wavelengths so that they can be controlled independently with minimal influence on each other [90].

In the experiment, the system qubit is encoded in the hyperfine levels of the $S_{1/2}$ manifold of the $^{171}\mathrm{Yb}^{+}$ ion, $|F=0, m_F=0\rangle = |0\rangle_{\mathrm{Yb}}$ and $|F=1, m_F=0\rangle = |1\rangle_{\mathrm{Yb}}$ with a splitting of 12.6428 GHz. The ancilla qubit is encoded in Zeeman levels of the $S_{1/2}$ manifold of the $^{138}\mathrm{Ba}^{+}$ ion, $|s_j=1/2\rangle = |0\rangle_{\mathrm{Ba}}$ and $|s_j=-1/2\rangle = |1\rangle_{\mathrm{Ba}}$ with an energy splitting of 16.2 MHz. Raman transitions are used to individually manipulate the $^{171}\mathrm{Yb}^{+}$ and $^{138}\mathrm{Ba}^{+}$ ion-qubits with 355 nm and 532 nm lasers, respectively. For the entangling operations for both qubits, we simultaneously apply the 355 nm and 532 nm laser beams with appropriately chosen frequencies (see Methods).

We implement the quantum circuit in Fig. 2 to reconstruct the multi-time QPD for a qubit system. The experimental realization for the essential parts of the circuit is shown in Fig. 3. At the beginning of the protocol, we optically pump the system qubit to $|0\rangle_{\mathrm{Yb}}$, then prepare the state of ρ_{Yb} by using a single-qubit rotation performed by applying 355 nm Raman laser beams. As depicted in Fig. 3(a), the Raman lasers have a frequency difference that matches the transition frequency of the $^{171}\mathrm{Yb}^{+}$ion-qubit. This frequency matching allows the Raman lasers to drive unitary evolutions, specifically single-qubit rotations, on the $^{171}\mathrm{Yb}^{+}$ion-qubit, At time t_1, we perform the ancilla-assisted measurement as illustrated in Fig. 3(a). The measurement procedure consists of initializing the ancilla qubit, applying a CNOT gate, and detecting the ancilla qubit state, where the first and third steps are regarded as the ICI and ICD. We perform the CNOT gate by using the Mølmer-Sørensen (M-S) gate [95] and single-qubit operations shown in Fig. 3(b). The z-basis measurement of the $^{138}\mathrm{Ba}^{+}$ ion is realized by fluorescence detection after shelving $|0\rangle_{\mathrm{Ba}}$ to $D_{5/2}$ manifold. The x- and y-basis measurements are realized by rotating the axis of the $^{138}\mathrm{Ba}^{+}$ ion state before the z-basis measurement. We repeat the protocol by applying the next unitary evolution on the system qubit, followed by the ancilla-assisted measurement. We simplify the final measurement by using a projection measurement on the system qubit of $^{171}\mathrm{Yb}^{+}$ ion in the basis $m_N \in \{|0\rangle, |1\rangle\}$, since no further measurements are performed after that.

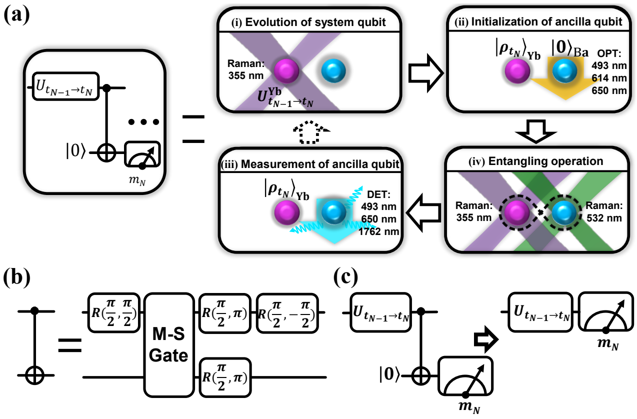

(a)
$U_{t_{N-1}\to t_N}$
$|0\rangle$
m_N
(i) Evolution of system qubit
Raman: 355 nm
$U^{\mathrm{Yb}}_{t_{N-1}\to t_N}$
(ii) Initialization of ancilla qubit
$|\rho_{t_N}\rangle_{\mathrm{Yb}}$
$|0\rangle_{\mathrm{Ba}}$
OPT: 493 nm 614 nm 650 nm
(iii) Measurement of ancilla qubit
$|\rho_{t_N}\rangle_{\mathrm{Yb}}$
DET: 493 nm 650 nm 1762 nm
(iv) Entangling operation
Raman: 355 nm
Raman: 532 nm
(b)
$R(\frac{\pi}{2},\frac{\pi}{2})$
M-S Gate
$R(\frac{\pi}{2},\pi)$
$R(\frac{\pi}{2},-\frac{\pi}{2})$
$R(\frac{\pi}{2},\pi)$
(c)
$U_{t_{N-1}\to t_N}$
$|0\rangle$
m_N
$U_{t_{N-1}\to t_N}$
m_N

FIG. 3. Experimental realization of unitary evolution and ancilla-assisted measurement with $^{171}\mathrm{Yb}^{+}$-$^{138}\mathrm{Ba}^{+}$ trapped-ion system. (a) A unitary operation $U_{t_{N-1}\to t_N}$ is performed by applying Raman laser beams to the system qubit represented by the pink ball. The ancilla-assisted measurement is realized with the following three steps: (i) initialization of the $^{138}\mathrm{Ba}^{+}$ qubit represented by the blue ball to $|0\rangle_{\mathrm{Ba}}$ by optical pumping (OPT), (ii) application of a CNOT gate between two qubits through an entangling operation, and (iii) measurement of the ancilla qubit with fluorescence detection (DET). (b) The CNOT gate consists of an M-S gate and four single-qubit rotations. The M-S gate can be described as $\exp(-i\frac{\pi}{4}X\otimes X)$, where X is the Pauli operator. The single-qubit rotation is defined as $R(\theta,\phi) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -ie^{-i\phi}\sin(\frac{\theta}{2}) \\ -ie^{i\phi}\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$. (c) The final time measurement can be performed by direct measurement in basis $m_N \in \{|0\rangle, |1\rangle\}$ on the system qubit.

As a concrete example, we reconstruct the three-time QPDs with the initial state $\rho_{\mathrm{Yb}} = (|1_x\rangle\langle 1_x|)_{\mathrm{Yb}}$ at time t_1, where $|1_x\rangle_{\mathrm{Yb}} = (|0\rangle_{\mathrm{Yb}} - |1\rangle_{\mathrm{Yb}})/\sqrt{2}$. The unitary evolution from time t_1 to t_2 is described as $U_{t_1\to t_2} = R_X(\theta) = e^{-i\frac{\theta}{2}X}$, and the evolution from t_2 to t_3 is described as $U_{t_2\to t_3} =$

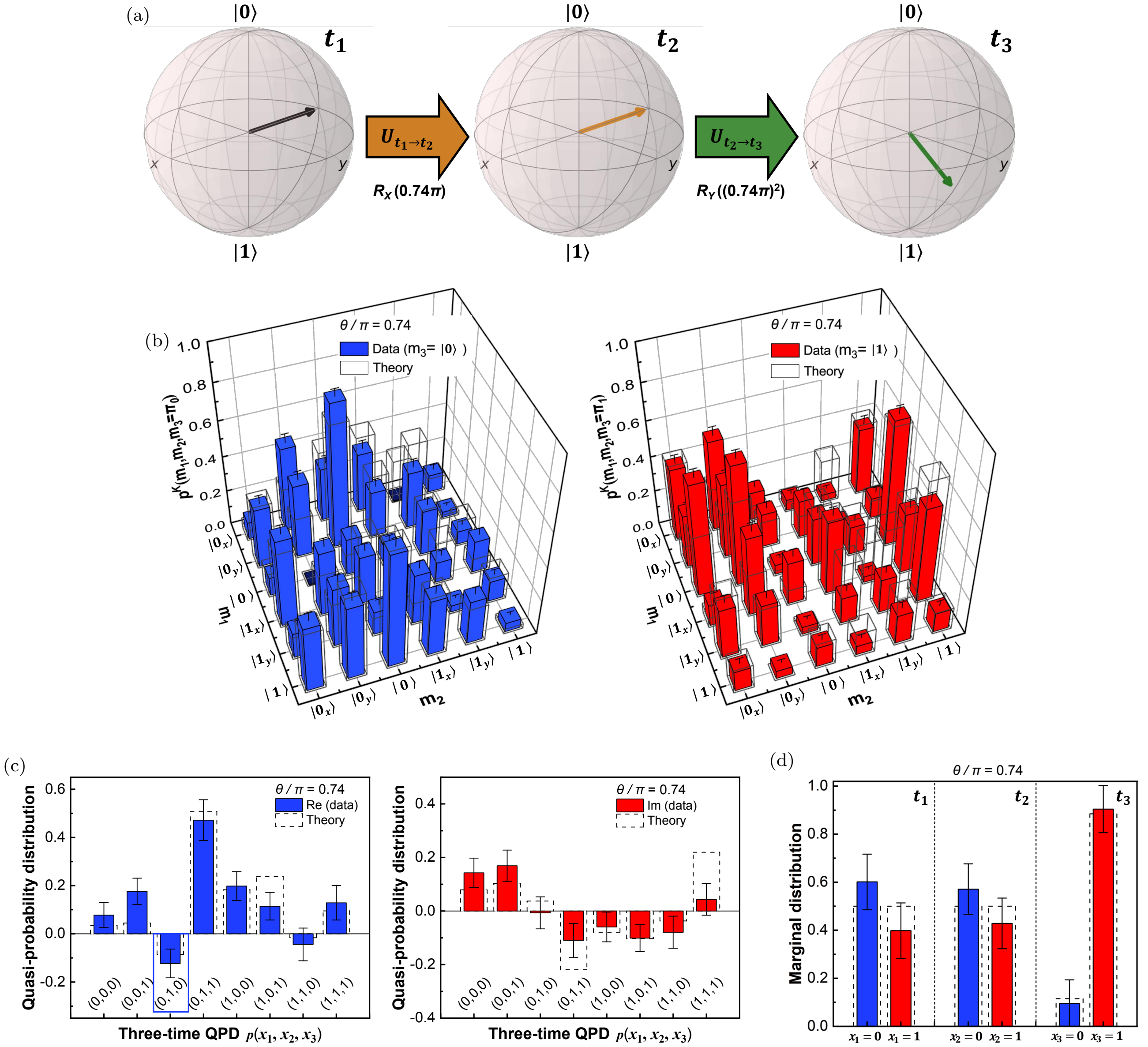


FIG. 4. The experimental reconstruction of the three-time QPD and marginal distribution by the ancilla-assisted measurement for $\theta/\pi = 0.74$. (a) The unitary evolution of the system qubit is shown in the Bloch representation. The operator $U_{t_1\to t_2} = R_X(\theta)$ rotates the initial state around the x-axis, and the operator $U_{t_2\to t_3} = R_Y(\theta^2)$ further rotates the system state around the y-axis. (b) The normalized observed trajectories from the measurements at t_1, t_2, and t_3 are represented by the 2D bar charts, where $m_1, m_2 \in \{|0_x\rangle, |0_y\rangle, |0\rangle, |1_x\rangle, |1_y\rangle, |1\rangle\}$. The bar charts on the left and right represent the observed trajectories of $m_3 = |0\rangle$ and $m_3 = |1\rangle$, respectively, which are the measurement results of t_3. (c) The three-time QPD $p(x_1, x_2, x_3)$ reconstructed from the observed trajectories by classical processing. (i) The left blue bars indicate the real parts of the reconstructed three-time QPD, and the negativity of the real QPD is verified for $p(x_1 = 0, x_2 = 1, x_3 = 0)$ (in blue-dashed-line boxes), which is −0.123(±0.060). (ii) The right red bars indicate the imaginary parts of the reconstructed three-time QPD. (d) The marginal distributions for t_1, t_2, and t_3 under the unitary dynamics $U_{t_1\to t_2}$ and $U_{t_2\to t_3}$ show the snapshotting of the state evolution. The distributions are marginalized over all the other time points of the QPDs. For all figures, error bars indicate standard deviations (STDs), and theoretical expectations are shown as dashed bars (see Methods for details).

$R_Y(\theta^2) = e^{-i\frac{\theta^2}{2}Y}$. Since the unitary evolution from time t_1 to t_2 is a rotation around the x-axis, the system state remains the same if no measurement is performed at time t_1. However, if a measurement is made on the z-basis at time t_1, the state collapses to $|0\rangle$ or $|1\rangle$ and then rotates under the evolution $U_{t_1\to t_2}$. This scenario illustrates how measurements can significantly influence the subsequent dynamics of a quantum system. From time t_2 to t_3, the unitary evolution rotates the system qubit around the y-axis with angle θ^2, which leads to non-trivial behaviors of the QPDs and correlation functions beyond sinusoidal functions of θ. The three-time QPD is then expressed as

$$\begin{aligned} &p(x_1,x_2,x_3)\\ =&\mathrm{Tr}\left[U_{t_2\to t_3}U_{t_1\to t_2}\rho_{t_1}\Pi_{x_1}U^\dagger_{t_1\to t_2}\Pi_{x_2}U^\dagger_{t_2\to t_3}\Pi_{x_3}\right]\\ =&\langle 1_x|x_1\rangle\langle x_1|e^{i(\theta/2)X}|x_2\rangle\langle x_2|e^{i(\theta^2/2)Y}|x_3\rangle\langle x_3|\\ &e^{-i(\theta^2/2)Y}e^{-i(\theta/2)X}|1_x\rangle, \end{aligned} \tag{12}$$

where $\Pi_x = |x\rangle\langle x|$ with $x\in\{0,1\}$.

Figure 4 shows the experimental results for the above procedure. The distribution of observed trajectories from three-time measurements, $p^{\mathcal{K}}(m_1,m_2,m_3)$, for the case of $\theta = 0.74\pi$ is shown in Fig. 4(b). At t_1 and t_2, we have the measurement results in the x-, y- and z-basis and only the z-basis measurement results for time t_3. As shown in the circuit of Fig. 2(b), x-, y- and z-basis measurements of the ancilla yield six measurement outcomes, $m_i\in\{|0_x\rangle,|1_x\rangle,|0_y\rangle,|1_y\rangle,|0\rangle,|1\rangle\}$. We post-select the data with only dark state outcomes to avoid heating of the vibrational modes (see Methods). We repeat each measurement configuration 100 times, for a total of 3600 measurements.

From the distribution of observed trajectories in Fig. 4(b), the three-time QPDs $p(x_1,x_2,x_3)$ are reconstructed as shown in Fig. 4(c). The quasi-probability of $p(x_1=0,x_2=0,x_3=0)$, as an example, is obtained directly from the relation of Eq. (7), $\sum_{m_1,m_2,m_3}\gamma_{0m_1}\gamma_{0m_2}\gamma_{0m_3}p^{\mathcal{K}}(m_1,m_2,m_3)$, where γ_{0m} can be calculated from Eq. (6). In our actual reconstruction, we perform an optimization procedure to obtain a proper $\gamma_{x_im_i}$ for all experimental data (see Methods). Some data points in Fig. 4(c) deviate from the theoretical expectations by more than one standard deviation. This is because several observed trajectories shown in Fig. 4(b) deviate from the ideal values. However, these deviations are mainly due to technical imperfections rather than fundamental problems. We discuss experimental limitations related to fluctuations of experimental control parameters in the last section before the conclusion section of the paper (see Methods for further details). Despite these deviations, our experimental results reveal the essential features of the QPDs, which are different from classical probability distributions. Classically, the joint probabilities at multiple time points can only have positive values. However, as shown in Fig. 4(c), the negative value for $p(x_1=0,x_2=1,x_3=0)$ and the imaginary values are observed for most cases.

The three-time QPDs enable us to evaluate the correct probability distribution of the system state during its unitary evolution. By taking the marginals of the QPDs, we recover the probability distribution at each point in time, which is not influenced by the previous measurements. As shown in Fig. 4(d), the measurement results at times t_1, t_2, and t_3 are consistent with those distributions where no measurements were performed before. The clear difference with and without previous measurements can be seen in the probability distribution at time t_3. If projective measurements were performed at time t_1 or t_2, the distribution of the measurement results at time t_3 should be 0.5 for each basis, which is not the case as shown in Fig. 4(d).

We can obtain any combination of two-time QPDs from the three-time QPDs and observe nonclassical features as shown in Fig. 5. The two-time QPDs are straightforwardly obtained from the three-time QPD by taking its marginals, $p(x_1,x_2) = \sum_{x_3}p(x_1,x_2,x_3)$, $p(x_1,x_3) = \sum_{x_2}p(x_1,x_2,x_3)$, and $p(x_2,x_3) = \sum_{x_1}p(x_1,x_2,x_3)$. We note that it is not always possible to do the reverse, that is, the reconstruction of the three-time QPDs from two-time QPDs, even with all possible combinations. Some data points in Fig. 5 deviate from the ideal values by more than their standard deviations. Despite these deviations, we observe imaginary and negative values in two-time QPDs as shown in Fig. 5, which indicate the coherence of the state with respect to the measurement basis [10–12, 64].

Imaginary and negative values in two-time QPDs are shown in Figs. 5(a-b) and Figs. 5(b-c), respectively. For the unitary evolution of the single-qubit state, the occurrence of imaginary and negative values in two-time QPDs can be understood from the relationship between the representation of the quantum state and the rotation axis in the Bloch sphere when the state contains coherence. For $U_{t_1\to t_2}$, the initial quantum state is represented on the x-axis, and the rotation axis for the unitary evolution is also aligned along the x-axis in the Bloch sphere. In this case, the QPDs reveal imaginary values, as shown in Fig. 5(a). For $U_{t_2\to t_3}$, the quantum state is on the x-axis of the Bloch sphere, but the axis of rotation is along the y-axis, perpendicular to the state. In this case, the QPDs reveal negative values, as shown in Fig. 5(c). In Fig. 5(b), the process contains parallel and perpendicular relations, resulting in imaginary and negative QPDs.

We also obtain quantum correlation functions from the observed trajectories. For different values of θ, time-ordered three-time correlation functions (Fig. 6(d)) and all combinations of two-time correlation functions (Fig. 6(c)) are deduced from the three-time QPDs. We also reconstruct out-of-time-ordered correlation functions based on Observation 1. We present $C(t_3,t_2,t_1)$ with the reversed time-ordering and $C(t_1,t_3,t_2)$ with an increasing-decreasing time-ordering in Figs. 6(e) and (f), respectively. The solid lines are from theoretical calculations, where their explicit forms can be found in Methods. The bands in Fig. 6 indicate the standard deviation (STD) of the experimental data. Although certain data points exhibit deviations exceeding the error bars, the overall trends observed in the data are generally consistent with the theoretical predictions.

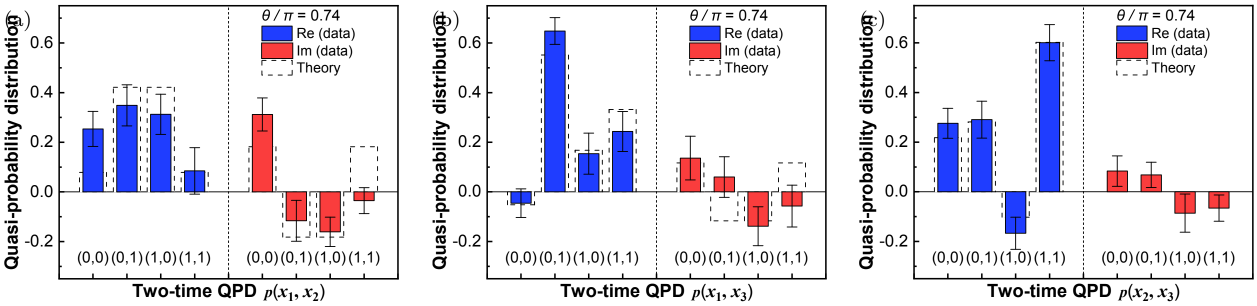


FIG. 5. The two-time QPDs obtained from the three-time QPDs. The blue and red bars indicate the real and imaginary parts of the QPDs. (a) The two-time QPD $p(x_1, x_2)$ from the unitary evolution $U_{t_1\to t_2}$. (b) The two-time QPD $p(x_1, x_3)$ from $U_{t_1\to t_3}$. (c) The two-time QPD $p(x_2, x_3)$ from $U_{t_2\to t_3}$. For all figures, the error bars indicate the STD, and the theoretical expectations are shown as dashed bars (see Methods for details).

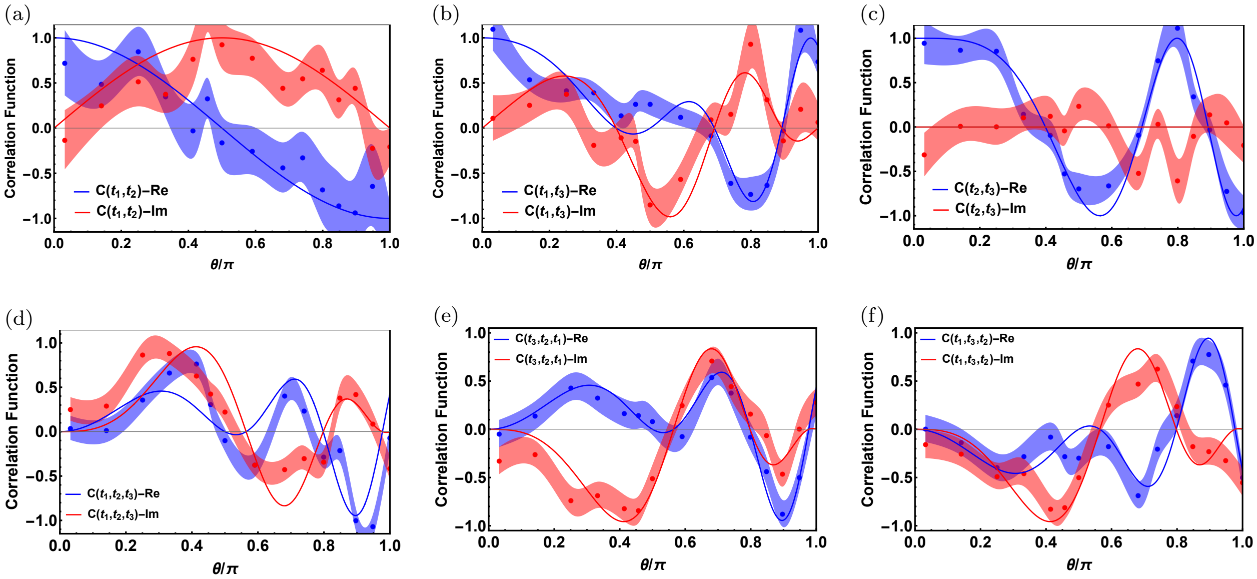


FIG. 6. The results of the two- and three-time correlation functions. Here, blue and red colors indicate the real and the imaginary parts of the correlation functions, respectively. Experimental data and theoretical expectations are shown as dots and solid lines, respectively. (a-c) The two-time correlation functions reconstructed from the three-time QPDs. (d) The time-ordered three-time correlation function reconstructed from the three-time QPDs. (e-f) $C(t_3, t_2, t_1)$ with the reversed time-ordering and $C(t_1, t_3, t_2)$ with an increasing-decreasing time-ordering respectively.

The majority of the experimental deviations stem from technical imperfections in controlling experimental parameters rather than fundamental issues in the underlying theoretical framework. Fluctuations in the parameters of the M-S gates are primarily responsible for the observed experimental deviations. In particular, more than 90% of the data points that deviate from theoretical predictions in Fig. 4(b) can be explained by fluctuations in the rotation angle of the M-S gates and the relative phase between two successive gates (see Methods). In the analysis, the amounts of the fluctuations in rotation angle and relative phase are required to be 0.03π (corresponding to 11.8% fluctuations) and 0.04π (approximately 4.4% fluctuations), respectively. We investigate the performance of the M-S gate using quantum process tomography, but we highlight that this data is not used for obtaining the joint distribution. The related details and other experimental imperfections are discussed in Methods.

Figure 7 indicates the fidelity $F(p, p_{\text{exp.}}) = \sum_{x_3} \sqrt{p(x_3)p_{\text{exp.}}(x_3)}$ between the theoretical distribution at time t_3 without intermediate measurements, $p(x_3) = \text{Tr}[\rho_{t_3}\Pi_{x_3}]$, and the marginal distribution of the QPD, $p_{\text{exp.}}(x_3) = \sum_{x_1,x_2} p_{\text{exp.}}(x_1, x_2, x_3)$, obtained from the experimental data. The marginal distribution obtained experimentally at time t_3 is closer to the ideal distribution compared to the case when intermediate projective measurements are performed at times t_1 and t_2.

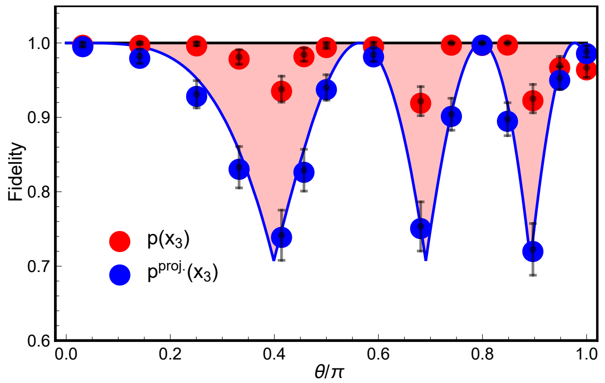


FIG. 7. Fidelity between the distributions for the z-basis measurement at time t_3. The error bars represent the standard error of the mean. Red dots refer to the fidelity between the marginal distribution from theory ($p(x_3)$) and the experimentally obtained three-time QPD ($p_{\text{exp.}}(x_3) = \sum_{x_1,x_2} p_{\text{exp.}}(x_1,x_2,x_3)$). The black line refers to the fidelity of 1 when the two distributions are equal. The blue line refers to the theoretical fidelity between $p(x_3)$ and $p^{\text{proj.}}(x_3)$ when projective measurements are performed at times t_1 and t_2. The blue dots refer to the corresponding experimental result.

CONCLUSION AND OUTLOOK

We have introduced a novel protocol named *snapshotting* to extract quantum statistics at multiple times from ancilla-assisted measurements and demonstrated it experimentally using the $^{171}\text{Yb}^{+}$-$^{138}\text{Ba}^{+}$ trapped-ion system. The key features of our approach are that the measurement effect can be entirely canceled out through classical post-processing of the ancilla measurement outcomes and that the measurement requires only a short-time system-ancilla interaction at each immediate time point. By snapshotting quantum dynamics, the QPD at multiple time points and various types of quantum correlation functions can be simultaneously obtained from a single distribution of observed trajectories. We highlight that this method is applicable to any quantum system and dynamics, serving as a valuable experimental tool for exploring the quantum statistics of both open and closed quantum systems.

The potential applications of the proposed protocol include exploring quantum dynamics in many-body physics. In principle, when considering local observables, the number of samples required to reconstruct QPDs and correlation functions does not scale with the size of the system or the number of qubits. This property is promising for obtaining various critical quantities based on correlation functions, such as OTOC, in quantum many-body systems [24, 25]. As the KD distribution itself has recently been recognized as an essential tool for investigating information scrambling and quantum thermodynamics [46, 49, 50, 59], its direct reconstruction from experimental data will open a new avenue for experimentally testing of the nonclassical phenomena arising from quantum dynamics.

METHODS

Proof of Theorem 1

Let us consider a slightly more general scenario such that the operators $A = \sum_{x=0}^{d-1} a_x \left|x\right\rangle\left\langle x\right|$ and $B = \sum_{x=0}^{d-1} b_x \left|x\right\rangle\left\langle x\right|$ diagonal in the same basis $\{\left|x\right\rangle\}_{x=0}^{d-1}$ are acting on the left and right sides of a d-dimensional quantum state, respectively, given as

$$\mathcal{E}_{B,A}(\rho) = B\rho A = \sum_m \gamma_m(B,A)\mathcal{K}_m(\rho), \tag{13}$$

where $\mathcal{K}_m(\rho) = K_m\rho K_m^\dagger$. We note that A and B is not required to be Hermitian. Theorem 1 in the main text to obtain the QPD $p(x_1, x_2, \cdots, x_N)$ is a special case with $A = \Pi_x = \left|x\right\rangle\left\langle x\right|$, $B = \mathbb{1}$, and $\gamma_{xm} = \gamma_m(\mathbb{1}, \Pi_x)$.

We then construct a set of Kraus operators $\{K_m\}$ to satisfy the condition in Eq. (13):

Proposition 1. *For the operators $A = \sum_x a_x \left|x\right\rangle\left\langle x\right|$ and $B = \sum_x b_x \left|x\right\rangle\left\langle x\right|$ diagonal in the same basis $\{\left|x\right\rangle\}$, there always exist $\gamma_m(B,A)$ satisfying Eq. (13) for a set of Kraus operators $\{K_m\}$ with*

$$K_m = \sum_{x=0}^{d-1}\left(\frac{\langle\phi_m|x\rangle}{\sqrt{\alpha}}\right)\left|x\right\rangle\left\langle x\right|,$$

where $\{\left|\phi_m\right\rangle\left\langle\phi_m\right|\}$ is a set of informationally complete projectors and satisfies $\sum_m \left|\phi_m\right\rangle\left\langle\phi_m\right| = \alpha\mathbb{1}$.

Proof. For the diagonal operators $A = \sum_x a_x\Pi_x$ and $B = \sum_x b_x\Pi_x$, let us rewrite Eq. (13) as

$$\begin{aligned}\mathcal{E}_{B,A}(\rho) &= B\rho A \\ &= \left(\sum_{y=0}^{d-1} b_y\Pi_y\right)\rho\left(\sum_{x=0}^{d-1} a_x\Pi_x\right) \\ &= \sum_{x,y=0}^{d-1} a_x b_y \Pi_y\rho\Pi_x \\ &= \sum_{x,y=0}^{d-1}\left\langle x\right|\left(\sum_{x',y'=0}^{d-1} a_{x'}b_{y'}\left|x'\right\rangle\left\langle y'\right|\right)|y\rangle\Pi_y\rho\Pi_x \\ &= \sum_{x,y=0}^{d-1}\langle x|O(B,A)|y\rangle\Pi_y\rho\Pi_x,\end{aligned} \tag{14}$$

where we define $O(B,A) = \sum_{x,y=0}^{d-1} a_x b_y \left|x\right\rangle\left\langle y\right|$. We note that any operator O can be expressed in terms of the informationally complete projectors $\{\left|\phi_m\right\rangle\left\langle\phi_m\right|\}$ as $O =$

$\sum_m c_m^O |\phi_m\rangle \langle\phi_m|$ with some complex coefficients c_m^O. This leads to an alternative expression

$$O(B,A) = \sum_m c_m^{O(B,A)} |\phi_m\rangle \langle\phi_m|.$$

By substituting this form into Eq. (14), we obtain

$$\begin{aligned}&\mathcal{E}_{B,A}(\rho)\\ &= \sum_m \sum_{x,y=0}^{d-1} c_m^{O(B,A)} \langle x|\phi_m\rangle\langle\phi_m|y\rangle \Pi_y \rho \Pi_x\\ &= \sum_m \alpha c_m^{O(B,A)} \left(\sum_{y=0}^{d-1} \frac{\langle\phi_m|y\rangle}{\sqrt{\alpha}}\Pi_y\right) \rho \left(\sum_{x=0}^{d-1} \Pi_x \frac{\langle x|\phi_m\rangle}{\sqrt{\alpha}}\right)\\ &= \sum_m \gamma_m(B,A) K_m \rho K_m^\dagger\\ &= \sum_m \gamma_m(B,A) \mathcal{K}_m(\rho),\end{aligned} \tag{15}$$

where we take $K_m = \sum_{y=0}^{d-1} \frac{\langle\phi_m|y\rangle}{\sqrt{\alpha}}\Pi_y$ to satisfy the normalization condition $\sum_m K_m^\dagger K_m = \mathbb{1}$ and define $\gamma_m(B,A) = \alpha c_m^{O(B,A)}$. □

To complete the proof of Theorem. 1, we show that these Kraus operators can be realized by the ancilla-assisted measurements. To this end, we introduce a d-dimensional ancilla state, initially prepared in $|0\rangle_R$. After applying the CSUM gate, a generalized CNOT gate, $U_{\mathrm{CSUM}} = \sum_{x,y=0}^{d-1} |x, x\oplus y\rangle \langle x,y|$ followed by the ancilla measurement with respect to the set of informationally complete projectors $\{|\phi_m\rangle\langle\phi_m|\}$, the Kraus operators for each measurement outcome become

$$K_m = \sum_{x=0}^{d-1}\left(\frac{\langle\phi_m|x\rangle}{\sqrt{\alpha}}\right)\Pi_x = \frac{\langle\phi_m|U_{\mathrm{CSUM}}|0\rangle_R}{\sqrt{\alpha}}. \tag{16}$$

For a d-dimensional system, a set of informationally complete projectors $\{|\phi_m\rangle\langle\phi_m|\}$ has at least d^2 elements. For example, the measurement set discussed in the main text, $\{|\phi_m\rangle\} = \{|0\rangle, |1\rangle, |0_y\rangle, |1_y\rangle, |0_x\rangle, |1_x\rangle\}$ has 6 elements, which is more than $d^2 = 4$, thus being overcomplete. However, this measurement set is easier to realize in experiments since all the projectors are the eigenvalues of the Pauli matrices.

Theorem 1 can be extended to local operators A and B of a multi-qudit system. This can be achieved by replacing Π_x with $\mathbb{1}\otimes\cdots\otimes\mathbb{1}\otimes\Pi_x\otimes\mathbb{1}\otimes\cdots\otimes\mathbb{1}$, where the projection is only applied to the target qudit. Consequently, K_m only acts on the target qubit while maintaining the same form as in Eq. (16), ensuring that the corresponding ancilla-assisted measurement requires only the interaction between the ancilla state and the target qudit. Since the coefficient $\gamma_m(B,A)$ for the local operators A and B remains the same as in the single-qudit case, the protocol does not scale with the size of the system as long as A and B act on a single-qudit.

We also note that there can be various choices of weight vectors $\gamma_m(B,A)$ that satisfy Eq. (13) for a given set of Kraus operators $\{K_m\}$. In this case, the optimal choice would be to minimize $|\gamma(B,A)|_{\max} := \max_m\{|\gamma_m(B,A)|\}$ as the number of samples to collect for a fixed precision scales with $|\gamma(B,A)|^2_{\max}$ from Hoeffding's inequality [67]. More precisely, the optimization problem can be formalized as follows:

$$\begin{aligned}\text{for given}: &\quad A,\ B,\ \{K_m\} &(17)\\ \text{minimize}: &\quad |\gamma|_{\max} = \max_m\{|\gamma_m|\} &(18)\\ \text{subject to}: &\quad B\otimes A^T = \sum_m \gamma_m K_m \otimes K_m^*. &(19)\end{aligned}$$

By vectorizing the density matrix ρ in Eq. (13), we note that Eq. (19) is equivalent to the condition that Eq. (13) holds for any ρ.

For $A = \sum_{x=0}^{d-1} a_x |x\rangle\langle x|$ and $B = \sum_{x=0}^{d-1} b_x |x\rangle\langle x|$ and the measurement operators described in Eq. (16), the condition in Eq. (19) is reduced to

$$\boldsymbol{T}\boldsymbol{\gamma} = \alpha\boldsymbol{\xi}, \tag{20}$$

where $[\boldsymbol{T}]_{x+yd,m} = \langle\phi_m|y\rangle\langle x|\phi_m\rangle$, $[\boldsymbol{\gamma}]_m = \gamma_m$, and $[\boldsymbol{\xi}]_{x+yd} = a_x b_y$. From numerical optimization for the measurement set $\{|\phi_m\rangle\} = \{|0\rangle, |1\rangle, |0_y\rangle, |1_y\rangle, |0_x\rangle, |1_x\rangle\}$ with $\alpha = 3$, which leads to $\{K_m\} = \left\{\frac{\Pi_0}{\sqrt{3}}, \frac{\Pi_1}{\sqrt{3}}, \frac{S^\dagger}{\sqrt{6}}, \frac{S}{\sqrt{6}}, \frac{\mathbb{1}}{\sqrt{6}}, \frac{Z}{\sqrt{6}}\right\}$, we obtain $\gamma_{\max} = \max_{x,m}\{|\gamma_m(\mathbb{1},\Pi_x)|\}| \approx 1.775$. This is a more efficient decomposition than that in Eq. (6) which yields $\gamma_{\max} = 3$.

Derivation of Observation 1

From the cyclic property of the trace, the correlation function can be rewritten as

$$\begin{aligned}&C(t_{\mu_1},\cdots,t_{\mu_j},\cdots,t_{\mu_k})\\ &\quad= \mathrm{Tr}[A(t_{\mu_{j+1}})\cdots A(t_{\mu_k})\rho_{t_0} A(t_{\mu_1})\cdots A(t_{\mu_j})].\end{aligned}$$

Then we note that both $t_{\mu_1} \le t_{\mu_2} \le \cdots \le t_{\mu_j}$ and $t_{\mu_k} \le t_{\mu_{k-1}} \le \cdots \le t_{\mu_{j+1}}$ are monotonically increasing time sequences, which leads to the following expression:

$$\begin{aligned}&C(t_{\mu_1},\cdots,t_{\mu_j},\cdots,t_{\mu_k})\\ &\quad= \mathrm{Tr}[(\mathcal{E}_{B_N,A_N}\circ\mathcal{U}_{t_{N-1}\to t_N}\circ\cdots\circ\mathcal{U}_{t_1\to t_2}\circ\mathcal{E}_{B_1,A_1})(\rho_{t_1})],\end{aligned}$$

where $\mathcal{U}_{t_i\to t_j}(\rho) = U_{t_i\to t_j}\rho U^\dagger_{t_i\to t_j}$ and we take $(B_i,A_i) = (\mathbb{1},A)$ when $A(t_i)$ is applied to the right side, $(B_i,A_i) = (A,\mathbb{1})$ when $A(t_i)$ is applied to the left side, and $(B_i,A_i) = (A,A)$ when $A(t_i)$ is applied to the both sides.

Since each $\mathcal{E}_{B_i,A_i}$ can be expressed as a linear combination of the actions of the Kraus operators $\{K_m\}$ from Proposition 1, we obtain the following form,

$$C(t_{\mu_1},\cdots,t_{\mu_j},\cdots,t_{\mu_k}) = \mathbb{E}\left[\prod_{i=1}^N \gamma_{m_i}(B_i,A_i)\right],$$

by averaging over all possible observed trajectories following the distribution $p^{\mathcal{K}}(m_1, m_2, \cdots, m_N) = \mathrm{Tr}[(\mathcal{K}_{m_N} \circ \mathcal{U}_{t_{N-1}\to t_N} \circ \cdots \circ \mathcal{U}_{t_1 \to t_2} \circ \mathcal{K}_{m_1})(\rho_{t_1})]$.

We highlight that the correlation functions with different time sequences $(t_{\mu_1}, \cdots, t_{\mu_k})$ are obtained by only replacing the coefficients $\gamma_{m_i}(B_i, A_i)$, which can be easily done in classical post-processing using the same data used to obtain $p^{\mathcal{K}}$.

Obtaining C_{OTOC} from intermediate measurements

Let us express the OTOC for the two operators $W(\tau) = U_\tau^\dagger W U_\tau$ and $V(0) = V$ as

$$\begin{aligned}
C_{\mathrm{OTOC}} &= \langle [W(\tau), V(0)]^\dagger [W(\tau), V(0)] \rangle \\
&= \langle W^\dagger(\tau) V^\dagger(0) V(0) W(\tau) \rangle - \langle V^\dagger(0) W^\dagger(\tau) V(0) W(\tau) \rangle \\
&\quad - \langle W^\dagger(\tau) V^\dagger(0) W(\tau) V(0) \rangle + \langle V^\dagger(0) W^\dagger(\tau) W(\tau) V(0) \rangle \\
&= \mathrm{Tr}[V U_\tau^\dagger W U_\tau \rho U_\tau^\dagger W^\dagger U_\tau V^\dagger] \\
&\quad - \mathrm{Tr}[V U_\tau^\dagger W U_\tau \rho V^\dagger U_\tau^\dagger W^\dagger U_\tau] \\
&\quad - \mathrm{Tr}[U_\tau^\dagger W U_\tau V \rho U_\tau^\dagger W^\dagger U_\tau V^\dagger] + \mathrm{Tr}[W U_\tau V \rho V^\dagger U_\tau^\dagger W^\dagger] \\
&= \mathrm{Tr}[(\mathcal{E}_{V,V^\dagger} \circ \mathcal{U}^{-1} \circ \mathcal{E}_{W,W^\dagger} \circ \mathcal{U} \circ \mathcal{E}_{\mathbb{1},\mathbb{1}})(\rho)] \\
&\quad - \mathrm{Tr}[(\mathcal{E}_{V,\mathbb{1}} \circ \mathcal{U}^{-1} \circ \mathcal{E}_{W,W^\dagger} \circ \mathcal{U} \circ \mathcal{E}_{\mathbb{1},V^\dagger})(\rho)] \\
&\quad - \mathrm{Tr}[(\mathcal{E}_{\mathbb{1},V^\dagger} \circ \mathcal{U}^{-1} \circ \mathcal{E}_{W,W^\dagger} \circ \mathcal{U} \circ \mathcal{E}_{V,\mathbb{1}})(\rho)] \\
&\quad + \mathrm{Tr}[(\mathcal{E}_{W,W} \circ \mathcal{U} \circ \mathcal{E}_{V,V^\dagger})(\rho)],
\end{aligned}$$

where we denote $\mathcal{U}(\rho) = U_\tau \rho U_\tau^\dagger$ and $\mathcal{U}^{-1}(\rho) = U_\tau^\dagger \rho U_\tau$, respectively.

One can then construct the intermediate measurements $\{K_{m_1}^V\} = \{K_{m_3}^V\}$ and $\{\mathcal{K}_{m_2}^W\}$ from Proposition 1 to express $\mathcal{E}_{\mathbb{1},\mathbb{1}}$, $\mathcal{E}_{\mathbb{1},V^\dagger}$, $\mathcal{E}_{V,\mathbb{1}}$, and $\mathcal{E}_{V,V^\dagger}$ as a weighted sum of $\mathcal{K}_{m_1}^V$ or $\mathcal{K}_{m_3}^V$, and $\mathcal{E}_{W,W^\dagger}$ as a weighted sum of $\mathcal{K}_{m_2}^W$. From this, all the four terms in C_{OTOC} can be obtained simultaneously from $p^{\mathcal{K}}(m_1, m_2, m_3) = \mathrm{Tr}[(\mathcal{K}_{m_3}^V \circ \mathcal{U}^{-1} \circ \mathcal{K}_{m_2}^W \circ \mathcal{U} \circ \mathcal{K}_{m_1}^V(\rho)]$.

Experimental setup

As shown in Fig. 8(a), we use a dual-species trapped-ion system, which traps one ^{171}Yb$^+$ ion and one ^{138}Ba$^+$ ion in a four-rod trap, to perform the ancilla-assisted measurements. The ^{171}Yb$^+$and ^{138}Ba$^+$ ions serve as the system and the ancilla qubits, respectively. The two ions have different energy structures and require different initialization and detection lasers. Therefore, operations on the ^{171}Yb$^+$ ion do not affect the ^{138}Ba$^+$ ion and vice versa. Therefore, it is possible to perform the ICD and ICI, where ^{138}Ba$^+$ ion-qubit is detected or initialized without affecting the other qubit [90], which is the essential property for the ancilla-assisted measurement. We perform single-qubit rotations and the two-qubit M-S gate by using 355 nm and 532 nm Raman laser beams for ^{171}Yb$^+$and ^{138}Ba$^+$ ions, respectively, as shown in Fig. 8(b).

Two- and three-time QPDs simulation data

Quantum process tomography of M-S gate

To quantitatively characterize the effect of imperfect M-S gates on the protocol, we perform quantum process tomography of the M-S gate. For quantum process tomography, we first prepare the system to one of the 16 states $|i\rangle \otimes |j\rangle$, where $|i\rangle$, $|j\rangle \in \{|0\rangle, |1\rangle, |1_x\rangle, |0_y\rangle\}$, then apply an M-S gate operation and then measure the system on one of the nine measurement bases $\{xx, xy, xz, yx, yy, yz, zx, zy, zz\}$. Using the maximum likelihood method[94, 96–98], we reconstruct the process matrix from the measurement results as shown in Fig. 11. Compared to the ideal M-S gate, the process matrix has a fidelity of 93.16%. The process matrix has a mean fidelity of 94.51%±1.18%, the average fidelity of the output state over all possible input states[94, 97, 99], which is consistent with the fidelity of the Bell state of 94% ± 2%.

We analyze the raw data, that is, 72 different observed trajectories shown in Fig. 4(b) with the result of quantum process tomography of the M-S gate. In our numerical analysis, fluctuations in the rotation angles of the M-S gate and relative phases between successive M-S gates can explain the deviations of the experimental results from the theoretical predictions. A parameterized M-S gate can be described as $\mathrm{MS} = \exp(-i\theta_{\mathrm{M}}(\sin(\phi_{\mathrm{M1}})Y + \cos(\phi_{\mathrm{M1}})X) \otimes (\sin(\phi_{\mathrm{M2}})Y + \cos(\phi_{\mathrm{M2}})X))$, where θ_{M} represents the rotation angle that should be $\pi/4$ for the ideal gate, and ϕ_{M1} and ϕ_{M2} represent the phases that determine the rotation axis for the ^{171}Yb$^+$and ^{138}Ba$^+$qubits, respectively, which should be zero for the ideal gate. For each trajectory, we numerically adjust the rotation angles and relative phases of the M-S gate process matrix so that the numerical calculation agrees with the experimental result. Then, we collect the adjusted rotation angles and relative phases for all observed trajectories. Among a total of 72 measurement results of $p^{\mathcal{K}}(m_1, m_2, m_3)$, more than 90% deviations in the data can be explained by fluctuations in the rotation angle of the M-S gate and relative phases between two gates. The distributions of the adjusted parameters are as follows. The rotation angles are overall shifted by 0.001π with a standard deviation of 0.03π, corresponding to approximately 11.8% fluctuations. The relative phases are shifted by 0.01π with a standard deviation of 0.04π, corresponding to 4.4%. Here, we note that phase fluctuations are only considered for the ^{171}Yb$^+$qubits.

To illustrate the experimental imperfections, we investigate the dependence of the contrasts of the two-time correlation functions on the infidelities of the M-S gates by using the experimental M-S gate process matrix. As

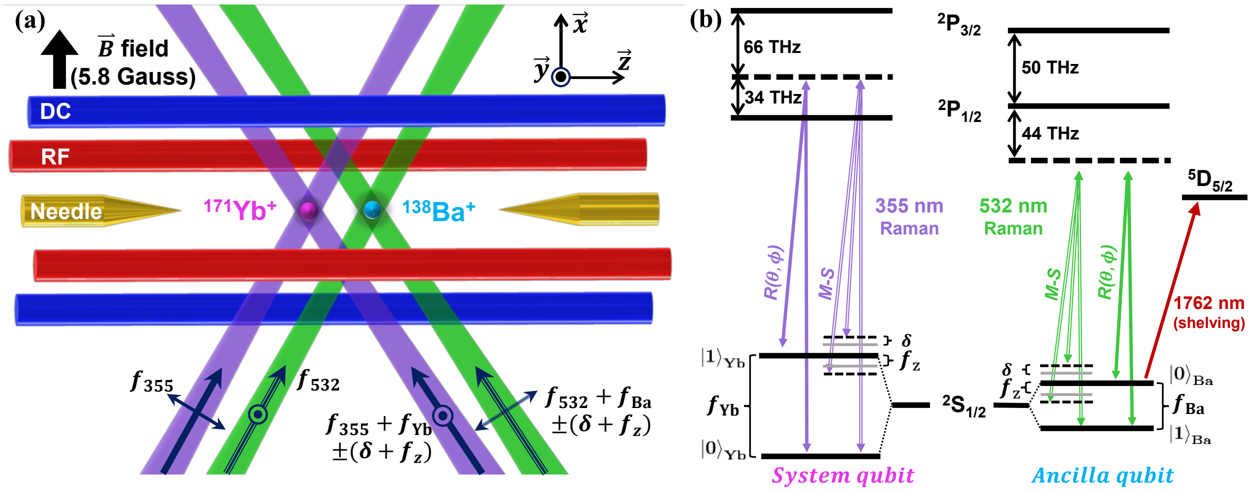


FIG. 8. Experimental setup. (a) ^{171}Yb$^+$ and ^{138}Ba$^+$ ions trapped in a four-rod trap. A magnetic field of 5.8 Gauss is applied along the x-axis. To realize the M-S gate between two ions, the ^{171}Yb$^+$ ion is controlled by illuminating a pair of 355 nm lasers (purple) with a frequency of f_{355} and $f_{355}+f_{\rm Yb}\pm(\delta+f_z)$, where $f_{\rm Yb}$ is the qubit splitting of the ^{171}Yb$^+$ qubit. The ^{138}Ba$^+$ ion is controlled by illuminating a pair of 532 nm lasers (green) with a frequency of f_{532} and $f_{532}+f_{\rm Ba}\pm(\delta+f_z)$, where $f_{\rm Ba}$ is the qubit splitting of the ^{138}Ba$^+$ ion-qubit, f_z is the frequency of the axial OOP (out-of-phase) mode, and δ is the laser detuning from the sideband of the OOP mode. Raman laser directions are represented by thick arrows, and the polarization is represented by thin arrows and dots. (b) Energy levels and related lasers for the ^{171}Yb$^+$ and ^{138}Ba$^+$ ions. The hyperfine qubit of the ^{171}Yb$^+$ ion and the Zeeman qubit of the ^{138}Ba$^+$ ion serve as the system qubit and the ancilla qubit, respectively. Single-qubit rotations are realized by resonant Raman transitions. The two-qubit entangling operation is realized by applying a bichromatic Raman laser for both ions. The 1762 nm laser is the shelving laser used for ^{138}Ba$^+$ ion-qubit detection.

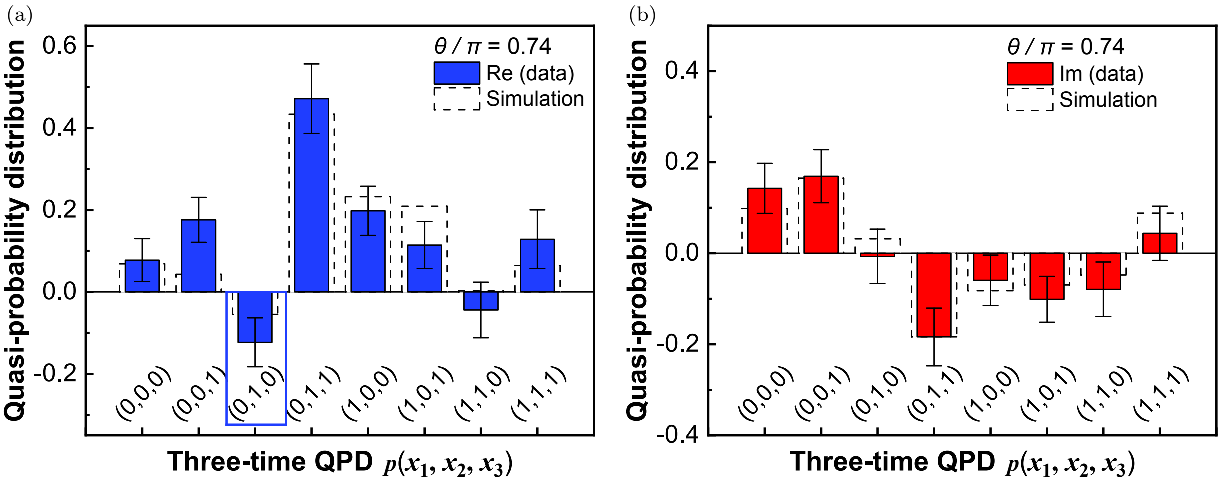


FIG. 9. Three-time QPDs simulation data

shown in Fig. 12(a), for the two-time correlation functions, the contrast of the real part decreases more than the contrast of the imaginary part. Here, we increase the infidelity by multiplying the operation of the M-S gate and assume that it increases linearly with the number of gates. Since multiplying the ideal CNOT gate twice equals an identity operator, we add two M-S gates at each step to increase the gate infidelity while maintaining the measurement scheme. Three-time measurements are also investigated using the experimental M-S gate process matrix. As shown in Fig. 12(b), the three-time correlation functions are simulated taking into account the process matrix infidelity. The experimental and simulated data with infidelity agree better than the ideal theory data, indicating that the infidelity of the M-S gate is one of the main causes of deviation. The major imperfections come from the rotation angle of the M-S gate. To be an ideal CNOT gate, the angle of the M-S gate should be

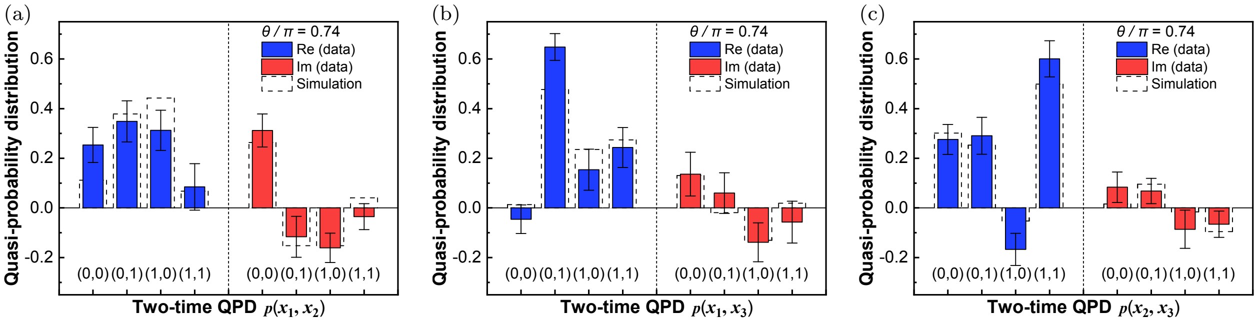


FIG. 10. Two-time QPDs simulation data

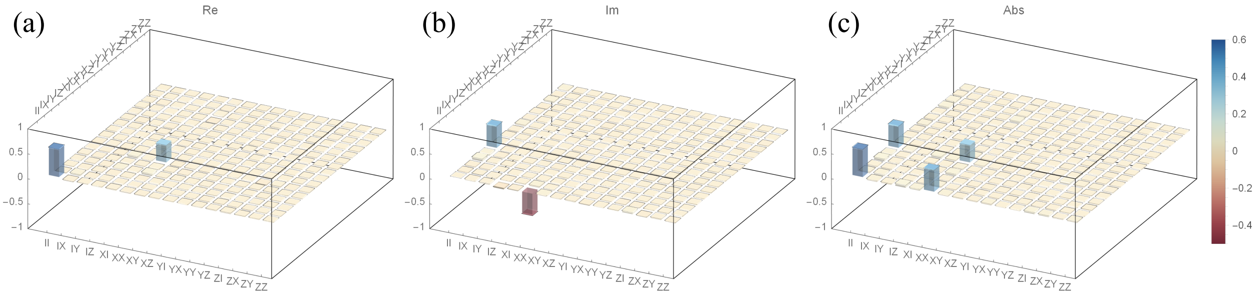


FIG. 11. The experimental process matrix of the M-S gate. (a-c) represent the real part, the imaginary part, and the absolute value of the process matrix, respectively.

$\pi/4$, but in our experiment, the angle is about 10% less than the ideal value. This angle imperfection explains well the disagreement in the imaginary parts for small θ values.

Further deviations can arise from phase fluctuation problems between successive M-S gates. The M-S gate can be described as $\exp\left(-i\frac{\pi}{4}X_{\text{Yb}}X_{\text{Ba}}\right)$, where X_{Yb} and X_{Ba} are Pauli operators σ_x of the $^{171}\text{Yb}^+$ and $^{138}\text{Ba}^+$ ion qubits. We need to control the laser phases for the M-S gate to make the gate work as $X_{\text{Yb}}X_{\text{Ba}}$ and not on other axes. For example, in the three-time correlation functions of Fig. 12(b), the second time point can be explained by the drift of the 0.1π phase for the $^{138}\text{Ba}^+$ ion qubit.

Post-selection detection and error analysis

Figure 13 shows the detailed process of the $^{138}\text{Ba}^+$ ion fluorescence detection. In this detection process, we first use a 1762 nm laser to shelve the $|0\rangle_{\text{Ba}}$ population to $\text{D}_{5/2}$, and then apply a 493 nm laser to drive the transition between $\text{S}_{1/2}$ and $\text{P}_{1/2}$. The shelving operation has no effect if the qubit state is $|1\rangle_{\text{Ba}}$, and a large number of photons will be produced by the subsequent 493 nm laser. In contrast, if the qubit state is $|0\rangle_{\text{Ba}}$, the population is shelved to $\text{D}_{5/2}$ and no photons are produced by the 493 nm laser. Hence, the number of scattered photons can be used to distinguish the qubit states.

In our multi-time measurements circuit, the ancilla ($^{138}\text{Ba}^+$ ion) is required to be detected and used repeatedly. However, as shown in Fig. 13(a), the detection of a bright state produces a large number of photons, thereby heating the ion chain and further degrading the performance of subsequent CNOT operations. To solve this problem, we adopt a post-selection approach for all ICDs, which uses only dark state data. For bright state data, we transfer bright states to dark states by a π pulse before the measurement.

All the error bars in the main text are obtained by the bootstrap method. We first re-sample the experimental raw data in Fig. 4(b), generating 1000 new datasets. Subsequently, we derive 1000 new results based on these datasets and obtain the standard deviations from the distribution of these 1000 results.

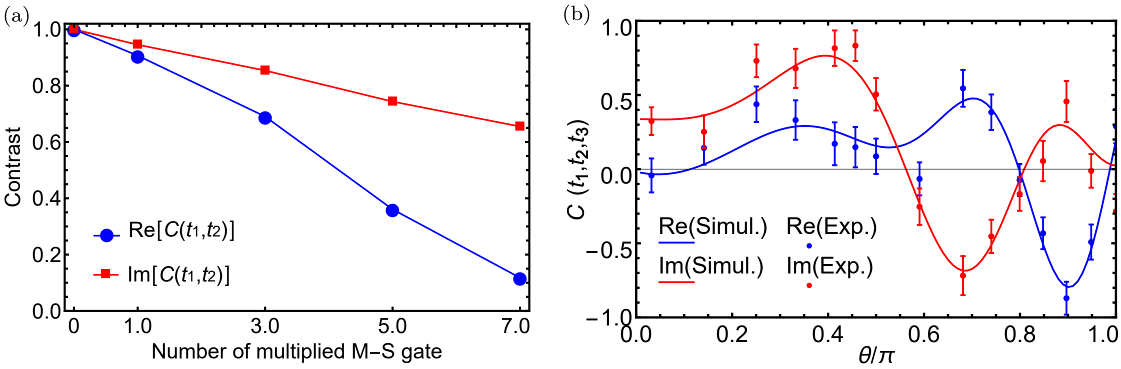


FIG. 12. The effect of imperfect M-S gates on the measurement scheme. (a) The blue circles and red squares represent the contrast of the real and imaginary parts of $C(t_1, t_2)$. The horizontal axis represents the number of imperfect M-S gates applied to the system, while 0 represents an ideal M-S gate. (b) Simulation results of three-time correlation functions based on the process matrix. Error bars are standard deviations. The blue and red lines represent the real and imaginary parts of $C(t_1, t_2, t_3)$. The blue and red dots represent the corresponding experimental results.

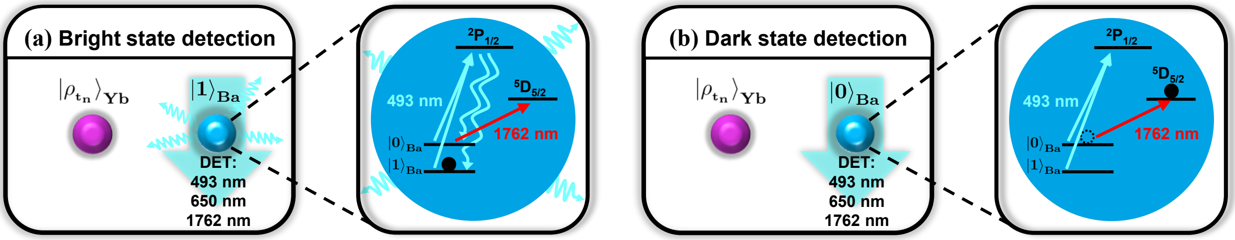

(a) Bright state detection
$|\rho_{t_n}\rangle_{\mathrm{Yb}}$
$|1\rangle_{\mathrm{Ba}}$
DET:
493 nm
650 nm
1762 nm
^{2}P$_{1/2}$
^{5}D$_{5/2}$
493 nm
1762 nm
$|0\rangle_{\mathrm{Ba}}$
$|1\rangle_{\mathrm{Ba}}$
(b) Dark state detection
$|\rho_{t_n}\rangle_{\mathrm{Yb}}$
$|0\rangle_{\mathrm{Ba}}$
DET:
493 nm
650 nm
1762 nm
^{2}P$_{1/2}$
^{5}D$_{5/2}$
493 nm
1762 nm
$|0\rangle_{\mathrm{Ba}}$
$|1\rangle_{\mathrm{Ba}}$

FIG. 13. Fluorescence detection of the ^{138}Ba$^+$ ion. The detection process consists of two steps: First, we use a 1762 nm laser to shelve the $|0\rangle_{\mathrm{Ba}}$ population to D$_{5/2}$, and then we use a 493 nm laser to drive the transition between S$_{1/2}$ and P$_{1/2}$. (a) Bright state detection. When the ancilla is in $|1\rangle_{\mathrm{Ba}}$, the shelving operation does not affect the qubit. The subsequent 493 nm laser produces a large number of photons. (b) Dark state detection. When the ancilla is in $|0\rangle_{\mathrm{Ba}}$, its population is shelved to D$_{5/2}$. Therefore, the 493 nm laser will not produce any photons.

Expectation values from theory

First, we consider two- and three-time correlation functions

$$\begin{aligned} &C(t_1,t_2)\\ &\quad = \mathrm{Tr}\left[\rho Z(t_1) Z(t_2)\right]\\ &\quad = \mathrm{Tr}\left[U_{t_1\to t_2}\rho_{t_1} Z U^\dagger_{t_1\to t_2} Z\right]\\ &C(t_1,t_2,t_3)\\ &\quad = \mathrm{Tr}\left[\rho Z(t_1) Z(t_2) Z(t_3)\right]\\ &\quad = \mathrm{Tr}\left[U_{t_2\to t_3} U_{t_1\to t_2}\rho_{t_1} Z U^\dagger_{t_1\to t_2} Z U^\dagger_{t_2\to t_3} Z\right], \end{aligned} \tag{21}$$

where $U_{t_i\to t_j}$ describes the unitary time evolution from time t_i to t_j, and ρ_{t_1} is the quantum state at time t_1. In this paper, we focus on the case where the initial state is prepared in $\rho_{t_1} = |1_x\rangle\langle 1_x|$ with $|1_x\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, and the evolution unitary operators are given as $U_{t_1\to t_2} = R_X(\theta) = e^{-i(\theta/2)X}$, and $U_{t_2\to t_3} = R_Y(\theta^2) = e^{-i(\theta^2/2)Y}$ with $\theta \in [0,\pi]$ and the Pauli matrices X, Y and Z. The theoretical expectation values of Eq. (21) are

$$\begin{aligned} &C(t_1,t_2)\\ &\quad = \mathrm{Tr}\left[U_{t_1\to t_2}|1_x\rangle\langle 1_x| Z U^\dagger_{t_1\to t_2} Z\right]\\ &\quad = \langle 1_x| Z U^\dagger_{t_1\to t_2} Z U_{t_1\to t_2}|1_x\rangle\\ &\quad = \langle 1_x| Z e^{i(\theta/2)X} Z e^{-i(\theta/2)X}|1_x\rangle\\ &\quad = \cos\theta + i\sin\theta\\ &C(t_1,t_3)\\ &\quad = \mathrm{Tr}\left[U_{t_2\to t_3}U_{t_1\to t_2}|1_x\rangle\langle 1_x| Z U^\dagger_{t_1\to t_2} U^\dagger_{t_2\to t_3} Z\right]\\ &\quad = \langle 1_x| Z U^\dagger_{t_1\to t_2} U^\dagger_{t_2\to t_3} Z U_{t_2\to t_3} U_{t_1\to t_2}|1_x\rangle\\ &\quad = \langle 1_x| Z e^{i(\theta/2)X} e^{i(\theta^2/2)Y} Z e^{-i(\theta^2/2)Y} e^{-i(\theta/2)X}|1_x\rangle\\ &\quad = \cos\theta^2(\cos\theta + i\sin\theta)\\ &C(t_2,t_3)\\ &\quad = \mathrm{Tr}\left[U_{t_2\to t_3}U_{t_1\to t_2}|1_x\rangle\langle 1_x| U^\dagger_{t_1\to t_2} Z U^\dagger_{t_2\to t_3} Z\right]\\ &\quad = \langle 1_x| U^\dagger_{t_1\to t_2} Z U^\dagger_{t_2\to t_3} Z U_{t_2\to t_3} U_{t_1\to t_2}|1_x\rangle\\ &\quad = \langle 1_x| e^{i(\theta/2)X} Z e^{i(\theta^2/2)Y} Z e^{-i(\theta^2/2)Y} e^{-i(\theta/2)X}|1_x\rangle\\ &\quad = \cos\theta^2, \end{aligned}$$

$$
\begin{aligned}
&C(t_1,t_2,t_3)\\
&\quad = \mathrm{Tr}\left[U_{t_2\to t_3}U_{t_1\to t_2}\left|1_x\right\rangle\left\langle 1_x\right|ZU^{\dagger}_{t_1\to t_2}ZU^{\dagger}_{t_2\to t_3}Z\right]\\
&\quad = \langle 1_x|ZU^{\dagger}_{t_1\to t_2}ZU^{\dagger}_{t_2\to t_3}ZU_{t_2\to t_3}U_{t_1\to t_2}\left|1_x\right\rangle\\
&\quad = \langle 1_x|Ze^{i(\theta/2)X}Ze^{i(\theta^2/2)Y}Ze^{-i(\theta^2/2)Y}e^{-i(\theta/2)X}\left|1_x\right\rangle\\
&\quad = \sin\theta^2(\cos\theta + i\sin\theta)\\
&C(t_2,t_3,t_1)\\
&\quad = \mathrm{Tr}\left[U_{t_2\to t_3}U_{t_1\to t_2}Z\left|1_x\right\rangle\left\langle 1_x\right|U^{\dagger}_{t_1\to t_2}ZU^{\dagger}_{t_2\to t_3}Z\right]\\
&\quad = \langle 1_x|U^{\dagger}_{t_1\to t_2}ZU^{\dagger}_{t_2\to t_3}ZU_{t_2\to t_3}U_{t_1\to t_2}Z\left|1_x\right\rangle\\
&\quad = \langle 1_x|e^{i(\theta/2)X}Ze^{i(\theta^2/2)Y}Ze^{-i(\theta^2/2)Y}e^{-i(\theta/2)X}Z\left|1_x\right\rangle\\
&\quad = \sin\theta^2(-\cos\theta + i\sin\theta)\\
&C(t_3,t_2,t_1)\\
&\quad = \mathrm{Tr}\left[U_{t_2\to t_3}ZU_{t_1\to t_2}Z\left|1_x\right\rangle\left\langle 1_x\right|U^{\dagger}_{t_1\to t_2}U^{\dagger}_{t_2\to t_3}Z\right]\\
&\quad = \langle 1_x|U^{\dagger}_{t_1\to t_2}U^{\dagger}_{t_2\to t_3}ZU_{t_2\to t_3}ZU_{t_1\to t_2}Z\left|1_x\right\rangle\\
&\quad = \langle 1_x|e^{i(\theta/2)X}e^{i(\theta^2/2)Y}Ze^{-i(\theta^2/2)Y}Ze^{-i(\theta/2)X}Z\left|1_x\right\rangle\\
&\quad = \sin\theta^2(\cos\theta - i\sin\theta).
\end{aligned}
\tag{22}
$$

Meanwhile, the two- and three-time QPDs are expressed as

$$
\begin{aligned}
&p(x_1,x_2)\\
&\quad = \mathrm{Tr}\left[U_{t_1\to t_2}\rho_{t_1}\Pi_{x_1}U^{\dagger}_{t_1\to t_2}\Pi_{x_2}\right]\\
&p(x_1,x_2,x_3)\\
&\quad = \mathrm{Tr}\left[U_{t_2\to t_3}U_{t_1\to t_2}\rho_{t_1}\Pi_{x_1}U^{\dagger}_{t_1\to t_2}\Pi_{x_2}U^{\dagger}_{t_2\to t_3}\Pi_{x_3}\right],
\end{aligned}
\tag{23}
$$

which can also be calculated similarly to the correlation functions. For the initial state $\rho_{t_1} = \left|1_x\right\rangle\left\langle 1_x\right|$ and the dynamics $U_{t_1\to t_2} = R_X(\theta) = e^{-i(\theta/2)X}$ and $U_{t_2\to t_3} = R_Y(\theta^2) = e^{-i(\theta^2/2)Y}$, we obtain

$$
\begin{aligned}
&p(x_1,x_2)\\
&\quad = \mathrm{Tr}\left[e^{-i(\theta/2)X}\left|1_x\right\rangle\left\langle 1_x\right|\Pi_{x_1}e^{i(\theta/2)X}\Pi_{x_2}\right]\\
&\quad = \langle 1_x|\Pi_{x_1}e^{i(\theta/2)X}\Pi_{x_2}e^{-i(\theta/2)X}\left|1_x\right\rangle\\
&\quad = \langle 1_x|x_1\rangle\langle x_1|e^{i(\theta/2)X}\left|x_2\right\rangle\left\langle x_2\right|e^{-i(\theta/2)X}\left|1_x\right\rangle\\
&p(x_1,x_2,x_3)\\
&\quad = \mathrm{Tr}\left[e^{-i(\theta^2/2)Y}e^{-i(\theta/2)X}\left|1_x\right\rangle\left\langle 1_x\right|\Pi_{x_1}e^{i(\theta/2)X}\Pi_{x_2}e^{i(\theta^2/2)Y}\Pi_{x_3}\right]\\
&\quad = \langle 1_x|\Pi_{x_1}e^{i(\theta/2)X}\Pi_{x_2}e^{i(\theta^2/2)Y}\Pi_{x_3}e^{-i(\theta^2/2)Y}e^{-i(\theta/2)X}\left|1_x\right\rangle\\
&\quad = \left\langle 1_x\right|\left.x_1\right\rangle\left\langle x_1\right|e^{i(\theta/2)X}\left|x_2\right\rangle\left\langle x_2\right|e^{i(\theta^2/2)Y}\left|x_3\right\rangle\left\langle x_3\right|\\
&\qquad e^{-i(\theta^2/2)Y}e^{-i(\theta/2)X}\left|1_x\right\rangle,
\end{aligned}
\tag{24}
$$

where each component can be straightforwardly obtained from the explicit form of the rotation matrices.

Data availability

The data that support the findings of this study are available from the corresponding author upon request.

Code availability

Code used in data analysis is available from the corresponding author upon reasonable request.

*, † First three authors contributed equally.

† hjkwon@kias.re.kr

‡ m.kim@imperial.ac.uk

§ kimkihwan@mail.tsinghua.edu.cn

[1] E. Wigner, On the quantum correction for thermodynamic equilibrium, Phys. Rev. **40**, 749 (1932).

[2] J. G. Kirkwood, Quantum statistics of almost classical assemblies, Phys. Rev. **44**, 31 (1933).

[3] P. A. M. Dirac, On the analogy between classical and quantum mechanics, Rev. Mod. Phys. **17**, 195 (1945).

[4] H. Margenau and R. N. Hill, Correlation between measurements in quantum theory, Prog. Theor. Exp. Phys. **26**, 722 (1961).

[5] J. S. BELL, On the problem of hidden variables in quantum mechanics, Rev. Mod. Phys. **38**, 447 (1966).

[6] A. J. Leggett and A. Garg, Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks?, Phys. Rev. Lett. **54**, 857 (1985).

[7] R. W. Spekkens, Negativity and contextuality are equivalent notions of nonclassicality, Phys. Rev. Lett. **101**, 020401 (2008).

[8] C. Ferrie and J. Emerson, Frame representations of quantum mechanics and the necessity of negativity in quasi-probability representations, Journal of Physics A: Mathematical and Theoretical **41**, 352001 (2008).

[9] H. F. Hofmann, On the role of complex phases in the quantum statistics of weak measurements, New J. Phys. **13**, 103009 (2011).

[10] S. De Bievre, Complete incompatibility, support uncertainty, and kirkwood-dirac nonclassicality, Phys. Rev. Lett. **127**, 190404 (2021).

[11] J. R. Hance, M. Ji, and H. F. Hofmann, Contextuality, coherences, and quantum cheshire cats, New J. Phys. **25**, 113028 (2023).

[12] R. Wagner and E. F. Galvão, Simple proof that anomalous weak values require coherence, Phys. Rev. A **108**, L040202 (2023).

[13] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, New J. Phys **14**, 113011 (2012).

[14] A. Mari and J. Eisert, Positive wigner functions render classical simulation of quantum computation efficient, Phys. Rev. Lett. **109**, 230503 (2012).

[15] M. F. Pusey, Anomalous weak values are proofs of contextuality, Phys. Rev. Lett. **113**, 200401 (2014).

[16] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Contextuality supplies the 'magic' for quantum computation, Nature **510**, 351 (2014).

[17] H. Pashayan, J. J. Wallman, and S. D. Bartlett, Estimating outcome probabilities of quantum circuits using quasiprobabilities, Phys. Rev. Lett. **115**, 070501 (2015).

[18] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, Sufficient conditions for efficient classical simulation of quantum optics, Phys. Rev. X **6**, 021039 (2016).

[19] H. Kwon, K. C. Tan, T. Volkoff, and H. Jeong, Nonclassicality as a quantifiable resource for quantum metrology, Phys. Rev. Lett. **122**, 040503 (2019).

[20] D. R. Arvidsson-Shukur, N. Yunger Halpern, H. V. Lepage, A. A. Lasek, C. H. Barnes, and S. Lloyd, Quantum advantage in postselected metrology, Nat. Commun. **11**, 1 (2020).

[21] M. Lostaglio, Certifying quantum signatures in thermodynamics and metrology via contextuality of quantum linear response, Phys. Rev. Lett. **125**, 230603 (2020).

[22] N. Lupu-Gladstein, Y. B. Yilmaz, D. R. Arvidsson-Shukur, A. Brodutch, A. O. Pang, A. M. Steinberg, and N. Y. Halpern, Negative quasiprobabilities enhance phase estimation in quantum-optics experiment, Phys. Rev. Lett. **128**, 220504 (2022).

[23] M. Perarnau-Llobet, E. Bäumer, K. V. Hovhannisyan, M. Huber, and A. Acin, No-go theorem for the characterization of work fluctuations in coherent quantum systems, Phys. Rev. Lett. **118**, 070601 (2017).

[24] J. Maldacena, S. H. Shenker, and D. Stanford, A bound on chaos, J. High Energy Phys. **2016** (8), 106.

[25] K. A. Landsman, C. Figgatt, T. Schuster, N. M. Linke, B. Yoshida, N. Y. Yao, and C. Monroe, Verified quantum information scrambling, Nature **567**, 61 (2019).

[26] P. Jayachandran, L. H. Zaw, and V. Scarani, Dynamics-based entanglement witnesses for non-gaussian states of harmonic oscillators, Phys. Rev. Lett. **130**, 160201 (2023).

[27] Y. Aharonov, D. Z. Albert, and L. Vaidman, How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100, Phys. Rev. Lett. **60**, 1351 (1988).

[28] A. J. Leggett, Comment on "how the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100", Phys. Rev. Lett. **62**, 2325 (1989).

[29] T. A. Brun, A simple model of quantum trajectories, Am. J. Phys. **70**, 719 (2002).

[30] K. J. Resch and A. M. Steinberg, Extracting joint weak values with local, single-particle measurements, Phys. Rev. Lett. **92**, 130402 (2004).

[31] G. Mitchison, R. Jozsa, and S. Popescu, Sequential weak measurement, Phys. Rev. A **76**, 062105 (2007).

[32] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, 2009).

[33] J. S. Lundeen, B. Sutherland, A. Patel, C. Stewart, and C. Bamber, Direct measurement of the quantum wavefunction, Nature **474**, 188 (2011).

[34] J. S. Lundeen and C. Bamber, Procedure for direct measurement of general quantum states using weak measurement, Phys. Rev. Lett. **108**, 070402 (2012).

[35] C. Bamber and J. S. Lundeen, Observing dirac's classical phase space analog to the quantum state, Phys. Rev. Lett. **112**, 070405 (2014).

[36] F. Piacentini, A. Avella, M. P. Levi, M. Gramegna, G. Brida, I. P. Degiovanni, E. Cohen, R. Lussana, F. Villa, A. Tosi, F. Zappa, and M. Genovese, Measuring incompatible observables by exploiting sequential weak values, Phys. Rev. Lett. **117**, 170402 (2016).

[37] G. S. Thekkadath, L. Giner, Y. Chalich, M. J. Horton, J. Banker, and J. S. Lundeen, Direct measurement of the density matrix of a quantum system, Phys. Rev. Lett. **117**, 120401 (2016).

[38] Y. Kim, Y.-S. Kim, S.-Y. Lee, S.-W. Han, S. Moon, Y.-H. Kim, and Y.-W. Cho, Direct quantum process tomography via measuring sequential weak values of incompatible observables, Nat. Commun. **9**, 192 (2018).

[39] C. A. Fuchs and A. Peres, Quantum-state disturbance versus information gain: Uncertainty relations for quantum information, Phys. Rev. A **53**, 2038 (1996).

[40] P. Busch, *"No Information Without Disturbance": quantum limitations of measurement* (Springer, 2009) pp. 229–256.

[41] F. Buscemi, M. J. W. Hall, M. Ozawa, and M. M. Wilde, Noise and disturbance in quantum measurements: An information-theoretic approach, Phys. Rev. Lett. **112**, 050401 (2014).

[42] L. M. Johansen, Quantum theory of successive projective measurements, Phys. Rev. A **76**, 012119 (2007).

[43] L. Mazzola, G. De Chiara, and M. Paternostro, Measuring the characteristic function of the work distribution, Phys. Rev. Lett. **110**, 230602 (2013).

[44] J. S. Pedernales, R. Di Candia, I. L. Egusquiza, J. Casanova, and E. Solano, Efficient quantum algorithm for computing n-time correlation functions, Phys. Rev. Lett. **113**, 020505 (2014).

[45] B. Swingle, G. Bentsen, M. Schleier-Smith, and P. Hayden, Measuring the scrambling of quantum information, Phys. Rev. A **94**, 040302 (2016).

[46] N. Yunger Halpern, Jarzynski-like equality for the out-of-time-ordered correlator, Phys. Rev. A **95**, 012120 (2017).

[47] N. Y. Yao, F. Grusdt, B. Swingle, M. D. Lukin, D. M. Stamper-Kurn, J. E. Moore, and E. A. Demler, Interferometric approach to probing fast scrambling, Preprint at https://arXiv.org/abs/1607.01801 (2016).

[48] K.-D. Wu, Y. Yuan, G.-Y. Xiang, C.-F. Li, G.-C. Guo, and M. Perarnau-Llobet, Experimentally reducing the quantum measurement back action in work distributions by a collective measurement, Sci. Adv. **5**, eaav4944 (2019).

[49] N. Yunger Halpern, B. Swingle, and J. Dressel, Quasiprobability behind the out-of-time-ordered correlator, Phys. Rev. A **97**, 042105 (2018).

[50] J. R. González Alonso, N. Yunger Halpern, and J. Dressel, Out-of-time-ordered-correlator quasiprobabilities robustly witness scrambling, Phys. Rev. Lett. **122**, 040404 (2019).

[51] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, State-independent experimental test of quantum contextuality, Nature **460**, 494 (2009).

[52] P. Schindler, J. T. Barreiro, T. Monz, V. Nebendahl, D. Nigg, M. Chwalla, M. Hennrich, and R. Blatt, Experimental repetitive quantum error correction, Science **332**, 1059 (2011).

[53] V. Negnevitsky, M. Marinelli, K. K. Mehta, H.-Y. Lo, C. Flühmann, and J. P. Home, Repeated multi-qubit readout and feedback with a mixed-species trapped-ion register, Nature **563**, 527 (2018).

[54] C. Ryan-Anderson, J. G. Bohnet, K. Lee, D. Gresh, A. Hankin, J. P. Gaebler, D. Francois, A. Chernoguzov, D. Lucchetti, N. C. Brown, T. M. Gatterman, S. K. Halit, K. Gilmore, J. A. Gerber, B. Neyenhuis, D. Hayes, and R. P. Stutz, Realization of real-time fault-tolerant quantum error correction, Phys. Rev. X **11**, 041058 (2021).

[55] M. DeCross, E. Chertkov, M. Kohagen, and M. Foss-Feig, Qubit-reuse compilation with mid-circuit measurement and reset, Phys. Rev. X **13**, 041057 (2023).

[56] W. H. Zurek, Decoherence, einselection, and the quantum origins of the classical, Rev. Mod. Phys. **75**, 715 (2003).

[57] M. Schlosshauer, Decoherence, the measurement problem, and interpretations of quantum mechanics, Rev. Mod. Phys. **76**, 1267 (2005).

[58] A. Bassi, K. Lochan, S. Satin, T. P. Singh, and H. Ulbricht, Models of wave-function collapse, underlying theories, and experimental tests, Rev. Mod. Phys. **85**, 471 (2013).

[59] M. Lostaglio, A. Belenchia, A. Levy, S. Hernández-Gómez, N. Fabbri, and S. Gherardini, Kirkwood-dirac quasiprobability approach to the statistics of incompatible observables, Quantum **7**, 1128 (2023).

[60] A. E. Allahverdyan, Nonequilibrium quantum fluctuations of work, Phys. Rev. E **90**, 032137 (2014).

[61] H. Kwon and M. S. Kim, Fluctuation theorems for a quantum channel, Phys. Rev. X **9**, 031029 (2019).

[62] T. Upadhyaya, W. F. Braasch Jr, G. T. Landi, and N. Y. Halpern, What happens to entropy production when conserved quantities fail to commute with each other, Preprint at https://arXiv.org/abs/2305.15480 (2023).

[63] K. Zhang and J. Wang, Quasiprobability fluctuation theorem behind the spread of quantum information, Communications Physics **7**, 91 (2024).

[64] D. R. M. Arvidsson-Shukur, J. C. Drori, and N. Y. Halpern, Conditions tighter than noncommutation needed for nonclassicality, J. Phys. A: Math. Theor. **54**, 284001 (2021).

[65] Y. S. Chow and H. Teicher, *Probability theory: independence, interchangeability, martingales* (Springer Science & Business Media, 2012).

[66] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (2002).

[67] W. Hoeffding, Probability inequalities for sums of bounded random variables, J. Am. Stat. Assoc. **58**, 13 (1963).

[68] F. Buscemi, M. Dall'Arno, M. Ozawa, and V. Vedral, Direct observation of any two-point quantum correlation function, Preprint at https://arXiv.org/abs/1312.4240 (2013).

[69] L. Calderaro, G. Foletto, D. Dequal, P. Villoresi, and G. Vallone, Direct reconstruction of the quantum density matrix by strong measurements, Phys. Rev. Lett. **121**, 230501 (2018).

[70] P. Rall, Quantum algorithms for estimating physical quantities using block encodings, Phys. Rev. A **102**, 022408 (2020).

[71] A. Souza, I. Oliveira, and R. Sarthour, A scattering quantum circuit for measuring bell's time inequality: a nuclear magnetic resonance demonstration using maximally mixed states, New J. Phys. **13**, 053023 (2011).

[72] T. Xin, J. S. Pedernales, L. Lamata, E. Solano, and G.-L. Long, Measurement of linear response functions in nuclear magnetic resonance, Sci. Rep. **7**, 1 (2017).

[73] M. Ringbauer, F. Costa, M. E. Goggin, A. G. White, and A. Fedrizzi, Multi-time quantum correlations with no spatial analog, npj Quantum Inf. **4**, 1 (2018).

[74] L. Del Re, B. Rost, M. Foss-Feig, A. Kemper, and J. Freericks, Robust measurements of n-point correlation functions of driven-dissipative quantum systems on a digital quantum computer, Phys. Rev. Lett. **132**, 100601 (2024).

[75] G. Zhu, M. Hafezi, and T. Grover, Measurement of many-body chaos using a quantum clock, Phys. Rev. A **94**, 062329 (2016).

[76] A. Bohrdt, C. B. Mendl, M. Endres, and M. Knap, Scrambling and thermalization in a diffusive quantum many-body system, New J. Phys. **19**, 063001 (2017).

[77] J. Dressel, J. R. G. Alonso, M. Waegell, and N. Y. Halpern, Strengthening weak measurements of qubit out-of-time-order correlators, Phys. Rev. A **98**, 012132 (2018).

[78] B. Swingle and N. Yunger Halpern, Resilience of scrambling measurements, Phys. Rev. A **97**, 062113 (2018).

[79] B. Yoshida and N. Y. Yao, Disentangling scrambling and decoherence via quantum teleportation, Phys. Rev. X **9**, 011006 (2019).

[80] D. Kielpinski, C. Monroe, and D. J. Wineland, Architecture for a large-scale ion-trap quantum computer, Nature **417**, 709 (2002).

[81] Y. Wan, D. Kienzler, S. D. Erickson, K. H. Mayer, T. R. Tan, J. J. Wu, H. M. Vasconcelos, S. Glancy, E. Knill, D. J. Wineland, *et al.*, Quantum gate teleportation between separated qubits in a trapped-ion processor, Science **364**, 875 (2019).

[82] V. Kaushal, B. Lekitsch, A. Stahl, J. Hilder, D. Pijn, C. Schmiegelow, A. Bermudez, M. Müller, F. Schmidt-Kaler, and U. Poschinger, Shuttling-based trapped-ion quantum information processing, AVS Quantum Sci. **2**, 014101 (2020).

[83] J. M. Pino, J. M. Dreiling, C. Figgatt, J. P. Gaebler, S. A. Moses, M. Allman, C. Baldwin, M. Foss-Feig, D. Hayes, K. Mayer, *et al.*, Demonstration of the trapped-ion quantum ccd computer architecture, Nature **592**, 209 (2021).

[84] D. Zhu, G. D. Kahanamoku-Meyer, L. Lewis, C. Noel, O. Katz, B. Harraz, Q. Wang, A. Risinger, L. Feng, D. Biswas, *et al.*, Interactive cryptographic proofs of quantumness using mid-circuit measurements, Nat. Phys. , 1 (2023).

[85] J. P. Home, Quantum science and metrology with mixed-species ion chains, Adv. At. Mol. Opt. Phys. **62**, 231 (2013).

[86] T. R. Tan, J. P. Gaebler, Y. Lin, Y. Wan, R. Bowler, D. Leibfried, and D. J. Wineland, Multi-element logic gates for trapped-ion qubits, Nature **528**, 380 (2015).

[87] C. Ballance, V. Schäfer, J. P. Home, D. Szwer, S. C. Webster, D. Allcock, N. M. Linke, T. Harty, D. Aude Craik, D. N. Stacey, *et al.*, Hybrid quantum logic and a test of bell's inequality using two different atomic isotopes, Nature **528**, 384 (2015).

[88] I. V. Inlek, C. Crocker, M. Lichtman, K. Sosnova, and C. Monroe, Multispecies trapped-ion node for quantum networking, Phys. Rev. Lett. **118**, 250502 (2017).

[89] C. Bruzewicz, R. McConnell, J. Stuart, J. Sage, and J. Chiaverini, Dual-species, multi-qubit logic primitives for Ca^{+}/Sr^{+} trapped-ion crystals, npj Quantum Inf. **5**, 1 (2019).

[90] P. Wang, J. Zhang, C.-Y. Luan, M. Um, Y. Wang, M. Qiao, T. Xie, J.-N. Zhang, A. Cabello, and K. Kim, Significant loophole-free test of kochen-specker contextuality using two species of atomic ions, Sci. Adv. **8**, eabk1660 (2022).

[91] D. Allcock, W. Campbell, J. Chiaverini, I. Chuang, E. Hudson, I. Moore, A. Ransford, C. Roman, J. Sage, and D. Wineland, omg blueprint for trapped ion quantum computing with metastable states, Appl. Phys. Lett. **119** (2021).

[92] H.-X. Yang, J.-Y. Ma, Y.-K. Wu, Y. Wang, M.-M. Cao, W.-X. Guo, Y.-Y. Huang, L. Feng, Z.-C. Zhou, and L.-M. Duan, Realizing coherently convertible dual-type qubits with the same ion species, Nat. Phys. **18**, 1058 (2022).

[93] Y. Wang, M. Um, J. Zhang, S. An, M. Lyu, J.-N. Zhang, L.-M. Duan, D. Yum, and K. Kim, Single-qubit quantum memory exceeding ten-minute coherence time, Nat. Photonics **11**, 646 (2017).

[94] P. Wang, C.-Y. Luan, M. Qiao, M. Um, J. Zhang, Y. Wang, X. Yuan, M. Gu, J. Zhang, and K. Kim, Single ion qubit with estimated coherence time exceeding one hour, Nat. Commun. **12**, 1 (2021).

[95] A. Sørensen and K. Mølmer, Quantum computation with ions in thermal motion, Phys. Rev. Lett. **82**, 1971 (1999).

[96] J. Fiurášek and Z. c. v. Hradil, Maximum-likelihood estimation of quantum processes, Phys. Rev. A **63**, 020101 (2001).

[97] M. Riebe, K. Kim, P. Schindler, T. Monz, P. O. Schmidt, T. K. Körber, W. Hänsel, H. Häffner, C. F. Roos, and R. Blatt, Process tomography of ion trap quantum gates, Phys. Rev. Lett. **97**, 220407 (2006).

[98] H. N. Tinkey, A. M. Meier, C. R. Clark, C. M. Seck, and K. R. Brown, Quantum process tomography of a mølmer-sørensen gate via a global beam, Quantum Sci. Technol. **6**, 034013 (2021).

[99] K. Zyczkowski and M. Kus, Random unitary matrices, J. Phys. A: Math. Gen. **27**, 4235 (1994).

Acknowledgments

This work was supported by the Innovation Program for Quantum Science and Technology under Grant No. 2021ZD0301602, the National Natural Science Foundation of China Grants No.92065205, No.11974200, and No.12304551. H.J.K. is supported by the KIAS Individual Grant No.CG085301 at the Korea Institute for Advanced Study. M.S.K. acknowledges the KIST Open Research Program.

Author contributions

H.J.K. and M.S.K. proposed the protocol. P.W. and C.-Y.L developed the experimental system with the assistance of W.C, M.Q., Z.Z, K.W. P.W., and C.-Y.L implemented the protocol and led the data-taking. K.K. supervised the experiment. P.W., H.J.K., C.-Y.L, M.S.K., and K.K. wrote the manuscript.

Corresponding author

Correspondence with H.J.K., M.S.K., and K.K.

Competing interests

The authors declare that they have no competing interests.

Tangling schedules eases hardware connectivity requirements for quantum error correction

György P. Gehér[1] * Ophelia Crawford[1] † Earl T. Campbell[1 2] ‡

[1] *Riverlane, St. Andrew's House, 59 St. Andrew's Street, Cambridge CB2 3BZ, United Kingdom*
[2] *Dept. of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, United Kingdom*

Abstract. Error-corrected quantum computers have the potential to change the way we solve computational problems. Quantum error correction involves repeated rounds of carefully scheduled gates to measure the stabilisers of a code. A set of scheduling rules are typically imposed on the order of gates to ensure the circuit can be rearranged into an equivalent circuit that can be easily seen to measure the stabilisers. In this work, we ask what would happen if we break these rules and instead use circuit schedules that we describe as tangled. We find that tangling schedules generates long-range entanglement not accessible using nearest-neighbour two-qubit gates. Our tangled schedules method provides a new tool for building quantum error correction circuits and we explore applications to design new architectures for fault-tolerant quantum computers. Notably, we show that, for the widely used Pauli-based model of computation (achieved by lattice surgery), this access to longer-range entanglement can reduce the device connectivity requirements, without compromising on circuit depth.

Keywords: Quantum error correction, quantum architecture, hardware constraints, Pauli-based model of computation, fault-tolerant logical quantum computation, lattice surgery

The technical manuscript is [5].

- DOI: 10.1103/PRXQuantum.5.010348,
- arXiv number 2307.10147.

1 Introduction

For certain types of quantum hardware, e.g. superconducting quantum computers, the quantum processing unit (QPU) typically has a fixed qubit layout and connectivity. Here, connectivity means which pairs of qubits can be acted on with native two-qubit gates. As connectivity increases, so too does crosstalk noise and related engineering challenges. Furthermore, a QPU with uniform connectivity structure is desirable so that different code sizes and algorithms can be executed. As such, uniform, low-degree QPUs are the natural choice.

Since qubits are unfortunately noisy, the need for quantum error correction (QEC) procedures arises. This may require the measurement of some irregular, non-local stabilisers, that cannot be measured in the standard way using one auxiliary qubit per stabiliser due to the QPU's low degree of connectivity. For instance, when performing a lattice surgery operation with the surface code that involves a Y Pauli term, the measurement of twist defects and elongated rectangles is needed, and it is not currently known how to do that on a square-grid connectivity QPU without increasing circuit depth substantially. Here, we present a general method of tangled syndrome extraction circuits, which enables measurement of observables involving distant qubits. We then apply this to the non-local stabilisers appearing during Pauli-based computation with the surface code, and construct low-depth circuits to measure them on a square-grid connectivity QPU. Therefore, tangling enables fault-tolerant logical quantum computation via Pauli-based computational model using the surface code on square-grid connectivity architectures.

2 Preliminaries

Consider a general stabiliser $g = P_1 P_2 \dots P_m$, where each of $P_1, P_2, \dots, P_m$ is a single-qubit Pauli operator, with no two of them acting on the same qubit. We can always measure g using the following circuit: prepare an auxiliary qubit in the $|+\rangle$ state; apply controlled-P_1; apply controlled-P_2; … apply controlled-P_m; and finally, measure out the auxiliary qubit in the X basis, see Figure 1. This measurement outcome corresponds to the measurement of g. In this circuit $\mathcal{C}$, all controlled gates use the auxiliary qubit as the control. Furthermore, we are free to shuffle the order of the controlled-P_j gates and we may also insert identity gates. We call this the *auxiliary syndrome extraction circuit of g*.

Next, consider a set of stabilisers $\{g_j\}_{j=1}^m$, and for each stabiliser g_j suppose an auxiliary syndrome extraction circuit $\mathcal{C}_j$. Assume the circuits have the same depth, i.e. number of layers including those with identity gates, and that we use different auxiliary qubits for different stabilisers. If we combine these circuits, so that they all occur simultaneously, the resulting circuit, which we denote by $\mathcal{C}$, then measures the set of stabilisers $\{g_j\}_{j=1}^m$ simultaneously and independently if and only if the following two conditions are satisfied:

(a) no qubit is involved in more than one gate at a time;

(b) for every pair of distinct circuits $j \neq k$, the simultaneous combination of $\mathcal{C}_j$ and $\mathcal{C}_k$ is equivalent to the serial execution $\mathcal{C}_j$ followed by $\mathcal{C}_k$.

The technical manuscript [5] contains a more formal equivalent statement of both (a) and (b) in its Section

*george.geher@riverlane.com
†ophelia.crawford@riverlane.com
‡earl.campbell@riverlane.com

2. An illustration of these two conditions can be found in [9, Figure 15].

3 Our main result

Our tangled syndrome extraction technique is based on the following violation of condition (b).

Definition 1 (Tangled circuits) *The auxiliary syndrome extraction circuits $\mathcal{C}_j$ and $\mathcal{C}_k$ are called tangled if condition (a) above is satisfied for them, but condition (b) is not.*

It turns out that by tangling the circuits $\{\mathcal{C}_j\}_{j=1}^m$, it is possible to measure the product $h = g_1 \cdots g_m$. Since, in this case, the operators g_j are no longer stabilisers themselves, we emphasise this by calling them *component operators* instead. We state our main result now.

Theorem 2 *Consider a set of pair-wise commuting Pauli product operators $\{g_j\}_{j=1}^m$ and an auxiliary syndrome extraction circuit for each: $\{\mathcal{C}_j\}_{j=1}^m$. Denote by $\mathcal{C}$ the combined circuit. Compose an (undirected) graph $G = (V, E)$ where $V = [1, \ldots, m]$ and $(j, k) \in E$ if and only if the circuits $\mathcal{C}_j$ and $\mathcal{C}_k$ are tangled. Suppose further that G is a forest whose connected components are $\mathcal{T}_1, \ldots, \mathcal{T}_\ell$. Then there exists a modification of $\mathcal{C}$ where*

- *we modify the single qubit Pauli measurements on the auxiliary qubits, and*
- *we apply a Clifford correction on the data qubits,*

such that the modified circuit $\tilde{\mathcal{C}}$ measures the products $h_r := \prod_{j \in \mathcal{T}_r} g_j$ for $r = 1, \ldots, \ell$ simultaneously and independently. Moreover, after two rounds of syndrome extraction $\tilde{\mathcal{C}}$, the accumulated Clifford corrections multiply into a Pauli correction that can be tracked in software.

The main feature of our tangling circuits technique is that it creates entanglement between the auxiliary qubits, unlike in the case when condition (b) is satisfied. This is illustrated in Figure 2 for the simplest case of our theorem, i.e. when G is a two-vertex tree graph. In this case we need to modify the basis of measurements on the auxiliary qubits from X to Y, and include a Clifford correction as shown in Figure 2. As can be seen, when we reorder the entangling gates of the circuit $\tilde{\mathcal{C}}$, so that the ones controlled on the first auxiliary qubit are in front of the ones controlled on the other auxiliary qubit, an additional CZ gate (red in bottom subfigure of fig. 2) appears between the two auxiliary qubits. In Section 2 of the technical manuscript [5], we prove a circuit pruning identity, depicted in Figure 5b there, which we then use to prove the above theorem. Namely, we iteratively identify leaves of G and remove them by using the pruning identity. We continue with this process until the remaining graph has no edges. The full details are in the technical manuscript [5].

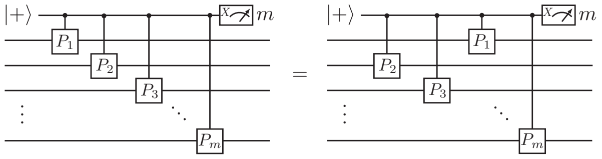


Figure 1: Auxiliary syndrome extraction circuit to measure the stabiliser $g = P_1 P_2 \ldots P_m$.

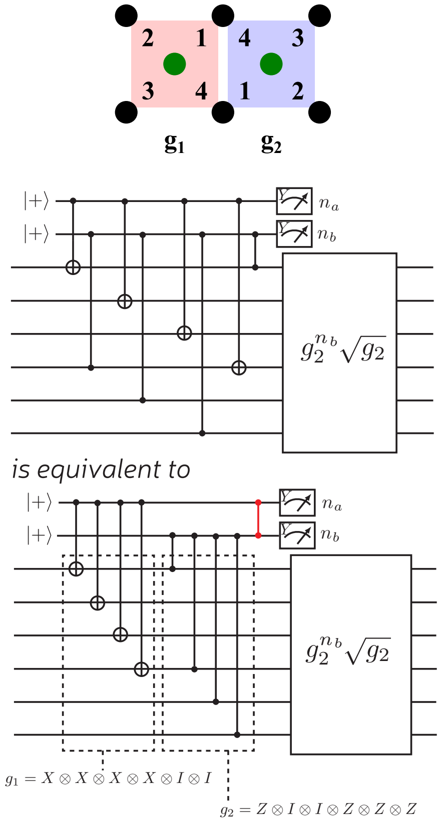

2
1
3
4
4
3
1
2
g1
g2
|+⟩
|+⟩
Y
Y
n_a
n_b
$g_2^{n_b}\sqrt{g_2}$
is equivalent to
|+⟩
|+⟩
Y
Y
n_a
n_b
$g_2^{n_b}\sqrt{g_2}$
$g_1 = X \otimes X \otimes X \otimes X \otimes I \otimes I$
$g_2 = Z \otimes I \otimes I \otimes Z \otimes Z \otimes Z$

Figure 2: (top) Graphical illustration of a pair of tangled syndrome extraction circuits that measures the stabiliser $h = g_1 g_2 = -XXYYZZ$ as a product of component operators $g_1 = XXXXII$ and $g_2 = IIZZZZ$. The X and Z Pauli terms of a component operator are coloured red and blue, respectively. (middle) Circuit for measuring h, as specified by the top subfigure, with the outcome given by $n_a \oplus n_b$. This circuit requires low connectivity and low depth to measure the product $g_1 g_2$ by violating the (b) condition. (bottom): An equivalent circuit that shows direct entanglement (red CZ gate) of auxiliary qubits. There is a Clifford correction to achieve the desired post-measurement state. However, after two rounds of the protocol, the Clifford correction becomes a Pauli correction.

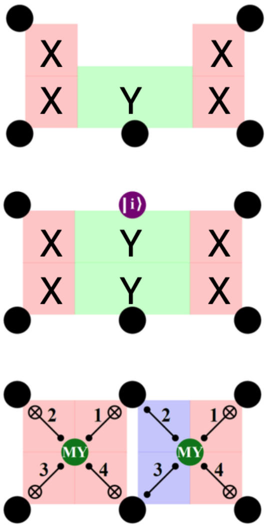


Figure 3: (top) A weight-5 twist-defect Pauli operator used for lattice surgery involving a Y Pauli term. The X, Y and Z Pauli terms are coloured red, green and blue, respectively. (middle) A sixth qubit (purple) initialised in the $|i\rangle$ state, and a weight-6 operator we can measure on these six qubits using our tangling schedules technique. (bottom) Graphical representation of the tangled circuit we can use to measure the weight-6 operator. Since the purple qubit was initialised in a Y-eigenstate, we effectively measure the weight-5 twist-defect $XXYXX$.

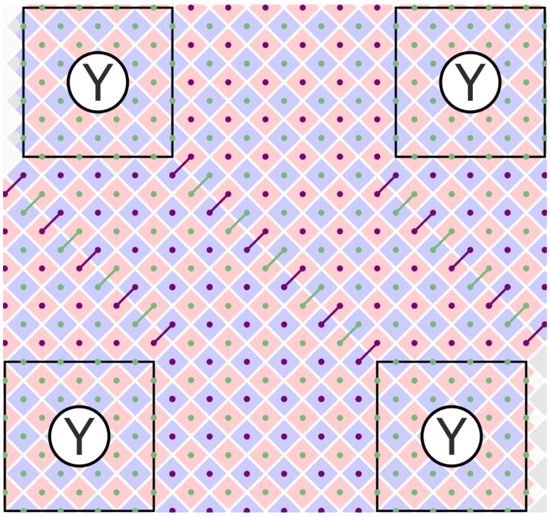


Figure 4: Example of a $YYYY$-lattice surgery patch whose stabilisers can be measured under square-grid connectivity using a low-depth circuit. The four logical qubits (enclosed in squares) are encoded into unrotated planar codes. Each red/blue plaquette is an X/Z-Pauli operator. Schedules between them are tangled if and only if their auxiliary qubits are connected with a line (essentially corresponding to the graph G from Theorem 2). The logical $YYYY$ measurement outcome corresponds to the joint parity of measurements made on the auxiliary qubits coloured in purple.

4 Fault-tolerant quantum computing on square-grid connectivity QPUs

In order to execute fault-tolerant quantum computation with the surface code, a popular way is to use the Pauli-based computational model [1, 2, 3, 8], where the major overhead is performing a series of multi logical qubit Pauli measurements. This can be achieved in a 2D planar architecture using *lattice surgery* [2, 3, 4, 7, 8, 9]. Some types of lattice surgery can be performed easily on a square-grid connectivity QPU by measuring only local stabilisers, meaning that one auxiliary qubit can be allocated for each stabiliser, connected to the qubits on which the stabiliser is supported. However, if the surface code patches are not positioned in a particular way, or if one of the logical Pauli terms is a Y, then the merge step of lattice surgery needs some irregularly-shaped, long-range stabilisers, typically so-called *elongated rectangles* or *twist defects*. A naive approach to measure these could be implemented using a high-depth circuit, swapping qubits as needed, but would be detrimental to logical fidelity and thresholds. More sophisticated, existing proposals to measure these irregular stabilisers mostly concentrate on changing the hardware either: globally by introducing additional connectivity (e.g. [2]); or locally by changing the connectivity of the QPU in certain regions (e.g. [3]).

With our tangled syndrome extraction, we show how to measure these elongated rectangles and twist defects under square-grid connectivity using a low-depth circuit. An example is shown in Figure 3 and the details can be found in Section 3 of the technical manuscript [5]. We also present two schemes to perform a general multi-qubit logical Pauli measurement, one with the unrotated planar code (see fig. 4) and another with the rotated planar code, thereby enabling fault-tolerant quantum computing under fourfold connectivity. We estimate their space-time cost based on numerical simulations that compare the quantum memory and stability experiment [6] performances of two types of rotated planar code patches: the default patches where each stabiliser is local, and their tangled versions where some stabilisers are replaced by elongated rectangles. The full details are in Section 4–5 and the Appendix of the technical manuscript [5].

5 Outlook

In our work, we have only considered applications of Theorem 2 where a stabiliser is a product of two component operators. It is, however, a very natural next step to explore schemes where we use more than two component operators to measure a stabiliser. Furthermore, whilst we have focused on planar codes in our work, we believe our tangled syndrome extraction method has applications for other stabiliser codes, and this would be another natural continuation of the present work.

References

[1] S. Bravyi, G. Smith, and J. A. Smolin. Trading classical and quantum computational resources. *Phys. Rev. X*, 6:021043, Jun 2016.

[2] C. Chamberland and E. T. Campbell. Circuit-level protocol and analysis for twist-based lattice surgery. *Physical Review Research*, 4(2):023090, 2022.

[3] C. Chamberland and E. T. Campbell. Universal quantum computing with twist-free and temporally encoded lattice surgery. *PRX Quantum*, 3(1):010331, 2022.

[4] A. G. Fowler and C. Gidney. Low overhead quantum computation using lattice surgery. *arXiv:1808.06709*, 2018.

[5] G. P. Gehér, O. Crawford, and E. T. Campbell. Tangling schedules eases hardware connectivity requirements for quantum error correction. *PRX Quantum*, 5:010348, Mar 2024.

[6] C. Gidney. Stability Experiments: The Overlooked Dual of Memory Experiments. *Quantum*, 6:786, Aug. 2022.

[7] C. Horsman, A. G. Fowler, S. Devitt, and R. Van Meter. Surface code quantum computing by lattice surgery. *New Journal of Physics*, 14(12):123011, 2012.

[8] D. Litinski. A game of surface codes: Large-scale quantum computing with lattice surgery. *Quantum*, 3:128, 2019.

[9] D. Litinski and F. von Oppen. Lattice surgery with a twist: simplifying Clifford gates of surface codes. *Quantum*, 2:62, 2018.

Extended Abstract: Compression of quantum shallow-circuit states

Yuxiang Yang[1] *

[1]*QICI, The University of Hong Kong, Hong Kong SAR, China*

Keywords: Quantum compression, shallow circuits, NISQ, identical-form quantum states

See arXiv 2404.11177 for the full paper.

1 Background

Shallow quantum circuits are a focus of recent research, for they are arguably the most accessible resources with genuine quantum features and advantages. At the fundamental level, shallow quantum circuits with constant depth have been shown to be hard to simulate classically (unless BQP $\subseteq$ AM) [1], and they outperform their classical counterparts in certain computational tasks [2, 3]. In practice, variational shallow circuits [4, 5, 6, 7] will remain a core ingredient of quantum algorithms in the noisy and intermediate-scale quantum (NISQ) era [8]. Efficient methods of learning shallow and bounded-complexity quantum circuits have recently been proposed [9, 10, 11].

Here we ask a fundamental question: Given N copies of an *unknown* n-qubit state and the promise that it is generated by a shallow circuit, is there a faithful compression protocol that encodes the N-copy state into a memory of fewer (qu)bits and then decodes it up to an error vanishing at $N \to \infty$? Processing quantum states in the many-copy form is important for extracting, storing, and distributing quantum information. Tasks where many-copy states serve as a fundamental resource, to list a few, include quantum metrology [12, 13, 14], quantum state tomography [15, 16] and shadow tomography [17, 18], quantum cloning [19, 20, 21, 22], and quantum hypothesis testing [23, 24, 25, 26]. Quantum algorithms, such as quantum principle component analysis [27], may also require states in the many-copy form. As such, compression of quantum states in the many-copy form is a basic and crucial protocol required for their storage and transmission. In the literature, compression of many-copy states was first studied for the simple case of pure qubits by Plesch and Bužek [28], experimentally demonstrated in Ref. [29], and later generalized in a series of works to mixed qudits [30, 31, 32, 33]. However, regarding states generated by shallow quantum circuits, the existing results are not applicable, for they all assume the state to be in a fixed-dimension space. Here, instead, we consider states in a growing-dimension ($D = 2^n$) space with complexity constraints. Therefore, studying the compression of shallow-circuit states not only requires better understanding of this important family of states but also demands new techniques of asymptotic quantum information processing.

2 Overview of main results

Given a set S of quantum states, the task of faithful N-copy compression is to design a protocol that consists of an encoder $\mathcal{E}_N$ and a decoder $\mathcal{D}_N$ such that the compression error vanishes for large N:

$$\lim_{N\to\infty} \sup_{\rho\in\mathsf{S}} d_{\mathrm{Tr}} \left(\mathcal{D}_N \circ \mathcal{E}_N(\rho^{\otimes N}), \rho^{\otimes N}\right) = 0. \tag{1}$$

Here d_{Tr} denotes the trace distance between quantum states. The encoder $\mathcal{E}_N$ and the decoder $\mathcal{D}_N$ are dependent on N but are independent of the input state. The memory cost is characterized by the dimension of the Hilbert space spanned by $\{\mathcal{E}_N(\rho^{\otimes N})\}$. The goal of compression is to reduce the memory cost

$$M := \log_2 \left|\mathsf{Supp}\left\{\mathcal{E}_N(\rho^{\otimes N})\right\}_{\rho\in\mathsf{S}}\right|, \tag{2}$$

i.e., the number of (qu)bits required for storing $\mathcal{E}_N(\rho^{\otimes N})$, while respecting the faithfulness condition (1).

Here, we are interested in the set of shallow-circuit states S_{sc}, which contains all n-qubit pure states that can be generated from $|0\rangle^{\otimes n}$ by circuits of depth no more than a constant d. As a proof-of-principle example, we focus on the most representative case of brickwork shallow circuits and consider the set of *shallow-circuit states*

$$\mathsf{S}_{\mathrm{sc}} := \left\{|\psi\rangle \ : \ |\psi\rangle = U_{\mathrm{sc}}|0\rangle^{\otimes n}\, \exists\, U_{\mathrm{sc}}\right\}, \tag{3}$$

where U_{sc} is a brickwork circuit with bounded depth ($\leq d$).

Without compression, the memory cost of storing the input state equals $N \cdot n$ qubits. Our main contribution is to show that a faithful N-copy compression exists for S_{sc}, as long as N grows at least as a polynomial of n with a high enough degree. The memory cost of the compression is linear in n and logarithmic in N, i.e., $M = O(n \cdot \log_2 N)$, achieving an exponential memory reduction in terms of N. Moreover, the memory does not have to be fully quantum. Instead, one may use a classical-quantum hybrid memory, where the ratio between the number of qubits and the number of classical bits decreases as $O(\log_2 n/\log_2 N)$. That is to say, when N is large, the memory consists mainly of classical bits, while a fully classical memory doesn't work. More details can be found in the technical manuscript.

Following the main result, it is natural to ask if the memory cost can be further reduced. We prove that a memory of size $\Omega(n \cdot \log_2 N)$ is required for keeping the

*yuxiang@cs.hku.hk

compression faithful. In this sense, our compression protocol is optimal in the scaling of n and N.

To establish the compression protocol, we develop novel tools for quantum information processing in the asymptotic regime of many copies, including a method of parameterizing shallow-circuit states in a small neighborhood with only $\mathsf{poly}(n)$ parameters and a correspondence between copies of a low-complexity state and a multi-mode coherent state. These tools can be further applied to other information processing tasks involving complexity-constrained quantum states.

3 Discussions

We have shown that N copies of an n-qubit shallow-circuit state can be optimally compressed to $\Theta(n \cdot \log_2 N)$ qubits. Intriguingly, the two key parameters n (the number of qubits per copy) and N (the number of copies) take distinct positions in the compression rate. We may give an interpretation to this phenomenon: n is the parameter of informativeness, as it is proportional to the number of free parameters of a shallow-circuit state. On the other hand, N is the parameter of accuracy, since $1/\sqrt{N}$ is the error scaling of tomography, i.e., of how well can we learn the information in the state. Our result shows that the N-copy state can be exponentially compressed only in the parameter of accuracy.

Besides memory efficiency, one may also be curious about the computational efficiency of shallow-circuit state compression. Unfortunately, the compression protocol in this work, despite being memory-efficient, is not computational efficient. The main obstacle is that the protocol requires searching over a covering mesh of shallow-circuit states, whose cost is exponentially large (in n). It is noteworthy that this is also the key step of converting a part of the memory to classical bits. It is thus intriguing to conjecture that any protocol using a hybrid memory is computationally inefficient. On the other hand, there exist compression protocols using fully quantum memory [30, 31] that do not require searching, and there remains hope that these protocols could inspire a computationally efficient protocol for shallow-circuit states.

As we focused on the most fundamental case, there is plenty room for extension. For example, one may consider shallow-circuit states with a 2D structure, and the techniques developed here should apply. Moreover, the circuit depth d is treated as a constant throughout this work, but from the derivation of results it can be seen that the compression will still be faithful when d grows very slowly (e.g., $d \ll \log n$) with n. In particular, it would be interesting to cover pesudorandom quantum states [34], which are low-depth states processing approximate Haar-randomness and are thus of particular interest in quantum cryptography. At last, one may even take into account the effect of noise and consider the compression of noisy shallow-circuit states. While similar results are expected there, some techniques in this work do not immediately generalize to mixed states and require moderate adaptation.

This work serves as the first step of establishing a new direction of coherent quantum information processing where the complexity of resources determines the rate and performance of processing, which goes beyond the existing literature that focused on incoherent information processing [9, 10, 11]. For future perspectives, it is our goal to consider more tasks such as cloning [19, 20, 21, 22] and gate programming [35, 36, 37, 38, 39] and, ultimately, to re-examine the entire quantum Shannon theory established in the past decade from the new perspective of the NISQ era.

References

[1] Barbara M. Terhal and David P. DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *Quantum Information and Computation*, 4(2):134–145, 2004.

[2] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[3] Sergey Bravyi, David Gosset, Robert König, and Marco Tomamichel. Quantum advantage with noisy shallow circuits. *Nature Physics*, 16(10):1040–1045, 2020.

[4] Marcello Benedetti, Erika Lloyd, Stefan Sack, and Mattia Fiorentini. Parameterized quantum circuits as machine learning models. *Quantum Science and Technology*, 4(4):043001, 2019.

[5] Marco Cerezo, Akira Sone, Tyler Volkoff, Lukasz Cincio, and Patrick J Coles. Cost function dependent barren plateaus in shallow parametrized quantum circuits. *Nature Communications*, 12(1):1791, 2021.

[6] Andrea Skolik, Jarrod R McClean, Masoud Mohseni, Patrick Van Der Smagt, and Martin Leib. Layerwise learning for quantum neural networks. *Quantum Machine Intelligence*, 3:1–11, 2021.

[7] Amira Abbas, David Sutter, Christa Zoufal, Aurélien Lucchi, Alessio Figalli, and Stefan Woerner. The power of quantum neural networks. *Nature Computational Science*, 1(6):403–409, 2021.

[8] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[9] Haimeng Zhao, Laura Lewis, Ishaan Kannan, Yihui Quek, Hsin-Yuan Huang, and Matthias C Caro. Learning quantum states and unitaries of bounded gate complexity. *arXiv:2310.19882*, 2023.

[10] Nengkun Yu and Tzu-Chieh Wei. Learning marginals suffices! *arXiv:2303.08938*, 2023.

[11] Hsin-Yuan Huang, Yunchao Liu, Michael Broughton, Isaac Kim, Anurag Anshu, Zeph Landau, and Jarrod R McClean. Learning shallow quantum circuits. *arXiv:2401.10095*, 2024.

[12] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[13] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical Review Letters*, 96(1):010401, 2006.

[14] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222–229, 2011.

[15] GM D'Ariano and P Lo Presti. Quantum tomography for measuring experimentally the matrix elements of an arbitrary quantum operation. *Physical Review Letters*, 86(19):4195, 2001.

[16] G Mauro D'Ariano, Matteo GA Paris, and Massimiliano F Sacchi. Quantum tomography. *Advances in Imaging and Electron Physics*, 128(10.1016):S1076–5670, 2003.

[17] Scott Aaronson. Shadow tomography of quantum states. In *Proceedings of the 50th annual ACM SIGACT symposium on theory of computing*, STOC 2018, pages 325–338, New York, NY, USA, 2018. Association for Computing Machinery.

[18] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020.

[19] Nicolas Gisin and Serge Massar. Optimal quantum cloning machines. *Physical Review Letters*, 79(11):2153, 1997.

[20] Reinhard F Werner. Optimal cloning of pure states. *Physical Review A*, 58(3):1827, 1998.

[21] Dagmar Bruss, Artur Ekert, and Chiara Macchiavello. Optimal universal quantum cloning and state estimation. *Physical Review Letters*, 81(12):2598, 1998.

[22] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Reviews of Modern Physics*, 77(4):1225, 2005.

[23] Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

[24] H. Yuen, R. Kennedy, and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Transactions on Information Theory*, 21(2):125–134, 1975.

[25] Carl W. Helstrom. *Quantum Detection and Estimation Theory*, volume 123. Elsevier Science, 1976.

[26] Alexander S Holevo. On asymptotically optimal hypothesis testing in quantum statistics. *Theory of Probability & Its Applications*, 23(2):411–415, 1979.

[27] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature Physics*, 10(9):631–633, 2014.

[28] Martin Plesch and Vladimír Bužek. Efficient compression of quantum information. *Physical Review A*, 81(3):032317, 2010.

[29] Lee A Rozema, Dylan H Mahler, Alex Hayat, Peter S Turner, and Aephraim M Steinberg. Quantum data compression of a qubit ensemble. *Physical Review Letters*, 113(16):160504, 2014.

[30] Yang, Yuxiang, Giulio Chiribella, and Daniel Ebler. Efficient quantum compression for ensembles of identically prepared mixed states. *Physical Review Letters*, 116:080501, 2016.

[31] Yang, Yuxiang, Giulio Chiribella, and Masahito Hayashi. Optimal compression for identically prepared qubit states. *Physical Review Letters*, 117:090502, 2016.

[32] Yang, Yuxiang, Giulio Chiribella, and Masahito Hayashi. Quantum stopwatch: how to store time in a quantum memory. *Proceedings of Royal Society A*, 474(2213):20170773, 2018.

[33] Yang, Yuxiang, Ge Bai, Giulio Chiribella, and Masahito Hayashi. Compression for quantum population coding. *IEEE Transactions on Information Theory*, 64(7):4766–4783, 2018.

[34] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III*, page 126–152, Berlin, Heidelberg, 2018. Springer-Verlag.

[35] Michael A Nielsen and Isaac L Chuang. Programmable quantum gate arrays. *Physical Review Letters*, 79(2):321, 1997.

[36] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical Review Letters*, 101(24):240501, 2008.

[37] Aleksander M Kubicki, Carlos Palazuelos, and David Pérez-García. Resource quantification for the no-programing theorem. *Physical Review Letters*, 122(8):080505, 2019.

[38] Michal Sedlák, Alessandro Bisio, and Mário Ziman. Optimal probabilistic storage and retrieval of unitary channels. *Physical Review Letters*, 122(17):170502, 2019.

[39] Yang, Yuxiang, Renato Renner, and Giulio Chiribella. Optimal universal programming of unitary gates. *Physical Review Letters*, 125:210501, 2020.

A polynomial-time quantum algorithm for solving the ground states of a class of classically hard Hamiltonians

Zhong-Xia Shang[1 2 3 *] Zi-Han Chen[1 2 3] Chao-Yang Lu[1 2 3] Jian-Wei Pan[1 2 3]
Ming-Cheng Chen[1 2 3]

[1] *Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*
[2] *Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*
[3] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

Abstract. In this work [arXiv:2401.13946], we present a polynomial-time quantum algorithm for solving the ground states of a class of classically hard Hamiltonians. The idea is to introduce a mapping $f: \rho \to |\rho\rangle$ to use density matrices to represent pure states. We show that this mapping makes sense by giving an efficient method to obtain the information of $|\rho\rangle$ from measurements on ρ. Under this mapping, the Lindblad master equation (LME) becomes a Schrödinger equation which contains natural imaginary time evolution. The steady state of the LME, therefore, corresponds to the ground state of $L^\dagger L$ with L the Liouvillian operator of the LME. We show the runtime of the LME has the $\mathcal{O}(log(\zeta^{-1}))$ scaling with ζ the overlap between the initial state and the ground state compared with the $\mathcal{O}(poly(\zeta^{-1}))$ scaling in other algorithms. We give concrete constructions on Hamiltonians that are quantumly easy by our algorithm and classically hard at the same time.

Keywords: Quantum algorithms, Open quantum systems, Quantum advantage

1 Introduction

Solving the ground states of general Hamiltonians is believed to be difficult for both classical and quantum computers. For quantum algorithms, a standard method is to use quantum phase estimation [1] (QPE) combined with amplitude amplification [2] (AA). Given a Hamiltonian whose spectral gap between the ground state and the first excited state is bounded by Δ, the required runtime to prepare its ground state to a fidelity $1-\varepsilon$ is of order $\mathcal{O}(poly(\Delta^{-1})poly(\varepsilon^{-1})poly(\zeta^{-1}))$ with ζ the overlap between the initial state and the ground state. More efficient algorithms based on linear combinations of unitaries and quantum signal processing [3, 4, 5] all adopt the idea of actively projecting out the ground state in some sense and can improve the runtime to an order $\mathcal{O}(poly(\Delta^{-1})log(\varepsilon^{-1})poly(\zeta^{-1}))$ with an exponential improvement over the precision ε.

However, from the $\mathcal{O}(poly(\zeta^{-1}))$ scaling of the runtime in the above algorithms, we can see why solving ground state can be even inefficient on quantum computers [6, 7]. As the number of qubits n of the system grows, with no prior knowledge, the overlap between an initial state and the ground state is exponentially small $\mathcal{O}(exp(n)^{-1})$, thus the runtime grows exponentially with the qubit number. However, in this work, we will present a quantum algorithm different from all the above types for solving ground states of a certain class of classically infeasible Hamiltonian with the runtime of order $\mathcal{O}(\Delta^{-1}log(\varepsilon^{-1/2}\zeta^{-1}))$ whose runtime is around $\Delta^{-1}(\frac{\ln(2)}{2}n+\ln(\varepsilon^{-\frac{1}{2}}))$.

2 Algorithm

We begin to introduce our algorithm. The first component comes from the dynamics of open quantum systems. Consider putting a system in an environment that is large enough such that the Markovian approximation is valid, then the dynamics of the system is governed by the Lindblad master equation (LME) [8, 9]:

$$\frac{d\rho}{dt} = \mathcal{L}[\rho] = -i[H,\rho] + \sum_i \lambda_i (F_i \rho F_i^\dagger - \frac{1}{2}\{\rho, F_i^\dagger F_i\}) \quad (1)$$

where $\rho = \sum_{ij}\rho_{ij}|i\rangle\langle j|$ is the density matrix of the system and F_i are quantum jump channels with strength λ_i. LME describes the dissipative nature of a system coupled with an environment. To see this more clearly, we can re-express the above LME as a vector form [10, 11]:

$$\frac{d\vec{\rho}}{dt} = L\vec{\rho} \quad (2)$$

where $\vec{\rho} = \sum_{ij}\rho_{ij}|i\rangle|j\rangle$ is the vector representation of the density matrix ρ and L is the Liouvillian generator for the LME semi-group which are not Hermitian in general has the following matrix form:

$$L = (-i(H\otimes I - I\otimes H^T) + \sum_i \lambda_i D[F_i]) \quad (3)$$

$$\text{where} \quad D[F_i] = F_i \otimes F_i^* - \frac{1}{2}F_i^\dagger F_i \otimes I - I \otimes \frac{1}{2}F_i^T F_i^*$$

Eq. 2 is attractive as it can be understood as a Schrödinger equation with non-Hermitian Hamiltonian iL which thus contains a natural imaginary time evolution. If the LME has a steady density matrix ρ_{ss} i.e. $\mathcal{L}[\rho_{ss}] = 0$, then the corresponding $\vec{\rho_{ss}}$ is the unnormalized ground state of Hermitian Hamiltonian $L^\dagger L$ with

[*] ustcszx@mail.ustc.edu.cn

ID	A	B	Spectra of B
1	II	$0.5II + 0.5XX + 0.5YY + 0.5ZZ$	{1,1,1,-1}
2	XX	$0.5II + 0.5XX - 0.5YY - 0.5ZZ$	{1,1,-1,1}
3	YY	$-0.5II + 0.5XX - 0.5YY + 0.5ZZ$	{1,-1,-1,-1}
4	ZZ	$0.5II - 0.5XX - 0.5YY + 0.5ZZ$	{1,-1,1,1}
5	IX	$0.5IX + 0.5XI + 0.5iYZ - 0.5iZY$	{-1,i,-i,1}
6	XI	$0.5IX + 0.5XI - 0.5iYZ + 0.5iZY$	{-1,i,-i,1}
7	YZ	$-0.5iIX + 0.5iXI + 0.5YZ + 0.5ZY$	{-1,i,-i,1}
8	ZY	$-0.5iIX + 0.5iXI - 0.5YZ - 0.5ZY$	{-1,i,-i,1}
9	IY	$-0.5IY + 0.5iXZ - 0.5YI - 0.5iZX$	{-1,i,-i,1}
10	YI	$0.5IY + 0.5iXZ + 0.5YI - 0.5iZX$	{-1,i,-i,1}
11	XZ	$0.5iIY + 0.5XZ - 0.5iYI + 0.5ZX$	{-1,i,-i,1}
12	ZX	$-0.5iIY + 0.5XZ + 0.5iYI + 0.5ZX$	{-1,i,-i,1}
13	IZ	$0.5IZ + 0.5iXY - 0.5iYX + 0.5ZI$	{i,-i,1,-1}
14	ZI	$0.5IZ - 0.5iXY + 0.5iYX + 0.5ZI$	{i,-i,1,-1}
15	XY	$0.5iIZ - 0.5XY - 0.5YX - 0.5iZI$	{1,-1,-i,i}
16	YX	$0.5iIZ + 0.5XY + 0.5YX - 0.5iZI$	{1,-1,-i,i}

Table 1: The 16 2-qubit Pauli operators (A) and their corresponding 2-qubit Pauli substitute operators (B). Each B is unitary whose eigenvalues are presented.

zero ground energy. Thus, the information of the ground state of $L^\dagger L$ is contained in ρ_{ss}. The question is how to retrieve the information, which leads to the second component of our algorithm. We introduce the following mapping:

$$f: \quad \rho \to |\rho\rangle \tag{4}$$

where $|\rho\rangle$ is defined as $\frac{1}{C_\rho}\sum_{ij}\rho_{ij}|i\rangle|j\rangle$ with the normalization factor $C_\rho = ||\rho||_F = \sqrt{\sum_{ij}|\rho_{ij}|^2}$. The key is how to understand this mapping. In this work, this mapping means that we are treating density matrices as pure states. For example, a single-qubit maximum mixed density matrix $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$ is treated as a two-qubit Bell state $(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$. We will call the subsystem labeled by index i the row subsystem and the subsystem labeled by index j the column subsystem. This mapping makes sense due to the following relation:

$$\langle\rho|A|\rho\rangle = \frac{Tr(B\rho\otimes\rho)}{Tr(\rho^2)} \tag{5}$$

where each matrix element of B $B_{il,jk} = \langle i|\langle l|B|j\rangle|k\rangle$ has the following relation with A:

$$B_{il,jk} = A_{ij,kl} \tag{6}$$

Eq. 5 means the information of $|\rho\rangle$ i.e. the value of $\langle\rho|A|\rho\rangle$ with A a Hermitian operator can be obtained from ρ by the value of the ratio of an operator B's expectation value under $\rho\otimes\rho$ to the purity of ρ. We name B as the substitute operator of A.

Having the formula Eq. 5, the following questions are how to measure its right-hand side and how efficient the measurement can be. Before introducing the measurement procedure, a prior thing to show is that the tensor product properties of A are not lost in B. More clearly, if each index of A in Eq. 6 actually contains indexes of n qubits e.g. $i \to i_1 i_2 ... i_n$, then the following relation is satisfied:

$$\begin{aligned}
&\text{if:} \quad A_{i_1 i_2 ... i_n j_1 j_2 ... j_n, k_1 k_2 ... k_n l_1 l_2 ... l_n} = \\
&\quad A^1_{i_1 j_1, k_1 l_1} A^2_{i_2 j_2, k_2 l_2} ... A^n_{i_n j_n, k_n l_n}, \\
&\text{then:} \quad B_{i_1 i_2 ... i_n l_1 l_2 ... l_n, j_1 j_2 ... j_n k_1 k_2 ... k_n} = \\
&\quad B^1_{i_1 l_1, j_1 k_1} B^2_{i_2 l_2, j_2 k_2} ... B^n_{i_n l_n, j_n k_n}
\end{aligned} \tag{7}$$

where relations between $A^1, A^2, ... A^n$ and $B^1, B^2, ... B^n$ satisfy the rules in Eq. 6. Due to the relation in Eq. 6, $n > 1$ situations can be generalized from the basic $n = 1$ case where A is a 2-qubit operator. For this case, the Hermitian A can be expressed as a real linear combination of 16 2-qubit Pauli operators. Each operator has a corresponding B operator which we will call the 2-qubit Pauli substitute operator. Interestingly, although the Hermiticity of 2-qubit Pauli operators is lost in the 2-qubit Pauli substitute operators, the unitarity is not, i.e. each 2-qubit Pauli substitute operator is unitary. All 16 2-qubit Pauli substitute operators are summarized in Table. 1. The unitarity of 2-qubit Pauli substitute operators makes sure that we can measure the expectation $Tr(B\rho\otimes\rho)$ by Hadamard tests [12]. Concretely, consider a to be measured $2n$-qubit Hermitian operator expressed as a combination of m terms:

$$A = \sum_{i=1}^{m} g_i P_i \tag{8}$$

where P_i are $2n$-qubit Pauli operators and g_i are the strengths which are real numbers. The substitute operator of A in Eq. 8 can be expressed as a similar form:

$$B = \sum_{i=1}^{m} g_i Q_i \tag{9}$$

where due to the transformation rule Eq. 6, the tensor product relation and the unitarity of the 2-qubit Pauli substitute operators, each $2n$-qubit Pauli substitute operator Q_i is unitary. Thus, the Hadamard test of $\mathcal{O}(1)$ depth can be used to evaluate each $Re(Tr(Q_i\rho\otimes\rho))$. The σ_z expectation value of the ancillary qubit gives the value of $Re(Tr(Q_i\rho\otimes\rho))$. By multiplying each estimated value of $Re(Tr(Q_i\rho\otimes\rho))$ by its weight g_i and summing up the results, we can obtain an estimation of the numerator $Tr(B\rho\otimes\rho)$ in Eq. 5. There is no need to measure the imaginary value of each Q_i since they will cancel out eventually guaranteed by the Hermiticity of A. For the purity $Tr(\rho^2)$ in the denominator, Swap tests [13] of $\mathcal{O}(1)$ depth are used to obtain the purity $Tr(\rho^2)$ in the denominator of Eq. 5 as $2p_s - 1$ where p_s is the probability of measuring the ancillary qubit in the $|0\rangle$ state. Thus, by using Hadamard tests and Swap tests, we can measure the value of $\langle\rho|A|\rho\rangle$.

Currently, the Hamiltonian $L^\dagger L$ we solved is calculated from the given L, which is easy as long as there are only polynomial terms in L. However, given a Hamiltonian H with given ground energy E_0 first, the reverse procedure of getting L that makes $H - E_0 = L^\dagger L$ is non-trivial. Fortunately, if we add some restrictions on L and $L^\dagger L$ such as locality or connectivity constraints which are very practical on real quantum computers, we can get the corresponding L in only polynomial-time by a classical algorithm called the XL algorithm [14, 15], which is the final component of our algorithm.

Having introduced the three components of our algorithm, we can now formally describe our algorithm. Given a Hamiltonian H with known ground energy E_0, we first judge and solve whether there exists L makes $H - E_0 = L^\dagger L$. If the XL algorithm gives a solution L, then we can generate a quantum system whose LME dynamics are governed by the $L \otimes L$. Then, let the system evolve freely to the steady state $\rho_{ss} \otimes \rho_{ss}$ of the LME. Next, we can do the measurement procedure introduced above and use Eq. 5 to obtain ground state information such as $\langle \rho_{ss} | A | \rho_{ss} \rangle$ with A an observable.

The total runtime of this algorithm depends on the time of the XL algorithm, the time of LME evolution, and the time of measurement. The evolution part depends on the overlap ζ between the initial state ρ_0 and the steady state ρ_{ss} defined as $\zeta = |\langle \rho_0 | \rho_{ss} \rangle|$, the smallest real part of the gaps between the steady state and other eigenvectors of L (assuming L is diagonalizable [11]) denoted as Δ and the required final overlap $1 - \varepsilon$ to be achieved. We prove the runtime of this part is of order $\mathcal{O}(\Delta^{-1} log(\varepsilon^{-1/2}) log(\zeta^{-1}))$ which is bounded by $\Delta^{-1}(\frac{\ln(2)}{2} n + \ln(\varepsilon^{-\frac{1}{2}}))$. The measurement part depends on the purity of ρ_{ss} and the number of terms in A. Assuming $Tr(\rho_{ss}^2) \geq \gamma$ and A contains m terms, then to achieve the MSE below an accuracy ϵ^2, the number of measurement is of order $\mathcal{O}(m\gamma^{-2}\epsilon^{-2})$.

3 Quantumly easy and classically hard examples

A direct example of quantumly easy and classically hard Hamiltonians under our algorithm can be found in Ref. [16] where LME is designed to encode quantum circuits. Suppose we want to simulate a quantum circuit: $|\psi_T\rangle = U_T U_{T-1} ... U_1 |0\rangle^{\otimes n}$ with all layers local, we can then define an LME with no internal Hamiltonian and with two types of jump operators:

$$F_i = |0\rangle_i \langle 1|_i \otimes |0\rangle_a \langle 0|_a \tag{10}$$

$$F_t = U_t \otimes |t+1\rangle_a \langle t|_a + U_t^\dagger \otimes |t\rangle_a \langle t+1|_a \tag{11}$$

with $i = 1, ..., n$ and $t = 0, ..., T$. This LME has a unique state state:

$$\rho_{ss} = \frac{1}{T+1} \sum_{t=0}^{T} |\psi_t\rangle \langle \psi_t| \otimes |t\rangle \langle t| \tag{12}$$

Thus, assuming P $\neq$ BQP, this LME is classically hard and satisfies all the conditions (spectral gap of L, purity of the steady state, and the locality of L.) for our algorithm to be in a polynomial time. Thus, its corresponding $L^\dagger L$ is exactly such an example.

References

[1] A Yu Kitaev. Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*, 1995.

[2] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002.

[3] Yimin Ge, Jordi Tura, and J Ignacio Cirac. Faster ground state preparation and high-precision ground energy estimation with fewer qubits. *Journal of Mathematical Physics*, 60(2):022202, 2019.

[4] Lin Lin and Yu Tong. Near-optimal ground state preparation. *Quantum*, 4:372, 2020.

[5] Yulong Dong, Lin Lin, and Yu Tong. Ground state preparation and energy estimation on early fault-tolerant quantum computers via quantum eigenvalue transformation of unitary matrices. *arXiv preprint arXiv:2204.05955*, 2022.

[6] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

[7] Christof Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60(4):2746, 1999.

[8] Crispin Gardiner, Peter Zoller, and Peter Zoller. *Quantum noise: a handbook of Markovian and non-Markovian quantum stochastic methods with applications to quantum optics*. Springer Science & Business Media, 2004.

[9] Serge Haroche and J-M Raimond. *Exploring the quantum: atoms, cavities, and photons*. Oxford university press, 2006.

[10] Victor V Albert and Liang Jiang. Symmetries and conserved quantities in lindblad master equations. *Physical Review A*, 89(2):022118, 2014.

[11] Fabrizio Minganti, Alberto Biella, Nicola Bartolo, and Cristiano Ciuti. Spectral theory of liouvillians for dissipative phase transitions. *Physical Review A*, 98(4):042118, 2018.

[12] Dorit Aharonov, Vaughan Jones, and Zeph Landau. A polynomial quantum algorithm for approximating the jones polynomial. *Algorithmica*, 55(3):395–421, 2009.

[13] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[14] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.

[15] Magali Bardet, Jean-Charles Faugere, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proc. of MEGA*, volume 5, pages 2–2, 2005.

[16] Frank Verstraete, Michael M Wolf, and J Ignacio Cirac. Quantum computation and quantum-state engineering driven by dissipation. *Nature physics*, 5(9):633–636, 2009.

Faster Quantum Algorithms with “Fractional”-Truncated Series

Yue Wang[1] * Qi Zhao[1] †

[1] *Department of Computer Science, University of Hong Kong, Pokfulam Road, Hong Kong*

Abstract. Quantum algorithms frequently rely on truncated series approximations, where the truncation order determines the circuit complexity. Achieving even moderate accuracy necessitates intensive circuit complexity. In response, we propose a general framework, the Randomized Truncated Series (RTS), which offers a quadratic improvement on the truncation error and enables a continuously adjustable effective truncation order. The core idea is that randomly mixing two series of specific forms substantially reduces the truncation error. We present an error analysis for RTS with a new mixing lemma accounting for near-unitary operators. We provide four illustrative examples to demonstrate the effectiveness and versatility of RTS. RTS shed light on the path towards practical quantum advantage.

Keywords: quantum algorithms, quantum computing, quantum simulation, series expansion

arXiv: https://arxiv.org/abs/2402.05595

1 Introduction

Quantum computing holds the promise to redefine the limits of information processing. Quantum algorithms, such as those for Hamiltonian simulation (HS) [1, 2, 3, 4, 5, 6, 7], solving differential equation [8, 9], and singular value transformation [10, 11], achieve at most exponential asymptotic speedup compared to their classical counterparts [12]. These algorithms provide the computational power necessary for exploring complex systems, holding the potential to empower researches like chemistry [13, 14, 15, 16, 17, 18], condensed matter physics [19, 20, 21], cryptography [22], engineering problems [23, 24, 25] and finance [26].

Realizing a transformation on an operator, $f(H)$, frequently appears in quantum algorithms such as Hamiltonian simulation, amplitude amplification, matrix inversion, and factoring [4, 3, 12]. We often approximate these functions by truncated series (TS) at an integer order K, i.e. $f(H) \approx \sum_{k=0}^{K} \alpha_k H^k$ for some real coefficients α_k, and treat the rest as truncation error δ. An increased K indicates higher precision but requires more qubits and gates, and a complicated circuit leads to vanishing quantum advantage [27, 28]. Yet, harnessing practical advantages from any quantum algorithm remains challenging.

Simplifying circuits without compromising precision can be achieved by reducing K. Inspired by Ref. [5], we utilize random mixing of TS such that multiple δ cancel out each other. Also, random mixing effectively produces fractional K, releasing the necessity of ceiling rounding K. In this work, we introduce Randomized Truncated Series (RTS), a simple and general framework featuring random mixing, applicable for general TS-based quantum algorithms. RTS results in a quadratically improved and continuously adjustable truncation error. On the high level, we mix $f_1(H) := \sum_{k=0}^{K_1} \alpha_k H^k$ and a modified TS of order $K_2 > K_1$, $f_2(H) := \sum_{k=0}^{K_1} \alpha_k H^k + 1/(1-p) \sum_{i=K_1+1}^{K_2} \alpha_k H^k$, where $p \in [0,1)$ is the mixing probability. By simple observation, the mixture, $f_{\text{mix}}(H) := pf_1(H) + (1-p)f_2(H) = \sum_{k=0}^{K_2} \alpha_k H^k$, better approximates $f(H)$. In real cases, we may not be able to implement $f_1(H)$ and $f_2(H)$ exactly with high probability. We thus denote V_1 and V_2 as corresponding actual operators. Moreover, $V_{1(2)}$ is generally non-unitary, and can only be probabilistically implemented by a quantum circuit $\mathfrak{V}_{1(2)}$. We thus renew the proof for the mixing lemma proposed in Ref. [29, 30] accounting for near-unitary dynamics.

To employ RTS, we first consider a general procedure: 1. prepare a quantum state with some ancilla $|\psi\rangle \otimes |ancilla\rangle$; 2. apply $\mathfrak{V}_{1(2)}$ on both system; 3. and heralding on correct measurement outcome on the ancilla system obtain the desired output state $V_{1(2)}|\psi\rangle$. We can then measure observable, perform tomography, or feed the resultant state into another quantum system. To employ RTS, we apply $\mathfrak{V}_{1(2)}$ with probability $p(1-p)$ in step 2 and collectively sample from the measurement result. In this manner, we can only reconstruct the classical information about the final state. However, we also find that we can obtain the final state coherently if $\mathfrak{V}_{1(2)}$ is a concatenation of identical segments. We call this kind of algorithm segmented algorithms. For example, in Hamiltonian simulation, we often split the entire evolution into pieces, where each segment corresponds to the evolution of a small time step. We, therefore, can perform randomization on these segments to enable coherent error cancellation.

RTS is a versatile protocol that optimizes various algorithms, and we demonstrate a few in detail. We anticipate further generalizations to analog quantum computing and time-dependent evolution. RTS is compatible with other circuit optimization tools, and we anticipate that RTS helps quantum devices handle more complicated tasks.

2 Main results

We obtain the following renewed mixing lemma.

Lemma 1 *Let V_1 and V_2 approximate an ideal operator U, and let the corresponding quantum channel on a den-*

*yuewang23@connect.hku.hk

†zhaoqi@cs.hku.hk

sity matrix $\rho = |\psi\rangle\langle\psi|$ be $\mathcal{V}_1 = V_1\rho V_1^\dagger$, $\mathcal{V}_2 = V_2\rho V_2^\dagger$ and $\mathcal{U} = U\rho U^\dagger$. Denote the operator $V_m := pV_1 + (1-p)V_2$. Assume the operator norm $\|V_1 - U\| \le \delta_1$, $\|V_2 - U\| \le \delta_2$, and $\|V_m - U\| \le \delta_m$, then the mixed channel $\mathcal{V}_{mix} := p\mathcal{V}_1 + (1-p)\mathcal{V}_2$ satisfies

$$R(\mathcal{V}_{mix}, \mathcal{U}) \le 2\varepsilon, \tag{1}$$

where $R(\mathcal{A}, \mathcal{B}) := \|\mathcal{A} - \mathcal{B}\|_1$ and $\varepsilon = 2\delta_m + p\delta_1^2 + (1-p)\delta_2^2$.

The protocol to conduct RTS is summarized below:

RTS Protocol

1. Random generate 1 and 2 with the probability p and $(1-p)$ respectively
2. Construct a quantum circuit $\mathfrak{V}_{1(2)}$ when the outcome in Step 1 is 1(2);
3. Post-select the measurement result on the ancilla system;
4. Post-process the output state.

The treatment of segmented algorithms differs in step 2, we instead concatenate proper amounts of $\mathfrak{V}_{1(2)}$ according to specification. The algorithmic error after applying RTS is quantified by the main theorem.

Theorem 2 *Let $U = \sum_{i=0}^{\infty} \alpha_k H^k$ be an operator in series expansion form and $\mathcal{U}(\rho) = U\rho U^\dagger$ be the corresponding quantum channel. Assume a quantum circuit $\mathfrak{V}_1$ encodes the truncated operator V_1 such that $\|U - V_1\| \le \delta_1$, there exist another quantum circuit $\mathfrak{V}_2$ that encodes V_2, where $\|U - V_2\| \le \delta_2$ and $\delta_2 = \mathcal{O}(\delta_1)$. Employing RTS on V_1 and V_2 yields an mixing channel $\mathcal{V}_{mix}$ such that*

$$R(\mathcal{V}_{mix}, \mathcal{U}) = \mathcal{O}\big(\delta_1^2\big) \tag{2}$$

In Theorem 2, we neglect δ_{m} in the asymptotic regime as it will be exponentially smaller than δ_1 in the case of large K_2.

When employing RTS, we choose a large p such that we only substitute a small portion of $\mathfrak{V}_1$ by $\mathfrak{V}_2$, introducing few extra costs. However, Theorem 2 indicates that a quadratic reduction in the algorithmic error will be generated. We demonstrate how to utilize RTS and the performances with several examples, and the results are shown below. Beginning with the simplest case, Hamiltonian Simulation (HS), as HS itself is implementing a function of a Hamiltonian, $f_{\mathrm{HS}} = e^{-iHt}$. In the BCCKS algorithm, we approximate f_{HS} in the Taylor series and truncated it at order K, i.e. $\tilde{f}_{\mathrm{HS}} = \sum_{k=0}^{K} \frac{(-iHt)^k}{k!}$. We can construct two series with maximum orders of K_1 and K_2. The BCCKS algorithm implements these two series with two operators, denoted as $V_{1,\mathrm{HS}}$ and $V_{2,\mathrm{HS}}$ respectively, such that $\|V_{1,\mathrm{HS}} - f_{\mathrm{HS}}\| \le \delta_{1,\mathrm{BCCKS}}$ and $\|(pV_{1,\mathrm{HS}} + (1-p)V_{2,\mathrm{HS}}) - f_{\mathrm{HS}}\| \le \delta_{\mathrm{m,BCCKS}}$.

Corollary 3 *For the BCCKS algorithm approximating the Hamiltonian dynamic $\mathcal{U}_{HS} = e^{-iHt}\rho e^{iHt}$ [4], RTS achieves an upper bound on algorithmic error*

$$R(\mathcal{V}_{mix,BCCKS}, \mathcal{U}_{HS}) \le \max\left\{\frac{40}{1-p}\delta_{1,\mathrm{BCCKS}}^2, 8\delta_{m,\mathrm{BCCKS}}\right\}, \tag{3}$$

where $\delta_{1,\mathrm{BCCKS}} = 2\frac{(\ln 2)^{K_1+1}}{(K_1+1)!}$ and $\delta_{m,\mathrm{BCCKS}} = 2\frac{(\ln 2)^{K_2+1}}{(K_2+1)!}$.

Quantum signal processing (QSP) implements Chebyshev's polynomials with quantum walk. Thus we instead approximate f_{HS} using Jacobi-Anger expansion and define the series expansion operator $V_{1(2),\mathrm{HS\_QSP}}$ and the corresponding error $\delta_{1(2),\mathrm{HS\_QSP}}$ similar to the BCCKS case. See the technical version for detailed constructions of operators.

Corollary 4 *In QSP implementation of $\mathcal{U}_{HS}$, the algorithmic error is upper bounded by*

$$R(\mathcal{V}_{mix,HS\_QSP}, \mathcal{U}_{HS}) \le \max\left\{28\delta_{1,\mathrm{HS\_QSP}}, 8\sqrt{\delta_{m,\mathrm{HS\_QSP}}}\right\}, \tag{4}$$

where $\delta_{1,\mathrm{HS\_QSP}} = \frac{4t^{K_1}}{2^{K_1}K_1!}$ and $\delta_{m,\mathrm{HS\_QSP}} = \frac{4t^{K_2}}{2^{K_2}K_2!}$.

QSP can also implement other function transformations on the Hamiltonian to realize all kinds of algorithms. In specific, we further elaborate on the truncated linear function (TLF), $f_{\Gamma,\mathrm{TLF}}(\lambda) = \frac{\lambda}{2\Gamma}, \forall|\lambda| \in [0, \Gamma]$, corresponding to the uniform spectral amplification algorithm. TLF can be implemented by a linear combination of two error functions, approximated by Jacobi-Anger expansion variants. We thus construct K_1 and K_2 truncated series expansions to approximate the error function and combine them to implement TLF.

Corollary 5 *In QSP implementation of $\mathcal{U}_{\Gamma,\mathrm{TLF}}$ to perform USA, the algorithmic error is upper bounded by*

$$R(\mathcal{V}_{mix,USA}, \mathcal{U}_{\Gamma,\mathrm{TLF}}) \le \max\left\{8\delta_{m,\mathrm{USA\_QSP}}, \frac{4}{1-p}\delta_{1,\mathrm{USA\_QSP}}^2\right\}, \tag{5}$$

where $\delta_{1,\mathrm{USA\_QSP}} = \frac{8\Gamma e^{-8\Gamma^2}}{\sqrt{\pi}}\frac{4(8\Gamma^2)^{K_1/2}}{2^{K_1/2}(K_1/2)!}$ and $\delta_{m,\mathrm{USA\_QSP}} = \frac{8\Gamma e^{-8\Gamma^2}}{\sqrt{\pi}}\frac{4(8\Gamma^2)^{K_2/2}}{2^{K_2/2}(K_2/2)!}$.

Lastly, we consider the application of RTS to solving ordinary differential equations in the form $d\vec{x}/dt = A\vec{x} + \vec{b}$. The solution is given by $\vec{x}(t) = e^{At}\vec{x}(0) + \big(e^{At} - \mathbb{1}\big)A^{-1}\vec{b}$, where e^{At} and $\big(e^{At} - \mathbb{1}\big)A^{-1}$ can be approximated by truncated Taylor series. We can achieve a much lower error by RTS.

Corollary 6 *Suppose $|x_{mix}^j\rangle$ is an approximated solution to the differential equation at time $t = jh$ using RTS and*

Table 1: Algorithmic error and corresponding cost for the BCCKS algorithm with and without RTS. $\tilde{G} = (7.5 \times 2^w + 6w - 26)r$ is the CNOT gate cost, where $w = \log_2 L$.

Cost Error	$7\tilde{G}$	$8\tilde{G}$	$9\tilde{G}$	$10\tilde{G}$
BCCKS	1.53×10^{-1}	1.17×10^{-2}	8.14×10^{-4}	5.13×10^{-5}
with RTS	3.59×10^{-3}	3.25×10^{-5}	2.14×10^{-7}	1.15×10^{-9}
Improvement	42.5×	361×	3810×	44500×

$|x(jh)\rangle$ is the exact solution. We can upper bound the estimation error by

$$\left\| |x^j_{mix}\rangle - |x(jh)\rangle \right\| \le \max\left\{ \frac{4}{1-p}\delta^2_{1,\mathrm{ODE}}, 8\delta_{m,\mathrm{ODE}} \right\}, \tag{6}$$

where $\delta_{1,\mathrm{ODE}} \le \frac{\mathcal{C}_j}{(K_1+1)!}$, and $8\delta_{m,\mathrm{ODE}} \le \frac{\mathcal{C}_j}{(K_2+1)!}$, and $\mathcal{C}_j$ is a problem specific constant.

For comparison, the original error upper bounds are, keeping the leading term, $2\delta_{1,\mathrm{BCCKS}}$, $\sqrt{\delta_{1,\mathrm{HS\_QSP}}}$, $\delta_{1,\mathrm{USA\_QSP}}$ and $\delta_{1,\mathrm{ODE}}$ for Corollaries 3, 4, 5, and 6 respectively. It can be easily seen that RTS achieves a quadratic speed-up.

Although any set of parameters $\{p, K_1, K_2\}$ provides a quadratic speed-up, the choice does influence the actual error, and a wise choice of parameters ensures better performance. However, it is hard to develop a procedure that provides the optimal parameters as $f(H)$ is arbitrary. We instead perform a brute force search over the error upper bound. Since K_1 and K_2 are discrete with typical values being less than 100 and the error upper bound function is smooth with respect to p, the classical computation for the brute force search is efficient. For algorithms with tight upper bounds, we generate a good suggestion on the actual error.

3 Numerical Result

We analyze the error upper bounds and costs implement RTS on the BCCKS algorithm [4] simulating the Ising model for $t = 100$ with

$$H = \sum_{i=1}^{n} \sigma_i^x \sigma_{i+1}^x + \sum_{i=1}^{n} \sigma_i^z, \tag{7}$$

where σ_i are Pauli operators acting on the i^{th} qubit and $n = 100$. The simulation consists of $r = 28854$ segments. To make a focused illustration of RTS, we only consider the gate cost of the **SELECT** oracle since it is the dominant contribution.

Each segment performing $\mathfrak{V}_{1(2)}$ need 3(4) **SELECT** oracles, and each costs $K(7.5\times2^w+6w-26)$ CNOT gates [31], where K is the truncation order and $w = \log_2(L)$. For a fixed cost budget, we traverse all feasible sets $\{K_1, K_2, p\}$ that use up the budget and find the minimum $r\epsilon$, which is the final algorithmic error with RTS. The result is shown in Fig. 1, with crosses representing the performance under discrete truncation, and the blue line indicating the optimal error achieved at a specific cost using RTS. We can see in Fig. 1 that the blue line declines faster than the orange dotted line, which is the line fitting the 4 cross marks, meaning we greatly improved the accuracy. Therefore we can use much fewer gates for simulation, i.e. targeting $\epsilon = 10^{-8}$, we save about 30% of CNOT gates.

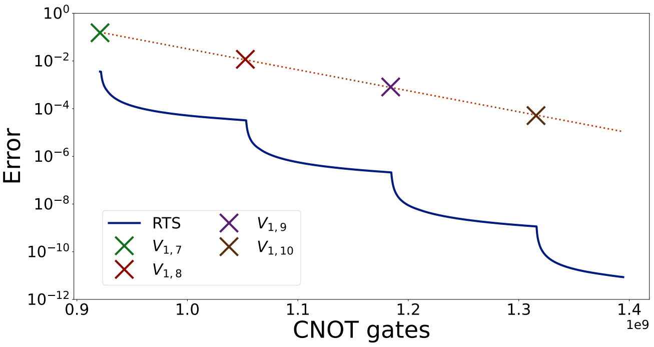


Figure 1: Algorithmic error and corresponding CNOT gate cost. Cross markers with different colors correspond to the original BCCKS algorithm with discrete truncation, where we denote V_{1,K_1} for a K_1-truncated V_1 operator. The solid blue line indicates the performance when employing RTS. Any point on the line corresponds to the error obtained by the optimal set of parameters $\{K_1, K_2, p\}$ using up all CNOT gates.

We also evaluate how much RTS improves the BCCKS algorithm in table 1. Note that we are restricted by only four costs with the original algorithm within the error range $\epsilon = [10^{-1}, 10^{-5}]$, whereas RTS enables a much finer adjustment on circuit cost.

4 Conclusion and open problems.

We presented a simple framework RTS that applies to arbitrary quantum algorithms relying on truncated series approximation. RTS enables a “fractional” truncation order and provides a quadratic improvement on algorithmic error. Essentially, we leverage random mixing to cancel out truncation error in two input quantum circuits $\mathfrak{V}_1$ and $\mathfrak{V}_2$. We specifically exhibit the implementation of RTS in various contexts to illustrate the flexibility of RTS. Although not evaluated in this work, RTS can also apply to non-unitary dynamics Ref. [32, 33, 34] and truncated-integral algorithms. We anticipate the generalization of the framework into dynamics determined by time-dependent operators, i.e. Dyson series, and analog quantum computing model.

References

[1] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996.

[2] Guang Hao Low and Isaac L. Chuang. Hamiltonian Simulation by Qubitization. *Quantum*, 3:163, July 2019.

[3] Guang Hao Low. *Quantum Signal Processing by Single-Qubit Dynamics.* Thesis, Massachusetts Institute of Technology, 2017.

[4] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating Hamiltonian Dynamics with a Truncated Taylor Series. *Physical Review Letters*, 114(9):090502, March 2015.

[5] Andrew M. Childs, Aaron Ostrander, and Yuan Su. Faster quantum simulation by randomization. *Quantum*, 3:182, September 2019.

[6] Andrew M. Childs and Yuan Su. Nearly optimal lattice simulation by product formulas. *Phys. Rev. Lett.*, 123:050503, Aug 2019.

[7] Qi Zhao, You Zhou, Alexander F. Shaw, Tongyang Li, and Andrew M. Childs. Hamiltonian simulation with random inputs. *Phys. Rev. Lett.*, 129:270502, Dec 2022.

[8] Dominic W. Berry, Andrew M. Childs, Aaron Ostrander, and Guoming Wang. Quantum algorithm for linear differential equations with exponentially improved dependence on precision. *Communications in Mathematical Physics*, 356(3):1057–1081, December 2017.

[9] Hari Krovi. Improved quantum algorithms for linear and nonlinear differential equations. *Quantum*, 7:913, February 2023.

[10] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, June 2019.

[11] Christoph Sünderhauf. Generalized quantum singular value transformation, 2023.

[12] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. A Grand Unification of Quantum Algorithms. *PRX Quantum*, 2(4):040203, December 2021.

[13] Daniel A. Lidar and Haobin Wang. Calculating the thermal rate constant with exponential speedup on a quantum computer. *Phys. Rev. E*, 59:2429–2438, Feb 1999.

[14] G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme. Quantum algorithms for fermionic simulations. *Phys. Rev. A*, 64:022319, Jul 2001.

[15] Dave Wecker, Bela Bauer, Bryan K. Clark, Matthew B. Hastings, and Matthias Troyer. Gate-count estimates for performing quantum chemistry on small quantum computers. *Physical Review A*, 90(2):022305, August 2014.

[16] Ryan Babbush, Craig Gidney, Dominic W. Berry, Nathan Wiebe, Jarrod McClean, Alexandru Paler, Austin Fowler, and Hartmut Neven. Encoding Electronic Spectra in Quantum Circuits with Linear T Complexity. *Physical Review X*, 8(4):041015, October 2018.

[17] Ryan Babbush, Nathan Wiebe, Jarrod McClean, James McClain, Hartmut Neven, and Garnet Kin-Lic Chan. Low Depth Quantum Simulation of Electronic Structure. *Physical Review X*, 8(1):011044, March 2018.

[18] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C. Benjamin, and Xiao Yuan. Quantum computational chemistry. *Rev. Mod. Phys.*, 92:015003, Mar 2020.

[19] Pedro C. S. Costa, Stephen Jordan, and Aaron Ostrander. Quantum algorithm for simulating the wave equation. *Physical Review A*, 99(1):012323, January 2019.

[20] Jeongwan Haah, Matthew B. Hastings, Robin Kothari, and Guang Hao Low. Quantum algorithm for simulating real time evolution of lattice Hamiltonians. *SIAM Journal on Computing*, 52(6):FOCS18–250–FOCS18–284, December 2023.

[21] Kaoru Mizuta and Keisuke Fujii. Optimal Hamiltonian simulation for time-periodic systems. *Quantum*, 7:962, March 2023.

[22] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[23] Xiangyu Li, Xiaolong Yin, Nathan Wiebe, Jaehun Chun, Gregory K. Schenter, Margaret S. Cheung, and Johannes Mülmenstädt. Potential quantum advantage for simulation of fluid dynamics, April 2023.

[24] Abtin Ameri, Erika Ye, Paola Cappellaro, Hari Krovi, and Nuno F. Loureiro. Quantum algorithm for the linear Vlasov equation with collisions. *Physical Review A*, 107(6):062412, June 2023.

[25] Noah Linden, Ashley Montanaro, and Changpeng Shao. Quantum vs. Classical Algorithms for Solving the Heat Equation. *Communications in Mathematical Physics*, 395(2):601–641, October 2022.

[26] Dylan Herman, Cody Googin, Xiaoyuan Liu, Alexey Galda, Ilya Safro, Yue Sun, Marco Pistoia, and Yuri Alexeev. A Survey of Quantum Computing for Finance, June 2022.

[27] Daniel Stilck França and Raul Garcia-Patron. Limitations of optimization algorithms on noisy quantum devices. *Nature Physics*, 17(11):1221–1227, 2021.

[28] Yiqing Zhou, E. Miles Stoudenmire, and Xavier Waintal. What Limits the Simulation of Quantum Computers? *Physical Review X*, 10(4):041038, November 2020.

[29] Earl Campbell. Shorter gate sequences for quantum computing by mixing unitaries. *Physical Review A*, 95(4):042306, April 2017.

[30] M. B. Hastings. Turning Gate Synthesis Errors into Incoherent Errors. https://arxiv.org/abs/1612.01011v1, December 2016.

[31] Andrew M. Childs, Dmitri Maslov, Yunseong Nam, Neil J. Ross, and Yuan Su. Toward the first quantum simulation with quantum speedup. *Proceedings of the National Academy of Sciences*, 115(38):9456–9461, September 2018.

[32] Dong An, Jin-Peng Liu, and Lin Lin. Linear Combination of Hamiltonian Simulation for Nonunitary Dynamics with Optimal State Preparation Cost. *Physical Review Letters*, 131(15):150603, October 2023.

[33] Dong An, Andrew M Childs, and Lin Lin. Quantum algorithm for linear non-unitary dynamics with near-optimal dependence on all parameters. *arXiv preprint arXiv:2312.03916*, 2023.

[34] Guang Hao Low and Yuan Su. Quantum eigenvalue processing, January 2024.

Quantum limits of covert target detection

Guo Yao Tham[1]* Ranjith Nair[1] † Mile Gu[1 2] ‡

[1] *Nanyang Quantum Hub, School of Physical & Mathematical Sciences, 21 Nanyang Link, Nanyang Technological University, Singapore 637371*

[2] *Centre for Quantum Technologies, 3 Science Drive 2, National University of Singapore, Singapore 117543*

Abstract. In covert target detection, Alice sends probe light to decide if a target is present within a region containing thermal background radiation while remaining undetected by an adversary, Willie, who is co-located with the target and collects all non-returning light. We rigorously formulate this problem and derive quantum limits on Alice's error probability in entanglement-assisted target detection given any level of her detectability by Willie. We demonstrate how Alice approaches this limit using two-mode squeezed vacuum probes for small to moderate background brightness while outperforming a scheme using Gaussian-distributed coherent states.

Keywords: Quantum illumination, Covert sensing, Target detection

Alice wishes to interrogate a distant region embedded in a thermal background for the presence or absence of a target adversary by probing it with a microwave or optical beam and monitoring the resulting reflections. Meanwhile, the adversary, Willie, monitors his thermal background for statistical deviations from thermal noise, aiming to detect if Alice is actively probing him. In this cat-and-mouse game, *how can Alice maximize her probability of correctly detecting Willie while minimizing Willie's chances of knowing he is being probed*? This question falls under the domain of *covert sensing* and naturally arises in the adversarial arms race between radar and radar detectors [1].

Sending a probe with greater energy can better sense Willie but also risks being detected. Alice thus faces a trade-off between performance and covertness. We seek the ultimate limit of Alice's performance, and ask whether moving towards this limit be facilitated by employing nonclassical light, as is well-known for quantum illumination (henceforth abbreviated as QI) in non-adversarial settings [2, 3, 4, 5, 6, 7, 8]? Indeed, several other covert protocols have been introduced in the continuous-variable setting [9, 10, 11, 12, 13, 14]. We suppose that Alice wishes to remain ϵ-covert, i.e., that the probability of Willie detecting her is at most $1/2+\epsilon$, and then obtain a closed-form lower bound on her error probability as a function of ϵ, the number of available optical modes M, and levels of loss and noise in the system. We show that two-mode squeezed vacuum (TMSV) probes can approach this limit in certain regimes. Comparing TMSV performance with that of Gaussian-distributed coherent state probes, we show that TMSV probes enable a reduction in error probability by a factor scaling exponentially with M.

1 Problem Setup

Entanglement-assisted target detection is illustrated in Fig. 1. Alice (A) wishes to detect the absence ($h=0$) or presence ($h=1$) of a weakly reflecting target (the two cases are assumed equally likely for simplicity) with round-trip reflectivity. The target is immersed in a thermal background such that each background mode is in a thermal state $\rho_{\mathsf{th}}(N_B) = \sum_{n=0}^{\infty} N_B^n/(N_B+1)^{n+1} |n\rangle\langle n|$ with average photon number N_B. Alice controls both the transmitter and receiver, and can prepare at most M signal modes. Thus, any covert sensing protocol involves preparing some incident probe state

$$|\psi\rangle_{IS} = \sum_{\mathbf{n}} \sqrt{p_{\mathbf{n}}}\, |\chi_{\mathbf{n}}\rangle_I\, |\mathbf{n}\rangle_S\,, \tag{1}$$

where $|\mathbf{n}\rangle_S = |n_1\rangle_1 |n_2\rangle_2 \cdots |n_M\rangle_M$ is an M-mode number state of the *signal* (S) system, $\{|\chi_{\mathbf{n}}\rangle_I\}$ are normalized (not necessarily orthogonal) states of an *idler* (I) system, and $p_{\mathbf{n}}$ is the probability mass function (pmf) of $\mathbf{n}$. The signal modes are sent to probe the target region while the idler is held losslessly. In the return (R) modes, Alice obtains an h-dependent return-idler state $\rho_{IR}^{(h)}$ that she measures to make a guess h_{est} for the value of h. Alice's performance is given by the *error probability* $P_{\mathfrak{e}}^{A}$, i.e., the probability that $h_{\text{est}} \neq h$.

The adversary, Willie (W), is situated at the target's location. We model the target by a beam splitter with reflectance $\eta \ll 1$. Let $\hat{a}_S^{(m)}$ and $\hat{a}_B^{(m)}$ be annihilation operators of the corresponding signal and background modes (see Fig. 1). Then

$$\hat{a}_R^{(m)} = \sqrt{\eta^{(h)}}\, \hat{a}_S^{(m)} + \sqrt{1-\eta^{(h)}}\, \hat{a}_B^{(m)}, \tag{2}$$

represents the annihilation operator of the mth mode returning to Alice, where $\eta^{(0)} = 0$ and $\eta^{(1)} = \eta$. When Willie is present ($h=1$), he receives the modes $\hat{a}_W^{(m)}$ for each $m = 1, \ldots, M$ from the other output of the beam splitter so that

$$\hat{a}_W^{(m)} = \sqrt{1-\eta}\, \hat{a}_S^{(m)} - \sqrt{\eta}\, \hat{a}_B^{(m)}. \tag{3}$$

Thus Alice faces the hypothesis test

$$\begin{aligned} &\mathrm{H}_0: \ \rho_0 = (\mathrm{Tr}_S\, \Psi) \otimes \rho_{\mathsf{th}}(N_B)^{\otimes M}, \\ &\mathrm{H}_1: \ \rho_1 = \left(\mathrm{id}_I \otimes \mathcal{L}_{\eta,N_B}^{\otimes M}\right) \Psi, \end{aligned} \tag{4}$$

*tham0157@e.ntu.edu.sg

†ranjith.nair@ntu.edu.sg

‡gumile@ntu.edu.sg

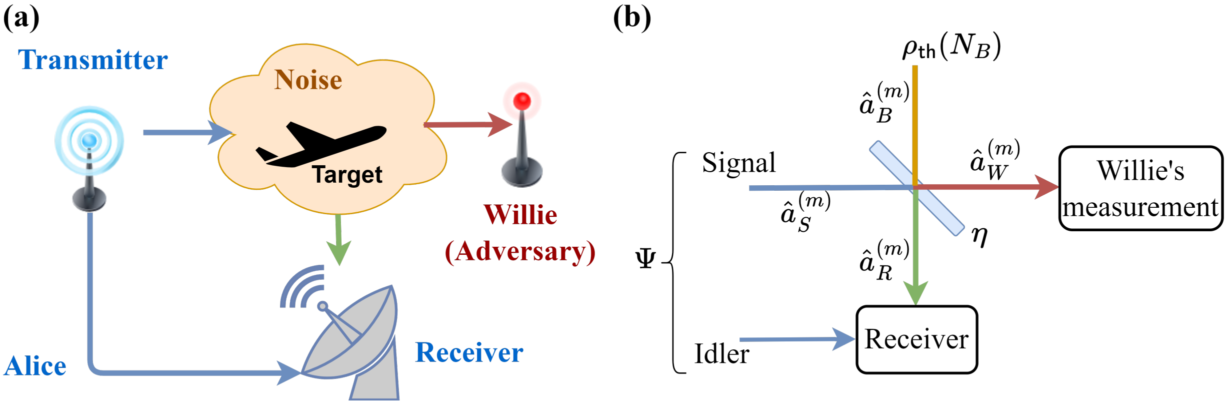


Figure 1: (a) In covert target detection, Alice (A) attempts to detect the presence of the adversary Willie (W) using an ancilla-entangled probe while remaining undetected herself. In the beam-splitter model (b), Alice prepares a joint state Ψ with M signal (S) and idler modes (I). Each signal mode $\hat{a}_S^{(m)}$ is either replaced by a background mode $\hat{a}_B^{(m)}$ when Willie is absent, or mixed with the background at a beam splitter with reflectance $\eta \ll 1$ representing the target. Alice makes an optimal measurement on the return modes $\hat{a}_R^{(m)}$, $m = 1, \dots M$ along with the idler system. Willie, when present, makes an optimal measurement on all his modes $\hat{a}_W^{(m)}$.

where $\mathcal{L}_{\kappa,N}$ denotes a thermal loss (or noisy attenuator) channel of transmittance κ and excess noise N [15]. Meanwhile, Willie is constrained only by the laws of physics and can have prior knowledge of which probe $\Psi = |\psi\rangle\langle\psi|_{IS}$ Alice plans to use. He thus faces the hypothesis test

$$\begin{aligned} \mathrm{H}_0' &: \ \sigma_0 = \rho_{\mathsf{th}}(N_B)^{\otimes M}, \\ \mathrm{H}_1' &: \ \sigma_1 = \mathcal{L}_{1-\eta,N_B}^{\otimes M}(\mathrm{Tr}_I\,\Psi). \end{aligned} \tag{5}$$

to decide whether Alice has sent a probe (H_1') or not (H_0').

Assuming that both parties make optimal quantum measurements and that their hypotheses are equally likely, their resulting average error probabilities are given by the Helstrom formula [16]:

$$P_{\mathfrak{e}}^A = 1/2 - \|\rho_0 - \rho_1\|_1/4 \le \inf_{0\le s\le 1} \mathrm{Tr}\,\rho_0^s\rho_1^{1-s}/2, \tag{6}$$

$$P_{\mathfrak{e}}^W = 1/2 - \|\sigma_0 - \sigma_1\|_1/4 \le \inf_{0\le s\le 1} \mathrm{Tr}\,\sigma_0^s\sigma_1^{1-s}/2, \tag{7}$$

where $\|X\|_1 := \mathrm{Tr}\,\sqrt{X^\dagger X}$ is the trace norm. We have also indicated the *quantum Chernoff bound* [17] (QCB) that is an exponentially tight upper bound on the average error probability. Alice's probe state is said to be ϵ-covert if

$$P_{\mathfrak{e}}^W \ge 1/2 - \epsilon. \tag{8}$$

We then ask: What is Alice's minimal error probability $P_{\mathfrak{e}}^A$ (as a function of M) when optimized over ϵ-covert probes?

The above framework deviates in several ways from previous studies of covert target detection. Firstly, our notion of ϵ-covertness defined by way of Willie's error probability has clear operational significance unlike previous formulations that use the relative entropy [18]. Secondly, the background brightness is fixed at N_B regardless of whether a target is present or absent. In contrast, most prior work on QI makes – for mathematical expediency – the so-called *No Passive Signature* (NPS) assumption which fine-tunes background brightness from its nominal value of N_B to $N_B/(1-\eta)$ when the target is present. While the NPS approximation is accurate when M is not very large, even standard QI has a quantum advantage only when $M \gg 1$, so that the physical basis of the assumption is questionable for standard QI and for covert detection (see [19] for a detailed discussion). As we show below, dropping the NPS assumption induces new qualitative behaviour in both non-adversarial and covert QI. Alice's performance then explicitly depends on the number M of signal modes, e.g. the available time-bandwidth product for temporal modes . This is the case for many other other quantum sensing and discrimination problems [20, 21, 22, 23] – since Alice gains some information even for a vacuum probe, this phenomenon is referred to as a *passive signature* (PS).

2 Technical Tools

2.1 QI with Passive Signature

We first derive analytical bounds on Alice's performance in the *non-adversarial* setting, i.e., for standard QI but without the NPS approximation. In ref. [19], we derive a general lower bound for Alice's error probability:

$$\begin{aligned} P_{\mathfrak{e}}^A &\ge \frac{1}{2}\left[1 - \sqrt{1 - \nu^{2M}\left[\sum_{n=0}^{\infty} p_n\left(1-\gamma_{\eta,N_B}\right)^{\frac{n}{2}}\right]^2}\,\right] \\ &\ge \frac{1}{2}\left[1 - \sqrt{1 - \nu^{2M}\left(1-\gamma_{\eta,N_B}\right)^{\mathcal{N}_S}}\,\right], \end{aligned} \tag{9}$$

where $\gamma_{\eta,N_B} = \frac{\eta}{(1-\eta)N_B+1}$, $\mathcal{N}_S := \sum_{n=0}^{\infty} np_n$ is the total signal energy, and we have used Jensen's inequality in the last step. The above result gives the ultimate limit of Alice's performance in QI with the PS assumption. It contrasts with the ultimate quantum limits of NPS QI derived in ref. [24] (see Eqs. (12)-(13) therein), which do not include the M-dependent factor ν^{2M} characteristic of the passive signature.

2.2 Necessary condition for ϵ-covertness

To incorporate the covertness constraint, we formulate a necessary condition for ϵ-covertness. Suppose that Alice transmits the probe Ψ of Eq. (1) with signal energy $\mathcal{N}_S$. The Fuchs-van de Graaf inequality $P_{\mathfrak{e}}^W \leq F(\sigma_0, \sigma_1)/2$ that relates the trace distance to the fidelity [25] between Willie's hypothesis states (5) implies that $F(\sigma_0, \sigma_1) \geq 1 - 2\epsilon$ is a necessary condition for ϵ−covertness. We use this to show that

$$\sum_{n=0}^{\infty} \sqrt{q_n} \sqrt{\binom{n+M-1}{n} \frac{N_B^n}{(N_B+1)^{n+M}}} \geq 1 - 2\epsilon \qquad (10)$$

is a necessary condition for ϵ−covertness, where $q_{\mathbf{n}} = \langle \mathbf{n} | \sigma_1 | \mathbf{n} \rangle_W$ and $\left\{ q_n = \sum_{\mathbf{n}: n_1 + \cdots + n_M} q_{\mathbf{n}} \right\}_{n=0}^{\infty}$ is the pmf of the total photon number seen by Willie under H_1' [19]. The condition of Eq. (10) implies that as ϵ is decreased, Alice's per-mode probe must look progressively more similar to the thermal background as we increase M (see [19] for details). In a significant departure from standard QI, it therefore does not make operational sense to consider the scaling of Alice's performance with signal energy $\mathcal{N}_S$. Instead, the key resource is the number of available optical modes M.

3 Fundamental limit of $P_{\mathfrak{e}}^A$ under ϵ-covertness

The thermal loss channel $\mathcal{L}_{1-\eta, N_B}$ connecting the modes in S to those in W (cf. Eq. (5)) admits the decomposition

$$\mathcal{L}_{1-\eta, N_B} = \mathcal{A}_G \circ \mathcal{L}_{(1-\eta)/G} \qquad (11)$$

into a quantum-limited amplifier $\mathcal{A}_G$ of gain $G = \eta N_B + 1$ and a pure-loss channel $\mathcal{L}_{(1-\eta)/G}$ of transmittance $(1 - \eta)/G$ [26]. The right-hand side of the bound of Eq. (9) is expressed in terms of the *probability generating function* (pgf) $\mathcal{P}_S(\xi)$ of the total photon number in S, defined as $\mathcal{P}_S(\xi) := \sum_{n=0}^{\infty} p_n \xi^n$ evaluated at $\xi = \sqrt{1 - \gamma_{\eta, N_B}}$. Using Eq. (11), we can extend Haus's pioneering work on connecting the input and output photon number pgfs of these single-mode quantum-limited channels [27] to multimode thermal loss channels and find the one-to-one mapping between the photon number pgf of the probe and the pgf $\mathcal{P}_W(\xi) := \sum_{n=0}^{\infty} q_n \xi^n$ of the total photon number in Willie's modes under H_1'. By connecting $\mathcal{P}_W(\xi)$ to the covertness condition of Eq. (10), we can show that [19]

$$P_{\mathfrak{e}}^A \geq \frac{1 - \sqrt{1 - (1-2\epsilon)^4 f_{\eta, N_B}^{2M}}}{2}, \qquad (12)$$

where $f_{\eta, N_B} = \nu(N_B + 1 - \frac{N_B}{x})[\eta N_B(1 - x) + 1]$, $x = 1 - \frac{\Theta}{\eta[1 + N_B(1-\Theta)]}$ and $\Theta = \frac{\sqrt{(1-\eta)(N_B+1)}}{\sqrt{1+(1-\eta)N_B}}$. This provides a universal, analytical and probe-independent lower bound for Alice's error probability for any desired covertness level ϵ.

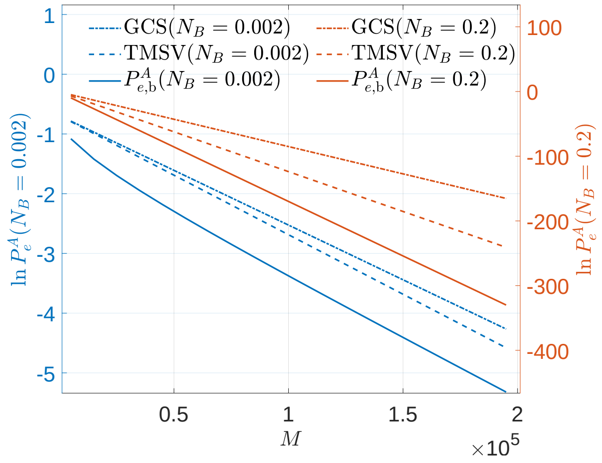


Figure 2: The lower bound Eq. (12) (solid) on Alice's error probability is compared to that of ϵ-covert TMSV (dashed) and GCS probes (dash-dotted line) for $N_B = 0.2$ (blue) and $N_B = 0.002$ (red). $\epsilon = 10^{-3}$ for both. For large M, the ratio of the error exponents predicted by the bound (12) and of TMSV probes are 1.37 (for $N_B = 0.2$) and 1.16 (for $N_B = 0.002$) respectively.

When limited to classical probes, Alice can generate Gaussian-distributed coherent state (GCS) probes − coherent states in each signal mode with amplitude $\alpha \in \mathbb{C}$ chosen according to a product circular Gaussian distribution $P(\alpha) = \frac{1}{(\pi N_S)} e^{-|\alpha|^2/N_S}$ with identical per-mode energy as for the TMSV probe (Alice's measurement can be conditioned on her knowledge of the amplitude transmitted in each of the M shots). Note that taking $N_S = N_B$ ensures perfect covertness. Figure 2 compares the lower bound of Eq. (12) to quantum TSMV and classical GCS probes. For each M, we consider the M-mode independently and identically distributed (iid) TMSV state with per-mode signal energy N_S chosen to be the maximum allowable by the covertness constraint. For $N_B = 0.2$, the large-M error exponent achieved by TMSV probes was about a factor of 1.37 lower than that of the bound, with the discrepancy becoming smaller for smaller N_B, along with the gap between the GCS and TMSV exponents.

4 Discussion & Outlook

We introduced an operational framework for ϵ-covert quantum target detection and obtained a fundamental lower bound (12) on Alice's error probability. As Fig. 2 indicates, the TMSV error exponent is close to that of our lower bound in the optical regime of $N_B \ll 1$, with the maximum advantage over the Gaussian-distributed coherent states being obtained for $N_B \simeq 0.2$. Equation (9) also constitutes the first universal performance limit for standard non-covert QI without the unphysical NPS assumption. For many further research avenues opened up by our work, as well as detailed proofs of our results, see ref. [19].

References

[1] P. E. Pace, *Detecting and classifying low probability of intercept radar*, vol. 1 (Artech House, 2004).

[2] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, "Quantum illumination with Gaussian states," Phys. Rev. Lett. **101**, 253,601 (2008).

[3] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," Nature Photonics **12**, 724–733 (2018).

[4] E. Polino, M. Valeri, N. Spagnolo, and F. Sciarrino, "Photonic quantum metrology," AVS Quantum Science **2**, 024,703 (2020).

[5] J. H. Shapiro, "The quantum illumination story," IEEE Aerospace and Electronic Systems Magazine **35**, 8–20 (2020).

[6] G. Sorelli, N. Treps, F. Grosshans, and F. Boust, "Detecting a target with quantum entanglement," IEEE Aerospace and Electronic Systems Magazine **37**, 68–90 (2022).

[7] A. Karsa, A. Fletcher, G. Spedalieri, and S. Pirandola, "Quantum illumination and quantum radar: A brief overview," quant-ph/2310.06049 (2023).

[8] R. Gallego Torromé and S. Barzanjeh, "Advances in quantum radar and quantum lidar," Progress in Quantum Electronics **93**, 100,497 (2024).

[9] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," Nature Communications **6**, 1–9 (2015).

[10] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," IEEE Journal on Selected Areas in Communications pp. 1–1 (2020).

[11] R. Di Candia, H. Yiğitler, G. Paraoanu, and R. Jäntti, "Two-way covert quantum communication in the microwave regime," PRX Quantum **2**, 020,316 (2021).

[12] B. A. Bash, C. N. Gagatsos, A. Datta, and S. Guha, "Fundamental limits of quantum-secure covert optical sensing," in "2017 IEEE International Symposium on Information Theory (ISIT)," (2017), pp. 3210–3214.

[13] C. N. Gagatsos, B. A. Bash, A. Datta, Z. Zhang, and S. Guha, "Covert sensing using floodlight illumination," Phys. Rev. A **99**, 062,321 (2019).

[14] S. Hao, H. Shi, C. N. Gagatsos, M. Mishra, B. Bash, I. Djordjevic, S. Guha, Q. Zhuang, and Z. Zhang, "Demonstration of entanglement-enhanced covert sensing," Phys. Rev. Lett. **129**, 010,501 (2022).

[15] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, 2017).

[16] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[17] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz Tapia, E. Bagan, L. Masanes, A. Acín, and F. Verstraete, "Discriminating states: The quantum Chernoff bound," Phys. Rev. Lett. **98**, 160,501 (2007).

[18] M. Tahmasbi, B. A. Bash, S. Guha, and M. Bloch, "Signaling for covert quantum sensing," in "2021 IEEE International Symposium on Information Theory (ISIT)," (2021), pp. 1041–1045.

[19] G. Y. Tham, R. Nair, and M. Gu, "Quantum limits of covert target detection," quant-ph/2310.11013 (2023).

[20] R. Nair, G. Y. Tham, and M. Gu, "Optimal gain sensing of quantum-limited phase-insensitive amplifiers," Phys. Rev. Lett. **128**, 180,506 (2022).

[21] R. Jönsson and R. Di Candia, "Gaussian quantum estimation of the loss parameter in a thermal environment," Journal of Physics A: Mathematical and Theoretical **55**, 385,301 (2022).

[22] H. Shi and Q. Zhuang, "Ultimate precision limit of noise sensing and dark matter search," npj Quantum Information **9**, 27 (2023).

[23] R. Nair and M. Gu, "Quantum sensing of phase-covariant optical channels," quant-ph/2306.15256 (2023).

[24] R. Nair and M. Gu, "Fundamental limits of quantum illumination," Optica **7**, 771–774 (2020).

[25] C. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," IEEE Transactions on Information Theory **45**, 1216 –1227 (1999).

[26] F. Caruso, V. Giovannetti, and A. S. Holevo, "One-mode bosonic Gaussian channels: a full weak-degradability classification," New Journal of Physics **8**, 310 (2006).

[27] H. A. Haus, *Electromagnetic Noise and Quantum Optical Measurements* (Springer Science & Business Media, New York, 2000).

Time-delayed single satellite quantum repeater node for global quantum communications

Mustafa Gündoğan[1] * Jasminder S. Sidhu[2] † Markus Krutzik[1] [3] Daniel K. L. Oi[2] [4]

[1] *Institut für Physik and IRIS Adlershof Humboldt-Universität zu Berlin, Newtonstr. 15, Berlin 12489, Germany*
[2] *SUPA Department of Physics, The University of Strathclyde, Glasgow, G4 0NG, UK*
[3] *Ferdinand-Braun-Institut (FBH), Gustav-Kirchoff-Str.4, 12489 Berlin*
[4] *Walton Institute for Information and Communication Systems Science, South East Technological University, Waterford X91 P20H, Ireland*

Abstract. Recent proposals for global-scale quantum networking leverage strings of space-borne quantum repeaters with on-board quantum memories. Here, we propose an alternative to such repeater constellations using only a single satellite with two memories that effectively acts as a time-delayed version of a single quantum repeater node. We estimate the secure finite keys and demonstrate an improvement of at least three orders of magnitude over prior single-satellite methods that rely on a single memory, while simultaneously reducing the necessary memory capacity by the same amount. We propose an experimental platform to realise this scheme based on rare-Earth ion doped crystals.

Keywords: Quantum networking, quantum key distribution, entanglement distribution.

Long-distance ($> 10^3$ km) quantum entanglement distribution will be crucial for the development of global networked quantum computers, sensors, positioning, navigation and timing, as well as for fundamental tests of physics. The main scientific and technical challenge is the high loss suffered by directly transmitted quantum signals that constrains the range and rate of entanglement distribution. Currently, fibre-based long-distance quantum communication experiments are limited to around a few hundred to a thousand kilometres [1], made possible by new techniques such as twin-field (TF) quantum key distribution (QKD) [2] and developments in low-loss fibre and low-noise single photon detectors. However, going beyond $\sim 10^3$ km requires alternate approaches, such as quantum repeaters (QRs) or free-space channels via space-based platforms.

The use of free-space channels can extend the direct-transmission limit, with fibre exponential loss scaling replaced by the (mainly) inverse square loss scaling of free-space propagation. Recently, the Micius satellite [3] demonstrated milestones such as ground-space teleportation [4], QKD with entangled photons across 1120 km [5], intercontinental QKD operated in trusted node [6] and the integration of satellite links into long-distance, trusted node ground networks [7]. These groundbreaking achievements are however limited by line-of-sight, the connection distance d between two ground stations is limited by the requirement to be in simultaneous view of the satellite ($d \leq 2000$ km for altitude $h = 500$ km) unless the satellite operates as a trusted node [8].

Fully global ($d > 10^4$ km) coverage with satellites has been proposed by several groups. An initial proposal was a hybrid, space-ground QR system [9] where quantum memories (QMs) were located in ground stations. This scheme was recently extended towards fully satellite-based QRs [10, 11] where the QMs are located onboard satellites, eliminating intermediate trans-atmospheric quantum links. These works demonstrated that entanglement distribution across the whole globe would be possible with a network of satellites equipped with QMs and entangled photon pair sources. It was shown that a storage time of around <1 s would be sufficient to reach global distances [10, 11] whereas intercontinental distances of > 8000 km would be possible with memory times of around 100 ms [11, 12].

An alternative to multiple QR nodes is to physically transport [13] entangled qubits, given sufficiently long qubit coherence times. This could be achieved via active quantum error correction [14] or by with ultra-long lifetime QMs [15, 16]. Here, we propose a time-delayed version of a single-node quantum repeater that can be implemented with a single orbiting satellite carrying an ultra-long-lived QM, which we refer to as QM1, in combination with a shorter lived (∼ms) QM (QM2). The addition of the lower requirement QM2 provides a feasible route towards dramatic improvements in secure key generation over QM1 alone. Using QKD as a benchmark for quantum communication, our scheme extends the performance and reduces the hardware requirements of a previous related proposal [15] by several orders of magnitude, especially when taking into account fine-block size effects.

To start, we first provide an overview of our time-delayed quantum repeater protocol. First, global quantum communications using a low-Earth orbit (LEO) satellite equipped with a QM with a lifetime in the order of the associated orbital period (90 minutes for LEO) and an entangled photon pair source has been previously proposed [15]. The source first sends one of the photons in each entangled pair to ground station A and the other half is stored in the on-board QM. The satellite then continues in its orbit and stored photons in the QM are retrieved and sent to ground station B as it flies over. Our scheme instead supplements a long-lived QM together with a second shorter-lived QM. QM1 needs to have $\tau_{QM1} > 1$ hour with a high multimode capacity

*guendomu@physik.hu-berlin.de
†jsmdrsidhu@gmail.com

whereas QM2 only needs $\tau_{QM2} \sim 2L/c$, where L is the range between the satellite and the ground station. Using a single QM limits the key length scaling to η_{ch}^2 whereas a second QM enhances the scaling to $\sim \eta_{ch}$, where η_{ch} is the average single channel loss, all else being equal. Our scheme can be regarded as the time delayed version of a single quantum repeater node [17, 18, 19] that enhances the achievable key rates and tolerable losses and eliminates the requirement for the two ground stations to be in simultaneous view.

The protocol begins with the start of the satellite pass over ground station A and operating its entangled photon-pair source (EPS, rate s). One photon in each pair is stored in QM1, the other photon is sent to ground station A through the space-ground channel. If this transmitted photon is lost, then the corresponding stored photon in the QM1 is erased, else the stored photon is kept if ground station A indicates successful reception. For QKD, the received photon is measured (as in BBM92 [20]) or, more generally, the ground stations could store the received photons in a QM if entanglement was required instead.

After the first overpass, the satellite continues in its orbit and the source again starts emitting entangled photon pairs when passing over ground station B. One photon of each pair is sent to ground station B whereas the other photon is stored in QM2. If ground station B successfully receives the transmitted photon, then the corresponding photon from QM2 is immediately retrieved together with a photon stored in QM1 and entanglement swapping performed by a Bell state measurement (BSM). The result of the BSM is then broadcast for local unitary corrective operations [17, 18]. Although we consider a QM paired with an entangled photon pair source, the same protocol can be realised with a DLCZ-type memory, where the QM can emit a single photon entangled with its internal atomic states [21].

Having now conceptually introduced our time-delayed quantum repeater protocol, we can quantify the relative performance against the previous single-memory scenario. Using QKD as a benchmark, we follow the approach of Ref. [5] to write the BBM92 finite-key length with symmetric basis choice. Specifically, considering the successfully entanglement-swapped pairs shared by ground stations A and B, the finite key length in the Z basis is then given by,

$$\begin{aligned} L_Z =& n_Z - n_Z h\left[\frac{e_X + \sqrt{\frac{(n_Z+1)\log\left(\frac{1}{\epsilon_{\rm sec}}\right)}{2n_X(n_X+n_Z)}}}{1-\Delta}\right] \\ &- f_{\rm e} n_Z h\left(e_Z\right) - n_Z\Delta - \log\frac{2}{\epsilon_{\rm corr}\epsilon_{\rm sec}^2}, \end{aligned} \tag{1}$$

where $\epsilon_{\rm sec}$ and $\epsilon_{\rm corr}$ are secrecy and correctness levels so that the protocol is ϵ-secure if $\epsilon \geq \epsilon_{\rm sec} + \epsilon_{\rm corr}$ [5], Δ is a factor to account for the mismatch of different detector efficiencies, $n_{Z/X}$ are the number of matching and coincident Z and X basis detection events respectively, and $e_{Z/X}$ are the quantum bit error rates (QBER) for each basis. The key length calculation for the X basis is similar to Eq. 1 thus the total key length becomes $L = L_X + L_Z$. Note that a more refined model of the key length is possible, but we choose this approach due to its relative simplicity for comparative purposes.

The QBERs with a single QR node (2 QMs) as in our protocol are given by [17],

$$\begin{aligned} e_X =& \lambda_{\rm BSM}\alpha_A\alpha_B\left[\epsilon_m\left(1-\epsilon_{\rm dp}\right) + \left(1-\epsilon_m\right)\epsilon_{\rm dp}\right] \\ &+ \frac{1}{2}\left[1-\lambda_{\rm BSM}\alpha_A\alpha_B\right], \end{aligned} \tag{2}$$

and

$$e_Z = \lambda_{\rm BSM}\alpha_A\alpha_B\epsilon_m + \frac{1}{2}\left[1-\lambda_{\rm BSM}\alpha_A\alpha_B\right]. \tag{3}$$

Here $\lambda_{\rm BSM}$ is a parameter that quantifies the ideality of the BSM and it is related to the BSM fidelity $F_{\rm BSM} = \sqrt{3(\lambda_{\rm BSM+1})/4}$; α_k is the probability of a real detection event in ground station k; ϵ_m is the misalignment error that also includes the source infidelity due to possible multi-photon excitations and ϵ_{dp} is total dephasing during the storage in memories which depends on the individual memory errors e_m. Ensemble based memories that we consider in this work have been shown to preserve the phase, independent of the storage time [22, 23, 24].

This is since re-emission of the stored information relies on rephasing of these excitations [25], any dephasing will result in lower operation efficiency while maintaining high fidelity. We assume a memory efficiency of $\sim 60\%$ at 90 minutes following the observed $T_2 = 6$ hours in a Europium doped crystal [16, 26] and $\lambda_{\rm BSM} = 0.98$ [17, 18] corresponding to $F_{\rm BSM} = 0.9925$. We further assume two identical passes over ground stations A and B each of 240 s duration and without memory constraints. Consequently, we will determine the required memory capacity as a result. We also do not assume a particular orbit, apart from being consistent with the overpass times and channel losses considered and achievable with realistic transmitter and receiver apertures. In the following, we finally assume an entangled photon pair source rate $s = 5$ MHz, a source infidelity $\epsilon_m = 2\%$, and a tight $\epsilon_{corr} = \epsilon_{sec} = 5\times10^{-12}$.

Compared with the 1-QM scheme [15], the second QM provides a marked advantage in the finite key setting (Fig. 1). With a single QM, finite size effects becomes significant after $\eta_{ch} \sim 26$ dB and the maximum tolerable average loss is 28 dB, beyond which secure key generation is not possible in a single set of overpasses. This also means that the 1-QM scheme would not produce any finite key with channel losses such as those reported in Ref. [5]. Fig. 1a shows the key rate per *received* pair, R, for the single and double memory scheme as a function of average single channel loss (η_{ch}). Notice that a crossover between finite key rates is observed at an average channel loss of $\eta_{ch} = 25.9$ dB. Fig. 1b explicitly demonstrates the advantage of the two-memory scheme, with higher loss tolerance and with up to three orders of magnitude (at around ~ 26.5 dB loss, beyond which 1-QM scheme is unable to generate secret keys) higher secure key lengths, L, due to the repeater effect on the

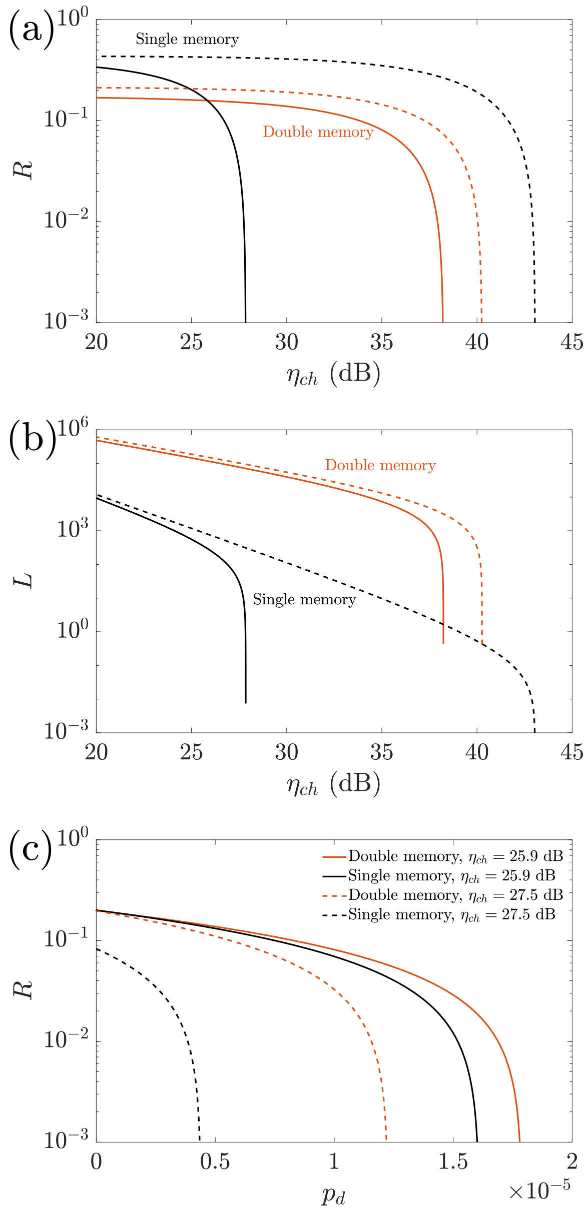


Figure 1: Comparison of 1-QM and 2-QM Key Generation. a) Finite key rate per received pair (R) for $e_m = 5\%$ (solid/dashed curves finite/asymptotic key rate); b) total finite key length (L) as a function of average single channel loss (η_{ch}) for $e_m = 5\%$ (solid/dashed curves finite/asymptotic key length). (c) Finite key rate per received pair versus total incoherent noise for fixed channel losses.

second downlink indicated by the lower slope of the curve for the 2-QM case.

The 2-QM protocol can achieve a finite key rate that approaches its asymptotic limit even for high channel loss and contact times of only a few minutes. In contrast, the 1-QM scheme shows a 15 dB gap between the maximum tolerable loss and finite key limit due to the greatly reduced number of received pairs, without the repeater effect of the second QM, imposing a severe finite block size penalty. In the asymptotic limit, however, the single-memory scheme could in principle tolerate higher losses than the two-memory case due to a reduction of errors from the absence of a non-perfect BSM ($\lambda_{\text{BSM}} = 1$ in the 1-QM case effectively) and the additional dephasing in QM2. We also note that in the 2-QM case, the BSM maximum success rate of 50% (assuming passive ancilla-less static linear optics) halves the number of received pairs, hence the implementation of deterministic entanglement swapping BSMs could provide a tangible improvement in finite key generation and increasing loss tolerance due to longer blocks and better finite statistics.

Fig. 1c shows the effect of incoherent detector clicks, p_d, on the key rate for $\eta_{ch} = 25.9$ dB, the crossover point in Fig. 1a between the two schemes in the finite key setting. The two-memory scheme is more resilient to noise, despite the additional errors introduced by the BSM/entanglement swapping and second memory required. This is due to the much larger block size achievable with 2-QMs leading to lower statistical uncertainties, hence tighter bounds in Eq. 1. The sensitivity on the single channel loss is also illustrated: the dashed curves for $\eta_{ch} = 27.5$ dB show that the double memory scheme has more than three times better noise tolerance than its single memory counterpart.

In conclusion, we conceptually propose a new quantum communication protocol that physically transports stored qubits in an ultra-long-lived QM (lifetime in the order of the orbital period) on an orbiting satellite, and uses a second shorter-lived QM (lifetime in the order of a round-trip classical communication signal) to substantially enhance entanglement distribution over long distances. We quantify the performance of our protocol, and find it dramatically reduces system complexity of global quantum networks by taking advantage of two different paradigms, i.e. quantum repeater behaviour and physically moving qubits, eliminating the need to coordinate orbiting strings of QR satellites and multiple optical links simultaneously. Using two QMs instead of one significantly increases the maximum tolerable channel loss while reducing the required multimode capacity from $\sim 10^8$ [15] to $\sim 10^6$ despite additional errors from the second QM, a non-ideal BSM, and 50% BSM outcome inefficiency in the 2-QM case. Recent progress in QMs indicates that the necessary storage time and multimode capacity should be achievable in the near future.

These results could be improved by utilising more recent finite key calculations that specifically address space-based QKD scenarios. The secure key lengths may be increased by approximately $\sim 10\%$ or else smaller block sizes could be used [27]. Wavelength division multiplexing may allow increased rates at which entangled pairs can be sent through the space-Earth quantum optical channel despite QM linewidth limitations. Finally, ultra-long-lived QMs in orbit may also serve as useful probes to investigate the intersection of quantum physics and general relativity and enable Bell tests across Earth-Moon distances.

References

[1] Jiu-Peng Chen et al. “Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km”. In: *Phys. Rev. Lett.* 124 (7 Feb. 2020), p. 070501. DOI: 10.1103/

PhysRevLett.124.070501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.124.070501.

[2] M. Lucamarini et al. “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters”. In: *Nature* 557.7705 (May 2018), pp. 400–403. ISSN: 1476-4687. DOI: 10.1038/s41586-018-0066-6.

[3] Chao-Yang Lu et al. “Micius quantum experiments in space”. In: *Rev. Mod. Phys.* 94 (3 July 2022), p. 035001. DOI: 10.1103/RevModPhys.94.035001. URL: https://link.aps.org/doi/10.1103/RevModPhys.94.035001.

[4] Ji-Gang Ren et al. “Ground-to-satellite quantum teleportation”. In: *Nature* 549.7670 (Sept. 2017), pp. 70–73. ISSN: 1476-4687. DOI: 10.1038/nature23675. URL: https://doi.org/10.1038/nature23675.

[5] Juan Yin et al. “Entanglement-based secure quantum cryptography over 1,120 kilometres”. In: *Nature* 582.7813 (June 2020), pp. 501–505. ISSN: 1476-4687. DOI: 10.1038/s41586-020-2401-y. URL: https://doi.org/10.1038/s41586-020-2401-y.

[6] Sheng-Kai Liao et al. “Satellite-Relayed Intercontinental Quantum Network”. In: *Phys. Rev. Lett.* 120 (3 Jan. 2018), p. 030501. DOI: 10.1103/PhysRevLett.120.030501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

[7] Yu-Ao Chen et al. “An integrated space-to-ground quantum communication network over 4,600 kilometres”. In: *Nature* 589.7841 (Jan. 2021), pp. 214–219. ISSN: 1476-4687. DOI: 10.1038/s41586-020-03093-8. URL: https://doi.org/10.1038/s41586-020-03093-8.

[8] Tom Vergoossen et al. “Modelling of satellite constellations for trusted node QKD networks”. In: *Acta Astronaut.* 173 (2020), pp. 164–171. ISSN: 0094-5765. DOI: https://doi.org/10.1016/j.actaastro.2020.02.010. URL: http://www.sciencedirect.com/science/article/pii/S0094576520300722.

[9] K. Boone et al. “Entanglement over global distances via quantum repeaters with satellite links”. In: *Phys. Rev. A* 91 (5 May 2015), p. 052325. DOI: 10.1103/PhysRevA.91.052325. URL: https://link.aps.org/doi/10.1103/PhysRevA.91.052325.

[10] Carlo Liorni, Hermann Kampermann, and Dagmar Bruß. “Quantum repeaters in space”. In: *New Journal of Physics* 23.5 (May 2021), p. 053021. DOI: 10.1088/1367-2630/abfa63. URL: https://doi.org/10.1088/1367-2630/abfa63.

[11] Mustafa Gündoğan et al. “Proposal for space-borne quantum memories for global quantum networking”. In: *npj Quant. Inf.* 7.1 (Aug. 2021), p. 128. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00460-9. URL: https://doi.org/10.1038/s41534-021-00460-9.

[12] Julius Wallnöfer et al. “Simulating quantum repeater strategies for multiple satellites”. In: *Communications Physics* 5.1 (June 2022), p. 169. ISSN: 2399-3650. DOI: 10.1038/s42005-022-00945-9. URL: https://doi.org/10.1038/s42005-022-00945-9.

[13] Wei Li, Parvez Islam, and Patrick Windpassinger. “Controlled Transport of Stored Light”. In: *Phys. Rev. Lett.* 125 (15 Oct. 2020), p. 150501. DOI: 10.1103/PhysRevLett.125.150501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.125.150501.

[14] Simon J. Devitt et al. “High-speed quantum networking by ship”. In: *Scientific Reports* 6.1 (Nov. 2016), p. 36163. ISSN: 2045-2322. DOI: 10.1038/srep36163. URL: https://doi.org/10.1038/srep36163.

[15] S. E. Wittig et al. *Concept for single-satellite global quantum key distribution using a solid state quantum memory.* http://iafastro.directory/iac/paper/id/36863/summary/. Sept. 2017.

[16] Joss Bland-Hawthorn, Matthew J. Sellars, and John G. Bartholomew. “Quantum memories and the double-slit experiment: implications for astronomical interferometry”. In: *J. Opt. Soc. Am. B* 38.7 (July 2021), A86–A98. DOI: 10.1364/JOSAB.424651. URL: http://opg.optica.org/josab/abstract.cfm?URI=josab-38-7-A86.

[17] D. Luong et al. “Overcoming lossy channel bounds using a single quantum repeater node”. In: *Appl. Phys. B* 122.4 (Apr. 2016), p. 96. ISSN: 1432-0649. DOI: 10.1007/s00340-016-6373-4. URL: https://doi.org/10.1007/s00340-016-6373-4.

[18] Róbert Trényi and Norbert Lütkenhaus. “Beating direct transmission bounds for quantum key distribution with a multiple quantum memory station”. In: *Phys. Rev. A* 101 (1 Jan. 2020), p. 012325. DOI: 10.1103/PhysRevA.101.012325. URL: https://link.aps.org/doi/10.1103/PhysRevA.101.012325.

[19] S. Langenfeld et al. “Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution”. In: *Phys. Rev. Lett.* 126 (23 June 2021), p. 230506. DOI: 10.1103/PhysRevLett.126.230506. URL: https://link.aps.org/doi/10.1103/PhysRevLett.126.230506.

[20] Charles H Bennett, Gilles Brassard, and N David Mermin. “Quantum cryptography without Bell’s theorem”. In: *Physical review letters* 68.5 (1992), p. 557. DOI: https://doi.org/10.1103/PhysRevLett.68.557.

[21] L.-M. Duan et al. “Long-distance quantum communication with atomic ensembles and linear optics”. In: *Nature* 414.6862 (Nov. 2001), pp. 413–418. ISSN: 1476-4687. DOI: 10.1038/35106500. URL: https://doi.org/10.1038/35106500.

[22] M. U. Staudt et al. “Interference of Multimode Photon Echoes Generated in Spatially Separated Solid-State Atomic Ensembles”. In: *Phys. Rev. Lett.* 99 (17 Oct. 2007), p. 173602. DOI: 10.1103/PhysRevLett.99.173602. URL: https://link.aps.org/doi/10.1103/PhysRevLett.99.173602.

[23] M Gündoğan et al. “Coherent storage of temporally multimode light using a spin-wave atomic frequency comb memory”. In: *New Journal of Physics* 15.4 (Apr. 2013), p. 045012. DOI: 10.1088/1367-2630/15/4/045012. URL: https://doi.org/10.1088/1367-2630/15/4/045012.

[24] Yu Ma et al. “One-hour coherent optical storage in an atomic frequency comb memory”. In: *Nat. Commun.* 12.1 (Apr. 2021), p. 2381. ISSN: 2041-1723. DOI: 10.1038/s41467-021-22706-y. URL: https://doi.org/10.1038/s41467-021-22706-y.

[25] Mikael Afzelius et al. “Multimode quantum memory based on atomic frequency combs”. In: *Phys. Rev. A* 79 (5 May 2009), p. 052329. DOI: 10.1103/PhysRevA.79.052329. URL: https://link.aps.org/doi/10.1103/PhysRevA.79.052329.

[26] Manjin Zhong et al. “Optically addressable nuclear spins in a solid with a six-hour coherence time”. In: *Nature* 517.7533 (2015), pp. 177–180. ISSN: 1476-4687. DOI: 10.1038/nature14025. URL: https://doi.org/10.1038/nature14025.

[27] Charles Ci-Wen Lim et al. “Security Analysis of Quantum Key Distribution with Small Block Length and Its Application to Quantum Space Communications”. In: *Phys. Rev. Lett.* 126 (10 Mar. 2021), p. 100501. DOI: 10.1103/PhysRevLett.126.100501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.126.100501.

Anonymous communication in quantum networks

Gláucia Murta[1 2 *]

[1] *Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria*

[2] *Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, D-40225 Düsseldorf, Germany*

Abstract. A fundamental cryptographic task is secure communication, in which two or more parties exchange confidential messages in the presence of an eavesdropper. In some scenarios, however, the identity of the communicating parties may also be sensitive information. In these situations, it is essential to ensure that the identities remain concealed throughout the protocol. In this talk, I will explore how quantum systems bring advantages to anonymous communication. I will then focus on the task of anonymously establishing a secret key among several users in a quantum network, introducing a security framework that encompasses both secrecy of the key and user anonymity. I will present efficient and noise-tolerant protocols that leverage the correlations of multipartite Greenberger–Horne–Zeilinger (GHZ) states, demonstrating their superiority over protocols based on bipartite entanglement. Finally, I will discuss a recent experiment showcasing that the advantages of multipartite entanglement can already be witnessed with current technology.

[*] glaucia.murta@tuwien.ac.at

Toward large-scale quantum computing –from the viewpoint of computer system architecture–

Teruo Tanimoto[1] *

[1] *Kyushu University*

Abstract. Quantum computers are recognized as an important computing platform in the post-Moore era. We need to scale quantum computers much more to achieve a quantum advantage with a practical problem. The talk will cover our recent activity on noisy-intermediate scale (NISQ) computers and fault-tolerant quantum computers (FTQCs) using superconducting qubits. Superconducting qubits require a cryogenic environment because they are sensitive to thermal noise. We have proposed system-level thermal modeling and power-efficient system architectures to scale cryogenic quantum computers. The bottleneck to scalability is the heat inflow through the wires transmitting and receiving microwaves in/out of the cryostat and the heat generation from the components installed in the cryostat.

For NISQ computers, target algorithm-specific system architecture has been explored. NISQ algorithms, such as the quantum approximate optimization algorithm and the variational quantum eigensolver, collect numerous samples by executing the same quantum circuit repeatedly. Based on the analysis of communication in/out of the cryostat, we have proposed a simple cryogenic digital information processing circuit in the 4 K stage.

FTQCs require various classical digital processing components for quantum error-corrected computation. The primary challenge was to establish a scalability analysis tool (XQsim) to identify the scalability bottleneck of FTQCs using superconducting qubits. By constructing a reference FTQC microarchitecture, we identified the major scalability factors as the power dissipation in the 4 K stage, the latency of quantum error decoding, and the required bandwidth in/out of the cryostat. On the basis of the scalability analysis, design improvements for further scalability from the viewpoint of computer architecture have been proposed.

[Our research activities are partly supported by JST Moonshot R&D Grant Number JPMJMS2067, JSPS KAKENHI Grant Numbers JP22K17868]

Keywords: Computer system architecture, scalability analysis, cryogenic quantum computers

*teruo.tanimoto@gmail.com

Extended abstract:
Noise-induced shallow circuits and absence of barren plateaus

Antonio Anna Mele[1] [*] Armando Angrisani[2] [4] [†] Soumik Ghosh[5] [‡] Sumeet Khatri[1] [§]
Jens Eisert[1] [6] [¶] Daniel Stilck França[7] [‖] Yihui Quek[8] [**]

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[2] *LIP6, CNRS, Sorbonne Université, 75005 Paris, France*
[3] *Institute of Physics, Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland*
[4] *Institute of Physics, Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland*
[5] *Department of Computer Science, University of Chicago, Chicago, Illinois 60637, USA*
[6] *Fraunhofer Heinrich Hertz Institute, 10587 Berlin, Germany*
[7] *Univ Lyon, ENS Lyon, UCBL, CNRS, Inria, LIP, F-69342, Lyon Cedex 07, France*
[8] *Departments of Mathematics and Physics, Massachusetts Institute of Technology, 182 Memorial Drive, Cambridge, MA 02138, USA*

Abstract. We show that any noise 'truncates' most quantum circuits to effectively logarithmic depth, in the task of estimating Pauli expectation values. We then prove that non-unital noise induces lack of barren plateaus for local cost functions, but we also design a classical algorithm to estimate Pauli expectation values within inverse-polynomial additive error with high probability over the ensemble. Its runtime is polynomial for 1D and quasi-polynomial for higher dimensional architectures. Taken together, our results showcase that, unless we carefully engineer the circuits to take advantage of the noise, it is unlikely that noisy circuits are preferable over shallow ones.

Keywords: Noise, Classical simulation, Random quantum circuits, Barren plateaus

1 Introduction

Note: This submission is based on this work recently posted on ArXiv [1].

In the era of pre-fault-tolerant quantum processors, two popular candidate tasks to demonstrate quantum advantage are random circuit sampling and solving optimization problems via variational algorithms. It is crucial to understand whether quantum advantage in these settings, proven or conjectured to hold with ideal noiseless circuits, persists when the circuits running these computations are affected by realistic hardware noise.

Previous works paint a pessimistic picture: in random circuit sampling, noise makes it possible to simulate the systems efficiently classically [2]. Similarly, in variational quantum algorithms, noise quickly drives the system to computationally trivial states, causing a phenomenon known as "barren plateaus"—the cost function landscape becomes effectively flat, making optimization difficult [3, 4]. However, the overwhelming majority of these results require strong structural assumptions on the noise—that the noise is *local, unital, primitive*, and often, even more specifically, depolarizing noise. In this work, we significantly generalize these results, focusing on random quantum circuits with possibly *non-unital noise.* Up to our knowledge, we prove the strongest result to date about how much such noisy circuits contract two input states, with the implication that unless these circuits are carefully engineered to take advantage of noise [7], quantum advantage will likely not materialize in its presence.

Why non-unital noise? Non-unital noise is physically relevant: for a number of current physical platforms (e.g. superconducting qubits and optical networks), it is more natural and realistic to take the noise to be *non-unital* [5, 6]. Mathematically, non-unital noise is a generalization of unital noise, with qualitatively different results on computation. Strikingly, Ref. [7] has shown a threshold theorem to perform exponentially long quantum computations under non-unital noise, with specially constructed circuits. This can never be the case with depolarizing noise, which converges to the maximally-mixed state in logarithmic time. Additionally, Ref. [8] shows how existing easiness and hardness proofs of random circuit sampling break down under non-unital noise. The intuition is that while unital noise always increases the entropy of its input, non-unital noise may not do so. Non-unital noise is not "depolarizing noise, but worse" – it is mathematically compelling in its own right.

2 Our contributions.

We study the impact of possibly non-unital noise on algorithms estimating expectation values. We consider families of random quantum circuits with local gates picked from a 2-design and show three main results:

- **Effective depth:** We show that arbitrary deep random quantum circuits, under *any* uncorrected any (possibly non-unital) noise, effectively get "truncated", in the following sense: the influence

[*] a.mele@fu-berlin.de

[†] armando.angrisani@epfl.ch

[‡] soumikghosh@uchicago.edu

[§] sumeet.khatri@fu-berlin.de

[¶] jense@zedat.fu-berlin.de

[‖] daniel.stilck$_{franca}@ens - lyon.fr$

[**] yquek@mit.edu

of gates on local expectation values decreases exponentially in their distance from the last layer, i.e., only the last $\log(n)$ layers contribute significantly to any expectation value.

Formally, we show the following:

Theorem 1 (Effective depth) *Let P be a Pauli, ρ_{in} and σ_{in} be any quantum states and Φ be a noisy random quantum circuit. Then*

$$\mathbb{E}_\Phi \left[\mathrm{Tr}(P\Phi(\rho_{in} - \sigma_{in}))^2\right] \leq \mathcal{O}(C^{depth(\Phi)}) \qquad (1)$$

where the expectation is taken over the choice of random gates and $C < 1$ is a parameter related to the noise (which we assume non-reversible, i.e., not associated to a unitary channel).

- **Lack of barren plateaus:** In the variational quantum algorithms (VQAs) setting, non-unital noise induces absence of barren plateaus for cost functions made out of local observables—the cost landscape is never flat, and the gradient of the cost function never vanishes, at any depth. This can be intuitively understood as originating from the shallowness of the effective circuit under noise. This phenomenon, however, is not good news for VQAs, as the resultant shallow circuits also have more limited computational power. This contrasts with the finding [4] that depolarizing noise in fact causes barren plateaus at $\log(n)$ depth.
- **Classical simulation:** We also give an algorithm to classically estimate Pauli expectation values up to ε additive inverse-polynomial precision and high success probability (over the ensemble), with runtime of $\sim \exp\left(\log^D\left(\varepsilon^{-2}\right)\right)$, where D is the spatial dimension of the system. The algorithm's runtime is independent of circuit depth. So, for constant precision, our algorithm is efficient for *any* spatial dimension; for inverse-polynomial precision, our algorithm is efficient for 1D architectures. Our algorithm is faster than the classical simulation algorithm of Ref. [9], which (for constant precision and in 2D) has a depth-dependent runtime that scales as $n2^{\mathcal{O}(L^2)}$ where L is depth.

Taken together, our results substantially advance our understanding of the effect of non-unital noise on near-term quantum computation. They showcase that even though we provably always avoid barren plateaus, unless we carefully engineer special circuits to take advantage of the noise, it is unlikely that noisy quantum computers provide any advantage in quantum processing tasks that output expectation values.

Preliminaries. We consider n-qubit, depth-L quantum circuits Φ consisting of layers of two-qubit gates interleaved by local (single-qubit) noise. No assumptions about geometrical locality are needed, except where explicitly mentioned. Let $\Phi^*_{[L,k]}$ denote the circuit in the Heisenberg picture from layer L to k, where $k \leq L$. Let $\Phi_{[1,k]}$ denote the circuit in the Schrödinger picture, i.e., the first $k-1$ layers.

Effective shallow circuits. To explain the significance of Theorem 1, let us restate it, via one application of Jensen's inequality, as

$$\mathbb{E}_\Phi[|\,\mathrm{Tr}(P\Phi(\rho)) - \mathrm{Tr}(P\Phi(\sigma))|] \leq \mathcal{O}(C^{\mathrm{depth}(\Phi)}), \qquad (2)$$

Proof. [Proof Sketch of Theorem 1] Observing that the quantity we need to bound is a second-moment quantity in the distribution over gates reduces the task to proving contraction over ensembles of random Clifford circuits. We also choose to work with a sparse parametrization of non-unital noise (the 'normal form' [10]). The proof is conducted by working in the "Heisenberg picture", peeling off a layer of noise and a layer of 2-qubit gates, and then applying the adjoint of these layers to the Pauli operator in the beginning. This incurs a multiplicative factor to the same quantity but with one less circuit layer. The process is then iterated for all remaining circuit layers, resulting in the claimed exponential-in-depth decrease. The above-described technique strengthens previous second moment bounds on non-unital noisy circuits found in Ref. [8]. □

To parse the previous result, take a noisy circuit of interest $\mathcal{C}$ and let $\Phi = \mathcal{C}_{[L-k,L]}$, $\rho = \mathcal{C}_{[1,L-k]}(\rho_0)$ and $\sigma = \rho_0 = |0^n\rangle\langle 0^n|$. From this, the connection to shallow circuits becomes clear, since we have

$$\mathbb{E}_\Phi[|\,\mathrm{Tr}(P\mathcal{C}(\rho_0)) - \mathrm{Tr}(P\mathcal{C}_{[1,L-k]}(\rho_0))|] \leq \mathcal{O}(C^{\mathrm{depth}(\Phi)})$$

Why taking averages over circuits is crucial. Eq.(1) talks about how much a noisy circuit *contracts* the distance between two different input states *on average over circuits* of a fixed architecture. This is known as a 'contraction result' in the literature and was previously proven for depolarizing and more general types of unital noise. The crux is that any quantum circuit affected by depolarizing noise *converges* to the maximally-mixed state exponentially fast in depth [12, 11] as

$$\left\|\Phi(\rho_{\mathrm{in}}) - \frac{\mathbb{I}}{2^n}\right\|_1 \leq \mathcal{O}(\sqrt{n}c^{\mathrm{depth}(\Phi)}), \qquad (3)$$

for some constant $c < 1$ depending on the noise strength. What is notable about this expression is that a *single* state – the maximally-mixed state – is the 'limit' to which all circuits affected by depolarizing noise converge, independent of what gates are actually in the circuit, or its input state. Because of this, no averages over circuits are necessary in Eq.3.

In contrast, for circuits affected by non-unital noise, the convergence point is some point in the Bloch sphere that is not necessarily the maximally mixed state—in fact, for many cases, a unique, circuit-independent convergence point need not exist! There is yet another subtlety to overcome for proving contraction: in [7] the authors show that if non-unital noise is small enough, it is possible to implement exponentially deep quantum circuits in our model. Thus, our families of random circuits *potentially contain circuits for which no contraction is observed for subexponential depths.* Thus, a worst-case bound is not possible in the depth regimes we study; only *on average over circuits* do we escape these 'pathologies'.

Proposition 2 (1-norm bound) *For any quantum states ρ, σ:*

$$\mathbb{E}_\Phi[\|\Phi(\rho)-\Phi(\sigma)\|_1] \leq 2^{n+1}c^{\frac{L-1}{2}}. \quad (4)$$

Notice that at linear depth $L=\Omega(n)$, the right-hand side of the above expression becomes $\exp(-\Theta(n))$. This is a *stronger* result than (1), for linear depth and beyond, as it talks about indistinguishability of the states themselves, and not just Pauli expectation values. Additionally, for high noise rates, we show that the statement in (4) can be strengthened to worst case circuits, even for non-unital noise. Specifically, we obtain

$$\|\Phi(\rho)-\Phi(\sigma)\|_1 \leq \mathcal{O}(nb^L), \quad (5)$$

where the parameter b is strictly smaller than one only if the noise rate exceeds a certain threshold.

Lack of barren plateaus. The *barren plateaus phenomenon* [3, 4] stands as a central obstacle for *variational quantum algorithms.* These algorithms involve encoding the solution to a problem in the minimization of a cost function, typically defined in terms of the expectation value of an observable, with the free parameters for optimization being the gate parameters. Barren plateaus, are characterized by the phenomenon where the gradient norm of the cost function exhibits, on average, an exponential decay $O(\exp(-n))$ in the number of qubits n. We prove that cost landscapes, with non-unital noise, are not flat, and as a result, we do not get barren plateaus. In more mathematical terms, we show that:

Theorem 3 (Lack of barren plateaus) *Let H be any local Hamiltonian and $C(\theta)=\mathrm{Tr}(H\Phi(\rho))$ the cost function. When the noise is non-unital, then at any depth, we have*

$$\mathrm{Var}[\mathrm{Tr}(H\Phi(\rho))]=\Omega(1), \quad \mathrm{Var}[\|\nabla C\|_2^2]=\Omega(1). \quad (6)$$

The main idea behind both proofs is similar to the proof of (1). We start from the end of the circuit, use the Heisenberg picture, and properties of the random circuit to simplify the expression. We also do a much finer grained analysis of partial derivatives to show that only the last few layers of the circuit have non-trivial partial derivatives. That is,

Proposition 4 (Trainability) *Let μ be any parameter (in the light cone) of the k-th layer of a L-depth circuit, evaluating a cost function $C=\mathrm{Tr}(H\Phi(\rho))$, for a local Hamiltonian H and an ensemble of non-unital noisy random circuits Φ. Then, we have*

$$\mathrm{Var}[\partial_\mu C]=\exp(-\Theta(L-k)). \quad (7)$$

Qualitatively, one way to think about the lack of barren plateaus for our setup is to argue that the circuits are "effectively" shallow, and shallow random circuits do not exhibit barren plateaus for local cost functions [13]. Along with a rigorous mathematical proof, we provide numerical simulations that strongly bear out this claim in our technical manuscript. The technical tools developed in this work also allow, in the unital-noise scenario, to improve upon the Barren Plateaus upper bounds presented in Ref. [4], as discussed in our main draft.

As an auxiliary result, we also give strong evidence that certain types of quantum kernels – a popular 'quantum' method for machine learning – also offer no advantage in optimization tasks, for similar mathematical reasons.

Classical simulation of noisy circuits at any depth. The effective shallowness of noisy circuits implies that they can be classically simulated. More formally, we prove that:

Proposition 5 (Classical simulation) *Let $\varepsilon,\delta>0$. Let P be a Pauli. Let $\rho_0 := |0^n\rangle\langle 0^n|$. Let Φ be a noisy geometrically local with spatial dimension D quantum circuit of depth L sampled according to the described circuit distribution. There is a classical algorithm that outputs a value $\hat{C}$ that satisfies:*

$$|\hat{C}-\mathrm{Tr}(P\Phi(\rho_0))| \leq \varepsilon \quad (8)$$

with at least $1-\delta$ probability of success and runtime $\mathcal{O}(\exp(\log^D(\varepsilon^{-2}\delta^{-1})))$. The runtime in the precision is polynomial for 1-D local architectures, and quasipolynomial for 2-D local architectures.

To prove this theorem, we work in the Heisenberg picture and 'propagate' the observable P only a few layers backwards—the number of layers we propagate it through is inversely proportional to the precision we want. Furthermore, we provide an alternative *early-break condition* that, if met at some step t, guarantees an ε approximation.

Discussion. In this work, we have shown how non-unital noise, when starting with a random ansatz, "truncates" the circuit. This truncated circuit escapes barren plateaus but the cost functional values, obtained from such a circuit, can be simulated classically. Thus, quantum advantage with uncorrected non–unital noise in quantum machine learning is implausible and elusive. Although, in the same vein as Ref. [8], the complexity of sampling from such circuits still remains open, we expect the effective depth picture and our techniques to help in resolving this question.

References

[1] A.A Mele, A. Angrisani, S. Ghosh, S. Khatri, J. Eisert, D.S. França, Y. Quek. Noise-induced shallow circuits and absence of barren plateaus. In ArXiv, 2024.

[2] D. Aharonov, X. Gao, Z. Landau, Y. Liu, U. Vazirani A Polynomial-Time Classical Algorithm for Noisy Random Circuit Sampling. In STOC '23, 2023.

[3] J.R. McClean, S. Boixo, V.N. Smelyanskiy, R. Babbush, H. Neven Barren plateaus in quantum neural network training landscapes In Nature Comm., 2018.

[4] S. Wang, E. Fontana, M. Cerezo, K. Sharma, A. Sone, L. Cincio, P.J. Coles Noise-induced barren plateaus in variational quantum algorithms In Nature Comm., 2021.

[5] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. W. Chow, J. M. Gambetta Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets In Nature, 2017.

[6] J. M. Pino, J. M. Dreiling, C. Figgatt, J. P. Gaebler, S. A. Moses, M. S. Allman, C. H. Baldwin, M. Foss-Feig, D. Hayes, K. Mayer, C. Ryan-Anderson, B. Neyenhuis Demonstration of the trapped-ion quantum CCD computer architecture In Nature, 2021.

[7] M. Ben-Or, D. Gottesman, A. Hassidim Quantum Refrigerator arXiv preprint arXiv:1301.1995, 2013.

[8] B. Fefferman, S. Ghosh, M. Gullans, K. Kuroiwa, K. Sharma Effect of non-unital noise on random circuit sampling arXiv preprint arXiv:2306.16659, 2023.

[9] S. Bravyi, D. Gosset, R. König, M. Tomamichel Quantum advantage with noisy shallow circuits In Nature Phys., 2020.

[10] C. King, M.B. Ruskai Minimal entropy of states emerging from noisy quantum channels In IEEE Trans. Inf. Th., 2001.

[11] A. Müller-Hermes, D. Stilck França, M.M. Wolf Relative entropy convergence for depolarizing channels In J. Math. Phys., 2016.

[12] D. Aharonov, M. Ben-Or Polynomial simulations of decohered quantum computers In Proceedings of 37th Conference on Foundations of Computer Science, 1996, pp. 46-55.

[13] J. Napp Quantifying the barren plateau phenomenon for a model of unstructured variational ansätze arXiv preprint arXiv:2203.06174, 2022.

Simulating the quantum switch using causally ordered circuits requires at least an exponential overhead in query complexity

Hlér Kristjánsson[1 2 3] * Tatsuki Odake[3] * Satoshi Yoshida[3] * Philip Taranto[3]
Jessica Bavaresco[4] Marco Túlio Quintino[5] Mio Murao[3 6]

[1] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada*
[2] *Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada*
[3] *Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo, Japan*
[4] *Département de Physique Appliquée, Université de Genève, Genéve, Switzerland*
[5] *Laboratoire d'Informatique de Paris 6 (LIP6), CNRS, Sorbonne Université, 4 Place Jussieu, Paris, France*
[6] *Trans-scale Quantum Science Institute, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo, Japan*

Abstract. Quantum theory is consistent with a model of computation that allows black-box operations to be applied in an indefinite causal order, going beyond the standard circuit model of computation. The simplest and most widely studied example of indefinite causal order is the quantum switch, which takes as input one call to each of two n-qubit black-box quantum channels, and has been shown to provide information-processing advantages in a wide variety of tasks. Yet, no exponential separation in query complexity has been shown between processes with an indefinite causal order and standard quantum circuits. In this work, we show that no quantum circuit with fixed causal order (or classical control of the causal order) using multiple calls to one of the two n-qubit channels can reproduce the output of the quantum switch if the number of calls is less than 2^n. This shows that quantum processes with indefinite causal order can exhibit an exponential enhancement in query complexity, as a function of the number of qubits, over all quantum circuits with fixed, or classically controlled, causal order.

Keywords: Quantum supermaps, Indefinite causal order, Higher-order quantum computation

1 Introduction

The possibility of performing classical or quantum operations in an indefinite causal order has attracted significant attention in the last two decades [1–10]. From a foundational perspective, this possibility has far-reaching consequences for our understanding of causality, with important implications for the quantum nature of spacetime [1, 2, 11, 12]. From an information-theoretic standpoint, this possibility is equally significant, challenging the standard conception of computation in which gates are performed in a well-defined causal order [3, 4, 6, 7, 13]. The simplest example of a quantum process with indefinite causal order is the quantum switch [4]: a transformation that maps two quantum channels $\mathcal{A}$ and $\mathcal{B}$ to a controlled operation between their two possible orderings $\mathcal{B} \circ \mathcal{A}$ and $\mathcal{A} \circ \mathcal{B}$ [4]. So far, the power of the quantum switch has been demonstrated in various tasks such as reducing the number of queries needed for quantum channel discrimination problems [14] and computational promise problems [15–18], reducing the number of communication rounds required for distributed computation tasks [19], increasing the winning probability in multiparty games [5–7], increasing the capacity of noisy communication channels [20–31], and providing enhancements in quantum metrology [32–35] and quantum thermodynamics [36, 37].

Yet, in the context of quantum computation, no exponential separation in query complexity has been shown between processes with indefinite causal order and those in which operations are performed in a definite order. Indeed, for the case of unitary channels it is known that the quantum switch can be simulated by a quantum circuit querying the unitary channels in a fixed order, with just one extra query to one of the channels [4]. This result holds for any size of the target system. A crucial open question is whether the same holds for general quantum channels.

In this work, we answer this question in the negative. We prove a no-go theorem which states that the quantum switch of two n-qubit channels cannot be simulated using a quantum circuit with fixed causal order, with a single call to one of the channels and M calls to the other channel, if $M \leq \max(2, 2^n - 1)$. Additionally, we conjecture that the same bound holds when M calls to both channels are allowed. Our theorem demonstrates the first known exponential separation in query complexity between quantum processes with indefinite causal order and standard quantum circuits, as a function of the number of qubits.

If our conjecture is proven to be correct, this would demonstrate that not all processes with indefinite causal order can be efficiently simulated using standard quantum circuits. The separation we prove is formulated with respect to a computational task where the inputs and outputs of the computation are both given by black-box quantum channels [4, 22, 38, 39]. This is in contrast to previous works on the query complexity of the quantum switch, where the output of the computation is a bit representing the evaluation of a classical function, in which case no exponential separation has been found [14–18].

In the remainder of this work, we will formalise the notion of indefinite causal order and the problem of simulat-

*These three authors contributed equally.

ing the quantum switch, then present our main theorem and sketch of the proof for the case of $M = 2$.

2 Framework

Processes with indefinite causal order arise as a special case of higher-order quantum transformations [4, 22, 38, 40] (also known as quantum supermaps [39] or process matrices [5]). These are defined according to the following hierarchy. We denote as $\mathbb{L}(A)$ the set of all bounded linear operators on a Hilbert space $\mathcal{H}^A$ corresponding to a physical system A. A *quantum state* is any linear operator $\rho \in \mathbb{L}(A)$ that is both positive semidefinite $\rho \geq 0$ and of unit trace $\operatorname{Tr} \rho = 1$. A *quantum channel* is any linear map $\mathcal{C} : [\mathbb{L}(I) \to \mathbb{L}(O)]$ from quantum states to quantum states that is both completely positive (**CP**) and trace preserving (**TP**). A *quantum supermap* $\mathcal{S}$ is any multilinear map $\mathcal{S} : \bigotimes_{i=1}^{M} [\mathbb{L}(I_i) \to \mathbb{L}(O_i)] \to [\mathbb{L}(P) \to \mathbb{L}(F)]$ from the space of M-tuples of quantum channels to the space of quantum channels that is both completely CP-preserving and TP-preserving [41, 42].

Throughout, we will find it useful to use the Choi representation [43, 44] of linear maps, which encompasses both channels and supermaps. For any linear operator $V : \mathcal{H}^A \to \mathcal{H}^B$, its Choi vector is defined as

$$|V\rangle\!\rangle := \sum_i |i\rangle^A \otimes V |i\rangle^A \in \mathcal{H}^A \otimes \mathcal{H}^B , \tag{1}$$

and for any linear map $\mathcal{Q} : [\mathbb{L}(A) \to \mathbb{L}(B)]$ its Choi matrix is defined by

$$Q := \sum_{ij} |i\rangle\!\langle j|^A \otimes \mathcal{Q}(|i\rangle\!\langle j|^A) \in \mathbb{L}(A \otimes B) , \tag{2}$$

where $\{|i\rangle\}_i$ is the computational basis.

The CPTP conditions imply that any quantum channel $\mathcal{C} : [\mathbb{L}(I) \to \mathbb{L}(O)]$ has a positive semidefinite Choi matrix $C \in \mathbb{L}(I \otimes O)$ normalised such that $\operatorname{Tr}_O C = \mathbb{1}^I$, where $\mathbb{1}^I$ is the identity matrix on $\mathcal{H}^I$. Similarly, any quantum supermap $\mathcal{S} : \bigotimes_{i=1}^{M} [\mathbb{L}(I_i) \to \mathbb{L}(O_i)] \to [\mathbb{L}(P) \to \mathbb{L}(F)]$ can be written in the Choi representation as a positive semidefinite matrix $W \in \mathbb{L}[P \otimes \bigotimes_{i=1}^{M} (I_i \otimes O_i) \otimes F]$, called the *process matrix*, satisfying the condition of being in a specific subspace corresponding to the TP preserving conditions, and normalised such that $\operatorname{Tr} W = d^P \Pi_{i=1}^{M} d^{I_i}$, where $d^A := \dim(\mathcal{H}^A)$ [45]. The composition of quantum states, quantum channels, and quantum supermaps can be represented by the *link product* $*$ on their Choi matrices [46]. In particular, the action of a quantum supermap on a set of quantum channels is represented as follows [46]: $\mathcal{S}(\mathcal{C}_1, \ldots, \mathcal{C}_M) \cong W * (C_1 \otimes \cdots \otimes C_M)$, where the link product on any two matrices $Q \in \mathbb{L}(A \otimes B), R \in \mathbb{L}(B \otimes C)$ is defined as $Q * R := \operatorname{Tr}_B[(Q^{AB} \otimes \mathbb{1}^C)^{\mathrm{T}_B} (\mathbb{1}^A \otimes R^{BC})]$, with $\mathrm{T_B}$ being the partial transpose with respect to system B.

Ordinary quantum circuits correspond to the special class of quantum supermaps known as *quantum circuits with fixed causal order* (QC-FOs) [10] or *quantum combs* [38]. An M-slot quantum circuit with fixed causal order is a quantum supermap which can be decomposed as a quantum circuit with $M + 1$ fixed quantum channels $\mathcal{V}_0 \in [\mathbb{L}(P) \to \mathbb{L}(I_1 \otimes E_1)], \mathcal{V}_1 \in [\mathbb{L}(O_1 \otimes E_1) \to \mathbb{L}(I_2 \otimes E_2)], \ldots, \mathcal{V}_M \in [\mathbb{L}(O_M \otimes E_M) \to \mathbb{L}(F)]$, connected sequentially with auxiliary systems $\{E_i\}_{i=1}^{M}$. The action of such a supermap on M input quantum channels $[\mathbb{L}(I_i) \to \mathbb{L}(O_i)]$ 'inserted' into the slots between each of the $\mathcal{V}_i$ is given by $W * (C_1 \otimes \cdots \otimes C_M) = V_M * C_M * \cdots * V_1 * C_1 * V_0$.

However, QC-FOs are not the most general quantum supermaps compatible with an underlying definite causal structure. Convex combinations of QC-FOs and supermaps where the order of operations is determined dynamically are also both possible. A more general class which includes such possibilities is *quantum circuits with classical control of causal order* (QC-CCs) [10, 47]. Quantum supermaps which are not compatible with an underlying definite causal structure are called *causally non-separable processes* [5, 45, 48] and are said to have indefinite causal order. Although it is currently an open question whether there exist processes compatible with a definite causal structure but are not QC-CCs [10], no such processes have been found to date, and therefore, any computational advantage of processes with indefinite causal order is most reasonably determined by comparing with QC-CCs.

3 Quantum switch and its simulations

The simplest and most widely studied example of a process with indefinite causal order is the quantum switch [4], which combines two quantum channels $\mathcal{A} \in [\mathbb{L}(I) \to \mathbb{L}(O)]$ and $\mathcal{B} \in [\mathbb{L}(I') \to \mathbb{L}(O')]$ in their two possible sequential orderings, depending on the state of a quantum control qubit P_C. The process matrix of the n-qubit quantum switch $\mathcal{S}_{\texttt{SWITCH}} : [[\mathbb{L}(I) \to \mathbb{L}(O)] \otimes [\mathbb{L}(I') \to \mathbb{L}(O')]] \to [\mathbb{L}(P_C \otimes P_T) \to \mathbb{L}(F_C \otimes F_T)]$, where I, O, I', O', P_T, F_T, correspond to n-qubit Hilbert spaces and P_C, F_C correspond to qubit Hilbert spaces, is given by $S_{\texttt{SWITCH}} = |S_{\texttt{SWITCH}}\rangle\!\rangle\langle\!\langle S_{\texttt{SWITCH}}|$, with

$$\begin{aligned} |S_{\texttt{SWITCH}}\rangle\!\rangle^{PFIOI'O'} &:= |0\rangle^{P_C} |0\rangle^{F_C} |\mathbb{1}\rangle\!\rangle^{P_T I} |\mathbb{1}\rangle\!\rangle^{OI'} |\mathbb{1}\rangle\!\rangle^{O'F_T} \\ &+ |1\rangle^{P_C} |1\rangle^{F_C} |\mathbb{1}\rangle\!\rangle^{P_T I'} |\mathbb{1}\rangle\!\rangle^{O'I} |\mathbb{1}\rangle\!\rangle^{OF_T} . \end{aligned} \tag{3}$$

For the case where the input channels are unitary, i.e. $\mathcal{U}(\cdot) = U(\cdot)U^\dagger$ and $\mathcal{V}(\cdot) = V(\cdot)V^\dagger$, the action of the quantum switch takes the particularly simple form:

$$\mathcal{S}_{\texttt{SWITCH}} : (U, V) \mapsto VU \otimes |0\rangle\!\langle 0| + UV \otimes |1\rangle\!\langle 1| . \tag{4}$$

To understand the computational power of the quantum switch, it is essential to understand whether its action can be efficiently simulated with causally ordered quantum supermaps by using more queries to one or both of the channels. It is known that the action of the quantum switch on unitary channels can be simulated deterministically and exactly with a quantum circuit with fixed causal order C_{sim}, using just one extra call to either of the two channels [4]:

$$\mathcal{C}_{\text{sim}}(\mathcal{U}, \mathcal{V}, \mathcal{U}) = \mathcal{S}_{\texttt{SWITCH}}(\mathcal{U}, \mathcal{V}) \quad \forall \mathcal{U}, \mathcal{V} . \tag{5}$$

The circuit for C_{sim} is depicted in Figure 1.

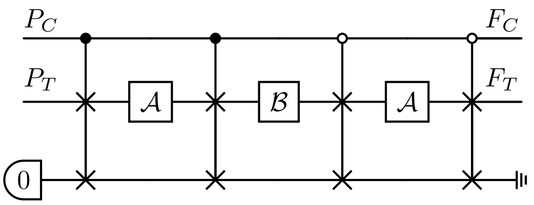


Figure 1: A quantum circuit with fixed causal order taking two calls to a quantum channel $\mathcal{A}$ and a single call to a quantum channel $\mathcal{B}$. When $\mathcal{A}$ is a unitary channel, this circuit simulates the action of the quantum switch of $\mathcal{A}$ and $\mathcal{B}$.

4 Main results

Interestingly, we observe that the same quantum circuit C_{sim} can simulate the action of the quantum switch on one unitary channel and one general quantum channel, with one extra call to the unitary channel. That is, for any unitary channel $\mathcal{U}$, and any quantum channel $\mathcal{B}$,

$$\mathcal{C}_{\text{sim}}(\mathcal{U},\mathcal{B},\mathcal{U}) = \mathcal{S}_{\texttt{SWITCH}}(\mathcal{U},\mathcal{B})\,. \tag{6}$$

However, when C_{sim} is applied to two general quantum channels $\mathcal{A},\mathcal{B}$, with 2 copies of $\mathcal{A}$, it does not in general reproduce the action of the quantum switch. This can be explained by the fact that the quantum switch correlates the randomness associated with a non-unitary channel between its $|0\rangle$ and $|1\rangle$ branches.

As such, one might wonder whether there exists some other causally ordered supermap, either a QC-FO or QC-CC, which can reproduce the action of the quantum switch, given $M \geq 2$ copies of one of the two channels. Here, we answer this in the negative for $M \leq \max(2, 2^n - 1)$:

Theorem 1. *There is no $(M+1)$-slot supermap $\mathcal{C} : \bigotimes_{i=1}^{M}[\mathbb{L}(I_i) \to \mathbb{L}(O_i)] \otimes [\mathbb{L}(I'_1) \to \mathbb{L}(O'_1)] \to [\mathbb{L}(P_C \otimes P_T) \to \mathbb{L}(F_C \otimes F_T)]$, where $\{I_i\}_i, \{O_i\}_i, I'_1, O'_j$ correspond to n-qubit Hilbert spaces, with fixed causal order or classical control of the causal order satisfying*

$$\mathcal{C}(\underbrace{\mathcal{A},\dots,\mathcal{A}}_{M},\mathcal{B}) = \mathcal{S}_{\texttt{SWITCH}}(\mathcal{A},\mathcal{B}) \tag{7}$$

for all quantum channels $\mathcal{A}$ and $\mathcal{B}$, if $M \leq \max(2, 2^n-1)$.

The full proof is given in the Technical Manuscript [47]. In the following, we give a sketch of the proof for the case of $M = 2$. We begin by assuming that a 3-slot QC-CC quantum supermap $\mathcal{C}$ simulates the quantum switch for all unitary channels and all convex combinations of unitary channels, i.e.,

$$\mathcal{C}\left(\frac{\mathcal{U}_1+\mathcal{U}_2}{2},\frac{\mathcal{U}_1+\mathcal{U}_2}{2},\mathcal{V}\right) = \mathcal{S}_{\texttt{SWITCH}}\left(\frac{\mathcal{U}_1+\mathcal{U}_2}{2},\mathcal{V}\right), \tag{8}$$

$$\forall l \in \{1,2\}: \quad \mathcal{C}(\mathcal{U}_l,\mathcal{U}_l,\mathcal{V}) = \mathcal{S}_{\texttt{SWITCH}}(\mathcal{U}_l,\mathcal{V})\,, \tag{9}$$

for all unitary operations $\mathcal{U}_1,\mathcal{U}_2,\mathcal{V}$. By linearity of supermaps, we obtain

$$\mathcal{C}(\mathcal{U}_1,\mathcal{U}_2,\mathcal{V}) + \mathcal{C}(\mathcal{U}_2,\mathcal{U}_1,\mathcal{V}) = \mathcal{S}_{\texttt{SWITCH}}(\mathcal{U}_1+\mathcal{U}_2,\mathcal{V}). \tag{10}$$

Since $\mathcal{C}(\mathcal{U}_2,\mathcal{U}_1,\mathcal{V})$ is a CP map, $\mathcal{S}_{\texttt{SWITCH}}(\mathcal{U}_1+\mathcal{U}_2,\mathcal{V}) - \mathcal{C}(\mathcal{U}_1,\mathcal{U}_2,\mathcal{V})$ is CP. In terms of the Choi matrix, this relation can be written as

$$\begin{aligned}&C \star (|U_1\rangle\rangle\langle\langle U_1| \otimes |U_2\rangle\rangle\langle\langle U_2| \otimes |V\rangle\rangle\langle\langle V|)\\ &\leq |S_{\texttt{SWITCH}}\rangle\rangle\langle\langle S_{\texttt{SWITCH}}| * [(|U_1\rangle\rangle\langle\langle U_1| + |U_2\rangle\rangle\langle\langle U_2|) \otimes |V\rangle\rangle\langle\langle V|].\end{aligned} \tag{11}$$

Since $\mathcal{C}$ can be implemented by a QC-CC, the Choi matrix C can be decomposed as $C = \sum_{(i,j,k)\in\text{Perm}(1,2,3)} C_{ijk}$ such that C_{ijk} satisfies $C_{ijk} \geq 0$ and several affine conditions (which we refer to the QC-CC conditions) [10, 47]. Using an eigendecomposition of C_{ijk} given by $C_{ijk} = \sum_a |C^{(a)}_{ijk}\rangle\rangle\langle\langle C^{(a)}_{ijk}|$, we obtain

$$\begin{aligned}&|C^{(a)}_{ijk}\rangle\rangle\langle\langle C^{(a)}_{ijk}| \star (|U_1\rangle\rangle\langle\langle U_1| \otimes |U_2\rangle\rangle\langle\langle U_2| \otimes |V\rangle\rangle\langle\langle V|)\\ &\leq |S_{\texttt{SWITCH}}\rangle\rangle\langle\langle S_{\texttt{SWITCH}}| * [(|U_1\rangle\rangle\langle\langle U_1| + |U_2\rangle\rangle\langle\langle U_2|) \otimes |V\rangle\rangle\langle\langle V|].\end{aligned} \tag{12}$$

Therefore, the left-hand side of Eq. (12) can be written as

$$\begin{aligned}&|C^{(a)}_{ijk}\rangle\rangle * (|U_1\rangle\rangle \otimes |U_2\rangle\rangle \otimes |V\rangle\rangle)\\ &= \sum_{l=1}^{2} p^{(a,l)}_{ijk}(U_1,U_2,V)|S_{\texttt{SWITCH}}\rangle\rangle * (|U_l\rangle\rangle \otimes |V\rangle\rangle),\end{aligned} \tag{13}$$

using $p^{(a,l)}_{ijk}(U_1,U_2,V) \in \mathbb{C}$. If $|C^{(a)}_{ijk}\rangle\rangle$ is given by

$$|C^{(a)}_{ijk}\rangle\rangle = \sum_{l=1}^{2} |S_{\texttt{SWITCH}}\rangle\rangle^{PI_lO_lI_3O_3F} \otimes |p^{(a,l)}_{ijk}\rangle\rangle \tag{14}$$

for $|p^{(a,1)}_{ijk}\rangle\rangle \in \mathbb{L}(I_2 \otimes O_2)$ and $|p^{(a,2)}_{ijk}\rangle\rangle \in \mathbb{L}(I_1 \otimes O_1)$, the corresponding quantum supermap $\mathcal{C}$ satisfies Eq. (13). We show that the converse holds, i.e., if Eq. (13) holds for all unitary operators U_1,U_2,V, $|C^{(a)}\rangle\rangle$ can be written as Eq. (14). The rough idea for this proof is based on differentiation with respect to a parametrisation of the input unitary operators, a technique introduced concurrently in Ref. [49] by some of the present authors. By considering the differentiation of $p^{(a,1)}_{ijk}(U_1,U_2,V)$ with respect to U_1 and U_2, we show that $p^{(a,1)}_{ijk}(U_1,U_2,V)$ can be given as a linear function of U_2 that does not depend on U_1 and V [47]. Then, $p^{(a,1)}_{ijk}(U_1,U_2,V)$ can be written as $p^{(a,1)}_{ijk}(U_1,U_2,V) = |p^{(a,1)}_{ijk}\rangle\rangle * |U_2\rangle\rangle$ using $|p^{(a,1)}\rangle\rangle \in \mathbb{L}(I_2 \otimes O_2)$. Similarly we show that $p^{(a,2)}_{ijk}(U_1,U_2,V)$ can be written as $p^{(a,2)}_{ijk}(U_1,U_2,V) = |p^{(a,2)}_{ijk}\rangle\rangle * |U_1\rangle\rangle$ using $|p^{(a,2)}\rangle\rangle \in \mathbb{L}(I_1 \otimes O_1)$. Then, we obtain

$$\begin{aligned}&|C^{(a)}_{ijk}\rangle\rangle * (|U_1\rangle\rangle \otimes |U_2\rangle\rangle \otimes |V\rangle\rangle)\\ &= \sum_{l=1}^{2} |S_{\texttt{SWITCH}}\rangle\rangle^{PI_lO_lI_3O_3F} \otimes |p^{(a,l)}_{ijk}\rangle\rangle * (|U_1\rangle\rangle \otimes |U_2\rangle\rangle \otimes |V\rangle\rangle).\end{aligned} \tag{15}$$

Since this holds for all unitary operators U_1,U_2,V, we obtain Eq. (14). Finally, we show that any quantum supermap given in the form of Eq. (14) does not satisfy the QC-CC conditions, thereby completing the proof [47].

References

[1] L. Hardy, arXiv:gr-qc/0509120 (2005).

[2] L. Hardy, in *Quantum reality, relativistic causality, and closing the epistemic circle* (Springer, 2009) pp. 379–401, arXiv:quant-ph/0701019 .

[3] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, arXiv:0912.0195v2 (2009).

[4] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Phys. Rev. A **88**, 022318 (2013), arXiv:0912.0195 .

[5] O. Oreshkov, F. Costa, and Č. Brukner, Nature communications **3**, 1092 (2012), arXiv:1105.4464 .

[6] Ä. Baumeler, A. Feix, and S. Wolf, Phys. Rev. A **90**, 042106 (2014), arXiv:1403.7333 .

[7] Ä. Baumeler and S. Wolf, New Journal of Physics **18**, 013036 (2016), arXiv:1507.01714 .

[8] M. Araújo, A. Feix, M. Navascués, and Č. Brukner, Quantum **1**, 10 (2017), arXiv:1611.08535 .

[9] K. Goswami, C. Giarmatzi, M. Kewming, F. Costa, C. Branciard, J. Romero, and A. White, Phys. Rev. Lett. **121**, 090503 (2018), arXiv:1803.04302 .

[10] J. Wechs, H. Dourdent, A. A. Abbott, and C. Branciard, PRX Quantum **2**, 030335 (2021), arXiv:2101.08796 .

[11] M. Zych, F. Costa, I. Pikovski, and Č. Brukner, Nature Communications **10**, 1 (2019), arXiv:1708.00248 .

[12] N. Paunković and M. Vojinović, Quantum **4**, 275 (2020), arXiv:1905.09682 .

[13] T. Colnaghi, G. M. D'Ariano, S. Facchini, and P. Perinotti, Physics Letters A **376**, 2940 (2012), arXiv:1109.5987 .

[14] G. Chiribella, Phys. Rev. A **86**, 040301 (2012), arXiv:1109.5154 .

[15] M. Araújo, F. Costa, and Č. Brukner, Phys. Rev. Lett. **113**, 250402 (2014), arXiv:1401.8127 .

[16] M. J. Renner and Č. Brukner, Phys. Rev. Lett. **128**, 230503 (2022), arXiv:2112.14541 .

[17] A. A. Abbott, M. Mhalla, and P. Pocreau, arXiv:2307.10285 (2023).

[18] M. M. Taddei, J. Cariñe, D. Martínez, T. García, N. Guerrero, A. A. Abbott, M. Araújo, C. Branciard, E. S. Gómez, S. P. Walborn, *et al.*, PRX Quantum **2**, 010320 (2021), arXiv:2002.07817 .

[19] P. A. Guérin, A. Feix, M. Araújo, and Č. Brukner, Phys. Rev. Lett. **117**, 100502 (2016), arXiv:1605.07372 .

[20] D. Ebler, S. Salek, and G. Chiribella, Phys. Rev. Lett. **120**, 120502 (2018), arXiv:1711.10165 .

[21] S. Salek, D. Ebler, and G. Chiribella, arXiv:1809.06655 (2018).

[22] G. Chiribella, M. Banik, S. S. Bhattacharya, T. Guha, M. Alimuddin, A. Roy, S. Saha, S. Agrawal, and G. Kar, New Journal of Physics **23**, 033039 (2021), arXiv:1810.10457 .

[23] N. Loizeau and A. Grinbaum, Phys. Rev. A **101**, 012340 (2020), arXiv:1906.08505 .

[24] L. M. Procopio, F. Delgado, M. Enríquez, N. Belabas, and J. A. Levenson, Entropy **21**, 1012 (2019), arXiv:1902.01807 .

[25] L. M. Procopio, F. Delgado, M. Enríquez, N. Belabas, and J. A. Levenson, Phys. Rev. A **101**, 012346 (2020), arXiv:1910.11137 .

[26] S. Sazim, M. Sedlak, K. Singh, and A. K. Pati, Phys. Rev. A **103**, 062610 (2021), arXiv:2004.14339 .

[27] G. Chiribella, M. Wilson, and H. Chau, Phys. Rev. Lett. **127**, 190502 (2021), arXiv:2005.00618 .

[28] K. Goswami, Y. Cao, G. A. Paz-Silva, J. Romero, and A. G. White, Phys. Rev. Research **2**, 033292 (2020), arXiv:1807.07383 .

[29] G. Rubino, L. A. Rozema, A. Feix, M. Araújo, J. M. Zeuner, L. M. Procopio, Č. Brukner, and P. Walther, Science Advances **3**, e1602589 (2017), arXiv:1608.01683 .

[30] G. Rubino, L. A. Rozema, D. Ebler, H. Kristjánsson, S. Salek, P. A. Guérin, A. A. Abbott, C. Branciard, Č. Brukner, G. Chiribella, *et al.*, Phys. Rev. Research **3**, 013093 (2021), arXiv:2007.05005 .

[31] Y. Guo, X.-M. Hu, Z.-B. Hou, H. Cao, J.-M. Cui, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, and G. Chiribella, Phys. Rev. Lett. **124**, 030502 (2020), arXiv:1811.07526 .

[32] X. Zhao, Y. Yang, and G. Chiribella, Phys. Rev. Lett. **124**, 190503 (2020), arXiv:1912.02449 .

[33] F. Chapeau-Blondeau, Phys. Rev. A **103**, 032615 (2021), arXiv:2104.06284 .

[34] Q. Liu, Z. Hu, H. Yuan, and Y. Yang, Phys. Rev. Lett. **130**, 070803 (2023), arXiv:2203.09758 .

[35] P. Yin, X. Zhao, Y. Yang, Y. Guo, W.-H. Zhang, G.-C. Li, Y.-J. Han, B.-H. Liu, J.-S. Xu, G. Chiribella, *et al.*, Nature Physics **19**, 1122 (2023), arXiv:2303.17223 .

[36] D. Felce and V. Vedral, Phys. Rev. Lett. **125**, 070603 (2020), arXiv:2003.00794 .

[37] X. Nie, X. Zhu, K. Huang, K. Tang, X. Long, Z. Lin, Y. Tian, C. Qiu, C. Xi, X. Yang, *et al.*, Phys. Rev. Lett. **129**, 100603 (2022), arXiv:2011.12580 .

[38] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008), arXiv:0712.1325 .

[39] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Europhysics Letters **83**, 30004 (2008), arXiv:0804.0180 .

[40] A. Bisio and P. Perinotti, Proceedings of the Royal Society A **475**, 20180706 (2019), arXiv:1806.09554 .

[41] G. Gour, IEEE Transactions on Information Theory **65**, 5880 (2019), arXiv:1808.02607 .

[42] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Phys. Rev. A **100**, 062339 (2019), arXiv:1909.01366 .

[43] M.-D. Choi, Linear algebra and its applications **10**, 285 (1975).

[44] A. Jamiołkowski, Reports on Mathematical Physics **3**, 275 (1972).

[45] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, and Č. Brukner, New Journal of Physics **17**, 102001 (2015), arXiv:1506.03776 .

[46] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **80**, 022339 (2009), arXiv:0904.4483 .

[47] See the Technical Manuscript for the details.

[48] J. Wechs, A. A. Abbott, and C. Branciard, New Journal of Physics **21**, 013027 (2019), arXiv:1807.10557 .

[49] T. Odake, S. Yoshida, and M. Murao, arXiv:2405.07625 (2024).

Complexity-theoretic foundations of BosonSampling with a linear number of modes

A. Bouland, D. J. Brod, I. Datta, B. Fefferman, D. Grier, F. Hernández, M. Oszmaniec

Abstract BosonSampling is the leading candidate for demonstrating quantum computational advantage in photonic systems. While we have recently seen many impressive experimental demonstrations, there is still a formidable distance between the complexity-theoretic hardness arguments and current experiments. One of the largest gaps involves the ratio of photons to modes–all current hardness evidence assumes a "high-mode" regime in which the number of linear optical modes scales at least quadratically in the number of photons. By contrast, current experiments operate in a "low-mode" regime with a linear number of modes. In this paper we bridge this gap, bringing the hardness evidence for the low-mode experiments to the same level as had been previously established for the high-mode regime. This involves proving a new worst-to-average-case reduction for computing the Permanent which is robust to both large numbers of row repetitions and also to distributions over matrices with correlated entries.

Introduction In the decade since it was proposed by Aaronson and Arkhipov [AA13], BosonSampling has become one of the most promising candidates for achieving quantum computational advantage the experimental demonstration of a quantum computation which exponentially surpasses classical computers. This requires a task which is both experimentally feasible and has strong complexity-theoretic evidence for hardness. We have now seen several experimental demonstrations of BosonSampling [WQD+19] and its Gaussian variant at scale [ZPL+19, ZDQ+21, MLA+22], as well as substantial work building the theory of these experiments and bringing them closer to feasibility (see e.g. [HKS+17, CC17, DMV+22, GBA+22]).

Despite this progress, there is still a formidable distance between experiment and theory. One of the most notable gaps involves the ratio between the number of modes and number of photons. The original BosonSampling proposal calls for a "high-mode regime" in which n photons are passed through an $m = \Omega(n^2)$-mode Haar-random interferometer followed by the measurement of each mode in the photon number basis.[1] By contrast, all experiments to date operate in a "low-mode regime" in which the number of modes scales linearly in the number of modes, $m = \Theta(n)$. Understanding this low-mode regime has long been cited as a major open problem going back to the original paper [AA13] which asked explicitly:

> *"Can we reduce the number of modes needed for our linear-optics experiment, perhaps from $O(n^2)$ to $O(n)$?"*

It is reasonable to conjecture that the need for such a high number of modes is an artifact of current proof techniques, rather than intrinsic to the hardness of the sampling problem. For one, state-of-the-art classical simulation algorithms are not able to take advantage of the low-mode regime to achieve dramatically faster runtimes[2] [CC18], albeit some improvements are possible [CC20, MRK+23]. Furthermore, the low-mode regime is sufficient to perform universal quantum computation [KLM01]. However, analyzing the hardness of BosonSampling in the low-mode regime is quite challenging for two reasons. First, current proof techniques rely heavily on a property of the high-mode regime known as the "Bosonic Birthday Paradox" [AK11] which ensures that most measurement outcomes are collision-free—i.e., have a single photon in each occupied output mode. By contrast, low-mode BosonSampling

[1] We note that the original paper used $m = \omega(n^5)$ modes, but they showed that an $O(n^2)$ experiment would suffice under a plausible random matrix theory conjecture, and subsequent work proved variants of BosonSampling like Bipartite BosonSampling [GBA+22] can be analyzed with as few as $O(n^2)$ modes.

[2] To be precise, these algorithms run in time which is exponential in the number of photons, but merely polynomial in the number of modes. In other words, high-mode experiments with few photons provably cannot lead to exponential quantum advantage.

has a large number of collisions. Second, in the high-mode regime the probability of each outcome is the squared permanent of a submatrix of the Haar random unitary that encodes the interferometer. These submatrices have i.i.d. Gaussian entries, which are convenient to analyze. In the low-mode regime, the relevant submatrices do not have i.i.d. entries and this is the case even in the absence of collisions.

In this work (see [BBD$^+$23] for the technical version of the manuscrip) we overcome these obstacles and build the complexity-theoretic foundations for BosonSampling in the low-mode regime, answering Aaronson and Arkhipov's question in the affirmative. The starting point, following Aaronson and Arkhipov, is to prove that hardness of classical approximate sampling from low-mode BosonSampling experiments follows from the hardness of an appropriate average-case hardness conjecture:

Theorem 1 (Informal)**.** *Assuming average-case hardness of computing output probabilities of low-mode BosonSampling experiments, there is no efficient randomized classical algorithm to sample from the output distribution of such an experiment to inverse polynomial additive error.*

Our main results give strong evidence in favor of this average-case hardness conjecture. In particular we show it is #P-hard to compute the output probabilities of random low-mode experiments, and also provide numerical evidence for anticoncentration in this regime. This brings low-mode BosonSampling to essentially the same level of theoretical support as high-mode experiments.

Proof sketch The first obstacle present in the low-mode regime—the presence of photon collisions in typical outcomes—breaks a property of the experiment known as *hiding*. Hiding[3] is the property that all outputs of the experiment are symmetrical over the choice of random experiment. This simple property plays a surprisingly key role in current quantum advantage arguments. The basic reason is that these arguments try to show no approximate classical sampler exists to small total variation distance error. If all outputs are on equal footing then this error can be spread over all outputs by Markov's inequality. However if only a few outputs matter for the hardness arguments, one might worry the approximate sampler could corrupt these outputs only, and the arguments become implausible. This symmetry property trivially holds for Random Circuit Sampling, IQP, Fermion Sampling, and many other advantage schemes, and also trivially carries over to BosonSampling experiments in the high-mode regime. However in the low-mode regime this symmetry fails spectacularly—the output space shatters into an exponential number of incomparable output types each with probability mass that is relatively well spread.[4]

We instead proceed by formulating a modified version of the Stockmeyer counting reduction which does not require the hiding symmetry. We choose a uniformly random outcome of the experiment and use Stockmeyer counting to estimate the probability of this outcome. By Markov's inequality we can ensure that most output probabilities of the approximate sampler are mostly correct. However, this modified reduction comes at a cost—to show hardness of sampling, it no longer suffices to show hardness of computing a single type of output, but instead we must now show an *entire suite* of hardness results for *most* outputs of the experiments. More formally, for low-mode BosonSampling the output space consists of an exponential number of incomparable collision patterns—i.e., unordered lists of occupation numbers of modes. We need to argue it is hard to estimate the output probabilities of most collision patterns under a suitable measure.

Our next step is to show such a suite of average-case hardness results of computing most outputs of low-mode experiments:

Theorem 2 (Informal)**.** *It is* #P*-hard to compute most output probabilities of most BosonSampling experiments in the low-mode regime to within additive error $e^{-O(n \log n)}$.*[5]

This is nearly what we need to show hardness of sampling via the modified Stockmeyer reduction ($e^{-O(n)}$ robustness). Here we need to overcome both of the major differences that distinguish the low and

[3] "Hiding" also refers to an input type conversion problem in the original paper [AA13], but in subsequent papers was used only to describe this symmetry property.

[4] That is, it is unclear if any particular output type occurs with a probability that scales as an inverse polynomial.

[5] We note that this additive error is dependent on the output type of the outcome, though this dependence is subleading in the exponent.

high-mode regimes. First, one must deal with the presence of collisions—to do this we identify a collection of output types which cover a large fraction of the output probability distribution of typical experiments. This requires a careful combinatorial accounting of typical collision patterns in typical outputs of low-mode experiments. Once a suitable collision pattern is identified, we need to show average-case hardness for computing outputs of that collision type over the random choice of interferometer. This is equivalent to showing hardness of computing the permanent of a large submatrix of a random unitary, with a particular pattern of repeated rows.

In the high-mode regime this average-case hardness argument proceeds using a variant of Lipton's argument. The basic idea is that since a Gaussian is perturbed only slightly by shifting and rescaling, one can in some sense "sneak" a tiny amount of a worst-case matrix into an average-case matrix. This uses an entry-by-entry analysis of the matrix. This proof strategy breaks in the low-mode case since the relevant submatrices are far from i.i.d. Gaussian [Jia06]—instead, the entries come from a highly correlated measure. We show that surprisingly, this highly correlated distribution is nonetheless approximately shift-and-scale invariant so that we recover Lipton's proof. To do this, we directly study the probability density of the singular values of a submatrix of a Haar-random unitary [Col03, Réf05]. We reduce the desired invariance property to estimating the gradient of this probability density, which we show is equivalent to proving sharp tail bounds on the maximum singular value. Our desired bounds require that we go beyond generic concentration inequalities such as Levy's lemma or log-Sobolev inequalities, and instead we derive them from high-dimensional geometry. Considering the ubiquity of the Haar measure over unitaries, we expect that this bound may be of independent interest.

Finally we address the issue of anticoncentration of low-mode experiments. Anticoncentration is a necessary ingredient for converting additive estimates of output probabilities to multiplicative estimates—which we conjecture to be hard. It remains open to prove anticoncentration for all variants of BosonSampling, but there has been partial progress in this direction [Nez21], as well as numerical evidence for anticoncentration in the high-mode regime [AA13]. However, as one reduces the number of modes, one might worry that anticoncentration might begin to fail, both due to the row repetitions in the submatrices, and the correlations between submatrix entries. This could be an issue as many of the known attacks on quantum advantage schemes hold in the non-anticoncentration regime, e.g. constant-depth random circuits [NLPD$^+$22]. To alleviate this concern and to support our anticoncentration conjecture, we provide numerical evidence that anticoncentration holds in the low-mode regime, and indeed has very similar behavior to the i.i.d. Gaussian case.

Discussion Our work better connects the theory of BosonSampling to its empirical implementation. Aaronson and Arkhipov's foundational work led to a number of important extensions which improved our understanding of the complexity of BosonSampling—from generalizations to Gaussian BosonSampling, to improving the robustness of average-case hardness arguments, to efficiently spoofing or verifying of experiments, to characterizing the effects of noise. While many of the more empirical works have focused on the low-mode regime due to its connection with experiment, most of the theoretical arguments have focused on high-mode regime and may need to be re-investigated in this new context. Many interesting questions remain. For example, can we improve the robustness of average-case hardness of these experiments to $e^{-O(n)}$, i.e. to be only off by a constant in the exponent as with high-mode BosonSampling [BFLL21]? Do spoofing algorithms for BosonSampling become easier or harder in the low-mode case? How few modes are needed for intractability, for example, for which α do $m = \alpha n$ experiments have the best evidence for hardness,[6] and are there any fundamental limits on this constant?

References

[AA13] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 4:143–252, 2013.

[6] For technical reasons, our strongest results hold in the regime of $m > 2n$, but we also discuss how the arguments scale down to generally $m = O(n)$ experiments with slightly worse parameters.

[AK11] Alex Arkhipov and Greg Kuperberg. The bosonic birthday paradox. *Geometry and Topology Monographs*, 06 2011.

[BBD$^+$23] Adam Bouland, Daniel Brod, Ishaun Datta, Bill Fefferman, Daniel Grier, Felipe Hernandez, and Michal Oszmaniec. Complexity-theoretic foundations of BosonSampling with a linear number of modes. *arXiv e-prints*, page arXiv:2312.00286, November 2023.

[BFLL21] Adam Bouland, Bill Fefferman, Zeph Landau, and Yunchao Liu. Noise and the frontier of quantum supremacy. *arXiv e-prints*, page arXiv:2102.01738, Feb 2021.

[CC17] L. Chakhmakhchyan and N. J. Cerf. Boson sampling with Gaussian measurements. *Phys. Rev. A*, 96:032326, Sep 2017.

[CC18] Peter Clifford and Raphaël Clifford. *The Classical Complexity of Boson Sampling*, pages 146–155. Society for Industrial and Applied Mathematics, 2018.

[CC20] Peter Clifford and Raphaël Clifford. Faster classical boson sampling. 2020.

[Col03] Benoît Collins. *Intégrales matricielles et probabilités non-commutatives.* PhD thesis, Université Pierre et Marie Curie-Paris VI, 2003.

[DMV$^+$22] Abhinav Deshpande, Arthur Mehta, Trevor Vincent, Nicolás Quesada, Marcel Hinsche, Marios Ioannou, Lars Madsen, Jonathan Lavoie, Haoyu Qi, Jens Eisert, Dominik Hangleiter, Bill Fefferman, and Ish Dhand. Quantum computational advantage via high-dimensional Gaussian boson sampling. *Science Advances*, 8(1):eabi7894, 2022.

[GBA$^+$22] Daniel Grier, Daniel J. Brod, Juan Miguel Arrazola, Marcos Benicio de Andrade Alonso, and Nicolás Quesada. The complexity of bipartite Gaussian boson sampling. *Quantum*, 6:863, November 2022.

[HKS$^+$17] Craig S. Hamilton, Regina Kruse, Linda Sansoni, Sonja Barkhofen, Christine Silberhorn, and Igor Jex. Gaussian boson sampling. *Phys. Rev. Lett.*, 119:170501, Oct 2017.

[Jia06] Tiefeng Jiang. How many entries of a typical orthogonal matrix can be approximated by independent normals? *The Annals of Probability*, 34(4):1497–1529, 2006.

[KLM01] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[MLA$^+$22] Lars S. Madsen, Fabian Laudenbach, Mohsen Falamarzi. Askarani, Fabien Rortais, Trevor Vincent, Jacob F. F. Bulmer, Filippo M. Miatto, Leonhard Neuhaus, Lukas G. Helt, Matthew J. Collins, Adriana E. Lita, Thomas Gerrits, Sae Woo Nam, Varun D. Vaidya, Matteo Menotti, Ish Dhand, Zachary Vernon, Nicolás Quesada, and Jonathan Lavoie. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[MRK$^+$23] Gregory Morse, Tomasz Rybotycki, Ágoston Kaposi, Zoltán Kolarovszki, Uros Stojic, Tamás Kozsik, Oskar Mencer, Michał Oszmaniec, Zoltán Zimborás, and Péter Rakyta. High performance Boson Sampling simulation via data-flow engines. *arXiv e-prints*, page arXiv:2309.07027, 2023.

[Nez21] Sepehr Nezami. Permanent of random matrices from representation theory: moments, numerics, concentration, and comments on hardness of boson-sampling. *arXiv preprint arXiv:2104.06423*, 2021.

[NLPD$^+$22] John C Napp, Rolando L La Placa, Alexander M Dalzell, Fernando GSL Brandao, and Aram W Harrow. Efficient classical simulation of random shallow 2D quantum circuits. *Physical Review X*, 12(2):021021, 2022.

[Réf05] Júlia Réffy. *Asymptotics of random unitaries.* PhD thesis, BUTE Institute of Mathematics, 2005.

[WQD$^+$19] Hui Wang, Jian Qin, Xing Ding, Ming-Cheng Chen, Si Chen, Xiang You, Yu-Ming He, Xiao Jiang, L You, Z Wang, et al. Boson sampling with 20 input photons and a 60-mode interferometer in a 10^{14}-dimensional hilbert space. *Physical review letters*, 123(25):250503, 2019.

[ZDQ$^+$21] Han-Sen Zhong, Yu-Hao Deng, Jian Qin, Hui Wang, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Dian Wu, Si-Qiu Gong, Hao Su, et al. Phase-programmable Gaussian boson sampling using stimulated squeezed light. *Phys. Rev. Lett.*, 127:180502, Oct 2021.

[ZPL$^+$19] Han-Sen Zhong, Li-Chao Peng, Yuan Li, Yi Hu, Wei Li, Jian Qin, Dian Wu, Weijun Zhang, Hao Li, Lu Zhang, Zhen Wang, Lixing You, Xiao Jiang, Li Li, Nai-Le Liu, Jonathan P. Dowling, Chao-Yang Lu, and Jian-Wei Pan. Experimental Gaussian boson sampling. *Science Bulletin*, 64(8):511–515, 2019.

Quantum Unpredictability

Tomoyuki Morimae[1] [*] Shogo Yamada[1] [†] Takashi Yamakawa[2] [3] [1] [‡]

[1] *Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan*
[2] *NTT Social Informatics Laboratories, Tokyo, Japan*
[3] *NTT Research Center for Theoretical Quantum Information, Atsugi, Japan*

Abstract. Unpredictable functions (UPFs) play essential roles in classical cryptography. In this paper, we introduce a quantum analog of UPFs, which we call unpredictable state generators (UPSGs). UPSGs are implied by pseudorandom function-like states generators (PRFSs), which are a quantum analog of pseudorandom functions (PRFs), and therefore UPSGs could exist even if one-way functions do not exist. Although UPFs are equivalent to PRFs, UPSGs could be weaker than PRFSs. Despite this, we demonstrate that all known applications of PRFSs are also achievable with UPSGs. Our findings suggest that, for many applications, quantum unpredictability, rather than quantum pseudorandomness, is sufficient.

Keywords: Quantum cryptography, unpredictability, secret-key encryption, message authentication codes with unclonable tags

1 Background

Pseudorandom functions (PRFs) [GGM86] are one of the most fundamental primitives in classical cryptography. A PRF is an efficiently computable keyed function that is computationally indistinguishable from a random function for any polynomial-time adversary that can query the function. PRFs have many important applications in cryptography, and in particular, they are essential building blocks of EUF-CMA-secure message authentication codes (MACs) and IND-CPA-secure secret-key encryption schemes (SKE).

Naor and Reingold [NR98] introduced a related primitive so-called unpredictable functions (UPFs). Like PRFs, a UPF is an efficiently computable keyed function $f_k(\cdot)$, but the crucial difference is that the goal of the adversary is not to distinguish it from the random function but to predict the output $f_k(x^*)$ without querying x^*. Naor and Reingold showed that the existence of PRFs is equivalent to that of UPFs.

What happens if we consider quantum versions of PRFs and UPFs? Recently, quantum analogs of elementary primitives have been extensively studied [JLS18, MY22b, AQY22, BCQ23, AGQY22, Yan22, MY22a, BBSS23, ALY23]. For example, pseudorandom states generators [JLS18], One-way states generators (OWSGs) [MY22b] and EFIs [BCQ23]. There are mainly two reasons why studying such new quantum elementary primitives are important. First, they could exist without (quantumly-secure) one-way functions (OWFs) [Kre21, KQST23], which are the most fundamental assumptions in classical cryptography. Second, despite that, they have many useful applications. These facts suggest that these primitives will play the role of the most fundamental assumptions in quantum cryptography, similar to OWFs in classical cryptography.

Quantum versions of PRFs have been already studied. Pseudorandom function-like states (generators) (PRFSs) [AQY22, AGQY22] are one of the quantum analogs of PRFs. A PRFS is a quantum polynomial-time (QPT) algorithm that, on input a secret key k and a classical bit string x, outputs a quantum state $|\phi_k(x)\rangle$. The security roughly means that no QPT adversary can tell whether it is querying the PRFS oracle or the oracle that returns Haar random states. PRFSs could also exist without OWFs, and imply EUF-CMA-secure MACs (with quantum tags) and IND-CPA-secure SKE (with quantum ciphertexts) [AQY22].

On the other hand, no quantum analog of UPFs was explored before. Is it equivalent to a quantum analog of PRFs, such as PRFSs? Does it imply EUF-CMA-secure MACs and IND-CPA-secure SKE like PRFSs? Can we gain any meaningful insight for quantum cryptography by studying it?

2 Our Results

The present paper aims to initiate the study of a quantum version of UPFs which we call unpredictable states generators (UPSGs). We define UPSGs and construct several cryptographic applications from UPSGs.

Defining UPSGs. Our first contribution is to define UPSGs. A UPSG is a QPT algorithm Eval that, on input a secret key k and a classical bit string x, outputs a quantum state $|\phi_k(x)\rangle$. Intuitively, the security (unpredictability) is as follows: no QPT adversary, which can quantumly query the oracle $\mathsf{Eval}(k,\cdot)$, can output (x^*,ρ) such that x^* was not queried and ρ is close to $|\phi_k(x^*)\rangle$.

In the classical case, PRFs and UPFs are equivalent [NR98]. What happens in the quantum case? In fact, we can show that PRFSs imply UPSGs. However, the other direction is not clear. In the classical case, the construction of PRFs from UPFs is done by using the Goldreich-Levin [NR98, GL89]: if $f_k(\cdot)$ is a UPF, $g_{k,r}(x) := f_k(x)\cdot r$ is a PRF with the key (k,r), where $x \cdot y$ is the inner product between bit strings x and y. However, we cannot directly apply that idea to UPSGs: In particular, what is $|\phi_k(x)\rangle \cdot r$?

[*] tomoyuki.morimae@yukawa.kyoto-u.ac.jp
[†] shogo.yamada@yukawa.kyoto-u.ac.jp
[‡] takashi.yamakawa@ntt.com

In summary, a quantum analog of UPFs, UPSGs, are implied by PRFSs, which especially means that UPSGs could also exist without OWFs. However, the equivalence is not clear, and UPSGs could be weaker than PRFSs. Then, a natural question is the following: Do UPSGs have useful applications like PRFSs?

IND-CPA-secure SKE. Our second contribution is to construct IND-CPA-secure SKE (with quantum ciphertexts) from UPSGs. In the classical case, unpredictability implies pseudorandomness [NR98], which implies encryption. However, as we have explained before, we do not know how to convert unpredictability to pseudorandomness in the quantum case. Therefore we cannot use the same technique in the quantum case.

Before the construction of IND-CPA-secure SKE from UPSGs, let us first recall the definition of IND-CPA-secure SKE. SKE consists of an encryption algorithm Enc and a decryption algorithm Dec. On input a secret key and a bit b, Enc outputs a (possibly quantum) ciphertext ct_b, and Dec, on input the secret key and ciphertext ct_b, outputs b. As the IND-CPA security, we require that no QPT adversary can distinguish ct_0 from ct_1.

Our idea to construct IND-CPA-secure SKE is based on the duality between the swapping and the distinction [AAS20, HMY23]. The duality intuitively means that distinguishing two orthogonal states $|\psi\rangle$ and $|\phi\rangle$ is as hard as swapping $|\psi\rangle + |\phi\rangle$ and $|\psi\rangle - |\phi\rangle$ with each other. Our ciphertext for a single-bit message $b \in \{0,1\}$ is, then, $\mathsf{ct}_b := (x, y, |\mathsf{ct}^b_{x,y}\rangle)$, where

$$|\mathsf{ct}^b_{x,y}\rangle := |0\rangle\,|x\rangle\,|\phi_k(x)\rangle + (-1)^b\,|1\rangle\,|y\rangle\,|\phi_k(y)\rangle\,,$$

and x and y are random bit strings. The secret key of our SKE scheme is the key k of the UPSGs. From the unpredictability of UPSGs, any QPT adversary cannot convert $|\phi_k(x)\rangle$ to $|\phi_k(y)\rangle$, which means that any QPT adversary cannot distinguish ct_0 and ct_1 due to the duality.

This argument seems to work. There is, however, one subtle issue here. The adversary of the IND-CPA security can query the encryption oracle. However, in general, we do not know whether the duality works if the distinguisher queries an oracle because the swapping unitary is constructed from the distinguishing unitary and its inverse.

We can solve the issue by observing that the oracle query by the adversary can actually be removed. Because the oracle is an encryption algorithm for single-bit messages and the adversary queries the oracle only polynomially many times, we can remove the oracle by giving sufficiently many outputs of the oracle to the adversary in advance as an auxiliary input. The duality in [HMY23] takes into account the auxiliary inputs to the adversary, and therefore now we can use the duality.

Moreover, since it is known that IND-CPA-secure SKE imply IND-CPA-secure SKE for quantum messages [BJ15], we get the following result.

Theorem 1 *If UPSGs exist, then IND-CPA-secure SKE (for quantum messages) exist.*

MACs with unclonable tags. Our third contribution is to define MACs with unclonable tags and to construct it from UPSGs. The unclonability of tags roughly means that no QPT adversary can, given t-copies of a quantum tag, output a large (possibly entangled) quantum state that contains at least $t+1$ valid tag states. MACs with unclonable tags are useful in practical applications. For example, consider the following attack (which is known as the *replay attack* in the classical cryptography): Alice sends the message "transfer \$100 to Bob" with a MAC tag to a bank. Malicious Bob can steal the pair of the message and the tag, and sends it ten times to the bank so that he can get \$1000. In classical cryptography, the standard EUF-CMA security of MACs cannot avoid such an attack, and some higher-level treatments are necessary.

If tags are unclonable, we can avoid such a replay attack. It is easy to see that UPSGs imply EUF-CMA-secure MACs with quantum tags. (We have only to take $|\phi_k(m)\rangle$ as the tag of the message m.) However, it is not self-evident whether the quantum unpredictability implies unclonability. For instance, if $f_k(\cdot)$ is a PRF, $|\phi_k(x)\rangle := |f_k(x)\rangle$ is a UPSG but $|\phi_k(x)\rangle$ is not unclonable.

Our idea to construct unclonable tags is to use the unclonability of random BB84 states. (In other words, to use Wiesner money [Wie83].) For two bit string x and θ, we define $|x\rangle_\theta := \bigotimes_i H^{\theta^i}|x^i\rangle$, where H is the Hadamard gate, and x^i and θ^i are ith bit of x and θ, respectively. If we set $\tau_m := |\phi_k(m)\rangle \otimes |x\rangle_\theta$, where x and θ are chosen at random, as a tag for classical message m, it seems unclonable.

Here, $\tau_m = |\phi_k(m)\rangle \otimes |x\rangle_\theta$ does not contain any information about x and θ except for $|x\rangle_\theta$. From this, two crucial issues arise. First, τ_m is not unclonable in general. To understand this issue, assume that $|\phi_k(m)\rangle$ is not unclonable. (As mentioned above, we cannot ensure that $|\phi_k(m)\rangle$ is unclonable.) Then, the following adversary $\mathcal{A}$ breaks unclonability: $\mathcal{A}$, given $\tau_m = |\phi_k(m) \otimes |x\rangle_\theta\rangle$, clones $|\phi_k(m)\rangle$ and generates $|x'\rangle_{\theta'}$ by choosing x' and θ' at random. It is clear that $\mathcal{A}$ can generate two valid tags $|\phi_k(m)\rangle \otimes |x\rangle_\theta$ and $|\phi_k(m)\rangle \otimes |x'\rangle_{\theta'}$ from a single copy of $\tau_m = |\phi_k(m)\rangle \otimes |x\rangle_\theta$.

How can we avoid this issue? It seems that we can avoid the first issue just by replacing the tag $\tau_m = |\phi_k(m)\rangle \otimes |x\rangle_\theta$ with $\tau'_m := |\phi_k(m,x,\theta)\rangle \otimes |x\rangle_\theta$, where $|\phi_k(m,x,\theta)\rangle$ is the output of UPSGs on input (m,x,θ). This is because, if no adversary can know x and θ from $|\phi_k(m,x,\theta)\rangle$, no adversary can clone $\tau'_m = |\phi_k(m,x,\theta)\rangle \otimes |x\rangle_\theta$ from the unclonability of random BB84 states. However, it is not clear whether UPSGs satisfy its property in general.

The second issue is that the verifier of MAC cannot verify whether $\tau_m = |\phi_k(m)\rangle \otimes |x\rangle_\theta$ (or $\tau'_m = |\phi_k(m,x,\theta)\rangle \otimes |x\rangle_\theta$) is a valid tag or not. This is because, in general, the verifier cannot know x and θ from the tag to verify the BB84 state $|x\rangle_\theta$. To solve this issue, we have to encode x and θ into a tag for the sake of verification. However, if we do so directly, e.g., we set $\tau''_m := (x, \theta, |\phi_k(m, x, \theta)\rangle \otimes |x\rangle_\theta)$, the new tag is not unclonable because x and θ are open.

From the above observation, if we can encrypt x, θ and $|\phi_k(m, x, \theta)\rangle$, we can construct a tag that is unclonable and verifiable. We can do it by using IND-CPA-secure SKE for quantum messages, which exist from Theorem 1 since we assume the existence of UPSGs. Therefore, by setting $\tau'''_m := \mathsf{Enc}(\mathsf{sk}, |(x,\theta)\rangle \otimes |\phi_k(m, x, \theta)\rangle) \otimes |x\rangle_\theta$, where Enc is the encryption algorithm of IND-CPA-secure SKE for quantum messages, we can construct MACs with unclonable tags from UPSGs. Therefore we have the following result.

Theorem 2 *If UPSGs exist, then MACs with unclonable tags exist.*

OWSGs with pure output and a necessary condition for UPSGs As our fourth contribution, we construct OWSGs with pure outputs from UPSGs, which means that $\mathbf{PP} \neq \mathbf{BQP}$ is necessary for the existence of UPSGs [CGG$^+$23]. At first glance, the former looks trivial since UPSGs imply IND-CPA-secure SKE from Theorem 1 and IND-CPA-secure SKE imply OWSGs [MY22a]. However, in general, the outputs of OWSGs constructed from IND-CPA-secure SKE are not pure states. Therefore, Theorem 1 does not mean that UPSGs imply OWSGs with pure outputs.

Before explaining how to construct OWSGs with pure outputs, let us recall the definition of OWSGs with pure outputs. An OWSG with pure outputs is the QPT algorithm that, on input secret key k, then outputs a pure state $|\psi_k\rangle$. The security is the following: no QPT adversary, given many copies of $|\psi_k\rangle$, can output the correct secret key k.

Our idea to construct OWSGs with pure outputs is based on the following observation: from the unpredictability of UPSGs, no QPT adversary $\mathcal{A}$ cannot correctly guess the secret key k of UPSGs using $|\phi_k(x)\rangle$ for polynomially many bit strings x. This is because, if $\mathcal{A}$ can do that, $\mathcal{A}$ breaks the unpredictability of UPSGs as follows: $\mathcal{A}$ query polynomially many bit strings x to $\mathsf{Eval}(k, \cdot)$ to guess the secret key k and output $|\phi_k(x')\rangle$ by running $\mathsf{Eval}(k, x')$, where x' is not queries before.

From the above observation, we construct OWSGs as follows. We set secret key $k' := (k, x_1, ..., x_t)$ of our OWSG. Here, k is a secret key of UPSGs, and $x_1, ..., x_t$ are bit strings chosen uniformly at random, where t is a polynomial of the length of k. Our OWSG runs $|\phi_k(x_i)\rangle \leftarrow \mathsf{Eval}(k, x_i)$ for all i and outputs

$$|\psi_{k'}\rangle := \bigotimes_{i=1}^{t} |x_i\rangle |\phi_k(x_i)\rangle .$$

As explained before, no QPT adversary can correctly guess k (and also $k' = (k, x_1, ..., x_t)$) even if the adversary gets many copies of $|\psi_{k'}\rangle$, which means our OWSG with pure outputs satisfies the security. Therefore, we have the following result.

Theorem 3 *If UPSGs exist, then OWSGs with pure outputs exist.*

Because pure OWSGs are broken if $\mathbf{PP} = \mathbf{BQP}$ [CGG$^+$23], we also have the following corollary, which means $\mathbf{PP} \neq \mathbf{BQP}$ is a necessary condition for the existence of UPSGs:

Corollary 4 *If UPSGs exist, then* $\mathbf{PP} \neq \mathbf{BQP}$.

Implication of our result. IND-CPA-secure SKE implies EFIs [MY22a]. Moreover, MACs with unclonable tags straightforwardly imply private-key quantum money schemes in the sense of [AC12, JLS18]. We therefore have the following as a corollary of Theorem 1 and Theorem 2.

Corollary 5 *If UPSGs exist, then EFIs and private-key money schemes exist.*

IND-CPA-secure SKE, MACs with unclonable tags, OWSGs, EFIs, and private-key money schemes are also implied by PRFSs, and these primitives are all known applications of PRFSs. This suggests the following: *For many applications, quantum unpredictability, rather than quantum pseudorandomness, is sufficient.*

References

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions. *Electron. Colloquium Comput. Complex.*, page 146, 2020.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60, 2012.

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 237–265. Springer, Heidelberg, November 2022.

[ALY23] Prabhanjan Ananth, Yao-Ting Lin, and Henry Yuen. Pseudorandom strings from pseudorandom quantum states. Cryptology ePrint Archive, Paper 2023/904, 2023. https://eprint.iacr.org/2023/904.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Heidelberg, August 2022.

[BBSS23] Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. Pseudorandomness with proof of destruction and applications. Cryptology ePrint Archive, Paper 2023/543, 2023. https://eprint.iacr.org/2023/543.

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. ITCS 2023: 14th Innovations in Theoretical Computer Science, 2023.

[BJ15] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low t-gate complexity. In *Annual Cryptology Conference*, pages 609–629. Springer, 2015.

[CGG$^+$23] Bruno Cavalar, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, and Angelos Pelecanos. On the computational hardness of quantum one-wayness. *arXiv preprint arXiv:2312.08363*, 2023.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986.

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32. ACM Press, May 1989.

[HMY23] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 639–667. Springer, Heidelberg, April 2023.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Heidelberg, August 2018.

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1589–1602, 2023.

[Kre21] W. Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021.

[MY22a] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. Cryptology ePrint Archive, Paper 2022/1336, 2022. https://eprint.iacr.org/2022/1336.

[MY22b] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 269–295. Springer, Heidelberg, August 2022.

[NR98] Moni Naor and Omer Reingold. From unpredictability to indistinguishability: A simple construction of pseudo-random functions from MACs (extended abstract). In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 267–282. Springer, Heidelberg, August 1998.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[Yan22] Jun Yan. General properties of quantum bit commitments (extended abstract). In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 628–657. Springer, Heidelberg, December 2022.

Certified randomness in tight space

Boris Bourdoncle[1] * Andreas Fyrillas[1] Alexandre Maïnos[2]
Pierre-Emmanuel Emeriau[1] Kayleigh Start[1] Nico Margaria[1] Martina Morassi[3]
Aristide Lemaître[3] Isabelle Sagnes[3] Petr Stepanov[1] Thi Huong Au[1]
Sébastien Boissier[1] Niccolo Somaschi[1] Nicolas Maring[1] Nadia Belabas[3]
Shane Mansfield[1]

[1] *Quandela, 91300 Massy, France*
[2] *Quantum Engineering Technology Labs, University of Bristol, BS81FD Bristol, UK*
[3] *Université Paris-Saclay, CNRS, Centre de Nanosciences et de nanotechnologies, 91120 Palaiseau, France*

Abstract. Reliable randomness is a core ingredient for cryptographic applications. The outcomes of measurements on entangled states can violate Bell inequalities, thus guaranteeing their intrinsic randomness, which constitutes the basis for certified randomness generation. However, this certification requires space- like separated devices, making it unfit for practical applications. Here we provide a general method to certify randomness on a small-scale apparatus and implement the corresponding protocol on a device that combines a solid-state emitter and a glass chip. In contrast to most existing randomness certification techniques, our protocol accounts for information leakage and is thus compatible with emerging compact devices.

Keywords: Quantum correlations, randomness certification, quantum cryptography, quantum photonics

This submission is based on the following pre-print: `https://arxiv.org/pdf/2301.03536v2` (new version published on 15 May 2024).

Reliable randomness is a core ingredient in algorithms and applications ranging from numerical simulations to statistical sampling and cryptography. The strictest requirements on randomness sources are typically destined to cryptographic applications. There, randomness should ideally be both unpredictable and private, so that no information about the generated sequence can be gained by an eavesdropper either prior to or immediately after its generation. Quantum sources admit certification of these properties, by exploiting links between the unpredictability of a quantum behaviour and the violation of Bell inequalities. A guarantee that numbers have been sampled from empirical data exhibiting Bell nonlocality or, more generally, contextuality can suffice to certify unpredictability and privacy.

Randomness certification and other Bell-inequality-based protocols offer attainable cryptographic advantages for quantum information processing but they are susceptible to loopholes. One way to close the locality, or more generally, the compatibility loophole, is to ensure space-like separation between the players of the non-local game [1, 2, 3, 4]. However, that is not an option for a practical compact device. Merely asserting that the relevant parts of the device are shielded [5] is unsatisfactory for users who would like to prevent themselves against a device deteriorating with time. For such a device, the compatibility loophole must be carefully addressed, because crosstalk can lead to detrimental information flow between components. This compromises theoretical analyses and security proofs even outside of adversarial scenarios. More broadly, all future on-chip quantum information processing will be susceptible to such effects, for which reason it is essential that they be taken into account in protocols and algorithms at the information processing level.

In this work, we introduce novel theoretical tools to take into account crosstalk and address the locality loophole. We demonstrate these tools in a randomness certification protocol performed on a compact photonic chip. Idealised analyses typically lead to relations between the relevant figure of merit (fidelity, rate, guessing probability...) on the one hand, and Bell violations or more general contextuality measures [6] on the other hand. Here, we provide relations suited to realistic devices, which allow the evaluation of the relevant figures of merit in terms of both beneficial contextuality and detrimental crosstalk. Moreover, we introduce a method to upper bound the amount of crosstalk by computing how far the device's observed behaviour is from the set of quantum correlations approximated by the Navascués–Pironio–Acín (NPA) hierarchy [7]. This enables detection of adversarial manipulation of the device which may seek to exploit the locality loophole to spoof certification.

We incorporate our method in a randomness certification protocol that is secure against quantum side information, meeting the highest security standards. Such protocols require acquiring large statistics while maintaining high photon purity and indistinguishability [8, 9], which puts knock-on constraints on hardware efficiency and stability. Our theoretical contribution bridging the gap between ideal situations and realistic implementations, combined with finely controlled and robust hardware, allow us to implement the first on-chip certified quantum random number generation protocol with a full security proof against quantum side information.

*`boris.bourdoncle@quandela.com`

1 Theoretical contribution

Our work uses the semi-device-independent framework: we aim to derive a lower bound on the randomness generated during the experiment, based on the input-output correlations that characterise this experiment and a physical assumption that restricts the correlations that can be accessed. The experiments we consider can be formulated as n-player games, where each (virtual) player can choose an input (that correspond to a measurement choice) and obtains an output (that corresponds to a measurement result). The set of probabilities of obtaining an output tuple given an input tuple is called a behaviour. If no information can flow between the players, the behaviour satisfies the property of no-signalling. If the input-output correlations stem from a quantum experiment (i.e., performing quantum measurements on potentially entangled particles), the behaviour is said to be quantum. If the probability distributions for each input tuples can't be obtained as the marginals of a single probability distribution of global assignments of outcomes to all measurements, the behaviour is said to be contextual. Thanks to Bell's theorem, we know there exist contextual quantum behaviours, and such behaviours are useful from a cryptographic perspective as the randomness with which the outputs are obtained can't be apparent: the outputs obtained during the experiment are inherently random [10, 11]. A behaviour is necessarily contextual when it violates a Bell inequality, or equivalently when it reaches a value above a certain score, called non-contextual or classical score, in a contextual game. The score corresponds to the sum of the probabilities weighted by a scalar for each input and output tuple and the input probabilities. The set of such scalars is called the scoring function and defines the game.

Our theoretical contribution is threefold.

- We define the signalling fraction SF (simultaneously introduced in a companion paper [12]), a measure of the information flow that can take place between the components of the experiment, which correspond to the players mentioned above. This measure is defined in a similar way as the contextual fraction [6] and the local fraction [13], but relative to the set of no-signalling behaviours: it is equal to 0 for a no-signalling behaviour and to 1 for a maximally signalling behaviour. We generalise the signalling fraction by defining the approximate quantum fractions SF_ℓ, that are relative to the set of quantum correlations approximated at the ℓ^{th} level of the NPA hierarchy [7, 14].

- We then define, for a given scoring function, two scores: the maximal score that can be reached by behaviour with maximal contextual fraction ξ, and the maximal score that be reached by behaviours with signalling fraction at most σ and the further requirement that the behaviour be deterministic on a specific input tuple. The first score is related to a characteristics of the game called consistency and can be easily computed, while the second one is the quantity of interest for the protocol we want to implement (see next point). We prove that the latter is upper-bounded by the former for any n-partite games with binary inputs.

- Finally, we introduce a protocol for private randomness generation and randomness expansion[1] in the presence of crosstalk. We use the approximate quantum fraction to quantify the crosstalk, and not the signalling fraction, because we assume that our experiment is governed by the laws of quantum mechanics, and thus want to discard supra-quantum behaviours. Our protocol is derived from Miller and Shi's spot-checking protocol [16] and provides a lower bound on the amount of randomness that it generates, valid even in the presence of quantum side information.

This protocol allows us to certify randomness generation with a compact apparatus, provided that the following assumption is satisfied: the measure of crosstalk by the approximate quantum fraction is a fair estimate of the information flow at the hidden variable level. This assumption is well-founded if the devices were fabricated by an honest provider, i.e. were not programmed to act maliciously in order to function with a high level of crosstalk while keeping the empirically observable signalling low. In that case, an eavesdropper can only take advantage of flaws in the implementation and deterioration of the devices with time to try and predict the outputs.

Compared to Ref. [17], which also uses the spot-checking security proof of Miller and Shi [16] and takes into account imperfect compatibility between the measurements, our analysis is more general, as it applies to any n-partite nonlocal game with binary inputs. Another approach to derive a lower bound on the physical crosstalk from the observed behaviour was proposed in [18], which puts a constraint at the level of the measurements rather than on the behaviours. Both metrics provide valid lower bounds on the crosstalk; the advantage of ours is that it integrates well with convex optimisation techniques used to compute maximal scores, Bell inequality violations and guessing probabilities.

2 Experimental contribution

We then implement our protocol on a photonic setup, which is depicted in Fig 1. The contextual game we implement is the Clauser-Horne-Shimony-Holt (CHSH) game [19]. It's a two-party game and we call the (virtual) players Alice and Bob. In the setup, an electrically controlled semiconductor quantum dot in a 2-µm-diameter micropilar cavity generates single photons that are sent to a reconfigurable glass chip, implementing the CHSH game by varying the measurement choices via optical phases and measuring output coincidences.

By a periodical calibration during the experiment, we maintain a high precision over the implemented measurement bases to limit crosstalk between the two par-

[1] Concerning the difference between the two notions, see [15].

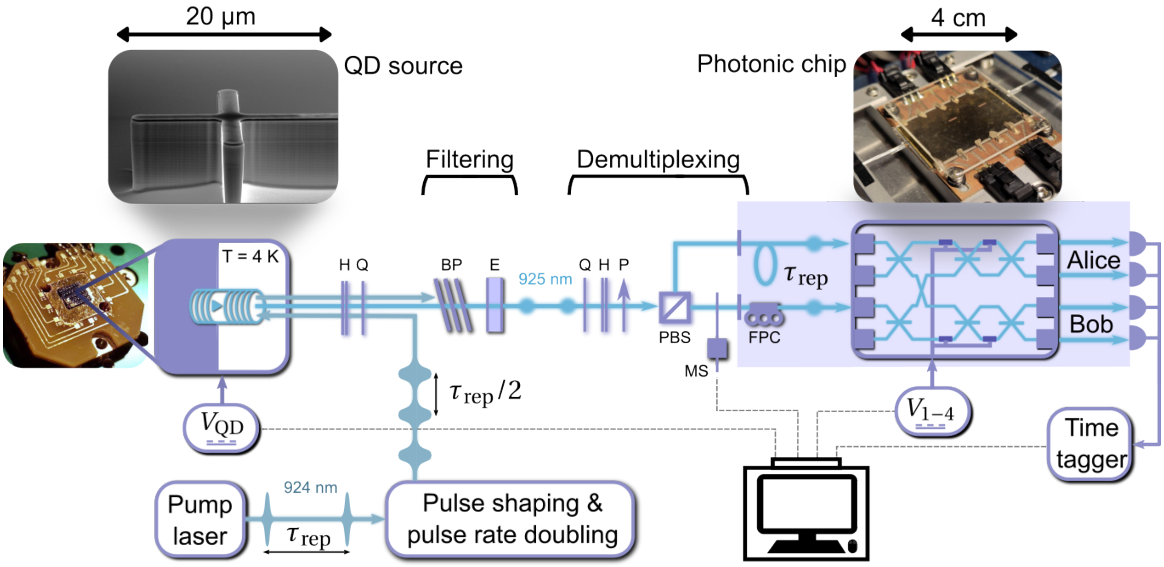


Figure 1: **Compact implementation of a certified quantum random number generator.** The quantum dot (QD) photon emitter generates photons at 925 nm via a phonon-assisted excitation scheme (see Methods). H, Q: half and quarter-wave plates. BP: bandpass filters. E: etalon. P: polarizer. After a demultiplexing stage (see Methods), the outputs of a polarizing beamsplitter (PBS) are collected with collimators. The setup is entirely fibered or waveguided in the blue area. A fibered delay τ_{rep}, allows to synchronize pairs of photons sent into the photonic chip. A motorized shutter (MS) enables chip voltage calibration. The fibered polarisation controller (FPC), ensures both photons enter the photonic chip with the same polarisation. Dashed grey lines indicate that elements of the setup are automated to implement the randomness generation protocol, by adapting the voltage on the photon source for optimal brightness and periodic calibrations of the thermo-optic phase-shifter voltages. V_{1-4} control the phases on chip and hence measurement bases of Alice and Bob. V_{QD} feedback loop ensures the QD emission remains bright and the emitted photons indistinguishable.

ties. We use a bright and stable Quandela semiconductor quantum dot (QD) based single photon source [20] that delivers indistinguishable single photons, allowing us to obtain high Bell inequality violations. The polarised fibered-device brightness of our QD-based single-photon source is 8.3(8) % (all error bars represent one standard deviation). The purity of the single photons, quantified by the second-order normalised correlation function, is $g^{(2)}(0) \approx 2.31(3)\,\%$ and their indistinguishability, quantified with the Hong-Ou-Mandel (HOM) visibility, is $V_{\text{HOM}} = 93.09(4)\,\%$ [21]. The train of emitted photons is converted with a passive demultiplexing stage into pairs of photons entering simultaneously the photonic chip. On exiting the chip, the photons are detected by high-efficiency single photon detectors and time tagged. The overall transmission of the setup is 2.7 %.

Certifiying randomness requires witnessing correlations that win the CHSH game, or equivalently that violate the CHSH inequality. This places requirements on the purity and indistinguishability of the photons emitted by the single-photon source. For the ideal case of a source emitting only pure photons in a lossless optical circuit, denoting I_{CHSH} the value obtained for the CHSH expression, we derive the following relation:

$$I_{\text{CHSH}} = \sqrt{2}(V_{\text{HOM}} + 1). \tag{1}$$

The choice of inputs for Alice and Bob corresponds to applying different phases on their side of the chip, that are controlled by thermo-optic phase shifters. We use a spatial encoding, which means that the outputs recorded by Alice and Bob are determined by the modes in which each of their photons exit the chip. The protocol alternates between generation rounds, for which Alice's and Bob's phases are fixed, and test rounds, for which they each choose at random one of their two possible measurement choices. We assume that the detected photons are representative of the whole optical setup behaviour, i.e. that the sampling is fair. The measured coincidence rate is about $14\,200(600)\,\text{s}^{-1}$. Before data acquisition we measured a violation of the CHSH inequality $I_{\text{CHSH}} = 2.68$, which we used to fix the optimal parameters for the protocol. We ran our protocol for a total number of rounds $N = 2.4 \times 10^9$, and we obtained a CHSH violation of $I_{\text{CHSH}} = 2.685$ and an approximate quantum fraction of 0.005 (at level 3 of the NPA hierarchy). Our protocol then certifies that this generates 7.21×10^6 private random bits, quantified by the min-entropy of the outputs. This amount of randomness is compatible with randomness expansion, in the sense that if we were to use the interval algorithm to generate our strongly biased input bits from a small number of uniform bits [22, 23], the input randomness required for our implementation would be 5.24×10^6, which is smaller than the amount of randomness we generate at the output.

References

[1] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, "Experimentally generated randomness certified by the impossibility of superluminal signals," *Nature*, vol. 556, no. 7700, pp. 223–226, 2018.

[2] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, "Device-independent quantum random-number generation," *Nature*, vol. 562, no. 7728, pp. 548–551, 2018.

[3] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, "Experimental Low-Latency Device-Independent Quantum Randomness," *Phys. Rev. Lett.*, vol. 124, no. 1, p. 010505, 2020.

[4] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, "Device-independent randomness expansion with entangled photons," *Nat. Phys.*, vol. 17, no. 4, pp. 452–456, 2021.

[5] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, "Device-independent randomness expansion against quantum side information," *Nat. Phys.*, vol. 17, no. 4, pp. 448–451, 2021.

[6] S. Abramsky, R. S. Barbosa, and S. Mansfield, "Contextual fraction as a measure of contextuality," *Phys. Rev. Lett.*, vol. 119, p. 050504, 2017.

[7] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," *Phys. Rev. Lett.*, vol. 98, p. 010401, 2007.

[8] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, "Distribution of time-bin entangled qubits over 50 km of optical fiber," *Phys. Rev. Lett.*, vol. 93, p. 180502, 2004.

[9] E. M. González-Ruiz, S. K. Das, P. Lodahl, and A. S. Sørensen, "Violation of Bell's inequality with quantum-dot single-photon sources," *Phys. Rev. A*, vol. 106, no. 1, p. 012222, 2022. arXiv:2109.14712 [quant-ph].

[10] R. Colbeck, *Quantum and Relativistic Protocols For Secure Multi-Party Computation.* PhD thesis, University of Cambridge, 2007.

[11] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[12] K. Vallée, P.-E. Emeriau, B. Bourdoncle, A. Sohbi, S. Mansfield, and D. Markham, "Corrected Bell and non-contextuality inequalities for realistic experiments," *Phil. Trans. R. Soc. A*, vol. 382, no. 2268, p. 20230011, 2024.

[13] L. Aolita, R. Gallego, A. Acín, A. Chiuri, G. Vallone, P. Mataloni, and A. Cabello, "Fully nonlocal quantum correlations," *Phys. Rev. A*, vol. 85, no. 3, p. 032107, 2011.

[14] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New J. Phys.*, vol. 10, no. 7, p. 073013, 2008.

[15] S. Pironio and S. Massar, "Security of practical private randomness generation," *Phys. Rev. A*, vol. 87, p. 012336, 2013.

[16] C. A. Miller and Y. Shi, "Universal security for randomness expansion from the spot-checking protocol," *SIAM J. Comput.*, vol. 46, no. 4, pp. 1304–1335, 2017.

[17] M. Um, Q. Zhao, J. Zhang, P. Wang, Y. Wang, M. Qiao, H. Zhou, X. Ma, and K. Kim, "Randomness expansion secured by quantum contextuality," *Phys. Rev. Applied*, vol. 13, p. 034077, 2020.

[18] J. Silman, S. Pironio, and S. Massar, "Device-independent randomness generation in the presence of weak cross-talk," *Phys. Rev. Lett.*, vol. 110, p. 100504, 2013.

[19] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, 1969.

[20] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaítre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart, "Near-optimal single-photon sources in the solid state," *Nat. Photonics*, vol. 10, no. 5, pp. 340–345, 2016.

[21] H. Ollivier, S. E. Thomas, S. C. Wein, I. M. de Buy Wenniger, N. Coste, J. C. Loredo, N. Somaschi, A. Harouri, A. Lemaitre, I. Sagnes, L. Lanco, C. Simon, C. Anton, O. Krebs, and P. Senellart, "Hong-Ou-Mandel Interference with Imperfect Single Photon Sources," *Phys. Rev. Lett.*, vol. 126, no. 6, p. 63602, 2021.

[22] D. Knuth and A. Yao, "The complexity of nonuniform random number generation," in *Algorithms and Complexity: New Directions and Recent Results*, pp. 357–428, Academic Press, New York, 1976.

[23] T. S. Hao and M. Hoshi, "Interval algorithm for random number generation," *IEEE Trans. Inf. Theory*, vol. 43, pp. 599–611, 1997.

A Cryptographic Perspective on the Verifiability of Quantum Advantage

Nai-hui Chia[1] * Honghao Fu[2] † Fang Song[3] ‡ Penghui Yao[4 5] §

[1] *Rice University, USA*
[2] *Massachusetts Institute of Technology, USA*
[3] *Portland State University, USA*
[4] *Nanjing University, China*
[5] *Hefei National Laboratory, China*

Abstract. In recent years, achieving verifiable quantum advantage on a NISQ device has emerged as an important open problem in quantum information. The sampling-based quantum advantages are not known to have efficient verification methods. This paper investigates the verification of quantum advantage from a cryptographic perspective. We establish a strong connection between the verifiability of quantum advantage and cryptographic and complexity primitives, including efficiently samplable, statistically far but computationally indistinguishable pairs of (mixed) quantum states (EFI), pseudorandom states (PRS), and variants of minimum circuit size problems (MCSP). Specifically, we prove that a) a sampling-based quantum advantage is either verifiable or can be used to build EFI and even PRS and b) polynomial-time algorithms for a variant of MCSP would imply efficient verification of quantum advantages. Full version: https://arxiv.org/pdf/2310.14464.

Keywords: Verifiable quantum advantage, EFI, Pseudorandom States, Minimal circuit size problem

1 Introduction

Quantum advantage experiments aim to demonstrate that quantum computers can perform some tasks faster than classical computers with a more favorable amount of computational resources. In the NISQ (Noisy Intermediate Scale Quantum) era, sampling tasks such as random circuit sampling (RCS) [2] and Boson sampling [1] emerge as promising candidates for quantum advantage experiments since they can be implemented on a NISQ device and are provably hard for classical computers. Besides classical hardness and implementation on a NISQ device, an equally important aspect is how to allow an efficient classical computer to verify the samples from such experiments. Consequently, the challenge remains open to designing a quantum advantage experiment that satisfies all three criteria.

In terms of the verifiability of RCS, the linear cross-entropy benchmarking (XEB) is first proposed as a verification method [2]. However, XEB is sample-efficient, but not computationally efficient. Moreover, XEB can be spoofed [9, 16]. Perhaps there is a better verification method for RCS? Hangleiter and his colleagues showed that the answer is no [10]. They show that if the target distribution anticoncentrates, certifying closeness to the target distribution requires exponentially many samples, which covers RCS, Boson sampling, and IQP sampling.

What about general quantum sampling experiments? How do we determine if such an experiment has an efficient verification method? In [8], the verification task is modeled as a game between a quantum party, a classical challenger, and a classical referee, which we will discuss later. However, they can only show the limitations of the verification method that calculates the empirical average of some scoring function of individual samples in this model.

2 Our results

In this paper, we investigate the verifiability of sampling-based quantum advantage experiments via a *cryptographic* perspective. To this end, we first put forth formal definitions of verifiability. Subsequently, we study the implication of the hardness of a variant of the minimal circuit size problem (MCSP) on verifiability. Furthermore, we establish the connection between verifiability and fundamental quantum cryptographic primitives: EFI (efficiently generated, statistically far, and computationally indistinguishable states) and PRS (pseudorandom states). Lastly, we generalize verifiable quantum advantage to capture the verifiability of interactive proof of quantumness. We hope that our work will advance the understanding of the verifiability of quantum advantage experiments and provide insights into the development of future quantum advantage experiments.

*nc67@rice.edu
†honghaof@mit.edu
‡fang.song@pdx.edu
§phyao1985@gmail.com

To address the verifiability of quantum advantage experiments, we model the verification process as an interaction between three parties: Alice (a quantum advocate and experiment designer), Bob (a quantum skeptic), and a verifier [1]. Alice runs the quantum experiment and sends transcripts of her experiment, including the setup of the experiment apparatus and outcomes, to the verifier. She also tells Bob about her experiment apparatus but not the outcomes. Bob proposes a classically samplable distribution that depends on Alice's experiment and is indistinguishable from Alice's distribution, and sends the description of his sampling algorithm along with samples of his distribution to the verifier. The verifier's goal is to distinguish Alice and Bob's samples, so we also call him the distinguisher. The distinguisher takes all the information from Alice and Bob as input. In the case of RCS, Alice publishes her random circuit C, and sends her measurement outcome on $C|0^n\rangle$ to the distinguisher. Bob proposes a C-dependent spoofing algorithm, and sends the description of the algorithm along with his samples to the distinguisher.

Definition 1 (Verifiable quantum advantage) *Let $\mathfrak{C}$ be a set of polynomial-sized quantum circuits on n qubits. We say the experiment that samples a $C \in \mathfrak{C}$ and repeatedly measures the output state in the computational basis achieves* verifiable quantum advantage *if for all $\mathfrak{D} = \{D_C, \mathcal{S}_C\}_{C\in\mathfrak{C}}$ where $\mathcal{S}_C$ is a time-s classical sampler for D_C, there exists a classical polynomial time distinguisher $\mathcal{A}$ such that*

$$\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{C}} |\Pr[\mathcal{A}(C, \mathcal{S}_C, \boldsymbol{z}_C) = 1] - \Pr[\mathcal{A}_D(C, \mathcal{S}_C, \boldsymbol{z}_{\mathcal{D}_C}) = 1]| \geq 1/\,\mathsf{poly}(n),$$

where $\boldsymbol{z}_C$ is a polynomial-sized set of samples generated from measuring $C|0^n\rangle$ in the computational basis, and $\boldsymbol{z}_{\mathcal{D}_C}$ is a set of samples drawn from $\mathcal{D}_C$.

We give several VQA examples to demonstrate the expressiveness of our verifiability definition, such as Fourier sampling (e.g., based on Shor's algorithm and Simon's problem). Note that our distinguisher is more general than the ones used in the experiments [2] and studied in [8]. Their distinguishers are agnostic about how the classical samples are sampled, and they score each sample individually, and make their decisions based on the average of the scores. As pointed out in [8], if the distinguisher knows the spoofing algorithm of XEB proposed in [16], the distinguisher can distinguish the spoofing samples from the quantum samples. Hence, we define VQA with respect to a more general distinguisher.

Minimum circuit size problem (MCSP) vs. VQA. We aim to identify the computational hardness of verifying quantum advantages. One potential approach is finding a problem for which the existence of efficient algorithms would lead to efficient verification. This is similar to the connections between Meta-complexity problems and cryptography.

Classical meta-complexity problems, which ask to identify specific complexity measures (e.g., circuit complexity) of given Boolean functions, is a fundamental topic in complexity theory. It is worth noting that efficient classical algorithms for these problems imply that one-way functions do not exist [12, 17]. Inspired by the connections between meta-complexity problems and cryptography, we introduce a variant of meta-complexity problems called the *minimum circuit size problems for samples* (SampMCSP), which asks the minimal size of classical samplers that can generate samples indistinguishable from the given samples. This problem is analogous to the state minimum circuit size problem introduced in [7], which asks to identify the quantum circuit complexity of given quantum states. We demonstrate that if SampMCSP can be solved in polynomial time, then quantum advantage experiments that only generate polynomially many samples can be verified efficiently.

EFI vs. VQA. Next, we study the relationships between verifiability and the quantum cryptographic primitive EFI. EFI is a fundamental quantum cryptographic primitive, which is equivalent to quantum commitment schemes, quantum oblivious transfer, quantum multi-party computation and others [3]. We show a *duality* between EFI and verifiable quantum advantage, when we consider classically-secure EFI pairs, i.e., whose computational indistinguishability holds only against classical algorithms.

Theorem 2 (Informal) *Suppose that a quantum experiment admits quantum advantage. Then, the experiment is verifiable if and only if there exists a sufficiently large faction of the circuits' output states that do not form an EFI pair with any quantum state that encodes a classical samplable distribution.*

If we allow verifying quantum advantage by a quantum computer, we obtain a similar duality between quantum-secure EFIs and quantum verifiability. These results provide necessary and sufficient conditions for verifiability based on whether the quantum circuit family can form EFI pairs with classical polynomial-time samplable distributions. To the best of our knowledge, all existing EFI pairs satisfy such a property, i.e., one of the EFI generators can be simulated by classical polynomial-time

[1] We came up with this model unaware of the two-party game proposed in [8], although the two models share some similarities

sampling algorithms.

Pseudorandom states (PRS) vs. VQA A set of states is a PRS if a random state in this set is computationally indistinguishable from a Haar random state [11]. PRS is an essential quantum cryptographic primitive that can be used to build other primitives, including one-time digital signature and EFI. Moreover, the existence of PRS implies the existence of EFI, and thus the aforementioned applications that are equivalent to EFI can also be constructed from PRS. There is also evidence showing that the existence of PRS is a weaker assumption than the existence of one-way functions [14].

Intuitively, if the output states of a quantum advantage experiment are pseudorandom, the measurement output distribution should be indistinguishable from the measurement output distribution of Haar random states. In addition, the measurement output distribution of Haar random states can be approximated by a classical distribution, so this quantum advantage experiment doesn't achieve verifiability. However, in the definition of PRS, the distinguisher is unaware of the preparation circuit of the given state, but the distinguisher in a quantum advantage experiment is. Hence, we can only prove this result for a subclass of PRS, called classically unidentifiable PRS, which intuitively says that when distinguishing samples from measuring different states, knowing the circuit doesn't help. Many existing PRS constructions, such as the random phase states and binary phase states [11, 6], are classically unidentifiable.

Theorem 3 (Informal) *If the quantum advantage of a quantum sampling algorithm is verifiable, then the output states are not classically unidentifiable PRS.*

The motivation behind Theorem 3 is that RCS is proposed as a candidate construction of PRS [15]. If the output states of random circuits are classically unidentifiable, Theorem 3 gives us a proof that RCS experiments are unverifiable. Note that [10] shows the distribution induced by measuring a random circuit is indistinguishable from some classical distribution, which doesn't imply RCS is not VQA according to Theorem 1. Conversely, Theorem 3 also tells us that if some construction of PRS fails, it is possible to use this construction for verifiable quantum advantage. This is a win-win situation.

What about interactive quantum advantage experiments? So far, we have focused on sampling-based quantum advantage experiments. There are interactive verifiable quantum advantage proposals called proof of quantumness (PoQ) [4, 5, 13]. These PoQs achieve verifiability, but one obstacle in implementing these protocols is maintaining coherence during the interactions.

Hence, we generalize Theorem 1 to capture the strength of both Theorem 1 and the verifiability of PoQ. In the generalized definition, the trusted party is the *designated verifier*, who generates public parameters and a private verification key. After getting all the samples, the designated verifier uses the verification key to distinguish Alice's quantum samples from Bob's samples. We call this *Designated verifiable quantum advantage* or DVQA.

Under this definition, the trusted verifier is offline, so Alice doesn't need to interact with the trusted verifier and can generate the samples on her own as in Theorem 1. Moreover, it is possible to compile existing PoQ to satisfy the new definition. For example: Assuming a random oracle, the interactive protocol of [4] fits this definition. The function keys and trapdoors of their protocol are the public parameters and private verification keys here. Then, the classical or quantum prover can run the operations of the verifier in the original protocol locally by querying the random oracle for the challenges. In the end, the prover sends all the generated transcripts to the distinguisher $\mathcal{A}$, who uses the verification key to distinguish the transcripts. In the compiled protocol, the verifier is offline as in Theorem 1, and the verifiability of the original PoQ is preserved.

3 Conclusion and discussions

In summary, our results show connections between the verifiability of quantum advantages and the quantum cryptographic primitives. It is worth noting that computational tasks demonstrating quantum advantages on near-term quantum devices might not directly result in useful applications; however, our results show that the quest for quantum advantages and their verifiability can provide new insights and methods to build fundamental quantum cryptographic primitives. For a quantum experiment designer: The study of quantum cryptography can provide new insights into designing a verifiable quantum advantage experiment. For a quantum cryptographer: The quest for verifiability of quantum advantages might lead to quantum cryptographic applications. Theorem 2 implies that if an experiment is not verifiable, then it will form a classical-secure EFI with a classical polynomial-time samplable distribution.

References

[1] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. *Theory OF Computing*, 9(4):143–252, 2013.

[2] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595–600, 2018.

[3] Z. Brakerski, R. Canetti, and L. Qian. On the Computational Hardness Needed for Quantum Cryptography. In *14th Innovations in Theoretical Computer Science Conference – ITCS 2023*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:21. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023.

[4] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM (JACM)*, 68(5):1–47, 2021.

[5] Z. Brakerski, V. Koppula, U. Vazirani, and T. Vidick. Simpler proofs of quantumness. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2020.

[6] Z. Brakerski and O. Shmueli. (Pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019.

[7] N.-H. Chia, C.-N. Chou, J. Zhang, and R. Zhang. Quantum meets the minimum circuit size problem. *arXiv preprint arXiv:2108.03171*, 2021.

[8] D. S. França and R. Garcia-Patron. A game of quantum advantage: linking verification and simulation. *Quantum*, 6:753, 2022.

[9] X. Gao, M. Kalinowski, C.-N. Chou, M. D. Lukin, B. Barak, and S. Choi. Limitations of linear cross-entropy as a measure for quantum advantage. *arXiv preprint arXiv:2112.01657*, 2021.

[10] D. Hangleiter, M. Kliesch, J. Eisert, and C. Gogolin. Sample complexity of device-independently certified "quantum supremacy". *Physical review letters*, 122(21):210502, 2019.

[11] Z. Ji, Y.-K. Liu, and F. Song. Pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2018*, pages 126–152. Springer, 2018.

[12] V. Kabanets and J.-Y. Cai. Circuit minimization problem. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 73–79, 2000.

[13] G. D. Kahanamoku-Meyer, S. Choi, U. V. Vazirani, and N. Y. Yao. Classically verifiable quantum advantage from a computational bell test. *Nature Physics*, 18(8):918–924, 2022.

[14] W. Kretschmer. Quantum pseudorandomness and classical complexity. *arXiv preprint arXiv:2103.09320*, 2021.

[15] W. Kretschmer, L. Qian, M. Sinha, and A. Tal. Quantum cryptography in algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1589–1602, 2023.

[16] F. Pan and P. Zhang. Simulation of quantum circuits using the big-batch tensor network method. *Physical Review Letters*, 128(3):030501, 2022.

[17] A. A. Razborov and S. Rudich. Natural proofs. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 204–213, 1994.

Tsirelson bounds for quantum correlations with indefinite causal order

Zixuan Liu[1] [2] [*] Giulio Chiribella[1] [2] [3] [4] [†]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *HKU-Oxford Joint Laboratory for Quantum Information and Computation*

[3]*Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, UK*

[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada*

Keywords: causal inequalities, indefinite causal order, Tsirelson bounds, device-independent certification

1 Extended abstract

Quantum theory is in principle compatible with processes that violate causal inequalities, an analogue of Bell inequalities that constrain the correlations observed by parties operating in a definite order [1–3]. To date, many examples of causal inequalities that are potentially violated by processes with indefinite causal order have been found [2, 4–11]. However, in general, the maximum quantum violations of these inequalities are still unknown even in the simplest cases, unlike in the case of Bell inequalities such as Clauser-Horne-Shimony-Holt (CHSH) inequality [12], for which Tsirelson bound provides the ultimate violation achievable in quantum theory. The lack of exact bounds on the quantum violation of causal inequalities limits our understanding of indefinite causal order in quantum mechanics. In addition, new questions have recently arisen from the introduction of a new class of scenarios where not only the causal order of the experiments, but also the temporal direction of the information flow within the local laboratories can be indefinite [13]. Can these scenarios lead to even larger violations? And in the affirmative case, where does the boundary lie between the correlations achievable with indefinite causal order alone and those achievable when indefinite causal order is combined with indefinite temporal direction?

Here we answer all the above questions. First, we develop a general method for bounding the violation of causal inequalities by quantum processes with indefinite causal order. We start by showing that the maximal violation of a special class of causal inequalities, termed *single-trigger causal inequalities*, can be determined explicitly. The maximal violation of single-trigger causal inequalities provides upper bounds on the violations of arbitrary causal inequalities. Mathematically, these upper bounds can be seen as an semidefinite programming (SDP) relaxation of the original problem of computing the maximal quantum violation of causal inequalities.

Using this method, we establish the analogue of Tsirelson bound for paradigmatic examples of causal inequalities. We show the maximal violation of the Oreshkov-Costa-Brukner (OCB) inequality [2] and the inequality associated with Lazy Guess Your Neighbor's Input game [5]. In addition, we provide a non-trivial upper bound of the success probability of Guess Your Neighbor's Input game [5]. Our results allow for a geometric representation of the quantum correlations arising from indefinite causal order. Intriguingly, we find that the geometric representation of the OCB correlations coincides with the representation of the CHSH correlations in the Bell inequality setting [14].

Then, we show that classical processes with indefinite causal order and time direction can violate all causal inequalities to their algebraic maximum. These processes are the classical version of the quantum processes with indefinite time direction introduced in Ref. [13]. They are in principle compatible with the validity of classical physics in the laboratories of the different parties, but do not assume a privileged direction of time outside each laboratory. In particular, we construct a classical process which allows two parties to perfectly signal to each other.

Our results offer new insights into the structure of the set of quantum correlations generated by quantum indefinite-causal-order processes, and can be used as a tool to better understand the operational implication of indefinite causal order in quantum

[*] `zixuanliu@connect.hku.hk`

[†] `giulio@cs.hku.hk`

theory. An open question is whether our general bound could be tight for all the other causal inequalities. The analogy with Bell inequalities, however, suggests a negative answer. In Bell scenarios, a converging sequence of upper bounds on the value of maximal quantum violations is provided by the Navascués-Pironio-Acín SDP hierarchy [15, 16]. The analogy with this situation suggests that our SDP relaxation may be just the first level of a a similar hierarchy of SDPs. Determining whether this analogy is correct, and, in the affirmative case, identifying the other levels of the hierarchy are among the most important research directions opened by our work. Another interesting direction is to extend our method for the calculation of the ICO bound to other type of inequalities with non-trivial causal structure, such as the inequalities recently studied in Refs. [17, 18]. Another interesting direction of future research is to establish self-testing results for causal inequalities, in analogy to the self-testing results in Bell scenarios [19, 20]. Such a self-testing result may have cryptographic implications, in a similar way as it was observed in the setting of Bell correlations. While the physical realization of the OCB process is still an open problem, these implications would provide important foundational insights into the operational understanding of indefinite causal order in quantum theory. Finally, our results open up a search for physical principles capable of explaining why the violation of causal inequalities by ICO quantum processes is not equal, in general, to the algebraic maximum, and, of determining the exact value of the quantum violation. In the context of Bell inequalities, the analogue question was originally raised by Popescu and Rohrlich [21], and led to the discovery of new information theoretic principles, such as non-trivial communication complexity [22–24], non-trivial nonlocal computation [25], information causality [26], macroscopic locality [27], and local orthogonality [28].

2 Technical version of the work

Our paper is available on arXiv (`https://arxiv.org/abs/2403.02749`).

References

[1] G. Chiribella, G. D'Ariano, P. Perinotti, and B. Valiron, "Beyond quantum computers," *arXiv preprint arXiv:0912.0195*, 2009.

[2] O. Oreshkov, F. Costa, and Č. Brukner, "Quantum correlations with no causal order," *Nature communications*, vol. 3, no. 1, pp. 1–8, 2012.

[3] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, "Quantum computations without definite causal structure," *Physical Review A*, vol. 88, no. 2, p. 022318, 2013.

[4] O. Oreshkov and C. Giarmatzi, "Causal and causally separable processes," *New Journal of Physics*, vol. 18, no. 9, p. 093020, 2016.

[5] C. Branciard, M. Araújo, A. Feix, F. Costa, and Č. Brukner, "The simplest causal inequalities and their violation," *New Journal of Physics*, vol. 18, no. 1, p. 013008, 2015.

[6] Ä. Baumeler, A. Feix, and S. Wolf, "Maximal incompatibility of locally classical behavior and global causal order in multiparty scenarios," *Physical Review A*, vol. 90, no. 4, p. 042106, 2014.

[7] Ä. Baumeler and S. Wolf, "Perfect signaling among three parties violating predefined causal order," in *2014 IEEE International Symposium on Information Theory*, pp. 526–530, IEEE, 2014.

[8] Ä. Baumeler and S. Wolf, "The space of logically consistent classical processes without causal order," *New Journal of Physics*, vol. 18, no. 1, p. 013036, 2016.

[9] S. S. Bhattacharya and M. Banik, "Biased non-causal game," *arXiv preprint arXiv:1509.02721*, 2015.

[10] A. Feix, M. Araújo, and Č. Brukner, "Causally nonseparable processes admitting a causal model," *New Journal of Physics*, vol. 18, no. 8, p. 083040, 2016.

[11] A. A. Abbott, C. Giarmatzi, F. Costa, and C. Branciard, "Multipartite causal correlations: polytopes and inequalities," *Physical Review A*, vol. 94, no. 3, p. 032131, 2016.

[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[13] G. Chiribella and Z. Liu, "Quantum operations with indefinite time direction," *Communications Physics*, vol. 5, no. 1, pp. 1–8, 2022.

[14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of modern physics*, vol. 86, no. 2, p. 419, 2014.

[15] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," *Physical Review Letters*, vol. 98, no. 1, p. 010401, 2007.

[16] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New Journal of Physics*, vol. 10, no. 7, p. 073013, 2008.

[17] S. Gogioso and N. Pinzani, "The geometry of causality," *arXiv preprint arXiv:2303.09017*, 2023.

[18] T. van der Lugt, J. Barrett, and G. Chiribella, "Device-independent certification of indefinite causal order in the quantum switch," *Nature Communications*, vol. 14, no. 1, p. 5811, 2023.

[19] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pp. 503–509, IEEE, 1998.

[20] D. Mayers and A. Yao, "Self testing quantum apparatus," *Quantum Info. Comput.*, vol. 4, p. 273–286, jul 2004.

[21] S. Popescu and D. Rohrlich, "Quantum nonlocality as an axiom," *Foundations of Physics*, vol. 24, pp. 379–385, 1994.

[22] W. Van Dam, *Nonlocality and communication complexity.* PhD thesis, University of Oxford, 1999.

[23] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, "Limit on nonlocality in any world in which communication complexity is not trivial," *Physical Review Letters*, vol. 96, no. 25, p. 250401, 2006.

[24] N. Brunner and P. Skrzypczyk, "Nonlocality distillation and postquantum theories with trivial communication complexity," *Physical review letters*, vol. 102, no. 16, p. 160403, 2009.

[25] N. Linden, S. Popescu, A. J. Short, and A. Winter, "Quantum nonlocality and beyond: limits from nonlocal computation," *Physical review letters*, vol. 99, no. 18, p. 180502, 2007.

[26] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, "Information causality as a physical principle," *Nature*, vol. 461, no. 7267, pp. 1101–1104, 2009.

[27] M. Navascués and H. Wunderlich, "A glance beyond the quantum model," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 466, no. 2115, pp. 881–890, 2010.

[28] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín, "Local orthogonality as a multipartite principle for quantum correlations," *Nature communications*, vol. 4, no. 1, p. 2263, 2013.

Entanglement-enabled advantage for learning a bosonic random displacement channel

Changhun Oh[1 2 *] Senrui Chen[1] Yat Wong[1] Sisi Zhou[3 4 5] Hsin-Yuan Huang[4 6 7]
Jens A.H. Nielsen[8] Zheng-Hao Liu[8] Jonas S. Neergaard-Nielsen[8] Ulrik L. Andersen[8]
Liang Jiang[1] John Preskill[4]

[1] *Pritzker School of Molecular Engineering, The University of Chicago, Chicago, Illinois 60637, USA*
[2] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*
[3] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[4] *Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA 91125, USA*
[5] *Department of Physics and Astronomy and Institute for Quantum Computing, University of Waterloo, Ontario N2L 2Y5, Canada*
[6] *Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[7] *Google Quantum AI, Venice, CA, USA*
[8] *Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, Building 307, Fysikvej, 2800 Kgs. Lyngby, Denmark*

Abstract. We show that quantum entanglement provides an exponential advantage in learning properties of a bosonic continuous-variable (CV) system. Considering learning n bosonic mode random displacement channel, we prove that without an ancillary quantum memory, an exponential number of copies of the channel in n is required to estimate its characteristic function to reasonable precision. In contrast, we present an entanglement-assisted scheme that only requires the number of samples independent of n, given a sufficient amount of squeezing. This establishes an exponential separation in sample complexity. We then show that the entanglement-assisted scheme is sufficiently robust against photon loss.

Keywords: Quantum learning, Continuous-variable systems, Quantum advantage

1 Introduction

Learning and characterizing a physical system is a crucial task in science and technology. Over the past few years, there has been a huge interest in studying quantum advantage in learning a quantum system. Many of the previous results discovered a quantum advantage in learning using quantum memory in the sense that learning schemes allowed the use of entanglement with quantum memory to provide an exponential sample complexity advantage over any schemes without quantum memory. Specifically, Refs. [1, 2] establish a framework for proving exponential separation in sample complexity between learning with and without a coherently controllable quantum memory.

However, most learning tasks studied so far are restricted to discrete-variable (DV) systems. It is natural to ask whether entanglement-enabled advantage can also be realized for learning properties of bosonic continuous-variable (CV) systems. This is particularly important because CV systems are ubiquitous in nature and have many applications, such as quantum sensing. The main obstacle for generalizing the results in DV systems to CV systems is that the latter has an infinite-dimensional Hilbert space, making it challenging to formulate rigorous results concerning the complexity of learning properties of these systems. Recent progress has been achieved in studies of entanglement-enhanced learning of CV-state characteristic functions [3]; however, the lower bounds obtained so far apply to a restricted class of learning strategies rather than to general entanglement-free schemes.

In this work, we rigorously prove an entanglement-enabled advantage in learning an n-mode bosonic random displacement channel. Specifically, we show that any schemes without ancillary quantum memory require an exponential number of samples in n to learn the characteristic functions of the channel with reasonably good precision and high success probability. In stark contrast, we present a simple scheme utilizing entanglement with ancillary quantum memory (i.e., entanglement-assisted) that can complete the same learning task with a sample complexity independent of n, given access to two-mode squeezed vacuum (TMSV) states with sufficiently large squeezing parameter and Bell measurements (BM). This establishes an exponential separation between learning with and without entanglement in bosonic systems. The two learning scenarios are illustrated in Fig. 1. We emphasize that our hardness results hold for arbitrarily high-energy input states and arbitrary measurements, while the presented entanglement-assisted scheme only requires a finite-energy TMSV and BM.

2 Results

2.1 Main result

Our main result is to prove the exponential separation of sample complexity between two types of learning schemes, (i) entanglement-free scheme and (ii) entanglement-assisted scheme, for the random displacement channel, as illustrated in Fig. 1. The main

[*] changhun0218@gmail.com

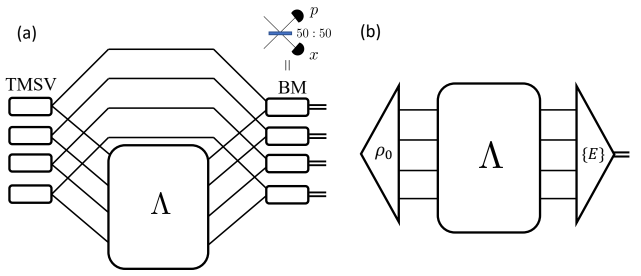


Figure 1: Schemes for learning an n-mode random displacement channel Λ. (a) TMSV+BM, a specific entanglement-assisted (EA) scheme. (b) General entanglement-free (EF) scheme (see the main text).

result is obtained by combining Theorem 1, proving the upper-bound of sample complexity for the proposed entanglement-assisted scheme and Theorem 2, proving the lower-bound of sample complexity for any entanglement-free schemes. Here, an entanglement-free scheme is (i) ancilla-free, i.e., not allowed to use ancillary memory, (ii) concatenation-free, i.e., the output of the channel is measured destructively after each channel use, but (iii) adaptive, i.e., for each channel use, the input to the channel and the measurement performed on the output may depend on measurement outcomes obtained in earlier rounds. On the other hand, a particular entanglement-assisted scheme we propose is allowed to use (i) ancilla, (ii) concatenation-free, and (iii) non-adaptive.

2.2 Problem setup

We consider the task of learning an n-mode random displacement channel characterized by a probability distribution $p(\alpha)$ with $\alpha \in \mathbb{C}^n$, which transforms an input state $\hat{\rho}$ as

$$\Lambda(\hat{\rho}) = \int d^{2n}\alpha\ p(\alpha)\hat{D}(\alpha)\hat{\rho}\hat{D}^\dagger(\alpha) \tag{1}$$

$$= \frac{1}{\pi^n}\int d^{2n}\beta\ \lambda(\beta)\mathrm{Tr}[\hat{\rho}\hat{D}(\beta)]\hat{D}^\dagger(\beta), \tag{2}$$

where $\hat{D}(\alpha) \equiv \otimes_{i=1}^n \hat{D}(\alpha_i)$ and $\hat{D}(\alpha_i) \equiv \exp(\alpha_i\hat{a}_i^\dagger - \alpha_i^*\hat{a}_i)$ is the displacement operator for the ith mode. Here, the second equivalent expression is by the characteristic function of $p(\alpha)$, i.e., its Fourier transform, as

$$\lambda(\beta) \equiv \int d^{2n}\alpha\ p(\alpha)e^{\alpha^\dagger\beta-\beta^\dagger\alpha}. \tag{3}$$

Here, because of the Fourier relation, $\lambda(\beta)$ with a large β contributes to rapidly oscillating $p(\alpha)$. Since the domain of β is infinite in principle, we will focus on a restricted finite domain specified later. The goal of our learning task is to learn the channel by estimating the characteristic function $\lambda(\beta)$. We emphasize that this is different from identifying a particular displacement that is drawn from the distribution $p(\alpha)$.

2.3 Entanglement-assisted scheme

Now, we present an entanglement-assisted scheme (see Fig. 1(a)). Consider an n-mode random displacement channel Λ_B acting on the n-mode system B. To learn this channel, we prepare n CV Bell states with a finite squeezing parameter r, which is a two-mode squeezed vacuum (TMSV) state, and half of the states go through the channel while the other half stays in quantum memory. Finally, we measure the output state by CV Bell measurement (BM), which can be implemented by passing through a 50:50 beam splitter and performing homodyne measurement on output ports along different quadratures. To see how to learn a random displacement channel using this TMSV+BM scheme, we invoke the probability of obtaining outcome ζ from BM:

$$p_{EA}(\zeta) = \frac{1}{\pi^{2n}}\int d^{2n}\alpha\ \lambda(\alpha)e^{-e^{-2r}|\alpha|^2}e^{\alpha^\dagger\zeta-\zeta^\dagger\alpha}. \tag{4}$$

Fourier transforming to invert this relation, we obtain

$$\lambda(\beta) = e^{e^{-2r}|\beta|^2}\int d^{2n}\zeta\ p_{EA}(\zeta)e^{\zeta^\dagger\beta-\beta^\dagger\zeta}. \tag{5}$$

This expression indicates that, by sampling N measurement outcomes $\{\zeta^{(i)}\}_{i=1}^N$ from a TMSV+BM scheme, one can obtain an unbiased estimator $\tilde{\lambda}(\beta)$ of $\lambda(\beta)$ by defining $\tilde{\lambda}(\beta) \equiv \frac{1}{N}e^{e^{-2r}|\beta|^2}\sum_{i=1}^N e^{\zeta^{(i)\dagger}\beta-\beta^\dagger\zeta^{(i)}}$. Note that the same set of samples can be used to estimate $\lambda(\beta)$ for different values of β just by modifying the estimator. Using the Hoeffding's bound, we prove the following theorem:

Theorem 1 *For any n-mode random displacement channel Λ, after the TMSV+BM scheme with squeezing parameter r has learned from N copies of Λ, and then received a query $\beta \in \mathbb{C}^n$, it can provide an estimator $\tilde{\lambda}(\beta)$ of Λ's characteristic function $\lambda(\beta)$ such that $|\tilde{\lambda}(\beta) - \lambda(\beta)| \leq \epsilon$ with probability at least $1-\delta$, with the number of samples $N = 8e^{2e^{-2r}|\beta|^2}\epsilon^{-2}\log 4\delta^{-1}$.*

Here, if we confine the domain of β to $|\beta|^2 \leq \kappa n$ with a constant $\kappa > 0$, we obtain an upper bound on the sample complexity for achieving an error ϵ with success probability $1-\delta$ using each scheme:

$$N_{EA} = O(e^{2e^{-2r}\kappa n}\epsilon^{-2}\log\delta^{-1}),. \tag{6}$$

In particular, if we choose the squeezing parameter as $r = \Omega(\log n)$, the sample complexity $N_{EA} = O(\epsilon^{-2}\log\delta^{-1})$ of the entanglement-assisted scheme becomes independent of the number of modes n, while our lower bound on sample complexity of the entanglement-free scheme increases exponentially with n (see below). Since the accessible squeezing parameter is bounded in practice, though, we will compare the sample complexities of the two schemes when r is an n-independent constant below.

2.4 Entanglement-free schemes

We now prove an exponential sample complexity lower bound for any entanglement-free scheme using information-theoretic methods. This highlights the indispensable role of entanglement for efficiently learning bosonic random displacement channels. Our result is as follows:

Theorem 2 *Let Λ be an arbitrary n-mode random displacement channel ($n \geq 8$) and consider an entanglement-free scheme that uses N copies of Λ. After all measurements are completed, the scheme receives the query $\beta \in \mathbb{C}^n$ and returns an estimate $\tilde{\lambda}(\beta)$ of Λ's characteristic function $\lambda(\beta)$. Suppose that, with success probability at least $2/3$, $|\tilde{\lambda}(\beta) - \lambda(\beta)| \leq \epsilon \leq 0.24$ for any β such that $|\beta|^2 \leq n\kappa$. Then $N \geq 0.01\epsilon^{-2}(1 + 1.98\kappa)^n$.*

Here, the success probability $2/3$ is arbitrary and can be easily amplified. Comparing with the sample complexity of the entanglement-assisted given in Eq. (6), Theorem 2 establishes an exponential separation in n for cutoff coefficient $\kappa = O(1)$ and squeezing parameter $r = \Omega(\log n)$. The intuition underlying this theorem is that displacement operators $\hat{D}(\beta)$ do not generally commute with each other. Consequently, entanglement-free measurements can resolve $\lambda(\beta)$ for only a small portion of β space.

The main idea of the proof of the theorem is (i) to define a family of "3-peak" random displacement channels $\mathbf{\Lambda}^{\epsilon,\sigma}_{\text{3-peak}} = \{\Lambda_\gamma\}_{\gamma \in \mathbb{C}^n}$ whose characteristic functions and distributions of displacement are, respectively,

$$\lambda_\gamma(\beta) = e^{-\frac{|\beta|^2}{2\sigma^2}} + 2i\epsilon_0 e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}} - 2i\epsilon_0 e^{-\frac{|\beta+\gamma|^2}{2\sigma^2}}, \qquad (7)$$

$$p_\gamma(\alpha) \propto e^{-2\sigma^2|\alpha|^2}\left(1 + 4\epsilon_0 \sin(2(\gamma_i\alpha_r - \gamma_r\alpha_i))\right), \qquad (8)$$

where $\sigma > 0$ and $\epsilon \equiv 0.98\epsilon_0$, and (ii) to consider a binary hypothesis testing of (1) $\Lambda = \Lambda_0$; (2) $\Lambda = \Lambda_\gamma$, for Gaussian random variable γ characterized by κ. Then, we can show that (iii) given a learning scheme satisfying the assumptions of Theorem 2, Bob can guess correctly with high probability. This means that the outcome distributions of Bob's scheme under hypotheses (1) and (2) must have a sufficiently large total variation distance (TVD). Finally, (iv) we can upper bound the contribution from each use of Λ to the TVD to be exponentially small. Therefore, the number of channel uses N must be exponentially large to ensure a large enough TVD, which gives us the desired lower bound.

2.5 Effect of loss

For practical applications, we analyze how the entanglement-assisted scheme is affected by photon loss, a dominant noise source in optical platforms. We consider two different places where the loss occurs: one is before applying the channel with loss rate $1-T_b$ to model the preparation imperfection, and the other is after applying the channel and before the perfect BM with loss rate $1 - T_a$, which models the finite efficiency of detection. As before, we derive the relation between the measurement probability distribution and the characteristic function of the channel:

$$\lambda(\beta) = e^{e^{-2r_{\text{eff}}}|\beta|^2} \int d^{2n}\zeta \; p_{loss}(\zeta) e^{(\zeta^\dagger\beta - \beta^\dagger\zeta)/\sqrt{T_a}}, \qquad (9)$$

where we define an effective squeezing parameter

$$r_{\text{eff}} \equiv -\frac{1}{2}\log\left(T_b e^{-2r} + (1 - T_b) + \frac{1 - T_a}{T_a}\right), \qquad (10)$$

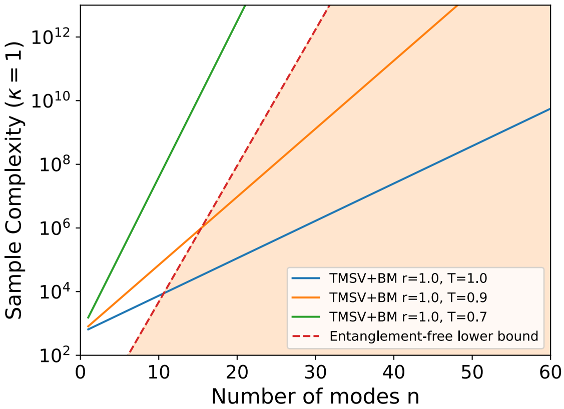


Figure 2: Comparison of TMSV+BM and the entanglement-free lower bound at $\kappa = 1$ for estimating any $\lambda(\beta)$ such that $|\beta|^2 \leq \kappa n$ with precision $\varepsilon = 0.2$ and success probability $1 - \delta = 2/3$. The orange region represents a rigorous advantage over all entanglement-free schemes.

which incorporates the loss rates. Because loss degrades the advantage from squeezing, the upper bound on sample complexity in Theorem 1 is modified as:

Theorem 3 *For the same task as in Theorem 1, a TMVS+BM scheme with squeezing parameter r and transmission rates before and after the channel to be T_b and T_a, respectively, can estimate any $\lambda(\beta)$ to error ϵ with success probability $1-\delta$ using the number of samples $N = 8e^{2e^{-2r_{\mathit{eff}}|\beta|^2}}\epsilon^{-2}\log 4\delta^{-1}$.*

Thus, when $|\beta|^2 \leq \kappa n$ with a constant $\kappa > 0$, $T_b = 1 - O(1/n)$, $T_a = 1 - O(1/n)$ and $r = \Omega(\log n)$, the sample complexity becomes $N = O(\epsilon^{-2}\log\delta^{-1})$ as in the lossless case. For practically relevant squeezing and including loss before BM, we compare the sample complexity for the lossy TMSV+BM protocol and the lossless entanglement-free lower bound in Fig. 2, finding a significant entanglement-enabled advantage in realistic experimental settings. Although the 10^9 number of samples required to achieve the advantage seems large, the state-of-the-art quantum optics experiments (e.g., Refs. [4, 5]) can attain such number of samples in a reasonable time with high sampling rate up to 160 GHz.

3 Discussion

We proved that schemes that exploit entanglement with an ancillary quantum memory can learn n-mode bosonic random displacement channels with exponentially fewer samples compared to entanglement-free schemes. Our results show that the information-theoretic framework for learning studied in DV quantum systems can be generalized to the CV setting and have powerful implications. We anticipate that these techniques can also be applied to other CV learning tasks. Besides generalizing other previous results known in DV systems, an interesting open question is to find a practical application of such an exponential advantage. We expect that it may have a direct connection to quantum sensing.

References

[1] H.-Y. Huang et al., Quantum advantage in learning from experiments, Science 376, 1182 (2022).

[2] S. Chen et al., Exponential separations between learning with and without quantum memory, in 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS) (IEEE, 2022) pp. 574–585.

[3] Y.-D. Wu et al., Quantum-enhanced learning of continuous-variable quantum states, arXiv:2303.05097 (2023).

[4] X. Guo et al., Distributed quantum sensing in a continuous-variable entangled network, Nature Physics 16, 281 (2020).

[5] A. Inoue et al., Toward a multi-core ultra-fast optical quantum processor: 43-ghz bandwidth real-time amplitude measurement of 5-db squeezed light using modularized optical parametric amplifier with 5g technology, Applied Physics Letters 122, 104001 (2023).

Entanglement-enabled advantage for learning a bosonic random displacement channel

Changhun Oh,[1, *] Senrui Chen,[1, *] Yat Wong,[1] Sisi Zhou,[2, 3, 4] Hsin-Yuan Huang,[3, 5, 6] Jens A.H. Nielsen,[7]
Zheng-Hao Liu,[7] Jonas S. Neergaard-Nielsen,[7] Ulrik L. Andersen,[7] Liang Jiang,[1, †] and John Preskill[3, ‡]

[1] *Pritzker School of Molecular Engineering, The University of Chicago, Chicago, Illinois 60637, USA*
[2] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[3] *Institute for Quantum Information and Matter,*
California Institute of Technology, Pasadena, CA 91125, USA
[4] *Department of Physics and Astronomy and Institute for Quantum Computing,*
University of Waterloo, Ontario N2L 2Y5, Canada
[5] *Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[6] *Google Quantum AI, Venice, CA, USA*
[7] *Center for Macroscopic Quantum States (bigQ),*
Department of Physics, Technical University of Denmark,
Building 307, Fysikvej, 2800 Kgs. Lyngby, Denmark

(Dated: March 1, 2024)

We show that quantum entanglement can provide an exponential advantage in learning properties of a bosonic continuous-variable (CV) system. The task we consider is estimating a probabilistic mixture of displacement operators acting on n bosonic modes, called a random displacement channel. We prove that if the n modes are not entangled with an ancillary quantum memory, then the channel must be sampled a number of times exponential in n in order to estimate its characteristic function to reasonable precision; this lower bound on sample complexity applies even if the channel inputs and measurements performed on channel outputs are chosen adaptively. On the other hand, we present a simple entanglement-assisted scheme that only requires a number of samples independent of n, given a sufficient amount of squeezing. This establishes an exponential separation in sample complexity. We then analyze the effect of photon loss and show that the entanglement-assisted scheme is still significantly more efficient than any lossless entanglement-free scheme under mild experimental conditions. Our work illuminates the role of entanglement in learning continuous-variable systems and points toward experimentally feasible demonstrations of provable entanglement-enabled advantage using CV quantum platforms.

Quantum science and technology holds promise to revolutionize how we understand and interact with nature, enabling computational speedups [1], classically impossible communication tasks [2, 3], and measurements with unprecedented sensitivity [4–6]. Rapid progress during the noisy intermediate-scale quantum (NISQ) era [7] has brought these promises closer to reality, but the challenge remains to demonstrate rigorous quantum advantage for practical problems.

Over the past few years, there has been ongoing theoretical and experimental progress in exploring quantum computational advantage [8–16]. Another recent line of research seeks quantum advantage in learning [17–24], revealing that access to quantum memory enables us to learn properties of nature more efficiently. Specifically, Refs. [18, 19] establish a framework for proving exponential separation in sample complexity between learning with and without a coherently controllable quantum memory. In contrast to its computational counterpart, this entanglement-enabled advantage in learning can be proven without invoking computational assumptions and can sometimes be more experimentally accessible. A proof-of-principle experiment has been conducted on Google's superconducting quantum processor using 40 qubits [18].

Most learning tasks studied so far are restricted to discrete-variable (DV) systems. It is natural to ask whether entanglement-enabled advantage can also be realized for learning properties of bosonic continuous-variable (CV) systems. This is particularly interesting and important because CV systems are ubiquitous in nature and have many applications in quantum information science, such as quantum sensing [6, 8, 25–27]. However, generalizing the results in DV systems to CV systems can be difficult because bosonic systems have infinite-dimensional Hilbert spaces, making it challenging to formulate rigorous results concerning the complexity of learning properties of these systems. Recent progress has been achieved in studies of entanglement-enhanced learning of CV-state characteristic functions [28]; however, the lower bounds obtained so far apply to a restricted class of learning strategies rather than to general entanglement-free schemes.

In this work, we rigorously establish an entanglement-enabled advantage in learning a probabilistic mixture of n-mode displacement operations, called a *bosonic random displacement channel*. Specifically, we show that any schemes without ancillary quantum memory require a number of samples exponential in n to learn the characteristic functions of the channel with reasonably good precision and high success probability. On the contrary, we present a simple scheme utilizing entanglement with ancillary quantum memory (*i.e.*, entanglement-assisted) that can complete the same learning task with a sample complexity independent of n, given access to two-mode squeezed vacuum (TMSV) states with sufficiently large squeezing parameter and Bell measurements (BM). This establishes an exponential separation between learning with and without entanglement in the bosonic system. The two learning scenarios are illustrated in Fig. 1. Note that our hardness results hold for arbitrarily high-energy input states and arbitrary measurements, while the presented entanglement-assisted scheme only requires a finite-energy TMSV and BM.

Furthermore, we analyze the robustness of this entanglement-enabled advantage under realistic experimental conditions. Specifically, we study the photon-loss effect, the most common noise source in optical platforms. Our results suggest that for squeezing parameters and loss rates achievable in a state-of-the-art bosonic experiment platform, the separation in sample complexity remains significant. Therefore, we anticipate that an experimental demonstration of entanglement-enabled advantage in CV quantum systems can be achieved in the near future.

Problem Setup.— We consider the task of learning an n-mode random displacement channel characterized by a probability distribution $p(\alpha)$ with $\alpha \in \mathbb{C}^n$, which transforms an input state $\hat{\rho}$ as

$$\Lambda(\hat{\rho}) = \int d^{2n}\alpha \; p(\alpha)\hat{D}(\alpha)\hat{\rho}\hat{D}^\dagger(\alpha), \tag{1}$$

where $\hat{D}(\alpha) := \otimes_{i=1}^n \hat{D}(\alpha_i)$ and $\hat{D}(\alpha_i) := \exp(\alpha_i\hat{a}_i^\dagger - \alpha_i^*\hat{a}_i)$ is the displacement operator for the ith mode. The random displacement channel can also be equivalently described by the characteristic function of $p(\alpha)$, *i.e.*, its Fourier transform, as (see SM S1 [29] for the derivation)

$$\Lambda(\hat{\rho}) = \frac{1}{\pi^n}\int d^{2n}\beta \; \lambda(\beta)\,\mathrm{Tr}[\hat{\rho}\hat{D}(\beta)]\hat{D}^\dagger(\beta), \tag{2}$$

$$\lambda(\beta) := \int d^{2n}\alpha \; p(\alpha)e^{\alpha^\dagger\beta - \beta^\dagger\alpha}. \tag{3}$$

Here, because of the Fourier relation, $\lambda(\beta)$ with a large β contributes to rapidly oscillating $p(\alpha)$. Since the domain of β is infinite in principle, we will focus on a restricted finite domain specified later. The goal is to learn the channel by estimating the characteristic function $\lambda(\beta)$. We emphasize that the goal is to characterize the channel, as opposed to identifying a particular displacement that is drawn from the distribution $p(\alpha)$. The value of β for which $\lambda(\beta)$ is to be estimated is revealed only after all measurements are completed.

We focus on the separation between two types of learning schemes for the random displacement channel distinguished by whether or not the scheme uses entanglement between the system and an ancilla, as illustrated in Fig. 1. Throughout this work, we define an entanglement-free scheme to be both ancilla-free and concatenation-free, i.e., the output of the channel is measured destructively after each channel use. However, the entanglement-free scheme is allowed to be adaptive; for each channel use, the input to the channel and the measurement performed on the output may depend on measurement outcomes obtained in earlier rounds. This scenario is similar to Refs. [17, 22]. Several recent works have obtained lower bounds on learning DV channels that hold even with concatenation [23, 30, 31], but we will not analyze the consequences of concatenating CV channels in this work for simplicity.

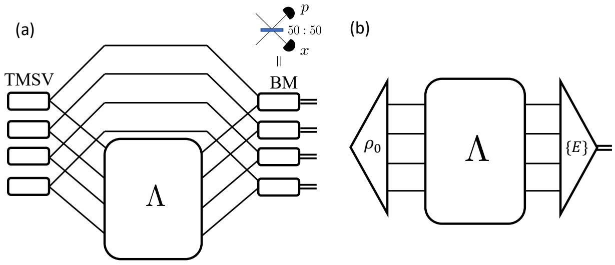


FIG. 1. Schemes for learning an n-mode random displacement channel Λ. (a) TMSV+BM, a specific entanglement-assisted (EA) scheme. (b) General entanglement-free (EF) scheme. Here we assume no concatenation is allowed, i.e., each copy of the channel acts on some input state ρ_0 and is measured destructively by some POVM $\{E\}$. The input state and measurement are allowed to be adaptively chosen depending on previous outcomes. An example of EF scheme is Vacuum+Heterodyne (see the main text).

Schemes.— Now, we present an entanglement-assisted scheme (see Fig. 1) inspired by a similar scheme to which has been proposed in DV Pauli channel estimation in Ref. [23]. Consider an n-mode random displacement channel Λ_B acting on the n-mode system B. To learn this channel, we prepare n CV Bell states with a finite squeezing parameter r, which is a two-mode squeezed vacuum (TMSV) state, and half of the states go through the channel while the other half stays in quantum memory. Finally, we measure the output state by CV Bell measurement (BM), which can be implemented by passing through a 50:50 beam splitter and performing homodyne measurement on output ports along different quadratures [27]. Formally, the BM POVM element labeled by $\{\zeta \in \mathbb{C}^n\}$ has the following form: $(I\otimes\hat{D}(\zeta))|\Psi\rangle\langle\Psi|(I\otimes\hat{D}^\dagger(\zeta))/\pi^n$; here $|\Psi\rangle$ denotes the tensor product of n infinitely squeezed TMSV states, each proportional to $\sum_{k=0}^\infty |k\rangle|k\rangle$ when expressed in the Fock basis. To see how to learn a random displacement channel using this TMSV+BM scheme, we invoke the probability of obtaining outcome ζ from BM (see SM S2 A [29] for the derivation):

$$p_{EA}(\zeta) = \frac{1}{\pi^{2n}}\int d^{2n}\alpha \; \lambda(\alpha)e^{-e^{-2r}|\alpha|^2}e^{\alpha^\dagger\zeta - \zeta^\dagger\alpha}. \tag{4}$$

Fourier transforming to invert this relation, we obtain

$$\begin{aligned}\lambda(\beta) &= e^{e^{-2r}|\beta|^2}\int d^{2n}\zeta\; p_{EA}(\zeta)e^{\zeta^\dagger\beta-\beta^\dagger\zeta} \\ &:= e^{e^{-2r}|\beta|^2}\lambda_{EA}(\beta).\end{aligned} \tag{5}$$

This expression indicates that, by sampling N measurement outcomes $\{\zeta^{(i)}\}_{i=1}^N$ from a TMSV+BM scheme, one can obtain an unbiased estimator $\tilde{\lambda}(\beta)$ of $\lambda(\beta)$ by defining $\tilde{\lambda}(\beta) := \frac{1}{N}e^{e^{-2r}|\beta|^2}\sum_{i=1}^N e^{\zeta^{(i)\dagger}\beta-\beta^\dagger\zeta^{(i)}}$. Note that the same set of samples can be used to estimate $\lambda(\beta)$ for different values of β just by modifying the estimator. Using the Hoeffding's bound, we prove the following theorem (see SM S2 A for the proof):

Theorem 1. *For any n-mode random displacement channel Λ, after the TMSV+BM scheme with squeezing parameter r has learned from N copies of Λ, and then received a query $\beta \in \mathbb{C}^n$, it can provide an estimator $\tilde{\lambda}(\beta)$ of Λ's characteristic function $\lambda(\beta)$ such that $|\tilde{\lambda}(\beta)-\lambda(\beta)| \le \epsilon$ with probability at least $1-\delta$, with the number of samples $N = 8e^{2e^{-2r}|\beta|^2}\epsilon^{-2}\log 4\delta^{-1}$.*

Let us compare the TMSV+BM scheme with a particular entanglement-free scheme that uses the vacuum state as input and heterodyne detection (Vacuum+Heterodyne). Here, heterodyne detection is defined as a projection onto the (overcomplete) basis of coherent states, i.e., $|\zeta\rangle\langle\zeta|/\pi^n$ with $\zeta \in \mathbb{C}^n$. Though it may not be the optimal entanglement-free scheme, this specific scheme helps us understand the limitations of entanglement-free schemes, which we capture more generally in Theorem 2 below.

In this scheme, the probability of obtaining POVM outcome ζ is (see SM S2 B [29])

$$p_{VH}(\zeta) = \frac{1}{\pi^{2n}}\int d^{2n}\alpha\; \lambda(\alpha)e^{\alpha^\dagger\zeta-\zeta^\dagger\alpha}e^{-|\alpha|^2}. \tag{6}$$

In fact, the Vacuum+Heterodyne scheme can be understood as the TMSV+BM scheme with $r=0$. Inverting this relation by Fourier transforming, we may express the channel's characteristic function in terms of the measurement probability distribution:

$$\lambda(\beta) = e^{|\beta|^2}\int d^{2n}\zeta\; p_{VH}(\zeta)e^{\zeta^\dagger\beta-\beta^\dagger\zeta} := e^{|\beta|^2}\lambda_{VH}(\beta), \tag{7}$$

which yields another unbiased estimator $\tilde{\lambda}(\beta) := \frac{1}{N}e^{|\beta|^2}\sum_{i=1}^N e^{\zeta^{(i)\dagger}\beta-\beta^\dagger\zeta^{(i)}}$ given N samples $\{\zeta^{(i)}\}_{i=1}^N$. Comparing to (5), we see that the r-dependent prefactor is missing from (7). Specifically, if we confine β to $|\beta|^2 \le \kappa n$ with a constant $\kappa > 0$, we obtain upper bounds on the sample complexity for achieving an error ϵ with success probability $1-\delta$ using each scheme:

$$N_{EA} = O(e^{2e^{-2r}\kappa n}\epsilon^{-2}\log\delta^{-1}), \tag{8}$$

$$N_{VH} = O(e^{2\kappa n}\epsilon^{-2}\log\delta^{-1}). \tag{9}$$

In particular, if we choose the squeezing parameter as $r = \Omega(\log n)$, the sample complexity $N_{EA} = O(\epsilon^{-2}\log\delta^{-1})$ of the entanglement-assisted scheme becomes independent of the number of modes n, while our upper bound on sample complexity of the entanglement-free scheme increases exponentially with n. Since the accessible squeezing parameter is bounded in practice, though, we will compare the sample complexities of the two schemes when r is an n-independent constant below.

To illustrate the difference, we compare TMSV+BM and Vacuum+Heterodyne strategies with an example in Fig. 2. We consider a single-mode channel for ease of visualization, characterized by

$$\begin{aligned}p(\alpha) = \frac{2\sigma^2}{\pi}e^{-2\sigma^2|\alpha|^2}[&\cos^2(\alpha_r\gamma_i-\alpha_i\gamma_r) \\ &+\sin^2(\alpha_r\gamma_r+\alpha_i\gamma_i)],\end{aligned} \tag{10}$$

$$\begin{aligned}\lambda(\beta) = e^{-\frac{|\beta|^2}{2\sigma^2}} &+ \frac{1}{4}e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}} + \frac{1}{4}e^{-\frac{|\beta+\gamma|^2}{2\sigma^2}} \\ &- \frac{1}{4}e^{-\frac{|\beta-i\gamma|^2}{2\sigma^2}} - \frac{1}{4}e^{-\frac{|\beta+i\gamma|^2}{2\sigma^2}},\end{aligned} \tag{11}$$

with $\sigma = 0.3$, $\gamma_r = 1.6$, $\gamma_i = 0$ ($\gamma := \gamma_r + i\gamma_i$), and $r = 2$ for the TMSV+BM scheme. The figure, where we present the underlying output probability distributions and their characteristic functions from Eqs. (4),(5),(6), and (7), clearly shows that in the TMSV+BM scheme with a sufficiently large squeezing parameter, the resultant probability distribution and characteristic function are almost identical to the ideal case. However, for the Vacuum+Heterodyne scheme, the vacuum noise distorts the initial probability distribution so significantly that we cannot see the signal clearly, which thus makes it harder to estimate the original characteristic function.

Lower bound.— Our upper bound on the sample complexity of the Vacuum+Heterodyne scheme scales exponentially with n. Can this scaling be improved using more advanced entanglement-free schemes, such as homodyne or general-dyne detection [27, 32], or by non-Gaussian resources like GKP states [33] or photon-number resolving measurements [34]? Here, using information-theoretic methods, we prove an exponential sample complexity lower bound for any entanglement-free scheme. This highlights the indispensable role of entanglement for efficiently learning bosonic random displacement channels. Our result is as follows:

Theorem 2. *Let Λ be an arbitrary n-mode random displacement channel ($n \ge 8$) and consider an entanglement-free scheme that uses N copies of Λ. After all measurements are completed, the scheme receives the query $\beta \in \mathbb{C}^n$ and returns an estimate $\tilde{\lambda}(\beta)$ of Λ's characteristic function $\lambda(\beta)$. Suppose that, with success probability at least 2/3, $|\tilde{\lambda}(\beta)-\lambda(\beta)| \le \epsilon \le 0.24$ for all β such that $|\beta|^2 \le n\kappa$. Then $N \ge 0.01\epsilon^{-2}(1+1.98\kappa)^n$.*

Here, the choice of success probability 2/3 is arbitrary and can be easily amplified. Comparing with the

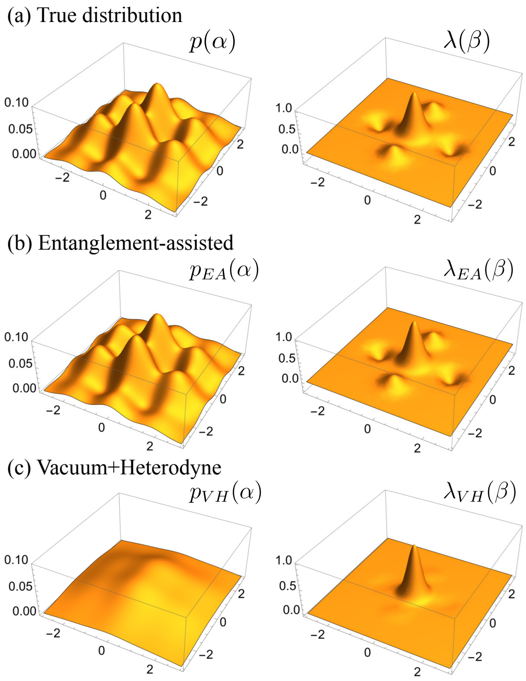


FIG. 2. Comparison between (a) the true distribution, (b) TMSV+BM, and (c) Vacuum+Heterodyne strategies. The left panel represents the probability distribution of the true distribution and measurement probability distributions for each scheme. The right panel represents the characteristic function of probability distributions.

entanglement-assisted sample complexity given in Eq. (8), Theorem 2 establishes a separation exponential in n for cutoff coefficient $\kappa = O(1)$ and squeezing parameter $r = \Omega(\log n)$. The intuition underlying this theorem is that displacement operators $\hat{D}(\beta)$ do not generally commute with each other. Consequently, entanglement-free measurements can resolve $\lambda(\beta)$ for only a small portion of β space. We sketch the proof below and leave the full details to SM S3 [29].

Proof Sketch. Our proof extends the techniques of Refs. [18, 23] to the CV case. We begin by defining the following family of "3-peak" random displacement channels $\mathbf{\Lambda}^{\epsilon,\sigma}_{\text{3-peak}} = \{\Lambda_\gamma\}_{\gamma\in\mathbb{C}^n}$ whose characteristic functions and distributions of displacement are, respectively,

$$\lambda_\gamma(\beta) = e^{-\frac{|\beta|^2}{2\sigma^2}} + 2i\epsilon_0 e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}} - 2i\epsilon_0 e^{-\frac{|\beta+\gamma|^2}{2\sigma^2}}, \qquad (12)$$

$$p_\gamma(\alpha) \propto e^{-2\sigma^2|\alpha|^2}\left(1 + 4\epsilon_0 \sin(2(\gamma_i\alpha_r - \gamma_r\alpha_i))\right). \qquad (13)$$

with positive parameters σ and $\epsilon := 0.98\epsilon_0$. We will show that, even with the prior knowledge that the channel is from this family, it is still hard for entanglement-free schemes to complete the learning tasks.

The key idea is to reduce learning to binary hypothesis testing. Consider the following game between Alice and Bob: Alice chooses one of two hypotheses with equal probability: (1) Set $\Lambda = \Lambda_0$; (2) Set $\Lambda = \Lambda_\gamma$, for γ sampled from a zero-mean homogeneous Gaussian distribution whose variance is determined by κ. Next, Alice allows Bob to use the channel Λ N times, and Bob uses his favorite entanglement-free scheme to learn from these channel uses. After Bob has finished all quantum measurements and keeps only classical data, Alice reveals some auxiliary information to Bob, who is then asked to decide whether Alice has chosen (1) or (2).

Given a learning scheme satisfying the assumptions of Theorem 2, Bob can guess correctly with high probability. This means that the outcome distributions of Bob's scheme under hypotheses (1) and (2) must have a sufficiently large total variation distance (TVD). On the other hand, we can upper bound the contribution from each use of Λ to the TVD to be exponentially small, where we use a technique inspired by Ref. [35] which derived the maximum fidelity of Gaussian random displacement channels. Therefore, the number of channel uses N must be exponentially large to ensure a large enough TVD, which gives us the desired lower bound. □

Effect of loss.— Now, for practical applications, we study how the entanglement-assisted scheme is affected by photon loss, a dominant noise source in optical platforms (see SM S2 D for a discussion of more general noise models, such as phase diffusion). Photon loss transforms the relevant bosonic operator $\hat{a}$ to $\sqrt{T}\hat{a} + \sqrt{1-T}\hat{e}$, where T is the transmission rate and $\hat{e}$ is the environmental mode, i.e., $1-T$ is the loss rate. We consider two different places where the loss occurs: one is before applying the channel with loss rate $1-T_b$ to model the preparation imperfection, and the other is after applying the channel and before the perfect BM with loss rate $1-T_a$, which models the finite efficiency of detection, *i.e.*, an imperfect BM [27]. As before, we derive the relation between the measurement probability distribution and the characteristic function of the channel (with appropriate rescaling of the phase):

$$\lambda(\beta) = e^{e^{-2r_{\text{eff}}}|\beta|^2} \int d^{2n}\zeta\; p_{loss}(\zeta) e^{(\zeta^\dagger\beta - \beta^\dagger\zeta)/\sqrt{T_a}}, \qquad (14)$$

where we define an effective squeezing parameter

$$r_{\text{eff}} := -\frac{1}{2}\log\left(T_b e^{-2r} + (1-T_b) + \frac{1-T_a}{T_a}\right), \qquad (15)$$

which incorporates the loss rates. Because loss degrades the advantage from squeezing, the upper bound on sample complexity in Theorem 1 is modified in the presence of loss (see SM S2 C for the proof):

Theorem 3. *For the same task as in Theorem 1, a TMVS+BM scheme with squeezing parameter r and transmission rates before and after the channel to be T_b and T_a, respectively, can estimate any $\lambda(\beta)$ to error ϵ with success probability $1-\delta$ using the number of samples*

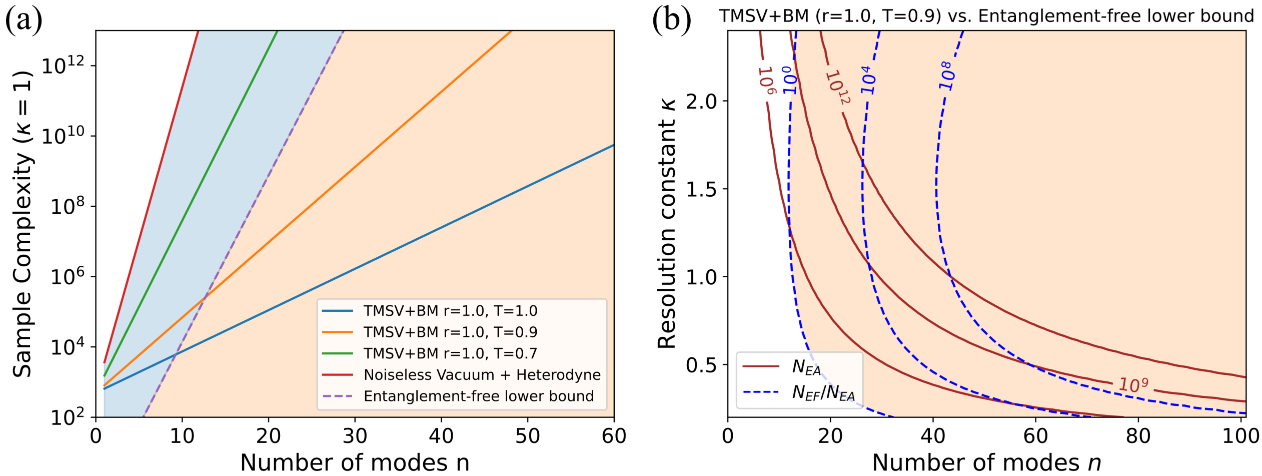


FIG. 3. (a) Comparison of TMSV+BM (with different loss rates), Vacuum+Heterodyne, and the entanglement-free lower bound at $\kappa = 1$. The task is to estimate any $\lambda(\beta)$ such that $|\beta|^2 \le \kappa n$ with precision $\varepsilon = 0.2$ and success probability $1 - \delta = 2/3$. The orange region represents a rigorous advantage over all entanglement-free schemes. The blue region represents an advantage over noiseless Vacuum+Heterodyne. (b) Comparison of the TMSV+BM scheme with squeezing parameter $r = 1.0$ and loss rate $1 - T = 0.1$ with the entanglement-free lower bound of Theorem 2. (See SM S3 A for further practical considerations.) The task is the same as (a). The brown solid contour lines represent the sample complexity of TMSV+BM given by Theorem 3. The blue dashed contour lines represent the ratio of sample complexity between the entanglement-free lower bound and TMSV+BM, indicating the entanglement-enabled advantage.

$N = 8e^{2e^{-2r_{\mathit{eff}}|\beta|^2}}\epsilon^{-2}\log 4\delta^{-1}$, *where* $r_{\rm eff}$ *is defined according to Eq.* (15).

Thus, when $|\beta|^2 \le \kappa n$ with a constant $\kappa > 0$, $T_b = 1 - O(1/n)$, $T_a = 1 - O(1/n)$ and $r = \Omega(\log n)$, the sample complexity becomes $N = O(\epsilon^{-2}\log\delta^{-1})$ as in the lossless case. For practically relevant squeezing and including loss prior to Bell measurement, we compare the sample complexity for the lossy TMSV+BM protocol and the lossless entanglement-free lower bound in Fig. 3, finding a significant entanglement-enabled advantage in realistic experimental settings. Specifically, for reasonable parameter choices such as squeezing parameter $r = 1$, loss rate 10%, and $\kappa = O(1)$, we can achieve a factor of 10^4 (10^8) advantage for around $n = 30$ (60) modes. Although the 10^9 number of samples required to achieve the advantage seems large, the state-of-the-art quantum optics experiments (e.g., Refs. [36, 37]) can attain such number of samples in a reasonable time with high sampling rate up to 160 GHz.

Discussion.— We proved that schemes that exploit entanglement with an ancillary quantum memory can learn n-mode bosonic random displacement channels with exponentially fewer samples compared to entanglement-free schemes. Our results show that the information-theoretic framework for learning studied in DV quantum systems [17, 19] can be generalized to the CV setting and have powerful implications. We anticipate that these techniques can be applied to other CV learning tasks as well. In addition, our analysis suggests that the separation in sample complexity between entanglement-assisted and entanglement-free protocols may be realized in the near future.

Apart from their theoretical interest, random displacement channels can also be practically relevant in, *e.g.*, modeling noise in bosonic systems. As in the qubit case [38], we expect that noise tailoring methods can transform more general noise models into random displacement channels; therefore efficiently learning random displacement channels can be useful for benchmarking CV quantum systems [39, 40] and for error mitigation.

Displacement estimation is also studied in quantum metrology (see *e.g.* [41–43]). A task often considered in metrology is learning an unknown *unitary* displacement or phase transformation acting independently on each mode [36, 42, 44–47] whereas the task analyzed in this word is learning an unknown *mixture* of multimode displacements. Furthermore, while the goal in metrology is typically to learn one or a few parameters, in our case, the parameter space is very large. Therefore, the methodology in the two settings is quite different. Connections between metrology and bosonic channel learning are worthy of further exploration.

We thank Mankei Tsang, Yuxin Wang, Ronald de Wolf, Mingxing Yao, Ming Yuan for insightful discussions. C.O., S.C., Y.W., L.J. acknowledge support from the ARO(W911NF-23-1-0077), ARO MURI (W911NF-21-1-0325), AFOSR MURI (FA9550-19-1-0399, FA9550-21-1-0209), NSF (OMA-1936118, ERC-1941583, OMA-2137642), NTT Research, Packard Foundation (2020-71479). J.P. acknowledges support from the U.S. Department of Energy Office of Science, Office of Advanced Scientific Computing Research (DE-NA0003525, DE-SC0020290), the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator, and the National Science Foundation (PHY-1733907). The Institute for Quantum Information and Matter is an NSF Physics Frontiers Center. S.Z. acknowledges funding provided by the Institute for Quantum Information and Matter and Perimeter Institute for Theoretical Physics, a research institute supported in part by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Colleges and Universities. J.A.H.N, Z.L., J.S.N and U.L.A acknowledge support from DNRF (bigQ, DNRF142), IFD (photoQ) and EU (CLUSTEC, ClusterQ ERC-101055224, GTGBS MC-101106833).

* These authors contributed equally to this work: C.O. (changhun0218@gmail.com); S.C. (csenrui@uchicago.edu).

† liang.jiang@uchicago.edu

‡ preskill@caltech.edu

[1] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (2002).

[2] N. Gisin and R. Thew, Quantum communication, Nature photonics **1**, 165 (2007).

[3] H. J. Kimble, The quantum internet, Nature **453**, 1023 (2008).

[4] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum metrology, Physical review letters **96**, 010401 (2006).

[5] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nature photonics **5**, 222 (2011).

[6] E. Polino, M. Valeri, N. Spagnolo, and F. Sciarrino, Photonic quantum metrology, AVS Quantum Science **2**, 024703 (2020).

[7] J. Preskill, Quantum computing in the NISQ era and beyond, Quantum **2**, 79 (2018).

[8] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the forty-third annual ACM symposium on Theory of computing* (2011) pp. 333–342.

[9] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, Nature Physics **14**, 595 (2018).

[10] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, Quantum supremacy using a programmable superconducting processor, Nature **574**, 505 (2019).

[11] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, *et al.*, Strong quantum computational advantage using a superconducting quantum processor, Physical review letters **127**, 180501 (2021).

[12] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, *et al.*, Quantum computational advantage using photons, Science **370**, 1460 (2020).

[13] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, *et al.*, Phase-programmable Gaussian boson sampling using stimulated squeezed light, Physical review letters **127**, 180502 (2021).

[14] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, *et al.*, Quantum computational advantage with a programmable photonic processor, Nature **606**, 75 (2022).

[15] A. Morvan, B. Villalonga, X. Mi, S. Mandra, A. Bengtsson, P. Klimov, Z. Chen, S. Hong, C. Erickson, I. Drozdov, *et al.*, Phase transition in random circuit sampling, arXiv preprint arXiv:2304.11119 (2023).

[16] Y.-H. Deng, Y.-C. Gu, H.-L. Liu, S.-Q. Gong, H. Su, Z.-J. Zhang, H.-Y. Tang, M.-H. Jia, J.-M. Xu, M.-C. Chen, J. Qin, L.-C. Peng, J. Yan, Y. Hu, J. Huang, H. Li, Y. Li, Y. Chen, X. Jiang, L. Gan, G. Yang, L. You, L. Li, H.-S. Zhong, H. Wang, N.-L. Liu, J. J. Renema, C.-Y. Lu, and J.-W. Pan, Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage, Phys. Rev. Lett. **131**, 150601 (2023).

[17] H.-Y. Huang, R. Kueng, and J. Preskill, Information-theoretic bounds on quantum advantage in machine learning, Physical Review Letters **126**, 190505 (2021).

[18] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Quantum advantage in learning from experiments, Science **376**, 1182 (2022).

[19] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, Exponential separations between learning with and without quantum memory, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2022) pp. 574–585.

[20] M. C. Caro, Learning quantum processes and hamiltonians via the pauli transfer matrix, arXiv preprint arXiv:2212.04471 (2022).

[21] S. Bubeck, S. Chen, and J. Li, Entanglement is necessary for optimal quantum property testing, in *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2020) pp. 692–703.

[22] D. Aharonov, J. Cotler, and X.-L. Qi, Quantum algorithmic measurement, Nature communications **13**, 1 (2022).

[23] S. Chen, S. Zhou, A. Seif, and L. Jiang, Quantum advantages for pauli channel estimation, Phys. Rev. A **105**, 032435 (2022).

[24] Z. M. Rossi, J. Yu, I. L. Chuang, and S. Sugiura, Quantum advantage for noisy channel discrimination, Physical Review A **105**, 032401 (2022).

[25] S. L. Braunstein and P. Van Loock, Quantum information with continuous variables, Reviews of modern physics **77**, 513 (2005).

[26] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Reviews of Modern Physics **84**, 621 (2012).

[27] A. Serafini, *Quantum continuous variables: a primer of theoretical methods* (CRC press, 2017).

[28] Y.-D. Wu, G. Chiribella, and N. Liu, Quantum-enhanced learning of continuous-variable quantum states, arXiv preprint arXiv:2303.05097 (2023).

[29] Supplemental material.

[30] S. Chen and W. Gong, Futility and utility of a few ancillas for pauli channel learning, arXiv preprint arXiv:2309.14326 (2023).

[31] S. Chen, C. Oh, S. Zhou, H.-Y. Huang, and L. Jiang, Tight bounds on pauli channel learning without entanglement, arXiv preprint arXiv:2309.13461 (2023).

[32] W. P. Schleich, *Quantum optics in phase space* (John Wiley & Sons, 2011).

[33] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, Physical Review A **64**, 012310 (2001).

[34] D. Schuster, A. A. Houck, J. Schreier, A. Wallraff, J. Gambetta, A. Blais, L. Frunzio, J. Majer, B. Johnson, M. Devoret, *et al.*, Resolving photon number states in a superconducting circuit, Nature **445**, 515 (2007).

[35] C. M. Caves and K. Wódkiewicz, Fidelity of gaussian channels, Open Systems & Information Dynamics **11**, 309 (2004).

[36] X. Guo, C. R. Breum, J. Borregaard, S. Izumi, M. V. Larsen, T. Gehring, M. Christandl, J. S. Neergaard-Nielsen, and U. L. Andersen, Distributed quantum sensing in a continuous-variable entangled network, Nature Physics **16**, 281 (2020).

[37] A. Inoue, T. Kashiwazaki, T. Yamashima, N. Takanashi, T. Kazama, K. Enbutsu, K. Watanabe, T. Umeki, M. Endo, and A. Furusawa, Toward a multi-core ultra-fast optical quantum processor: 43-ghz bandwidth real-time amplitude measurement of 5-db squeezed light using modularized optical parametric amplifier with 5g technology, Applied Physics Letters **122**, 104001 (2023).

[38] J. J. Wallman and J. Emerson, Noise tailoring for scalable quantum computation via randomized compiling, Physical Review A **94**, 052325 (2016).

[39] Y.-D. Wu and B. C. Sanders, Efficient verification of bosonic quantum channels via benchmarking, New Journal of Physics **21**, 073026 (2019).

[40] G. Bai and G. Chiribella, Test one to test many: a unified approach to quantum benchmarks, Physical Review Letters **120**, 150502 (2018).

[41] H. Shi and Q. Zhuang, Ultimate precision limit of noise sensing and dark matter search, npj Quantum Information **9**, 27 (2023).

[42] Q. Zhuang, Z. Zhang, and J. H. Shapiro, Distributed quantum sensing using continuous-variable multipartite entanglement, Physical Review A **97**, 032329 (2018).

[43] Y. Xia, W. Li, W. Clark, D. Hart, Q. Zhuang, and Z. Zhang, Demonstration of a reconfigurable entangled radio-frequency photonic sensor network, Physical Review Letters **124**, 150502 (2020).

[44] K. Duivenvoorden, B. M. Terhal, and D. Weigand, Single-mode displacement sensor, Physical Review A **95**, 012305 (2017).

[45] C. Oh, C. Lee, S. H. Lie, and H. Jeong, Optimal distributed quantum sensing using gaussian states, Physical Review Research **2**, 023030 (2020).

[46] C. Oh, L. Jiang, and C. Lee, Distributed quantum phase sensing for arbitrary positive and negative weights, Physical Review Research **4**, 023164 (2022).

[47] H. Kwon, Y. Lim, L. Jiang, H. Jeong, and C. Oh, Quantum metrological power of continuous-variable quantum networks, Physical Review Letters **128**, 180503 (2022).

Entanglement-enabled advantage for learning a bosonic random displacement channel: Supplemental Material

Changhun Oh,[1,*] Senrui Chen,[1,*] Yat Wong,[1] Sisi Zhou,[2,3,4]
Hsin-Yuan Huang,[3,5,6] Jens A.H. Nielsen,[7] Zheng-Hao Liu,[7] Jonas S. Neergaard-Nielsen,[7] Ulrik L. Andersen,[7] Liang Jiang,[1,†] and John Preskill[3,‡]

[1] *Pritzker School of Molecular Engineering, The University of Chicago, Chicago, Illinois 60637, USA*
[2] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[3] *Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA 91125, USA*
[4] *Department of Physics and Astronomy and Institute for Quantum Computing, University of Waterloo, Ontario N2L 2Y5, Canada*
[5] *Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[6] *Google Quantum AI, Venice, CA, USA*
[7] *Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, Building 307, Fysikvej, 2800 Kgs. Lyngby, Denmark*

(Dated: March 1, 2024)

CONTENTS

S1. PRELIMINARY

In this section, we provide some identities that are frequently used in Supplemental Material (more details can be found in Refs. [1–3]). First, an elementary operator in n-mode bosonic system is n-mode displacement operator $\hat{D}(\beta) \coloneqq e^{\beta\hat{a}^\dagger - \beta^\dagger\hat{a}}$, where $\beta \coloneqq (\beta_1, \dots, \beta_n)^{\mathrm{T}} \in \mathbb{C}^n$, $\hat{a} \coloneqq$

[*] These authors contributed equally to this work: C.O. (changhun0218@gmail.com); S.C. (csenrui@uchicago.edu).
[†] liang.jiang@uchicago.edu
[‡] preskill@caltech.edu

$(\hat{a}_1, \dots, \hat{a}_n)^{\mathrm{T}}$ and $\hat{a}^\dagger \coloneqq (\hat{a}_1^\dagger, \dots, \hat{a}_n^\dagger)^{\mathrm{T}}$ are annihilation and creation operator of bosons, which follow the commutation relation $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$. Displacement operator $\hat{D}(\beta)$ forms an orthogonal basis in the operator space; thus, any operator $\hat{O}$ can be expanded by displacement operators as

$$\hat{O} = \frac{1}{\pi^n} \int d^{2n}\beta \, \mathrm{Tr}\Big[\hat{O}\hat{D}(\beta)\Big] \hat{D}^\dagger(\beta), \tag{S1}$$

where $\mathrm{Tr}[\hat{O}\hat{D}(\beta)]$ is called the characteristic function of an operator $\hat{O}$. The n-mode displacement operator has the following properties

$$\hat{D}^\dagger(\beta) = \hat{D}(-\beta), \quad \hat{D}^*(\beta) = \hat{D}(\beta^*), \quad \hat{D}^{\mathrm{T}}(\beta) = \hat{D}(-\beta^*), \quad \mathrm{Tr}\Big[\hat{D}(\beta)\Big] = \pi^n \delta^{(2n)}(\beta), \tag{S2}$$

$$\hat{D}(\beta_1)\hat{D}(\beta_2) = \hat{D}(\beta_1 + \beta_2) e^{(\beta_2^\dagger \beta_1 - \beta_1^\dagger \beta_2)/2}, \quad \hat{D}(\alpha)\hat{D}^\dagger(\beta)\hat{D}^\dagger(\alpha) = \hat{D}^\dagger(\beta) e^{\alpha^\dagger \beta - \beta^\dagger \alpha}, \tag{S3}$$

$$\int \frac{d^{2n}\beta}{\pi^n} \hat{D}(\beta) O \hat{D}^\dagger(\beta) = \mathrm{Tr}[O]\mathbb{1}, \tag{S4}$$

where the last identity is the twirling identity. We also frequently use the following identity:

$$\delta^{(2n)}(\alpha) = \frac{1}{\pi^{2n}} \int d^{2n}\beta e^{\beta^\dagger \alpha - \alpha^\dagger \beta}. \tag{S5}$$

Also, we employ the Wigner function of an operator $\hat{O}$ defined as

$$W_O(\alpha) = \frac{1}{\pi^{2n}} \int d^{2n}\beta \, \mathrm{Tr}\Big[\hat{O}\hat{D}(\beta)\Big] e^{\beta^\dagger \alpha - \alpha^\dagger \beta}. \tag{S6}$$

In Sec. S1 A, we show that for a given random displacement channel, which is defined by the probability distribution $p(\alpha)$, we can rewrite it by the Fourier transformation $\lambda(\beta)$ of $p(\alpha)$, i.e., its characteristic function, as

$$\Lambda(\hat{\rho}) \coloneqq \int d^{2n}\alpha p(\alpha) \hat{D}(\alpha) \hat{\rho} \hat{D}^\dagger(\alpha) = \frac{1}{\pi^n} \int d^{2n}\beta \lambda(\beta) \, \mathrm{Tr}\Big[\hat{\rho}\hat{D}(\beta)\Big] \hat{D}^\dagger(\beta), \tag{S7}$$

where the probability $p(\alpha)$ and the characteristic function $\lambda(\beta)$ follow the relation

$$\lambda(\beta) = \int d^{2n}\alpha \; p(\alpha) e^{\alpha^\dagger \beta - \beta^\dagger \alpha}, \quad p(\alpha) = \frac{1}{\pi^{2n}} \int d^{2n}\beta \; \lambda(\beta) e^{\beta^\dagger \alpha - \alpha^\dagger \beta}. \tag{S8}$$

A. Fourier relation

Here, we derive the expression of a random displacement channel characterized by a probability distribution $p(\alpha)$ by its characteristic function $\lambda(\beta)$. To see the relation, we use the identity (S1). Applying this for the density operator $\hat{\rho}$, we can show that

$$\Lambda(\hat{\rho}) = \int d^{2n}\alpha p(\alpha) \hat{D}(\alpha) \hat{\rho} \hat{D}^\dagger(\alpha) = \int d^{2n}\alpha p(\alpha) \hat{D}(\alpha) \left[\frac{1}{\pi^n} \int d^{2n}\beta \, \mathrm{Tr}\Big[\hat{\rho}\hat{D}(\beta)\Big] \hat{D}^\dagger(\beta)\right] \hat{D}^\dagger(\alpha) \tag{S9}$$

$$= \frac{1}{\pi^n} \int d^{2n}\alpha \int d^{2n}\beta p(\alpha) \, \mathrm{Tr}\Big[\hat{\rho}\hat{D}(\beta)\Big] \hat{D}(\alpha) \hat{D}^\dagger(\beta) \hat{D}^\dagger(\alpha) \tag{S10}$$

$$= \frac{1}{\pi^n} \int d^{2n}\alpha \int d^{2n}\beta p(\alpha) \, \mathrm{Tr}\Big[\hat{\rho}\hat{D}(\beta)\Big] \hat{D}^\dagger(\beta) e^{\alpha^\dagger \beta - \beta^\dagger \alpha} \tag{S11}$$

$$= \frac{1}{\pi^n} \int d^{2n}\beta \lambda(\beta) \, \mathrm{Tr}\Big[\hat{\rho}\hat{D}(\beta)\Big] \hat{D}^\dagger(\beta), \tag{S12}$$

where we used the identities from Eqs. (S3),(S5). Here, the last line renders the identity

$$\lambda(\beta) = \int d^{2n}\alpha p(\alpha) e^{\alpha^\dagger\beta - \beta^\dagger\alpha}. \tag{S13}$$

Thus, $\lambda(\beta)$ is the Fourier transform of $p(\alpha)$. Its inverse Fourier transformation gives

$$p(\alpha) = \frac{1}{\pi^{2n}} \int d^{2n}\beta \lambda(\beta) e^{\beta^\dagger\alpha - \alpha^\dagger\beta}. \tag{S14}$$

S2. DERIVATION OF OUTPUT PROBABILITY DISTRIBUTIONS OF EACH SCHEME

A. Entanglement-assisted (TMSV+BM) schemes

In this section, we consider the two-mode squeezed vacuum and Bell measurement (TMSV+BM) strategy (see Fig. 1(a) in the main text.) and prove Theorem 1 in the main text by deriving the sample complexity of the strategy. We assume a lossless system and a perfect Bell measurement, whereas the input squeezed state has a finite squeezing parameter r since the input squeezing parameter r is typically upper-bounded by a constant in practice. We then analyze the effect of the imperfect measurement and loss in Sec. S2 C.

We now derive the probability of outcomes of the strategy, i.e., the outcomes obtained by applying an n-mode channel Λ onto a product state of a subsystem of n TMSV states $|\tilde{\Psi}\rangle$ and measuring in the Bell basis $|\Psi(\zeta)\rangle\langle\Psi(\zeta)|/\pi^n$ with $\zeta \in \mathbb{C}^n$:

$$p_{EA}(\zeta) = \frac{1}{\pi^n} \operatorname{Tr}\Big[(|\Psi(\zeta)\rangle\langle\Psi(\zeta)|_{AB})(\mathcal{I}_A \otimes \Lambda_B)(|\tilde{\Psi}\rangle\langle\tilde{\Psi}|_{AB})\Big]. \tag{S15}$$

To simplify the expression, we rewrite a TMSV state. To do that, let us first consider a single-mode squeezed state $|r\rangle := \hat{S}(r)|0\rangle$:

$$|r\rangle\langle r| = \frac{1}{\pi}\int d^2\alpha \hat{D}^\dagger(\alpha) \operatorname{Tr}\Big[\hat{D}(\alpha)|r\rangle\langle r|\Big] := \frac{1}{\pi}\int d^2\alpha \hat{D}^\dagger(\alpha) f(\alpha, r), \tag{S16}$$

where $\hat{S}(r) := \exp\Big[r(\hat{a}^{\dagger 2} - \hat{a}^2)/2\Big]$ is the squeezing operation and we have defined

$$f(\alpha, r) := \operatorname{Tr}\Big[\hat{D}(\alpha)|r\rangle\langle r|\Big] = \langle 0|\hat{S}^\dagger(r)\hat{D}(\alpha)\hat{S}(r)|0\rangle = \langle 0|\hat{D}(\alpha\cosh r - \alpha^*\sinh r)|0\rangle \tag{S17}$$

$$= \exp\left(-\frac{1}{2}|\alpha\cosh r - \alpha^*\sinh r|^2\right). \tag{S18}$$

Here, we have used the relation, $\hat{S}^\dagger(r)\hat{a}\hat{S}(r) = \hat{a}\cosh r + \hat{a}^\dagger \sinh r$. Using the fact that a TMSV state can be generated by injecting two single-mode squeezed states into the 50:50 beam splitter, i.e., $\hat{U}_{\rm BS}(|r\rangle\langle r| \otimes |-r\rangle\langle -r|)\hat{U}_{\rm BS}^\dagger = |\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)|$, where $\hat{U}_{\rm BS}$ is 50:50 beam splitter, we can rewrite the TMSV state $|\tilde{\Psi}(r)\rangle$ as

$$|\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)| = \frac{1}{\pi^2}\int d^2\alpha_1 d^2\alpha_2 \hat{U}_{\rm BS}[\hat{D}^\dagger(\alpha_1)\otimes\hat{D}^\dagger(\alpha_2)]\hat{U}_{\rm BS}^\dagger f(\alpha_1, r) f(\alpha_2, -r) \tag{S19}$$

$$= \frac{1}{\pi^2}\int d^2\alpha_1 d^2\alpha_2 \hat{D}^\dagger\left(\frac{\alpha_1-\alpha_2}{\sqrt{2}}\right)\otimes\hat{D}^\dagger\left(\frac{\alpha_1+\alpha_2}{\sqrt{2}}\right) f(\alpha_1, r) f(\alpha_2, -r) \tag{S20}$$

$$= \frac{1}{\pi^2}\int d^2\omega_1 d^2\omega_2 \hat{D}^\dagger(\omega_1)\otimes\hat{D}^\dagger(\omega_2) f\left(\frac{\omega_1+\omega_2}{\sqrt{2}}, r\right) f\left(\frac{\omega_2-\omega_1}{\sqrt{2}}, -r\right) \tag{S21}$$

$$:= \frac{1}{\pi^2}\int d^2\omega_1 d^2\omega_2 \hat{D}^\dagger(\omega_1)\otimes\hat{D}^\dagger(\omega_2) g(w_1, w_2, r), \tag{S22}$$

where we defined

$$g(\omega_1,\omega_2,r) := f\left(\frac{\omega_1+\omega_2}{\sqrt{2}},r\right) f\left(\frac{\omega_2-\omega_1}{\sqrt{2}},-r\right) \tag{S23}$$

$$= \exp\left[-\frac{1}{2}\Big[(|\omega_1|^2+|\omega_2|^2)\cosh 2r - (\omega_1\omega_2+\omega_1^*\omega_2^*)\sinh 2r\Big]\right], \tag{S24}$$

which is the characteristic function of the TMSV state $|\tilde{\Psi}(r)\rangle$ by Eq. (S1), i.e.,

$$g(\omega_1,\omega_2,r) := \mathrm{Tr}\Big[|\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)|(\hat{D}(\omega_1)\otimes\hat{D}(\omega_2))\Big]. \tag{S25}$$

Multiple TMSV states are straightforward to generalize:

$$g(\omega_1,\omega_2,r) := \exp\left[-\frac{1}{2}\Big[(|\omega_1|^2+|\omega_2|^2)\cosh 2r - (\omega_1\cdot\omega_2+\omega_1^*\cdot\omega_2^*)\sinh 2r\Big]\right], \tag{S26}$$

where $\omega_{1,2}$ are now n-dimensional complex vectors. Especially when $\omega_2=\omega_1^*$, it reduces to

$$g(\omega_1,\omega_1^*,r) = \exp\Big(-e^{-2r}|\omega_1|^2\Big). \tag{S27}$$

Therefore, the input TMSV states can be written as

$$|\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)| = \frac{1}{\pi^{2n}}\int d^{2n}\omega_1 d^{2n}\omega_2 \hat{D}^\dagger(\omega_1)\otimes\hat{D}^\dagger(\omega_2)g(w_1,w_2,r). \tag{S28}$$

Similarly, by generalizing an entangled state with a single-mode ancilla to an entangled state with n modes and infinite squeezing, the measurement POVM of CV Bell measurement can be written as [2, 3]

$$\frac{1}{\pi^n}|\Psi(\zeta)\rangle\langle\Psi(\zeta)| = \frac{1}{\pi^n}(I\otimes\hat{D}(\zeta))|\Psi\rangle\langle\Psi|(I\otimes\hat{D}^\dagger(\zeta)) = \int\frac{d^{2n}\omega}{\pi^{2n}}e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}\hat{D}^\dagger(\omega)\otimes\hat{D}^{\mathrm{T}}(\omega), \tag{S29}$$

where

$$|\Psi\rangle\langle\Psi| := \int\frac{d^{2n}\omega}{\pi^n}\hat{D}^\dagger(\omega)\otimes\hat{D}^{\mathrm{T}}(\omega) \tag{S30}$$

corresponds to a multimode generalization of a TMSV state with infinite squeezing parameter, i.e., $|\Psi\rangle\propto\sum_{k=0}^\infty|k\rangle|k\rangle$. Here, the normalization factor $1/\pi^n$ is introduced to ensure the completeness

$$\frac{1}{\pi^n}\int d^{2n}\zeta|\Psi(\zeta)\rangle\langle\Psi(\zeta)| = \mathbb{1}\otimes\mathbb{1}. \tag{S31}$$

We now simplify the expression of the output probability distribution of the scheme:

$$p_{EA}(\zeta)$$
$$= \frac{1}{\pi^n}\mathrm{Tr}\left[(|\Psi(\zeta)\rangle\langle\Psi(\zeta)|_{AB})(\mathcal{I}_A\otimes\Lambda_B)(|\tilde{\Psi}\rangle\langle\tilde{\Psi}|_{AB})\right] \tag{S32}$$
$$= \frac{1}{\pi^n}\mathrm{Tr}\left[\int\frac{d^{2n}\omega}{\pi^n}\frac{d^{2n}\beta_1 d^{2n}\beta_2}{\pi^{2n}}g(\beta_1,\beta_2,r)e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}\hat{D}^\dagger(\omega)_A\otimes\hat{D}^{\mathrm{T}}(\omega)_B(\mathcal{I}_A\otimes\Lambda_B)(\hat{D}^\dagger(\beta_1)_A\otimes\hat{D}^\dagger(\beta_2)_B)\right]. \tag{S33}$$

Here, we have

$$(\mathcal{I}_A\otimes\Lambda_B)(\hat{D}^\dagger(\beta_1)_A\otimes\hat{D}^\dagger(\beta_2)_B) = \hat{D}^\dagger(\beta_1)_A\otimes\frac{1}{\pi^n}\int d^{2n}\omega\lambda(\omega)\,\mathrm{Tr}\Big[\hat{D}^\dagger(\beta_2)_B\hat{D}(\omega)_B\Big]\hat{D}^\dagger(\omega)_B \tag{S34}$$
$$= \hat{D}^\dagger(\beta_1)_A\otimes\int d^{2n}\omega\lambda(\omega)\delta(\omega-\beta_2)\hat{D}^\dagger(\omega)_B \tag{S35}$$
$$= \lambda(\beta_2)\hat{D}^\dagger(\beta_1)_A\otimes\hat{D}^\dagger(\beta_2)_B. \tag{S36}$$

Thus, we can simplify Eq. (S32) as

$$\frac{1}{\pi^n}\operatorname{Tr}\left[\int \frac{d^{2n}\omega}{\pi^n}\frac{d^{2n}\beta_1 d^{2n}\beta_2}{\pi^{2n}} g(\beta_1,\beta_2,r)e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}\hat{D}^\dagger(\omega)_A\otimes\hat{D}^{\mathrm{T}}(\omega)_B(\mathcal{I}_A\otimes\Lambda_B)(\hat{D}^\dagger(\beta_1)_A\otimes\hat{D}^\dagger(\beta_2)_B)\right] \tag{S37}$$

$$= \frac{1}{\pi^n}\int \frac{d^{2n}\omega}{\pi^n}\frac{d^{2n}\beta_1 d^{2n}\beta_2}{\pi^{2n}}\lambda(\beta_2) g(\beta_1,\beta_2,r)e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}\operatorname{Tr}\Big[\hat{D}^\dagger(\omega)_A\hat{D}^\dagger(\beta_1)_A\Big]\operatorname{Tr}\Big[\hat{D}^{\mathrm{T}}(\omega)_B\hat{D}^\dagger(\beta_2)_B\Big] \tag{S38}$$

$$= \frac{1}{\pi^{2n}}\int d^{2n}\omega d^{2n}\beta_1 d^{2n}\beta_2\lambda(\beta_2)g(\beta_1,\beta_2,r)e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}\delta(\omega+\beta_1)\delta(\omega^*+\beta_2) \tag{S39}$$

$$= \frac{1}{\pi^{2n}}\int d^{2n}\omega\lambda(-\omega^*)g(-\omega,-\omega^*,r)e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}. \tag{S40}$$

Hence, we finally obtain the probability of obtaining ζ from Bell measurement with an initial Bell state with finite squeezing:

$$p_{EA}(\zeta) = \frac{1}{\pi^{2n}}\int d^{2n}\omega\lambda(-\omega^*)g(-\omega,-\omega^*,r)e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega} = \frac{1}{\pi^{2n}}\int d^{2n}\omega\lambda(-\omega^*)e^{-e^{-2r}|\omega|^2}e^{\zeta^*\cdot\omega^*-\zeta\cdot\omega}. \tag{S41}$$

By inverting the relation using Fourier transformation,

$$\int d^{2n}\zeta p_{EA}(\zeta)e^{\zeta^\dagger\beta-\beta^\dagger\zeta} = \frac{1}{\pi^{2n}}\int d^{2n}\omega\lambda(-\omega^*)g(-\omega,-\omega^*,r)e^{(\omega^*+\beta)\cdot\zeta^*-(\omega^*+\beta)^*\cdot\zeta} \tag{S42}$$

$$= \lambda(\beta)g(\beta^*,\beta,r), \tag{S43}$$

we obtain the relation between the characteristic function of the channel $\lambda(\beta)$ and the probability distribution of outcomes $p_{EA}(\zeta)$:

$$\lambda(\beta) = \frac{1}{g(\beta^*,\beta,r)}\int d^{2n}\zeta p_{EA}(\zeta)e^{\zeta^\dagger\beta-\beta^\dagger\zeta} = \exp\Big(e^{-2r}|\beta|^2\Big)\int d^{2n}\zeta p_{EA}(\zeta)e^{\zeta^\dagger\beta-\beta^\dagger\zeta}. \tag{S44}$$

The expression shows that by obtaining samples ζ's following the probability distribution using sampling in experiment and taking Fourier transformation, one can obtain the estimate of $\lambda(\beta)$. Now, we show the number of samples $N \geq \frac{8}{\epsilon^2}\log\frac{4}{\delta}e^{2e^{-2r}|\beta|^2} = O(e^{2e^{-2r}|\beta|^2}\epsilon^{-2}\log\delta^{-1})$ suffices to have a good precision ϵ with a high probability $1-\delta$. As observed above, for N number of samples, $\{\zeta^{(i)}\}_{i=1}^N$, we set the estimator of $\lambda(\beta)$ to be $\tilde{\lambda}(\beta) = \frac{1}{N}\sum_{i=1}^N \exp(e^{-2r}|\beta|^2)e^{\zeta^{(i)\dagger}\beta-\beta^\dagger\zeta^{(i)}}$ for measurement outcome ζ and apply the Hoeffding bound for the estimator. To do that, we find the bound for real part and imaginary part, respectively and combine them. We first obtain two different probabilities' bound by the Hoeffding bound such that

$$\Pr[|\tilde{\lambda}_r(\beta)-\lambda_r(\beta)|\leq\epsilon/2]\geq 1-2e^{-\frac{N\epsilon^2}{8}e^{-2e^{-2r}|\beta|^2}},\ \Pr[|\tilde{\lambda}_i(\beta)-\lambda_i(\beta)|\leq\epsilon/2]\geq 1-2e^{-\frac{N\epsilon^2}{8}e^{-2e^{-2r}|\beta|^2}}, \tag{S45}$$

where $\lambda_r = \mathrm{Re}(\lambda)$ and $\lambda_i = \mathrm{Im}(\lambda)$ and similar for $\tilde{\lambda}$. Applying the union bound and the triangle inequality, we obtain

$$\Pr[|\tilde{\lambda}(\beta)-\lambda(\beta)|\leq\epsilon]\geq 1-4e^{-\frac{N\epsilon^2}{8}e^{-2e^{-2r}|\beta|^2}}. \tag{S46}$$

Thus, if we choose the number of samples to be

$$N \geq \frac{8}{\epsilon^2}\log\frac{4}{\delta}e^{2e^{-2r}|\beta|^2} = O(e^{2e^{-2r}|\beta|^2}\epsilon^{-2}\log\delta^{-1}) \tag{S47}$$

the estimation error is upper-bounded by ϵ with high probability $1-\delta$. This completes the proof of Theorem 1 in the main text.

Note that in an ideal case where the input squeezing parameter r can be chosen to be arbitrarily large, the sample complexity can be reduced to $N = O(1/\epsilon^2)$ for any β.

B. Entanglement-free (Vacuum+Heterodyne) schemes

Now, let us consider the entanglement-free scheme with vacuum input and heterodyne detection (Vacuum+Heterodyne). In general, denoting Π_ϕ as a POVM with an outcome ϕ and $|\phi_0\rangle\langle\phi_0|$ as an input state, the probability of a classical scheme is written as

$$\begin{aligned}
p_{EF}(\phi) &= \mathrm{Tr}[\Pi_\phi \Lambda(|\phi_0\rangle\langle\phi_0|)] && \text{(S48)}\\
&= \frac{1}{\pi^{2n}} \int d^{2n}\alpha d^{2n}\beta \, \mathrm{Tr}\Big[\hat{D}(\alpha)\Lambda(\hat{D}^\dagger(\beta))\Big] \, \mathrm{Tr}\Big[\Pi_\phi \hat{D}^\dagger(\alpha)\Big] \, \mathrm{Tr}\Big[|\phi_0\rangle\langle\phi_0|\hat{D}(\beta)\Big] && \text{(S49)}\\
&= \frac{1}{\pi^{n}} \int d^{2n}\alpha d^{2n}\beta \lambda(\beta)\delta(\alpha-\beta) \, \mathrm{Tr}\Big[\Pi_\phi \hat{D}^\dagger(\alpha)\Big] \, \mathrm{Tr}\Big[|\phi_0\rangle\langle\phi_0|\hat{D}(\beta)\Big] && \text{(S50)}\\
&= \frac{1}{\pi^{n}} \int d^{2n}\beta \lambda(\beta) \, \mathrm{Tr}\Big[\Pi_\phi \hat{D}^\dagger(\beta)\Big] \, \mathrm{Tr}\Big[|\phi_0\rangle\langle\phi_0|\hat{D}(\beta)\Big]. && \text{(S51)}
\end{aligned}$$

For the Vacuum+Heterodyne scheme, we employ vacuum state input $|\phi_0\rangle = |0\rangle$ and heterodyne detection, whose POVM elements are described by projectors onto the (overcomplete) basis of coherent states, $|\zeta\rangle\langle\zeta|/\pi^n$, where $|\zeta\rangle$ is a coherent state with complex amplitude $\zeta \in \mathbb{C}^n$. Note that such a scheme is informationally complete in the sense that it provides distinct probability distributions for different channels. For this scheme, we can obtain the probability distribution

$$p_{VH}(\zeta) = \frac{1}{\pi^{2n}} \int d^{2n}\alpha \lambda(\alpha) \, \mathrm{Tr}\Big[|\zeta\rangle\langle\zeta|\hat{D}^\dagger(\alpha)\Big] \, \mathrm{Tr}\Big[|0\rangle\langle 0|\hat{D}(\alpha)\Big] = \frac{1}{\pi^{2n}} \int d^{2n}\alpha \lambda(\alpha) e^{\alpha^\dagger\zeta - \zeta^\dagger\alpha} e^{-|\alpha|^2}. \tag{S52}$$

Again, by inverting the probability distribution as

$$\int d^{2n}\zeta p_{VH}(\zeta) e^{\zeta^\dagger\beta - \beta^\dagger\zeta} = \frac{1}{\pi^{2n}} \int d^{2n}\zeta d^{2n}\alpha \lambda(\alpha) e^{\zeta^\dagger(\beta-\alpha) - (\beta-\alpha)^\dagger\zeta} e^{-|\alpha|^2} = \lambda(\beta) e^{-|\beta|^2}, \tag{S53}$$

we obtain the final relation between the measurement probability distribution and the characteristic function of the channel:

$$\lambda(\beta) = e^{|\beta|^2} \int d^{2n}\xi p_{VH}(\zeta) e^{\zeta^\dagger\beta - \beta^\dagger\zeta}. \tag{S54}$$

It clearly shows the difference from the quantum strategies, which is the prefactor $e^{|\beta|^2}$. Thus, similarly, after sampling ζ from experiments following $p_{EF}(\zeta)$ and averaging $e^{|\beta|^2} e^{\zeta^\dagger\beta - \beta^\dagger\zeta}$ over the samples, we obtain the estimate of $\lambda(\beta)$. As for the entanglement-assisted case, for N samples, $\{\zeta^{(i)}\}_{i=1}^N$, by setting the estimator $\tilde{\lambda}(\beta) = \frac{1}{N}\sum_{i=1}^N e^{|\beta|^2} e^{\zeta^{(i)\dagger}\beta - \beta^\dagger\zeta^{(i)}}$ and using the Hoeffding bound, we obtain

$$\Pr[|\tilde{\lambda}(\beta) - \lambda(\beta)| \leq \epsilon] \geq 1 - 4e^{-\frac{N\epsilon^2}{8}e^{-2|\beta|^2}}. \tag{S55}$$

Thus, in this case, it indicates that the sufficient number of samples is

$$N \geq \frac{8}{\epsilon^2} \log\frac{4}{\delta} e^{2|\beta|^2} = O(e^{2|\beta|^2}\epsilon^{-2}\log\delta^{-1}) \tag{S56}$$

for the estimation error to be upper-bounded by ϵ with high probability $1-\delta$. It clearly shows the significant difference of the sample complexity from the entanglement-assisted case.

C. Entanglement-assisted scheme with imperfection

We now consider the effect of imperfections and prove Theorem 3 in the main text. More specifically, we consider the cases where photon loss occurs before and after applying the random displacement channel we want to learn and a regularized Bell measurement. Here, the photon loss before and after the random displacement channel models an imperfect input state preparation and imperfect Bell measurement. On the other hand, we introduce parameter s to regularize the Bell measurement POVM by a general-dyne measurement POVM, where we recover the perfect Bell measurement by taking $s \to \infty$. By considering the regularized Bell measurement POVM, we assume the same condition as the lower bound in Sec. S3 in that the measurement POVM is normalizable, i.e., its norm is finite.

Let us first consider the effect of the loss channel on a single-mode displacement operator. Using the equivalent description of a loss channel $\mathcal{L}$ by a beam splitter interaction with a vacuum environment, we can show that

$$\mathcal{L}[\hat{D}^\dagger(\alpha)_S] = \mathrm{Tr}_E[U_T(\hat{D}^\dagger(\alpha)_S \otimes |0\rangle\langle 0|_E)U_T^\dagger] \tag{S57}$$

$$= \int \frac{d^2z}{\pi^n} e^{-\frac{1}{2}|z|^2}\, \mathrm{Tr}_E[U_T\hat{D}^\dagger(\alpha)_S \otimes \hat{D}^\dagger(z)_E U_T^\dagger] \tag{S58}$$

$$= \int \frac{d^2z}{\pi^n} e^{-\frac{1}{2}|z|^2}\, \mathrm{Tr}_E[\hat{D}^\dagger(\sqrt{T}\alpha - \sqrt{1-T}z)_S \otimes \hat{D}^\dagger(\sqrt{T}z + \sqrt{1-T}\alpha)_E] \tag{S59}$$

$$= T^{-1}e^{-\frac{1-T}{2T}|\alpha|^2}\hat{D}^\dagger(\alpha/\sqrt{T})_S, \tag{S60}$$

where $\hat{U}_T$ is the beam splitter interaction with the environment with the transmission rate T, and thus $1-T$ is the loss rate. Here, we used the identity [1]

$$|0\rangle\langle 0| = \int \frac{d^{2n}z}{\pi^n} e^{-\frac{1}{2}|z|^2}\hat{D}^\dagger(z). \tag{S61}$$

Recall that the input state is two-mode squeezed states with a finite squeezing parameter, which is written as

$$|\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)| = \frac{1}{\pi^{2n}}\int d^{2n}\omega_1 d^{2n}\omega_2 g(w_1, w_2, r)\hat{D}^\dagger(\omega_1)\otimes\hat{D}^\dagger(\omega_2). \tag{S62}$$

Let us first study how the displacement operator transforms over the channels.

First, after a loss channel with loss rate $1-T_b$, the random displacement channel Λ and another loss channel with loss rate $1-T_a$, an n-mode displacement operator transforms as

$$\mathcal{L}^{T_a}_{AB}(\mathcal{I}_A\otimes\Lambda_B)\mathcal{L}^{T_b}_{AB}(\hat{D}^\dagger(\omega_1)_A\otimes\hat{D}^\dagger(\omega_2)_B) \tag{S63}$$

$$= T_b^{-2n}e^{-\frac{1-T_b}{2T_b}(|\omega_1|^2+|\omega_2|^2)}\mathcal{L}^{T_a}_{AB}(\mathcal{I}_A\otimes\Lambda_B)(\hat{D}^\dagger(\omega_1/\sqrt{T_b})_A\otimes\hat{D}^\dagger(\omega_2/\sqrt{T_b})_B) \tag{S64}$$

$$= T_b^{-2n}e^{-\frac{1-T_b}{2T_b}(|\omega_1|^2+|\omega_2|^2)}\lambda(\omega_2/\sqrt{T_b})\mathcal{L}^{T_a}_{AB}(\hat{D}^\dagger(\omega_1/\sqrt{T_b})_A\otimes\hat{D}^\dagger(\omega_2/\sqrt{T_b})_B) \tag{S65}$$

$$= (T_bT_a)^{-2n}e^{-\frac{1-T_b}{2T_b}(|\omega_1|^2+|\omega_2|^2)}e^{-\frac{1-T_a}{2T_aT_b}(|\omega_1|^2+|\omega_2|^2)}\lambda(\omega_2/\sqrt{T_b})(\hat{D}^\dagger(\omega_1/\sqrt{T_bT_a})_A\otimes\hat{D}^\dagger(\omega_2/\sqrt{T_bT_a})_B). \tag{S66}$$

Now we implement the regularized Bell measurement. Recall that the perfect Bell measurement can be conducted by applying a 50:50 beam splitter and then performing homodyne detection. Here, we will regularize the homodyne detection by general-dyne detection and tracing out some quadratures.

After 50:50 beam splitters $\hat{U}_{\mathrm{BS}}$, the displacement operators transform as

$$\hat{D}^\dagger(\omega_1/\sqrt{T_bT_a})_A\otimes\hat{D}^\dagger(\omega_2/\sqrt{T_bT_a})_B \to \hat{D}^\dagger\left(\frac{\omega_1-\omega_2}{\sqrt{2T_bT_a}}\right)_A\otimes\hat{D}^\dagger\left(\frac{\omega_1+\omega_2}{\sqrt{2T_bT_a}}\right)_B. \tag{S67}$$

We then perform measurements described by the following POVM:

$$\{\hat{\Pi}^A_\alpha(-s) \otimes \hat{\Pi}^B_\beta(s)\}_{\alpha,\beta} \quad \text{where} \quad \hat{\Pi}_\gamma(s) \coloneqq \frac{1}{\pi^n} \hat{D}(\gamma) \left|s\right\rangle\!\left\langle s\right| \hat{D}^\dagger(\gamma), \tag{S68}$$

where $s \geq 0$ is the squeezing parameter for the Bell measurement. We note that this measurement corresponds to a special type of general-dyne measurement [3] and that when $s \to \infty$, we recover the Bell measurement studied in Sec. S2 A. Then, the output probability is written as

$$q(\alpha, \beta) \coloneqq \frac{1}{\pi^{2n}} \int d^{2n}\omega g(\omega_1, \omega_2, r) \operatorname{Tr}\Big[\hat{\Pi}^A_\alpha(-s) \otimes \hat{\Pi}^B_\beta(s) \hat{U}_{BS} \left(\mathcal{L}^{T_a}_{AB}(\mathcal{I}_A \otimes \Lambda_B)\mathcal{L}^{T_b}_{AB}(\hat{D}^\dagger(\omega_1)_A \otimes \hat{D}^\dagger(\omega_2)_B)\right) \hat{U}^\dagger_{BS}\Big]. \tag{S69}$$

Here, we have

$$\operatorname{Tr}\Big[\hat{\Pi}_\alpha(-s)\hat{D}^\dagger(\omega)\Big] = \frac{1}{\pi^n}\langle -s|\hat{D}^\dagger(\alpha)\hat{D}^\dagger(\omega)\hat{D}(\alpha)| - s\rangle = \frac{1}{\pi^n} e^{-\frac{1}{2}(|\omega|^2 \cosh 2s + (\omega^2 + \omega^{*2}) \sinh 2s/2)} e^{\omega^\dagger \alpha - \alpha^\dagger \omega}, \tag{S70}$$

$$\operatorname{Tr}\Big[\hat{\Pi}_\beta(s)\hat{D}^\dagger(\omega)\Big] = \frac{1}{\pi^n} e^{-\frac{1}{2}(|\omega|^2 \cosh 2s - (\omega^2 + \omega^{*2}) \sinh 2s/2)} e^{\omega^\dagger \beta - \beta^\dagger \omega}, \tag{S71}$$

and

$$\operatorname{Tr}\left[\hat{\Pi}_\alpha(-s)\hat{D}^\dagger\left(\frac{\omega_1 - \omega_2}{\sqrt{2T_aT_b}}\right)\right] \operatorname{Tr}\left[\hat{\Pi}_\beta(s)\hat{D}^\dagger\left(\frac{\omega_1 + \omega_2}{\sqrt{2T_aT_b}}\right)\right] \tag{S72}$$

$$= \frac{1}{\pi^{2n}} e^{-\frac{1}{2}\left[(|\omega_1|^2 + |\omega_2|^2)\frac{\cosh 2s}{T_aT_b} - (\omega_1 \cdot \omega_2 + \omega_1^* \cdot \omega_2^*)\frac{\sinh 2s}{T_aT_b}\right]} \exp\left[\omega_1^*\left(\frac{\alpha + \beta}{\sqrt{2T_aT_b}}\right) + \omega_2^*\left(\frac{\beta - \alpha}{\sqrt{2T_aT_b}}\right) - c.c.\right] \tag{S73}$$

$$= \frac{1}{\pi^{2n}} g(\omega_1/\sqrt{T_aT_b}, \omega_2/\sqrt{T_aT_b}, s) \exp\left[\omega_1^\dagger\left(\frac{\alpha + \beta}{\sqrt{2T_aT_b}}\right) + \omega_2^\dagger\left(\frac{\beta - \alpha}{\sqrt{2T_aT_b}}\right) - c.c.\right]. \tag{S74}$$

We now trace out one of two quadratures for each mode. To do that, we take integral over the imaginary part of α and the real part of β. Here, we define $\alpha \coloneqq \alpha_r + i\alpha_i$ and $\beta \coloneqq \beta_r + i\beta_i$. If we take the integral, the relevant part reduces to

$$\frac{1}{\pi^n}\int d^n\alpha_i \exp\left[\alpha\left(\frac{\omega_1^* - \omega_2^*}{\sqrt{2T_aT_b}}\right) - \alpha^*\left(\frac{\omega_1 - \omega_2}{\sqrt{2T_aT_b}}\right)\right] = \delta(\operatorname{Re}(\omega_1 - \omega_2)/\sqrt{2T_aT_b}) e^{-i\sqrt{2}\operatorname{Im}(\omega_1 - \omega_2)\alpha_r/\sqrt{T_aT_b}}, \tag{S75}$$

$$\frac{1}{\pi^n}\int d^n\beta_r \exp\left[\beta\left(\frac{\omega_1^* + \omega_2^*}{\sqrt{2T_aT_b}}\right) - \beta^*\left(\frac{\omega_1 + \omega_2}{\sqrt{2T_aT_b}}\right)\right] = \delta(\operatorname{Im}(\omega_1 + \omega_2)/\sqrt{2T_aT_b}) e^{i\sqrt{2}\operatorname{Re}(\omega_1 + \omega_2)\beta_i/\sqrt{T_aT_b}}, \tag{S76}$$

where the delta function gives us $\omega_2 = \omega_1^*$. Thus,

$$\int d^n\alpha_i d^n\beta_r \operatorname{Tr}\left[\hat{\Pi}_\alpha(-s)\hat{D}^\dagger\left(\frac{\omega_1 - \omega_2}{\sqrt{2T_aT_b}}\right)\right] \operatorname{Tr}\left[\hat{\Pi}_\beta(s)\hat{D}^\dagger\left(\frac{\omega_1 + \omega_2}{\sqrt{2T_aT_b}}\right)\right] \tag{S77}$$

$$= g(\omega_1/\sqrt{T_aT_b}, \omega_2/\sqrt{T_aT_b}, s)\delta\left(\frac{\omega_1 - \omega_2^*}{\sqrt{2T_aT_b}}\right) e^{-i\sqrt{2}\operatorname{Im}(\omega_1 - \omega_2)\alpha_r/\sqrt{T_aT_b}} e^{i\sqrt{2}\operatorname{Re}(\omega_1 + \omega_2)\beta_i/\sqrt{T_aT_b}}. \tag{S78}$$

Thus, the output probability is, by defining the measurement output variable as $\xi = -\alpha_r + i\beta_i$, given by

$$\begin{aligned}
&q(\xi) \qquad \text{(S79)}\\
&= \int d^n\alpha_i d^n\beta_r q(\alpha,\beta) \qquad \text{(S80)}\\
&= \frac{1}{\pi^{2n}}\int d^n\alpha_i d^n\beta_r d^{2n}\omega_1 d^{2n}\omega_2 (T_bT_a)^{-n} e^{-(\frac{1-T_b}{2T_b}+\frac{1-T_a}{2T_aT_b})(|\omega_1|^2+|\omega_2|^2)} g(\omega_1,\omega_2,r)\lambda(\omega_2/\sqrt{T_b})\\
&\qquad\qquad \times \mathrm{Tr}\left[\hat{\Pi}_\alpha(-s)\hat{D}^\dagger\left(\frac{\omega_1-\omega_2}{\sqrt{2T_aT_b}}\right)\right]\mathrm{Tr}\left[\hat{\Pi}_\beta(s)\hat{D}^\dagger\left(\frac{\omega_1+\omega_2}{\sqrt{2T_aT_b}}\right)\right] \qquad \text{(S81)}\\
&= \frac{1}{\pi^{2n}}\int d^{2n}\omega_1 d^{2n}\omega_2 (T_bT_a)^{-2n} e^{-(\frac{1-T_b}{2T_b}+\frac{1-T_a}{2T_aT_b})(|\omega_1|^2+|\omega_2|^2)} \lambda(\omega_2/\sqrt{T_b}) g(\omega_1,\omega_2^*,r) g(\omega_1/\sqrt{T_aT_b},\omega_2/\sqrt{T_aT_b},s)\\
&\qquad\qquad \times \delta\left(\frac{\omega_1-\omega_2^*}{\sqrt{2T_aT_b}}\right) e^{-i\sqrt{2}\,\mathrm{Im}(\omega_1-\omega_2)\alpha_r/\sqrt{T_aT_b}} e^{i\sqrt{2}\,\mathrm{Re}(\omega_1+\omega_2)\beta_i/\sqrt{T_aT_b}} \qquad \text{(S82)}\\
&= \left(\frac{2}{T_aT_b}\right)^n \frac{1}{\pi^{2n}}\int d^{2n}\omega e^{-(\frac{1-T_b}{T_b}+\frac{1-T_a}{T_aT_b})|\omega|^2} \lambda(\omega^*/\sqrt{T_b}) g(\omega,\omega^*,r) g(\omega/\sqrt{T_aT_b},\omega^*/\sqrt{T_aT_b},s) e^{\sqrt{2}(\xi\cdot\omega-\omega^*\cdot\xi^*)/\sqrt{T_aT_b}}\\
&\qquad \text{(S83)}\\
&= \left(\frac{2}{T_aT_b}\right)^n \frac{1}{\pi^{2n}}\int d^{2n}\omega e^{-(\frac{1-T_b}{T_b}+\frac{1-T_a}{T_aT_b})|\omega|^2} \lambda(\omega^*/\sqrt{T_b}) e^{-(e^{-2r}+e^{-2s}/T_aT_b)|\omega|^2} e^{\sqrt{2}(\xi\cdot\omega-\omega^*\cdot\xi^*)/\sqrt{T_aT_b}}\\
&\qquad \text{(S84)}\\
&= \left(\frac{2}{T_a}\right)^n \frac{1}{\pi^{2n}}\int d^{2n}\omega e^{-((1-T_b)+\frac{1-T_a}{T_a})|\omega|^2} \lambda(\omega^*) e^{\sqrt{2}(\xi\cdot\omega-\omega^*\cdot\xi^*)/\sqrt{T_a}}. \qquad \text{(S85)}
\end{aligned}$$

Here, for consistency with Sec. S2 A, we rescale $\sqrt{2}\xi = \zeta$ and define $p_{loss}(\zeta)$ such that

$$p_{loss}(\zeta) = \left(\frac{1}{T_a}\right)^n \frac{1}{\pi^{2n}}\int d^{2n}\omega e^{-((1-T_b)+\frac{1-T_a}{T_a})|\omega|^2} \lambda(\omega^*) e^{-(T_be^{-2r}+e^{-2s}/T_a)|\omega|^2} e^{(\omega\cdot\zeta-\omega^*\cdot\zeta^*)/\sqrt{T_a}}, \tag{S86}$$

where 2^n factor is canceled because of the relation $2^n d^{2n}\xi = d^{2n}\zeta$ (This rescaling is because the convention of Bell measurement outcome ζ in Sec. S2 A is different from ξ in this section by $\sqrt{2}$ factor.). Therefore, after Fourier transformation, we obtain

$$\int d^{2n}\zeta p_{loss}(\zeta) e^{(\zeta^\dagger\beta-\beta^\dagger\zeta)/\sqrt{T_a}} = \lambda(\beta) e^{-(T_be^{-2r}+e^{-2s}/T_a)|\beta|^2} e^{-(1-T_b)|\beta|^2} e^{-\frac{1-T_a}{T_a}|\beta|^2}. \tag{S87}$$

Consequently, the characteristic function is written by the probability distribution as

$$\begin{aligned}
\lambda(\beta) &= e^{(T_be^{-2r}+e^{-2s}/T_a)|\beta|^2} e^{(1-T_b)|\beta|^2} e^{\frac{1-T_a}{T_a}|\beta|^2} \int d^{2n}\zeta p_{loss}(\zeta) e^{(\zeta^\dagger\beta-\beta^\dagger\zeta)/\sqrt{T_a}}, \qquad \text{(S88)}\\
&= e^{e^{-2r_{\mathrm{eff}}}|\beta|^2} \int d^{2n}\zeta p_{loss}(\zeta) e^{(\zeta^\dagger\beta-\beta^\dagger\zeta)/\sqrt{T_a}}. \qquad \text{(S89)}
\end{aligned}$$

where we defined an effective squeezing parameter r_{eff} due to all kinds of imperfections via

$$e^{-2r_{\mathrm{eff}}} := (T_be^{-2r} + T_a^{-1}e^{-2s}) + (1-T_b) + \frac{1-T_a}{T_a}. \tag{S90}$$

In order to estimate any $\lambda(\beta)$, one simply obtains N samples $\{\zeta^{(i)}\}_{i=1}^N$ from $p(\zeta)$ and set the estimator to be $\tilde{\lambda}(\beta) := \frac{1}{N}\sum_{i=1}^N e^{e^{-2r_{\mathrm{eff}}}|\beta|^2} e^{(\zeta^{(i)\dagger}\beta-\beta^\dagger\zeta^{(i)})/\sqrt{T_b}}$. According to the Hoeffding's inequality as the ideal case, averaging over $N \geq 8/\epsilon^2 \log(4/\delta) e^{2e^{-2r_{\mathrm{eff}}}|\beta|^2}$ copies is sufficient to estimate $\lambda(\beta)$ to ϵ additive error with high probability.

Meanwhile, the effects of imperfections are thus the envelope of Fourier transforms. Especially when $s \to \infty$, the effective squeezing parameter under loss is given by

$$r_{\mathrm{eff}} = -\frac{1}{2}\log\left(T_be^{-2r} + (1-T_b) + \frac{1-T_a}{T_a}\right). \tag{S91}$$

This completes the proof of Theorem 3 in the main text.

To be clearer, for photon loss before the channel without any other imperfections, i.e., $s \to \infty$ and $T_a = 1$, the envelope is given by

$$e^{[T_b e^{-2r}+(1-T_b)]|\beta|^2}, \tag{S92}$$

and for photon loss after the channel without other imperfections, the envelope is given by

$$e^{[e^{-2r}+(1-T_a)/T_a]|\beta|^2}. \tag{S93}$$

D. Discussion on more general input states

In this section, we study more general sources of noise other than finite squeezing and photon loss. To begin with, consider the case where we use an arbitrary input state while the CV Bell measurement is still employed. To this end, note that Eq. (S44) from Sec. S2 A does not use any special properties of TMSV, and actually holds for any $2n$-mode input state, *i.e.*,

$$\lambda(\beta) = \frac{1}{g_{\hat{\rho}}(\beta^*, \beta)} \int d^{2n}\zeta p_{EA}(\zeta) e^{\zeta^\dagger \beta - \beta^\dagger \zeta}, \tag{S94}$$

where g is the characteristic function of the input state $\hat{\rho}$:

$$g_{\hat{\rho}}(w_1, w_2) = \mathrm{Tr}\Big[\hat{\rho}\hat{D}(\omega_1) \otimes \hat{D}(\omega_2)\Big]. \tag{S95}$$

The fact that the same relation holds by replacing the g function properly indicates that for different types of input states, we still have a very similar form of an unbiased estimator for N samples:

$$\tilde{\lambda}(\beta) = \frac{1}{N}\sum_{i=1}^{N} \frac{1}{g_{\hat{\rho}}(\beta^*, \beta)} e^{\zeta^{(i)\dagger}\beta - \beta^\dagger \zeta^{(i)}}. \tag{S96}$$

It implies that the sampling complexity is determined by the function $g_{\hat{\rho}}(\beta^*, \beta)$. More specifically, by the Hoeffding inequality, the number of samples to achieve an error ϵ with high probability $1-\delta$ is given by

$$N = O(|g_{\hat{\rho}}(\beta^*, \beta)|^{-2}\epsilon^{-2}\log\delta^{-1}). \tag{S97}$$

For example, for TMSV states, this function reduces to

$$g_{\tilde{\Psi}}(\beta^*, \beta) = \exp\Big(-e^{-2r}|\beta|^2\Big). \tag{S98}$$

Therefore, as long as the function g of the input state is sufficiently large for the β of interest, we can still expect the scheme to be sample efficient.

Such a general form enables us to analyze the effect of general noise on input states. Let us again focus on TMSV states but assume a noise channel $\mathcal{N}$. Then, the characteristic function g of the noisy TMSV states can be written as

$$g_{\mathcal{N}(\tilde{\Psi})}(w_1, w_2) = \mathrm{Tr}\Big[\mathcal{N}(|\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)|)\hat{D}(\omega_1) \otimes \hat{D}(\omega_2)\Big]. \tag{S99}$$

As discussed, it suffices to analyze how the characteristic function changes by noise to ensure that a significant advantage is still maintained for noisy states. In typical experiments, while the CV Bell measurement noise can be modeled by photon loss, as we considered already in the previous section, other types of noise may exist in the TMSV state preparation procedure. An example is

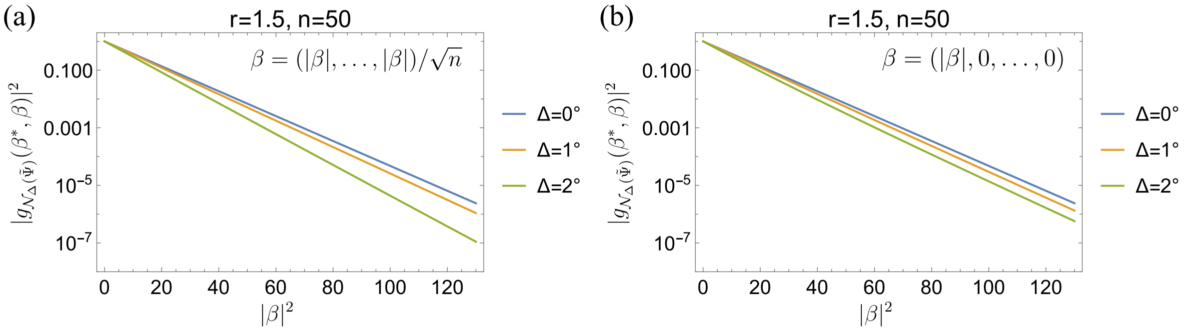


FIG. S1. Effect of phase diffusion on the squared characteristic function $|g_{\mathcal{N}_\Delta(\hat{\rho})}(\beta^*, \beta)|^2$, where we choose a specific form of $\beta \in \mathbb{C}^n$ as (a) $\beta := (|\beta|/\sqrt{n}, \ldots, |\beta|/\sqrt{n})$ and (b) $\beta := (|\beta|, 0, \ldots, 0)$ for two extreme cases with a given $|\beta|^2$. We fix the squeezing parameter $r = 1.5$ of the input TMSV states and set the number of modes $n = 50$. For the standard deviation $\Delta = 1°$ of phase noise, following Gaussian distributions, one may observe that the characteristic function is almost identical to the noiseless case ($\Delta = 0°$). For the standard deviation $\Delta = 2°$ as well, the effect is not very significant.

phase diffusion, which can be modeled by a photon-number-dependent random phase following a Gaussian distribution. For $2n$-mode state input, we can write the noise channel as

$$\mathcal{N}_\Delta(\hat{\rho}) \tag{S100}$$

$$= \int d^n\phi_A d^n\phi_B \frac{e^{-\frac{|\phi_A|^2+|\phi_B|^2}{2\Delta^2}}}{(2\pi\Delta^2)^n} e^{-i\phi_A\cdot\hat{n}_A - i\phi_B\cdot\hat{n}_B} \hat{\rho} e^{i\phi_A\cdot\hat{n}_A + i\phi_B\cdot\hat{n}_B} \tag{S101}$$

$$= \frac{1}{\pi^{2n}} \int d^{2n}\omega_1 d^{2n}\omega_2 g_{\hat{\rho}}(\omega_1, \omega_2) \int d^n\phi_A d^n\phi_B \frac{e^{-\frac{|\phi_A|^2+|\phi_B|^2}{2\Delta^2}}}{(2\pi\Delta^2)^n} e^{-i\phi_A\cdot\hat{n}_A - i\phi_B\cdot\hat{n}_B} [\hat{D}^\dagger(\omega_1) \otimes \hat{D}^\dagger(\omega_2)] e^{i\phi_A\cdot\hat{n}_A + i\phi_B\cdot\hat{n}_B}, \tag{S102}$$

where ϕ_A and ϕ_B are n-dimensional real vectors and $\hat{n}_A$ and $\hat{n}_B$ are photon number operator vectors for A and B parts, respectively. Then, noting that

$$e^{-i\phi_A\cdot\hat{n}_A - i\phi_B\cdot\hat{n}_B} [\hat{D}^\dagger(\omega_1) \otimes \hat{D}^\dagger(\omega_2)] e^{i\phi_A\cdot\hat{n}_A + i\phi_B\cdot\hat{n}_B} = \hat{D}^\dagger(\omega_1 e^{-i\phi_A}) \otimes \hat{D}^\dagger(\omega_2 e^{-i\phi_B}), \tag{S103}$$

where $\omega_1 e^{-i\phi_A}$ and $\omega_2 e^{-i\phi_B}$ are interpreted as vectors obtained by an elementwise product, the corresponding g function for TMSV states is written as

$$g_{\mathcal{N}(\tilde{\Psi})}(w_1, w_2) \tag{S104}$$

$$= \mathrm{Tr}\Big[\mathcal{N}_\Delta(|\tilde{\Psi}(r)\rangle\langle\tilde{\Psi}(r)|) \hat{D}(\omega_1) \otimes \hat{D}(\omega_2)\Big] \tag{S105}$$

$$= \frac{1}{\pi^{2n}} \int d^{2n}\beta_1 d^{2n}\beta_2 g_{\tilde{\Psi}}(\beta_1, \beta_2) \int d^n\phi_A d^n\phi_B \frac{e^{-\frac{|\phi_A|^2+|\phi_B|^2}{2\Delta^2}}}{(2\pi\Delta^2)^n} \mathrm{Tr}\Big[\hat{D}^\dagger(\beta_1 e^{-i\phi_A}) \otimes \hat{D}^\dagger(\beta_2 e^{-i\phi_B}) \hat{D}(\omega_1) \otimes \hat{D}(\omega_2)\Big] \tag{S106}$$

$$= \int d^{2n}\beta_1 d^{2n}\beta_2 g_{\tilde{\Psi}}(\beta_1, \beta_2) \int d^n\phi_A d^n\phi_B \frac{e^{-\frac{|\phi_A|^2+|\phi_B|^2}{2\Delta^2}}}{(2\pi\Delta^2)^n} \delta(\omega_1 - \beta_1 e^{-i\phi_A}) \delta(\omega_2 - \beta_2 e^{-i\phi_B}) \tag{S107}$$

$$= \int d^n\phi_A d^n\phi_B \frac{e^{-\frac{|\phi_A|^2+|\phi_B|^2}{2\Delta^2}}}{(2\pi\Delta^2)^n} g_{\tilde{\Psi}}(\omega_1 e^{i\phi_A}, \omega_2 e^{i\phi_B}). \tag{S108}$$

Thus, the effect of phase noise is to transform the g function as a mixture with random phases. We present examples to illustrate the effect of the phase noise on the sample complexity in Fig. S1.

We have chosen the parameters $\beta \in \mathbb{C}^n$ of two extreme cases as $\beta := (|\beta|/\sqrt{n}, \dots, |\beta|/\sqrt{n})$ and $\beta := (|\beta|, 0, \dots, 0)$. Recall that the typical choice of the regime of interest in the main text is $|\beta|^2 \leq \kappa n$; here, the range $|\beta|^2 \in [0, 130]$ in the figure covers up to $\kappa = 2.5$ for $n = 50$. We see that the advantages of the entanglement-assisted scheme look robust against small-phase diffusion noise.

S3. FUNDAMENTAL LIMITS FOR ENTANGLEMENT-FREE SCHEMES

In this section, we prove the fundamental limit on general entanglement-free schemes for learning n-mode random displacement channels. In this work, we will focus on the ancilla-free schemes without concatenation. This means that, for each copy of the channel, we act it on some input state and apply a destructive POVM measurement right after. The input states and measurements can be adaptively chosen depending on previous measurement outcomes. See Fig. S2. Bounds for such schemes have been investigated in different tasks [4–6]. One can also study ancilla-free protocols with concatenation, the lower bounds for which have been obtained in several recent works [6–8], but we leave that for future study as continuous-variable system puts an additional level of complexity. Throughout this work, we assume entanglement-free schemes to have no concatenation.

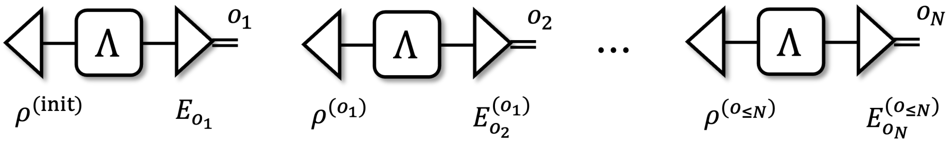


FIG. S2. Schematics for entanglement-free schemes. In this work we assume no concatenation is allowed. Such a scheme can be completely specificed by a collection of input states and POVM measurements that adaptively depend on the measurement outcomes from the previous round.

Theorem S1. *Let Λ be an arbitrary n-mode random displacement channel ($n \geq 8$) and consider an entanglement-free scheme that uses N copies of Λ. After all measurements are completed, the scheme receives the query $\beta \in \mathbb{C}^n$ and returns an estimate $\tilde{\lambda}(\beta)$ of Λ's characteristic function $\lambda(\beta)$. Suppose that, with success probability at least 2/3, $|\tilde{\lambda}(\beta) - \lambda(\beta)| \leq \epsilon \leq 0.24$ for all β such that $|\beta|^2 \leq n\kappa$. Then $N \geq 0.01\epsilon^{-2}(1 + 1.98\kappa)^n$.*

Recall that an entanglement-assisted scheme can achieve the same task using $O(\epsilon^{-2})$ copies of channels given sufficient squeezing and $\kappa = O(1)$. Therefore, we establish an exponential separation between learning bosonic random displacement channels with and without entanglement. In the following, we start proving this result in Sec. S3 A and present a core lemma in Sec. S3 B. We also prove a bound for learning with Gaussian schemes in Sec. S3 C, which might be of independent interest.

Before proceeding, let us specify some regularization conditions. We will only work with proper vectors (i.e., normalizable vector) in the Hilbert space and bounded operator acting on the Hilbert space. That is to say, all the quantum states we considered can be expressed as a density operator $\hat{\rho}$ with trace 1, and all the POVM element $\hat{E}$ is a bounded positive semi-definite operator satisfying $\hat{E} \leq \hat{I}$. Perhaps the most representative example that does not admit the above form is the perfect homodyne detection projector $|x\rangle\langle x|$, which represents projection onto the quadrature x. While $|x\rangle$ is not a proper vector in the relevant Hilbert space, it can be treated as a limit of proper vectors in any physical setting. Concretely, homodyne detection is implemented by applying a 50:50 beam splitter between the input state and a strong local oscillator [3], and the above improper projector $|x\rangle\langle x|$ is obtained by taking the limit where the power of the oscillator goes to infinity. Therefore, in a reasonable physical setup, the actual projector is constructed with a proper vector in the Hilbert space, thus satisfying our assumptions. We emphasize that our entanglement-assisted strategy also satisfies the same assumption as we regularize the Bell measurements with general-dyne detection with a parameter $s < \infty$, see Sec. S2 C.

A. Lower bound for entanglement-free schemes

Given positive number $n \geq 8$ and $\epsilon \leq 0.24$, we introduce a family of "3-peak" random displacement channels, defined by their characteristic functions,

$$\Lambda_\gamma : \ \lambda_\gamma(\beta) \coloneqq e^{-\frac{|\beta|^2}{2\sigma^2}} + 2i\epsilon_0 e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}} - 2i\epsilon_0 e^{-\frac{|\beta+\gamma|^2}{2\sigma^2}}, \quad \gamma \in \mathbb{C}^n, \tag{S109}$$

where $\epsilon_0 \coloneqq \epsilon/0.98 \leq 0.25$. The corresponding distributions of displacements, computed via Fourier transformation, are

$$\Lambda_\gamma : \ p_\gamma(\alpha) = \left(\frac{2\sigma^2}{\pi}\right)^n e^{-2\sigma^2|\alpha|^2} \left(1 + 4\epsilon_0 \sin(2(\operatorname{Im}[\gamma]\operatorname{Re}[\alpha] - \operatorname{Re}[\gamma]\operatorname{Im}[\alpha]))\right), \tag{S110}$$

from which we see that the typical strength of displacement is of order $1/\sigma$. Roughly, the smaller σ is, the larger energy the channel carries. We define $\Lambda_{\text{dep}} \coloneqq \Lambda_0$ as the CV analogy of the depolarizing channel, and the other Λ_γ can be viewed as perturbed depolarizing channels. The set of 3-peak channels with parameters (ϵ, σ) is denoted as $\mathbf{\Lambda}^{\epsilon,\sigma}_{\text{3-peak}}$. With this, we are going to prove a strictly stronger result than Theorem S1. That is, even if one knows the channel to be estimated is from the restricted family, $\mathbf{\Lambda}^{\epsilon,\sigma}_{\text{3-peak}}$, an exponential lower bound still applies.

Theorem S2. *Given positive numbers $n, \sigma, \kappa, \epsilon$ such that*

$$2\sigma^2 \leq \max\left\{1 - 1.98\kappa,\ 0.99\kappa\left(\sqrt{1 + (0.99\kappa)^{-2}} - 1\right)\right\}, \quad n \geq 8, \quad \epsilon \leq 0.24. \tag{S111}$$

If there exists an entanglement-free scheme such that, after learning from N copies of an n-mode random displacement channel $\Lambda \in \mathbf{\Lambda}^{\epsilon,\sigma}_{\text{3-peak}}$, and then receiving a query $\beta \in \mathbb{C}^n$, can return an estimate $\tilde{\lambda}(\beta)$ of $\lambda(\beta)$ such that $|\tilde{\lambda}(\beta) - \lambda(\beta)| \leq \epsilon$ with probability at least $2/3$ for all β such that $|\beta|^2 \leq n\kappa$, then

$$N \geq 0.01\epsilon^{-2}\left(1 + \frac{1.98\kappa}{1 + 2\sigma^2}\right)^n. \tag{S112}$$

It is not hard to see that a $\sigma > 0$ satisfying the assumptions can always be found for any $\kappa > 0$. Indeed, Theorem S1 follows from Theorem S2 by choosing $\sigma \to 0$. Note that Theorem S2 does not place any constraint on the input state and measurement. This means that learning a finite-energy random displacement channel is hard without ancilla even given energy-unbounded input state and measurement. Also, Theorem S2 enables an experimental test, as it only requires generating finite displacement with high probability. The practical performance of this bound with $\sigma = 0.3$ is shown in Fig. S3.

Proof of Theorem S2. Now we introduce the following game between Alice and Bob that helps reduce the learning task to a partially-revealed hypothesis testing task [9]. First, Alice samples $s \in \{\pm 1\}$ with equal probability and $\gamma \in \mathbb{C}^n$ according to the multivariate normal distribution $q(\gamma)$ defined as

$$q(\gamma) \coloneqq \left(\frac{1}{2\pi\sigma_\gamma^2}\right)^n e^{-\frac{|\gamma|^2}{2\sigma_\gamma^2}}, \tag{S113}$$

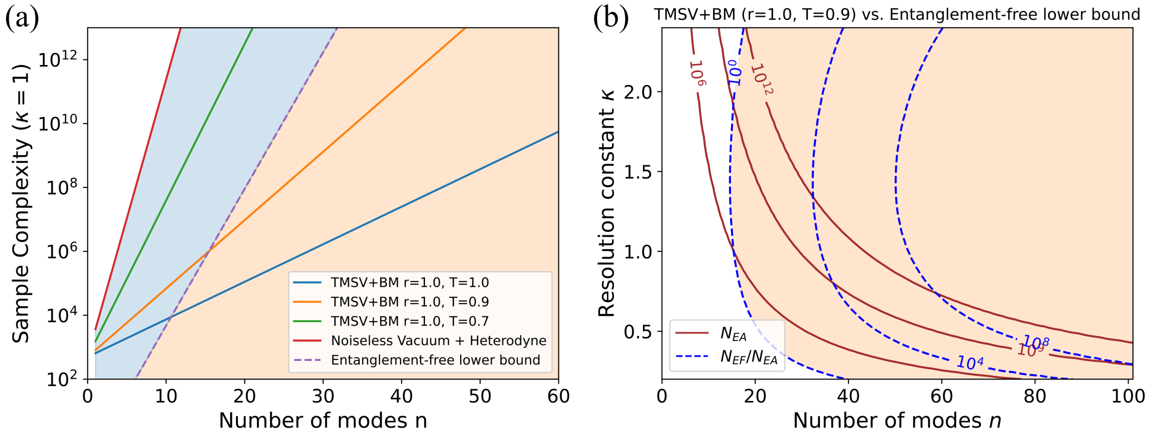


FIG. S3. Learning random displacement channels from the family with $\sigma = 0.3$ as in Theorem S2. (In the main text, we set $\sigma = 0$.) All κ shown in the figure satisfies Eq. (S111). (a) Comparison of TMSV+BM (with different loss rates), Vacuum+Heterodyne, and the entanglement-free lower bound at $\kappa = 1$. The task is to estimate any $\lambda(\beta)$ such that $|\beta|^2 \leq \kappa n$ with precision $\varepsilon = 0.2$ and success probability $1 - \delta = 2/3$. The orange region represents a rigorous advantage over any entanglement-free schemes. The blue region represents an advantage over Vacuum+heterodyne. (b) Comparison of the TMSV+BM scheme with squeezing parameter $r = 1.0$ and loss rate $1 - T = 0.1$ with the entanglement-free lower bound of Theorem 2. The task is the same as (a). The brown solid contour lines represent the sample complexity of TMSV+BM given by Theorem 3. The blue dashed contour lines represent the ratio of sample complexity between the entanglement-free lower bound and TMSV+BM, which clearly indicates the entanglement-enabled advantages.

where we will set $2\sigma_\gamma^2 := 0.99\kappa$ to ensure the tail probability, i.e., $\Pr(|\gamma|^2 > \kappa n)$, to be sufficiently small. Next, Alice does one of the following with equal probability:

1. Prepare N copies of Λ_{dep} for Bob;

2. Prepare N copies of $\Lambda_{s\gamma}$ for Bob.

Bob then measures the N copies of the channels Alice prepared. After Bob has finished the measurements and retains only classical information, Alice reveals the value of γ to Bob. Now Bob is asked to distinguish between the two hypotheses: whether Alice has prepared copies of Λ_{dep} or $\Lambda_{s\gamma}$. Crucially, Bob must have completed all quantum measurements before Alice reveals γ, and can only perform classical post-processing after that.

We first argue that if there is a scheme satisfying the assumptions of Theorem S2, then Bob can use it to win the game with an average probability much better than random guess. Bob's strategy is as follows: If the γ he received satisfies $2\sigma^2 < |\gamma|^2 \leq \kappa n$, use the scheme to query $\lambda(\gamma)$. Note that for any $\gamma \in \mathbb{C}^n$:

$$|\lambda_{\text{dep}}(\gamma) - \lambda_{\pm\gamma}(\gamma)| = \frac{1}{2}|\lambda_\gamma(\gamma) - \lambda_{-\gamma}(\gamma)| = 2\epsilon_0 \left|1 - e^{-\frac{4|\gamma|^2}{2\sigma^2}}\right|. \tag{S114}$$

For $|\gamma|^2 > 2\sigma^2$, the R.H.S. is lower bounded by $2\epsilon_0 \times 0.98 = 2\epsilon$. By assumption, this allows Bob to distinguish among $\{\Lambda_{\text{dep}}, \Lambda_\gamma, \Lambda_{-\gamma}\}$ and thus guess correctly with at least $2/3$ chance; For other γ, Bob just makes a uniformly random guess. Note that

$$\Pr\left(2\sigma^2 < |\gamma|^2 \leq \kappa n\right) = 1 - \Pr\Big(|\gamma|^2 > \kappa n\Big) - \Pr\Big(|\gamma|^2 \leq 2\sigma^2\Big) \tag{S115}$$

$$= 1 - \left(\frac{\Gamma(n, n/0.99)}{\Gamma(n)}\right) - \left(1 - \frac{\Gamma(n, \sigma^2/\sigma_\gamma^2)}{\Gamma(n)}\right) \tag{S116}$$

$$\geq \frac{1}{2} - \left(1 - \frac{\Gamma(n, \sigma^2/\sigma_\gamma^2)}{\Gamma(n)}\right) \tag{S117}$$

$$= \frac{1}{2} - \frac{\int_0^{\sigma^2/\sigma_\gamma^2} t^{n-1} e^{-t} dt}{(n-1)!} \tag{S118}$$

$$\geq 0.49987. \tag{S119}$$

The first inequality is shown in Sec. S4. The second inequality requires $n \geq 8$ and $2\sigma^2 \leq 0.99\kappa := 2\sigma_\gamma^2$. Bob's average success probability is lower bounded by

$$\Pr[\text{Success}] \geq \Pr\left(2\sigma^2 < |\gamma|^2 \leq \kappa n\right) \times 2/3 + \left(1 - \Pr\left(2\sigma^2 < |\gamma|^2 \leq \kappa n\right)\right) \times 1/2. \tag{S120}$$

Now we investigate the probability distribution of Bob's measurement outcomes for any γ. For any adaptive entanglement-free strategy, one specifies an input state and a POVM for the ith copy of Λ that can depend on previous measurement outcomes. We denote the ith measurement outcomes as o_i and the outcomes up to the ith round as $o_{<i} = [o_1, ..., o_{i-1}]$. The latter is added as a superscript to the ith input states $\rho^{o_{<i}}$ and POVM element $E_{o_i}^{o_{<i}}$ to emphasize their adaptive nature. With these notations, the probability of obtaining outcomes $o_{1:N}$ on N copies of Λ is

$$p(o_{1:N}|\Lambda) = \prod_{k=1}^{N} \mathrm{Tr}\Big[\hat{E}_{o_i}^{o_{<i}} \Lambda(\hat{\rho}^{o_{<i}})\Big]. \tag{S121}$$

For a fixed γ, let $p_1(o_{1:N}) := p(o_{1:N}|\Lambda_{\text{dep}})$, $p_{2,\gamma}(o_{1:N}) := \mathbb{E}_{s=\pm1} p(o_{1:N}|\Lambda_{s\gamma})$, which is the distribution of Bob's outcomes under the two hypotheses, respectively, conditioned on the γ he received. According to the property of total variation distance, the maximal probability that Bob can distinguish p_1 and $p_{2,\gamma}$ is bounded by

$$\Pr[\text{Success}|\gamma] \leq \frac{1}{2}(1 + \mathrm{TVD}(p_1, p_{2,\gamma})), \tag{S122}$$

where TVD is the *total variation distance* defined as

$$\mathrm{TVD}(p_1, p_{2,\gamma}) := \sum_{o_{1:N}} \max\left\{0,\ p_1(o_{1:N}) - p_{2,\gamma}(o_{1:N})\right\}. \tag{S123}$$

We note that the sum over $o_{1:N}$ should be understood as integral for continuous-variable outcomes. Thus, the average probability that Bob can win the game is upper bounded by

$$\Pr[\text{Success}] = \mathbb{E}_{\gamma\sim q} \Pr[\text{Success}|\gamma] \leq \frac{1}{2}(1 + \mathbb{E}_\gamma \mathrm{TVD}(p_1, p_{2,\gamma})). \tag{S124}$$

Combining Eq. (S120) and Eq. (S124), we get

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1, p_{2,\gamma}) \geq 0.1666. \tag{S125}$$

In the following, we show by direct calculation that this is impossible unless N is exponentially large in n, which yields a desired lower bound for the sample complexity.

Thanks to convexity, we assume pure input states and rank-1 measurement without decreasing the TVD, i.e., the kth round's input state and POVM are written as $|A^{o_{<k}}\rangle$ and $\{|B^{o_{<k}}_{o_k}\rangle\langle B^{o_{<k}}_{o_k}|\}$, which are conditioned on the previous measurement outcomes $o_{<k}$. Here, the input state has unit length and $\sum_{o_k}|B^{o_{<k}}_{o_k}\rangle\langle B^{o_{<k}}_{o_k}| = \mathbb{1}$. We note that since any density matrix is trace-class, a spectrum decomposition always exists. On the other hand, the POVM element can be non-compact operator and might not have spectrum decomposition, but it is known that they can always be composed into rank-1 projectors with positive coefficients (see [10, Theorem 6]). Thus, making both the input state and measurement projector to be rank-1 is indeed justified.

Now, let us rewrite the probabilities as

$$\begin{aligned} p_1(o_{1:N}) &= \prod_{k=1}^{N} \langle B^{o_{<k}}_{o_k}|\Lambda_{\mathrm{dep}}(|A^{o_{<k}}\rangle\langle A^{o_{<k}}|)|B^{o_{<k}}_{o_k}\rangle \qquad \text{(S126)}\\ &= \prod_{k=1}^{N}\left(\frac{1}{\pi^n}\int d^{2n}\beta_k \lambda_{\mathrm{dep}}(\beta_k)\langle B^{o_{<k}}_{o_k}|\hat{D}^\dagger(\beta_k)|B^{o_{<k}}_{o_k}\rangle\langle A^{o_{<k}}|\hat{D}(\beta_k)|A^{o_{<k}}\rangle\right), \qquad \text{(S127)}\\ p_{2,\gamma}(o_{1:N}) &= \mathbb{E}_{s=\pm1}\prod_{k=1}^{N}\langle B^{o_{<k}}_{o_k}|\Lambda_{s\gamma}(|A^{o_{<k}}\rangle\langle A^{o_{<k}}|)|B^{o_{<k}}_{o_k}\rangle \qquad \text{(S128)}\\ &= \mathbb{E}_{s=\pm1}\prod_{k=1}^{N}\left(\frac{1}{\pi^n}\int d^{2n}\beta_k \lambda_{s\gamma}(\beta_k)\langle B^{o_{<k}}_{o_k}|\hat{D}^\dagger(\beta_k)|B^{o_{<k}}_{o_k}\rangle\langle A^{o_{<k}}|\hat{D}(\beta_k)|A^{o_{<k}}\rangle\right). \qquad \text{(S129)} \end{aligned}$$

Let $\lambda^{\mathrm{add}}_{\gamma}(\beta_k) := \lambda_\gamma(\beta_k) - \lambda_{\mathrm{dep}}(\beta_k)$. The difference of the probabilities can then be written as

$$\begin{aligned} &p_1(o_{1:N}) - p_{2,\gamma}(o_{1:N}) \qquad \text{(S130)}\\ =&p_1(o_{1:N})\left(1-\frac{p_{2,\gamma}(o_{1:N})}{p_1(o_{1:N})}\right) \qquad \text{(S131)}\\ =&p_1(o_{1:N})\left(1-\mathbb{E}_{s=\pm1}\prod_{k=1}^{N}\left(1+\frac{\frac{1}{\pi^n}\int d^{2n}\beta_k\lambda^{\mathrm{add}}_{s\gamma}(\beta_k)\langle B^{o_{<k}}_{o_k}|\hat{D}^\dagger(\beta_k)|B^{o_{<k}}_{o_k}\rangle\langle A^{o_{<k}}|\hat{D}(\beta_k)|A^{o_{<k}}\rangle}{\frac{1}{\pi^n}\int d^{2n}\beta_k\lambda_{\mathrm{dep}}(\beta_k)\langle B^{o_{<k}}_{o_k}|\hat{D}^\dagger(\beta_k)|B^{o_{<k}}_{o_k}\rangle\langle A^{o_{<k}}|\hat{D}(\beta_k)|A^{o_{<k}}\rangle}\right)\right) \qquad \text{(S132)}\\ =&p_1(o_{1:N})\left(1-\mathbb{E}_{s=\pm1}\prod_{k=1}^{N}\left(1-4\epsilon_0\,\mathrm{Im}\,G^{o_{\le k}}_{\sigma}(s\gamma)\right)\right), \qquad \text{(S133)} \end{aligned}$$

where we have defined

$$G^{o_{\le k}}_{\sigma}(\gamma) := \frac{\int d^{2n}\beta e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}}G^{o_{\le k}}(\beta)}{\int d^{2n}\beta' e^{-\frac{|\beta'|^2}{2\sigma^2}}G^{o_{\le k}}(\beta')}, \tag{S134}$$

where

$$G^{o_{\le k}}(\beta) := \frac{\langle B^{o_{<k}}_{o_k}|\hat{D}^\dagger(\beta)|B^{o_{<k}}_{o_k}\rangle}{\langle B^{o_{<k}}_{o_k}|B^{o_{<k}}_{o_k}\rangle}\cdot\langle A^{o_{<k}}|\hat{D}(\beta)|A^{o_{<k}}\rangle, \tag{S135}$$

which satisfies $G^{o_{\le k}}(\gamma) = G^{o_{\le k}}(-\gamma)^*$.

We thus have

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1, p_{2,\gamma}) = \mathbb{E}_\gamma\sum_{o_{1:N}} p_1(o_{1:N})\max\left\{0,\ 1-\mathbb{E}_{s=\pm1}\prod_{k=1}^{N}\left(1-4\epsilon_0\,\mathrm{Im}\,G^{o_{\le k}}_{\sigma}(s\gamma)\right)\right\}. \tag{S136}$$

Now we can lower bound the following term,

$$\mathbb{E}_{s=\pm1}\prod_{k=1}^{N}\left(1-4\epsilon_0\,\mathrm{Im}\,G_\sigma^{o_{\leq k}}(s\gamma)\right) \tag{S137}$$

$$\geq \prod_{k=1}^{N}\sqrt{\left(1-4\epsilon_0\,\mathrm{Im}\,G_\sigma^{o_{\leq k}}(+\gamma)\right)\left(1-4\epsilon_0\,\mathrm{Im}\,G_\sigma^{o_{\leq k}}(-\gamma)\right)} \tag{S138}$$

$$= \prod_{k=1}^{N}\sqrt{1-16\epsilon_0^2\left(\mathrm{Im}\,G_\sigma^{o_{\leq k}}(\gamma)\right)^2} \tag{S139}$$

$$\geq \prod_{k=1}^{N}\left(1-16\epsilon_0^2\left(\mathrm{Im}G_\sigma^{o_{\leq k}}(\gamma)\right)^2\right) \tag{S140}$$

$$\geq 1-\sum_{k=1}^{N}16\epsilon_0^2|G_\sigma^{o_{\leq k}}(\gamma)|^2, \tag{S141}$$

where the second line uses the AM-GM inequality and the fact that the expression inside the bracket is the ratio of two conditional probabilities and is thus non-negative; the third line uses the fact that $\mathrm{Im}\,G_\sigma^{o_{\leq k}}(\gamma) = -\,\mathrm{Im}\,G_\sigma^{o_{\leq k}}(-\gamma)$; the fourth line uses $\sqrt{1-x}\geq 1-x, \forall\, 0\leq x\leq 1$; and the final line uses the inequality $\prod_i(1-x_i)\geq 1-\sum_i x_i$ for all $0\leq x_i\leq 1$. Thus, we can get rid of the maximum in the expression of the average TVD as

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1,p_{2,\gamma}) \leq \sum_{o_{1:N}} p_1(o_{1:N})\sum_{k=1}^{N}16\epsilon_0^2\mathbb{E}_\gamma|G_\sigma^{o_{\leq k}}(\gamma)|^2. \tag{S142}$$

To further upper bound the R.H.S., we need the following Lemma S1. The lemma is analogous to Pauli twirling in discrete-variable systems but also takes finite energy into consideration. The proof of Lemma S1 is given in Sec. S3 B; Alternatively, when the input states and measurements are restricted to be Gaussian, a more straightforward calculation is possible, yielding different bounds, which we will present in Sec. S3 C.

Lemma S1. *For any* $|A^{o_{<k}}\rangle, |B_{o_k}^{o_{<k}}\rangle$ *we have*

$$\mathbb{E}_\gamma|G_\sigma^{o_{\leq k}}(\gamma)|^2 \leq \left(\frac{1+2\sigma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^n, \tag{S143}$$

given that $\sigma^2 \leq \max\left\{\frac{1}{2}-2\sigma_\gamma^2,\ \sigma_\gamma^2\left(\sqrt{1+\frac{1}{4\sigma_\gamma^4}}-1\right)\right\}$.

Thanks to Lemma S1, we get the following upper bound

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1,p_{2,\gamma}) \leq \sum_{o_{1:N}} p_1(o_{1:N})\sum_{k=1}^{N}16\epsilon_0^2\left(\frac{1+2\sigma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^n = 16N\epsilon_0^2\left(\frac{1+2\sigma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^n. \tag{S144}$$

Combining this with the lower bound in Eq. (S125) and substituting $\epsilon = 0.98\epsilon_0$,

$$N \geq 0.01\epsilon^{-2}\left(1+\frac{4\sigma_\gamma^2}{1+2\sigma^2}\right)^n. \tag{S145}$$

By substituting $2\sigma_\gamma^2 = 0.99\kappa$, we obtain the lower bound as claimed in Theorem S2. □

In Fig. S3, we compare the upper bound of the TMSV+BM scheme to the derived lower bound of entanglement-free schemes. In contrast to the main text, we set $\sigma = 0.3$ to consider a more practical case for experimental realization in the near future. To see how much energy is required to realize the 3-peak channel, one can easily check that for a given σ, the corresponding single-mode depolarizing channel Λ_0 transforms a vacuum input state to a thermal state of mean photon number $1/2\sigma^2$. Since this channel is a product channel, it implies that we need $1/2\sigma^2$ average photons per mode. For our choice $\sigma = 0.3$, $1/2\sigma^2 \approx 5.56$. Since the envelope determined by σ has a larger contribution than γ that determines the oscillation, we are required to produce approximately $1/2\sigma^2$ photon number on average. It is worth emphasizing that for $\kappa \leq 2.5$, the choice satisfies the condition of Theorem S2.

B. Proof of Lemma S1

In this section we prove Lemma S1. Let $|A\rangle, |B\rangle$ be arbitrary normalized pure states in the n-mode bosonic Hilbert space. Define

$$G(\beta) \coloneqq \langle B|\hat{D}^\dagger(\beta)|B\rangle\langle A|\hat{D}(\beta)|A\rangle, \tag{S146}$$

$$G_\sigma(\gamma) \coloneqq \frac{[\mathcal{N}_\sigma * G](\gamma)}{[\mathcal{N}_\sigma * G](0)} \coloneqq \frac{\int d^{2n}\beta \exp(-|\beta-\gamma|^2/2\sigma^2)G(\beta)}{\int d^{2n}\beta \exp(-|\beta|^2/2\sigma^2)G(\beta)}. \tag{S147}$$

Here $*$ stands for convolution. We are going to prove the following inequality

$$\mathbb{E}_\gamma|G_\sigma(\gamma)|^2 = \frac{\mathbb{E}_\gamma|[\mathcal{N}_\sigma * G](\gamma)|^2}{|[\mathcal{N}_\sigma * G](0)|^2} \leq \left(\frac{1+2\sigma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^n, \tag{S148}$$

where $\gamma \sim q(\gamma) \coloneqq \left(\frac{1}{2\pi\sigma_\gamma^2}\right)^n \exp\left(-\frac{|\gamma|^2}{2\sigma_\gamma^2}\right)$ and $\sigma^2 \leq \max\left\{\frac{1}{2} - 2\sigma_\gamma^2,\ \sigma_\gamma^2\left(\sqrt{1+\frac{1}{4\sigma_\gamma^4}} - 1\right)\right\}$.

First of all, write the following expression in the Fourier basis

$$[\mathcal{N}_\sigma * G](\gamma) = \frac{1}{\pi^{2n}}\int d^{2n}\omega e^{\omega^\dagger\gamma-\gamma^\dagger\omega}F_{[\mathcal{N}_\sigma * G]}(\omega) = \frac{1}{\pi^{2n}}\int d^{2n}\omega e^{\omega^\dagger\gamma-\gamma^\dagger\omega}F_{\mathcal{N}_\sigma}(\omega)F_G(\omega), \tag{S149}$$

where the last equality uses the convolution theorem [11]. The Fourier component of $\mathcal{N}_\sigma$ is

$$F_{\mathcal{N}_\sigma}(\omega) = \int d^{2n}\beta e^{-\frac{|\beta|^2}{2\sigma^2}} e^{\beta^\dagger\omega-\omega^\dagger\beta} = (2\pi\sigma^2)^n e^{-2\sigma^2|\omega|^2}. \tag{S150}$$

The Fourier component of G can be computed as

$$F_G(\omega) = \int d^{2n}\beta \langle B|\hat{D}^\dagger(\beta)|B\rangle\langle A|\hat{D}(\beta)|A\rangle e^{\beta^\dagger\omega-\omega^\dagger\beta} \tag{S151}$$

$$= \int d^{2n}\beta \langle B|\hat{D}^\dagger(\beta)|B\rangle\langle A|\hat{D}^\dagger(\omega)\hat{D}(\beta)\hat{D}(\omega)|A\rangle \tag{S152}$$

$$= \pi^n|\langle B|\hat{D}(\omega)|A\rangle|^2, \tag{S153}$$

where the second line uses $\hat{D}^\dagger(\omega)\hat{D}(\beta)\hat{D}(\omega) = e^{\beta^\dagger\omega-\omega^\dagger\beta}\hat{D}(\beta)$, and the last line is by Eq. (S1). Thus,

$$|[\mathcal{N}_\sigma * G](\gamma)|^2 \tag{S154}$$

$$= \left|\frac{1}{\pi^{2n}}\int d^{2n}\omega e^{\omega^\dagger\gamma-\gamma^\dagger\omega}F_{\mathcal{N}_\sigma}(\omega)F_G(\omega)\right|^2 \tag{S155}$$

$$= \frac{1}{\pi^{4n}}\int d^{2n}\omega d^{2n}\omega' e^{(\omega-\omega')^\dagger\gamma-\gamma^\dagger(\omega-\omega')}F_{\mathcal{N}_\sigma}(\omega)F^*_{\mathcal{N}_\sigma}(\omega')F_G(\omega)F^*_G(\omega') \tag{S156}$$

$$= (2\sigma^2)^{2n}\int d^{2n}\omega d^{2n}\omega' e^{(\omega-\omega')^\dagger\gamma-\gamma^\dagger(\omega-\omega')}e^{-2\sigma^2(|\omega|^2+|\omega'|^2)}|\langle B,B|\hat{D}(\omega)\otimes\hat{D}(\omega')|A,A\rangle|^2. \tag{S157}$$

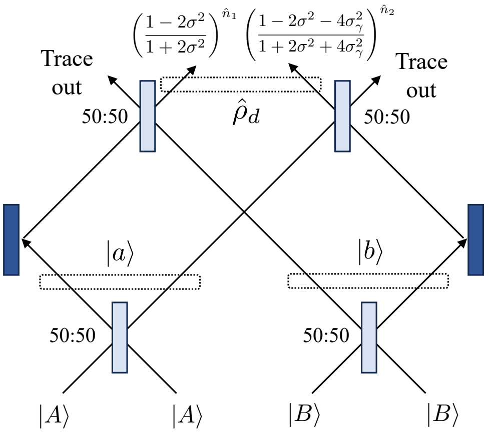

$\left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1}$
$\left(\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^{\hat{n}_2}$
Trace out
Trace out
50:50
$\hat{\rho}_d$
50:50
$|a\rangle$
$|b\rangle$
50:50
50:50
$|A\rangle$
$|A\rangle$
$|B\rangle$
$|B\rangle$

FIG. S4. Schematics for Eq. (S164) to (S169). Here, each line represents n-mode state, and we omit the phase factors for simplicity.

After averaging over Gaussian distribution of γ, we obtain the numerator

$$\mathbb{E}_\gamma|[\mathcal{N}_\sigma * G](\gamma)|^2 = (2\sigma^2)^{2n}\int d^{2n}\omega d^{2n}\omega' e^{-2\sigma_\gamma^2|\omega-\omega'|^2}e^{-2\sigma^2(|\omega|^2+|\omega'|^2)}|\langle B,B|\hat{D}(\omega)\otimes\hat{D}(\omega')|A,A\rangle|^2 \tag{S158}$$

$$= (2\sigma^2)^{2n}\int d^{2n}\alpha d^{2n}\beta e^{-4\sigma_\gamma^2|\beta|^2}e^{-2\sigma^2(|\alpha|^2+|\beta|^2)}|\langle B,B|\hat{U}_{\text{BS}}^\dagger\hat{D}(\alpha)\otimes\hat{D}(\beta)\hat{U}_{\text{BS}}|A,A\rangle|^2. \tag{S159}$$

Here, we changed the variable as $\omega = (\alpha+\beta)/\sqrt{2}$ and $\omega' = (\alpha-\beta)/\sqrt{2}$, i.e., $(\omega+\omega')/\sqrt{2} = \alpha$ and $(\omega-\omega')/\sqrt{2} = \beta$ and chose the 50:50 beam splitter such that

$$\hat{U}_{\text{BS}}^\dagger\hat{D}(\alpha)\otimes\hat{D}(\beta)\hat{U}_{\text{BS}} = \hat{D}((\alpha+\beta)/\sqrt{2})\otimes\hat{D}((\alpha-\beta)/\sqrt{2}). \tag{S160}$$

The denominator follows similarly from Eq. (S157) as

$$|[\mathcal{N}_\sigma * G](0)|^2 = (2\sigma^2)^{2n}\int d^{2n}\omega d^{2n}\omega' e^{-2\sigma^2(|\omega|^2+|\omega'|^2)}|\langle B,B|\hat{D}(\omega)\otimes\hat{D}(\omega')|A,A\rangle|^2 \tag{S161}$$

$$= (2\sigma^2)^{2n}\int d^{2n}\alpha d^{2n}\beta e^{-2\sigma^2(|\alpha|^2+|\beta|^2)}|\langle B,B|\hat{U}_{\text{BS}}^\dagger\hat{D}(\alpha)\otimes\hat{D}(\beta)\hat{U}_{\text{BS}}|A,A\rangle|^2. \tag{S162}$$

To further simplify the expressions, note that by applying the convolution theorem to Eq. (S151), we have

$$\frac{1}{\pi^n}|\langle B|\hat{D}(\alpha)|A\rangle|^2 = \int d^{2n}\beta W_A(\beta)W_B(\beta-\alpha), \tag{S163}$$

where W_A and W_B are the Wigner functions of the states $|A\rangle$ and $|B\rangle$, respectively. Here, note the sign in the arguments due to the complex conjugate of the characteristic function, $\langle B|\hat{D}^\dagger(\beta)|B\rangle$, in

Eq. (S151). Thus, by defining the $2n$-mode states $|a\rangle := \hat{U}_{\mathrm{BS}}|A, A\rangle$ and $|b\rangle := \hat{U}_{\mathrm{BS}}|B, B\rangle$, we have

$$\int d^{2n}\alpha d^{2n}\beta e^{-4\sigma_\gamma^2|\beta|^2} e^{-2\sigma^2(|\alpha|^2+|\beta|^2)} |\langle B, B|\hat{U}_{\mathrm{BS}}^\dagger \hat{D}(\alpha) \otimes \hat{D}(\beta)\hat{U}_{\mathrm{BS}}|A, A\rangle|^2 \tag{S164}$$

$$= \pi^{2n} \int d^{2n}\omega_1 d^{2n}\omega_2 d^{2n}\alpha d^{2n}\beta e^{-2\sigma^2|\alpha|^2} e^{-(4\sigma_\gamma^2+2\sigma^2)|\beta|^2} W_a(\omega_1, \omega_2) W_b(\omega_1 - \alpha, \omega_2 - \beta) \tag{S165}$$

$$= \pi^{2n} \int d^{2n}\omega_1 d^{2n}\omega_2 d^{2n}\gamma_1 d^{2n}\gamma_2 e^{-2\sigma^2|\omega_1-\gamma_1|^2} e^{-(4\sigma_\gamma^2+2\sigma^2)|\omega_2-\gamma_2|^2} W_a(\omega_1, \omega_2) W_b(\gamma_1, \gamma_2) \tag{S166}$$

$$= \pi^{2n} \int d^{2n}\alpha_1 d^{2n}\alpha_2 d^{2n}\beta_1 d^{2n}\beta_2 e^{-4\sigma^2|\alpha_1|^2} e^{-(8\sigma_\gamma^2+4\sigma^2)|\alpha_2|^2} W_a\left(\frac{\alpha_1+\beta_1}{\sqrt{2}}, \frac{\alpha_2+\beta_2}{\sqrt{2}}\right) W_b\left(\frac{\beta_1-\alpha_1}{\sqrt{2}}, \frac{\beta_2-\alpha_2}{\sqrt{2}}\right) \tag{S167}$$

$$= \pi^{2n} \int d^{2n}\alpha_1 d^{2n}\alpha_2 e^{-4\sigma^2|\alpha_1|^2} e^{-(8\sigma_\gamma^2+4\sigma^2)|\alpha_2|^2} W_d(\alpha_1, \alpha_2) \tag{S168}$$

$$= \pi^{2n}(1+2\sigma^2)^{-n}(1+2\sigma^2+4\sigma_\gamma^2)^{-n} \operatorname{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^{\hat{n}_2}\right], \tag{S169}$$

where we used the convolution theorem for the first equality, and we changed the variables for the second and third equalities, and

$$W_d(\alpha_1, \alpha_2) = \int d^{2n}\beta_1 d^{2n}\beta_2 W_a\left(\frac{\alpha_1+\beta_1}{\sqrt{2}}, \frac{\alpha_2+\beta_2}{\sqrt{2}}\right) W_b\left(\frac{\beta_1-\alpha_1}{\sqrt{2}}, \frac{\beta_2-\alpha_2}{\sqrt{2}}\right) \tag{S170}$$

is the Wigner function of the state $\hat{\rho}_d$ obtained by applying a 50:50 beam splitter to the state $|a\rangle$ and $|b\rangle$ and tracing out half of the output. For the last equality, $\hat{n}_1$ and $\hat{n}_2$ are the sum of the photon number operators for the first and second n modes, respectively, and we use the following correspondence between the Wigner function and the operator

$$\frac{e^{-4x|\alpha|^2}}{\pi^n} \iff \frac{[(1-2x)/(1+2x)]^{\hat{n}}}{(1+2x)^n}, \tag{S171}$$

for any $x > 0$ (see e.g. [12, Eq. (3.6.39)]). Note that, when $x > 1/2$ the R.H.S. is proportional to a thermal state. Similar methods have been used to prove the maximum fidelity of Gaussian channels [13]. We illustrate the procedure in Fig. S4. With the same logic, we have

$$\int d^{2n}\alpha d^{2n}\beta e^{-2\sigma^2(|\alpha|^2+|\beta|^2)} |\langle B, B|\hat{U}_{\mathrm{BS}}^\dagger \hat{D}(\alpha) \otimes \hat{D}(\beta)\hat{U}_{\mathrm{BS}}|A, A\rangle|^2 \tag{S172}$$

$$= \pi^{2n}(1+2\sigma^2)^{-2n} \operatorname{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_2}\right]. \tag{S173}$$

Hence, we have

$$\mathbb{E}_\gamma |G_\sigma(\gamma)|^2 = \left(\frac{1+2\sigma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^n \frac{\operatorname{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^{\hat{n}_2}\right]}{\operatorname{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_2}\right]}. \tag{S174}$$

We now consider two parameter regimes. First, if $2\sigma^2 + 4\sigma_\gamma^2 \leq 1$, the operators on the R.H.S. are positive-semidefinite, and it is not hard to see, by monotonicity, that

$$\frac{\operatorname{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^{\hat{n}_2}\right]}{\operatorname{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_2}\right]} \leq 1. \tag{S175}$$

Second, if $2\sigma^2 + 4\sigma_\gamma^2 > 1$ but $2\sigma^2 \leq 2\sigma_\gamma^2 \left(\sqrt{1+\frac{1}{4\sigma_\gamma^4}} - 1\right) \leq 1$ (the last inequality holds for all $\sigma_\gamma > 0$), the above can be bounded as

$$\frac{\mathrm{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^{\hat{n}_2}\right]}{\mathrm{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_2}\right]} \leq \frac{\mathrm{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left|\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right|^{\hat{n}_2}\right]}{\mathrm{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_2}\right]} \tag{S176}$$

$$= \frac{\mathrm{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\Sigma^2}{1+2\Sigma^2}\right)^{\hat{n}_2}\right]}{\mathrm{Tr}\left[\hat{\rho}_d \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_1} \otimes \left(\frac{1-2\sigma^2}{1+2\sigma^2}\right)^{\hat{n}_2}\right]} \tag{S177}$$

$$\leq 1, \tag{S178}$$

where, in the second line, we define $-\frac{1-2\sigma^2-4\sigma_\gamma^2}{1+2\sigma^2+4\sigma_\gamma^2} := \frac{1-2\Sigma^2}{1+2\Sigma^2}$, i.e., $\Sigma^2 = \frac{1}{4(\sigma^2+2\sigma_\gamma^2)}$. In the third line, we use $\Sigma^2 \geq \sigma^2$, which can be easily verified under our assumptions for σ. Therefore, as long as $\sigma^2 \leq \max\left\{\frac{1}{2} - 2\sigma_\gamma^2,\ \sigma_\gamma^2\left(\sqrt{1+\frac{1}{4\sigma_\gamma^4}} - 1\right)\right\}$, we have the following bound

$$\mathbb{E}_\gamma |G_\sigma(\gamma)|^2 \leq \left(\frac{1+2\sigma^2}{1+2\sigma^2+4\sigma_\gamma^2}\right)^n. \tag{S179}$$

This completes the proof of Lemma S1. Note that the equality can be achieved if $\hat{\rho}_d$ is chosen to be the vacuum state. One can verify this holds when $|A\rangle = |B\rangle = |\alpha\rangle$ for some coherent state $|\alpha\rangle$.

C. Lower bound for entanglement-free Gaussian schemes

In this section, we give a lower bound for a specific class of scheme, the *Gaussian schemes*, which may be of independent interest. An ancilla-free Gaussian scheme is specified by collections of adaptively chosen Gaussian input state and Gaussian measurements. Again, thanks to convexity, we again consider only pure input states and rank-1 POVM measurements. A Gaussian input state can be expressed as $|A\rangle = \hat{D}(\omega)|\bar{A}\rangle$, where $|\bar{A}\rangle$ is a centered (*i.e.*, zero-mean) Gaussian state; A Gaussian POVM can be written as

$$\hat{\Pi}(\alpha) = |B\rangle\langle B| = \frac{1}{\pi^n}\hat{D}(\alpha)|\bar{B}\rangle\langle\bar{B}|\hat{D}^\dagger(\alpha), \tag{S180}$$

for outcomes $\alpha \in \mathbb{C}^n$, where $|\bar{B}\rangle$ is a centered Gaussian state. We refer the readers to Ref. [1–3] for more details about Gaussian quantum information.

Proposition S3. *Given positive numbers $n, \sigma, \kappa, \epsilon$ such that*

$$n \geq 8, \quad \epsilon \leq 0.24. \tag{S181}$$

If there exists an entanglement-free Gaussian scheme such that, after learning from N copies of an n-mode random displacement channel $\Lambda \in \mathbf{\Lambda}^{\epsilon,\sigma}_{\text{3-peak}}$, and then receiving a query $\beta \in \mathbb{C}^n$, can return an estimate $\tilde{\lambda}(\beta)$ of $\lambda(\beta)$ such that $|\tilde{\lambda}(\beta) - \lambda(\beta)| \leq \epsilon$ with probability at least $2/3$ for all β such that $|\beta|^2 \leq n\kappa$, then

$$N \geq 0.01\epsilon^{-2}\min\left\{\left(1+\frac{0.99\kappa}{\sigma^2}\right)^{n/2},\ \left(1+\frac{1.98\kappa}{1+2\sigma^2}\right)^n\right\}. \tag{S182}$$

A few remarks before presenting the proof: When $\kappa = O(1)$ and $\sigma^2 \ll \kappa$, the second expression in the minimization dominates, and we recover Theorem S2. On the other hand, the bound for Gaussian schemes also holds for arbitrarily large σ, though the upper bound will enter a different branch and the separation with entanglement-assisted schemes becomes weaker.

Proof. Consider the same partially-revealed hypothesis-testing task and the same strategy used by Bob in the proof of Theorem S2. Recall that the average TVD under the two hypotheses is lower bounded by

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1, p_{2,\gamma}) \geq 0.1666. \tag{S183}$$

To upper bound the average TVD, recall the following bound derived in Eq. (S142),

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1, p_{2,\gamma}) \leq \sum_{o_{1:N}} p_1(o_{1:N}) \sum_{k=1}^{N} 16\epsilon_0^2 \mathbb{E}_\gamma |G_\sigma^{o_{\leq k}}(\gamma)|^2, \tag{S184}$$

with $G_\sigma^{o_{\leq k}}$ defined as

$$G_\sigma^{o_{\leq k}}(\gamma) = \frac{\int d^{2n}\beta e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}} G^{o_{\leq k}}(\beta)}{\int d^{2n}\beta' e^{-\frac{|\beta'|^2}{2\sigma^2}} G^{o_{\leq k}}(\beta')}, \tag{S185}$$

$$G^{o_{\leq k}}(\beta) = \frac{\langle B_{o_k}^{o_{<k}} | \hat{D}^\dagger(\beta) | B_{o_k}^{o_{<k}} \rangle}{\langle B_{o_k}^{o_{<k}} | B_{o_k}^{o_{<k}} \rangle} \cdot \langle A^{o_{<k}} | \hat{D}(\beta) | A^{o_{<k}} \rangle, \tag{S186}$$

Note that this bound holds for any σ. Now we calculate the R.H.S. with Gaussian schemes. First compute $G^{o_{\leq k}}(\beta)$,

$$G^{o_{\leq k}}(\beta) = \langle \bar{B} | \hat{D}^\dagger(\alpha) \hat{D}^\dagger(\beta) \hat{D}(\alpha) | \bar{B} \rangle \langle A | \hat{D}(\beta) | A \rangle = \langle \bar{B} | \hat{D}^\dagger(\beta) | \bar{B} \rangle \langle \bar{A} | \hat{D}(\beta) | \bar{A} \rangle e^{\beta^\dagger(\alpha-\omega)-(\alpha-\omega)^\dagger\beta}, \tag{S187}$$

Here, without loss of generality, we can always write $|\bar{A}\rangle = \hat{U}_{\mathrm{BS}_A} \hat{U}_{\mathrm{sq}_A} |0\rangle$, where $\hat{U}_{\mathrm{BS}_A}$ represents the unitary operator for a beam-splitter network and $\hat{U}_{\mathrm{sq}_A}$ represents the product of single-mode squeezing operations. Similarly, $|\bar{B}\rangle = \hat{U}_{\mathrm{BS}_B} \hat{U}_{\mathrm{sq}_B} |0\rangle$.

To simplify $G^{o_{\leq k}}(\beta)$, using $\hat{a} := (\hat{x} + i\hat{p})/\sqrt{2}$, we can rewrite the displacement operator as

$$\hat{D}(\beta) := \exp\Big(\beta \hat{a}^\dagger - \beta^\dagger \hat{a}\Big) = \exp\Big(\sqrt{2}i \operatorname{Im}\beta \hat{x} - \sqrt{2}i \operatorname{Re}\beta \hat{p}\Big) = \exp\Big(\sqrt{2}iv \cdot \hat{q}\Big), \tag{S188}$$

where $\hat{q} := (\hat{x}_1, \ldots, \hat{x}_n, \hat{p}_1, \ldots, \hat{p}_n)^{\mathrm{T}}$ and $v(\beta) := (\operatorname{Im}\beta_1, \ldots, \operatorname{Im}\beta_n, \operatorname{Re}\beta_1, \ldots, \operatorname{Re}\beta_n)^{\mathrm{T}}$. And

$$\langle 0 | \hat{D}(\beta) | 0 \rangle = e^{-\frac{1}{2}|\beta|^2} = e^{-\frac{1}{2}|v|^2}. \tag{S189}$$

Now, let us introduce the symplectic matrix S that describes the dynamics of quadrature operators under Gaussian unitary operation $\hat{U}$:

$$\hat{U}^\dagger \hat{q}_i \hat{U} = (S\hat{q})_i. \tag{S190}$$

Since the Gaussian unitary operation we consider is written as $\hat{U}_{\mathrm{BS}} \hat{U}_{\mathrm{sq}}$, the symplectic matrix can be decomposed as $S = S_{\mathrm{BS}} S_{\mathrm{sq}}$. Here, S_{BS} is an orthogonal matrix and $\hat{S}_{\mathrm{sq}}$ can be explicitly written as $\mathrm{diag}(e^{r_1}, \ldots, e^{r_n}, e^{-r_1}, \ldots, e^{-r_n})$, where $r_1, \ldots, r_n \geq 0$ represent squeezing parameters for each mode. We use r for squeezing parameters for $|A\rangle$ and s for $|\bar{B}\rangle$. After the symplectic transformation S, the displacement operator transforms as

$$\exp\Big(\sqrt{2}iv^{\mathrm{T}}\hat{q}\Big) \to \exp\Big(\sqrt{2}iv\cdot(S\hat{q})\Big) = \exp\Big(\sqrt{2}i(S^{\mathrm{T}}v)\cdot\hat{q}\Big), \tag{S191}$$

and

$$\langle 0|\exp\Big(\sqrt{2}i(S^{\mathrm{T}}v)\cdot\hat{q}\Big)|0\rangle = e^{-\frac{1}{2}|S^{\mathrm{T}}v|^2} \tag{S192}$$

Thus,

$$\langle\bar{A}|\hat{D}(\beta)|\bar{A}\rangle = \langle 0|\hat{U}^{\dagger}_{\mathrm{sq}_A}\hat{U}^{\dagger}_{\mathrm{BS}_A}\hat{D}(\beta)\hat{U}_{\mathrm{BS}_A}\hat{U}_{\mathrm{sq}_A}|0\rangle = e^{-\frac{1}{2}|S_A^{\mathrm{T}}v|^2}, \tag{S193}$$

and

$$\langle\bar{B}|\hat{D}^{\dagger}(\beta)|\bar{B}\rangle = \langle\bar{B}|\hat{D}(\beta)|\bar{B}\rangle = e^{-\frac{1}{2}|S_B^{\mathrm{T}}v'|^2} = e^{-\frac{1}{2}|S_B^{\mathrm{T}}v|^2}, \tag{S194}$$

where $v \coloneqq v(\beta)$. The first equality is due to the fact that $\langle\bar{B}|\hat{D}^{\dagger}(\beta)|\bar{B}\rangle$ is real. And we can write the phase factor as

$$\exp\left(\beta^{\dagger}(\alpha-\omega)-\beta(\alpha-\omega)^{\dagger}\right) = \exp\Big(2iv^{\mathrm{T}}u\Big), \tag{S195}$$

where $u \coloneqq (-\operatorname{Re}(\alpha_1-\omega_1),\ldots,-\operatorname{Re}(\alpha_n-\omega_n),\operatorname{Im}(\alpha_1-\omega_1),\ldots,\operatorname{Im}(\alpha_n-\omega_n))^{\mathrm{T}}$. Thus,

$$G^{o_{\leq k}}(\beta) = \langle\bar{B}|\hat{D}^{\dagger}(\beta)|\bar{B}\rangle\langle\bar{A}|\hat{D}(\beta)|\bar{A}\rangle e^{\beta^{\dagger}(\alpha-\omega)-(\alpha-\omega)^{\dagger}\beta} \tag{S196}$$

$$= \exp\left[-\frac{1}{2}v^{\mathrm{T}}(S_AS_A^{\mathrm{T}}+S_BS_B^{\mathrm{T}})v + 2iv^{\mathrm{T}}u\right] \tag{S197}$$

$$\coloneqq \exp\left[-\frac{1}{2}v^{\mathrm{T}}\Sigma v + 2iv^{\mathrm{T}}u\right] \tag{S198}$$

$$= \exp\left[-\frac{1}{2}(Ov)^{\mathrm{T}}D(Ov) + 2i(Ov)^{\mathrm{T}}\cdot(Ou)\right] \tag{S199}$$

$$= \prod_{i=1}^{2n}\exp\left[-\frac{d_i}{2}\left(v_i'-\frac{2i}{d_i}u_i'\right)^2-\frac{2u_i'^2}{d_i}\right], \tag{S200}$$

where $\Sigma \coloneqq S_AS_A^{\mathrm{T}}+S_BS_B^{\mathrm{T}} > 0$ is diagonalized as $\Sigma = O^{\mathrm{T}}DO$ with diagonal matrix $D = \operatorname{diag}(d_1,\ldots,d_{2n}) > 0$, and $v' \coloneqq Ov$, $u' \coloneqq Ou$. Let us analyze the spectrum of D. Note that since $S_AS_A^{\mathrm{T}}$ and $S_BS_B^{\mathrm{T}}$ are physical covariance matrices, $S_AS_A^{\mathrm{T}} \geq i\Omega$, $S_BS_B^{\mathrm{T}} \geq i\Omega$, and thus $\Sigma \geq 2i\Omega$ [3], where

$$\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes \mathbb{1}_M. \tag{S201}$$

Hence, by the Williamson decomposition [3], the spectrum of Σ is composed of pairs such that the product of the ith and $(i+n)$th eigenvalues of this matrix is no smaller than 4. Without loss of generality, we label the eigenvalues $d_1,\ldots,d_{2n}$ in such a way that $d_id_{i+n} \geq 4$ for all $1 \leq i \leq n$.

Now let us compute $G_{\sigma}^{o_{\leq k}}(\gamma)$.

$$G_{\sigma}^{o_{\leq k}}(\gamma) = \frac{\int d^{2n}\beta e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}}G^{o_{\leq k}}(\beta)/(2\pi\sigma^2)^n}{\int d^{2n}\beta' e^{-\frac{|\beta'|^2}{2\sigma^2}}G^{o_{\leq k}}(\beta')/(2\pi\sigma^2)^n} \tag{S202}$$

By defining $z \coloneqq (\operatorname{Im}\gamma_1, \dots, \operatorname{Im}\gamma_n, \operatorname{Re}\gamma_1, \dots, \operatorname{Re}\gamma_n)$, and $z' \coloneqq Oz$, we have

$$\begin{aligned}
&\frac{1}{(2\pi\sigma^2)^n}\int d^{2n}\beta e^{-\frac{|\beta-\gamma|^2}{2\sigma^2}} G^{o_{\le k}}(\beta) \qquad \text{(S203)}\\
=\ &\frac{1}{(2\pi\sigma^2)^n}\int d^{2n}v' \prod_{i=1}^{2n}\exp\left[-\frac{(v_i'-z_i')^2}{2\sigma^2} - \frac{d_i}{2}\left(v_i' - \frac{2i}{d_i}u_i'\right)^2 - \frac{2u_i'^2}{d_i}\right] \qquad \text{(S204)}\\
=\ &\prod_{i=1}^{2n}\left[\frac{1}{\sqrt{1+d_i\sigma^2}}\exp\left(-\frac{2u_i'^2\sigma^2}{1+d_i\sigma^2}\right)\exp\left(\frac{1}{2}\left(\frac{-d_iz_i'^2+4iu_iz_i'}{1+d_i\sigma^2}\right)\right)\right], \qquad \text{(S205)}
\end{aligned}$$

Therefore, we obtain

$$G_\sigma^{o_{\le k}}(\gamma) = \prod_{i=1}^{2n}\exp\left[\frac{1}{2}\left(\frac{-d_iz_i'^2+4iu_iz_i'}{1+d_i\sigma^2}\right)\right], \quad \text{and} \quad |G_\sigma^{o_{\le k}}(\gamma)| = \prod_{i=1}^{2n}\exp\left[\frac{-d_iz_i'^2}{2(1+d_i\sigma^2)}\right]. \tag{S206}$$

Thus, after taking the average over γ, we obtain

$$\mathbb{E}_\gamma|G_\sigma^{o_{\le k}}(\gamma)|^2 = \int d^{2n}z' \frac{e^{-\frac{|z|^2}{2\sigma_\gamma^2}}}{(2\pi\sigma_\gamma^2)^n}\prod_{i=1}^{2n}\exp\left[\frac{-d_iz_i'^2}{(1+d_i\sigma^2)}\right] = \prod_{i=1}^{2n}\sqrt{\frac{1}{1+2d_i\sigma_\gamma^2/(1+d_i\sigma^2))}}. \tag{S207}$$

Substituting this back to Eq. (S184), we obtain the following upper bound for the average TVD

$$\mathbb{E}_\gamma \mathrm{TVD}(p_1, p_{2,\gamma}) \le 16N\epsilon_0^2\prod_{i=1}^{2n}\sqrt{\frac{1}{1+2d_i\sigma_\gamma^2/(1+d_i\sigma^2))}}, \tag{S208}$$

which, combined with the lower bound Eq. (S183) and substituting $\epsilon_0 = \epsilon/0.98$, yields the following sample complexity bound

$$N \ge 0.01\epsilon^{-2}\left(\prod_{i=1}^{2n}\sqrt{1+\frac{2d_i\sigma_\gamma^2}{1+d_i\sigma^2}}\right). \tag{S209}$$

To find a lower bound independent of d_i's, focus on the following product, for any $1 \le i \le n$,

$$\left(1+\frac{2d_i\sigma_\gamma^2}{1+d_i\sigma^2}\right)\left(1+\frac{2d_{i+n}\sigma_\gamma^2}{1+d_{i+n}\sigma^2}\right) \tag{S210}$$

This is an increasing function in d_i and d_{i+n}. We know the spectrum satisfies $d_id_{i+n} \ge 4$. Hence, we can lower bound it by setting $d_{i+n}/2 = 2/d_i \coloneqq d > 0$, which leads to

$$\left(1+\frac{2d_i\sigma_\gamma^2}{1+d_i\sigma^2}\right)\left(1+\frac{2d_{i+n}\sigma_\gamma^2}{1+d_{i+n}\sigma^2}\right) \ge \frac{(d+2\sigma^2+4\sigma_\gamma^2)(1+2d(\sigma^2+2\sigma_\gamma^2))}{(d+2\sigma^2)(1+2d\sigma^2)}. \tag{S211}$$

The R.H.S. is differentiable in d, with its only extreme value at $d=1$ being

$$\left(1+\frac{4\sigma_\gamma^2}{1+2\sigma^2}\right)^2. \tag{S212}$$

Meanwhile, when $d \to 0$ or $d \to \infty$, it becomes $1+2\sigma_\gamma^2/\sigma^2$. We thus have the following lower bound,

$$\left(1+\frac{2d_i\sigma_\gamma^2}{1+d_i\sigma^2}\right)\left(1+\frac{2d_{i+n}\sigma_\gamma^2}{1+d_{i+n}\sigma^2}\right) \ge \min\left\{1+\frac{2\sigma_\gamma^2}{\sigma^2}, \left(1+\frac{4\sigma_\gamma^2}{1+2\sigma^2}\right)^2\right\}, \tag{S213}$$

which gives us the following sample complexity lower bound:

$$N \geq 0.01\epsilon^{-2} \min\left\{\left(1+\frac{2\sigma_\gamma^2}{\sigma^2}\right)^{n/2}, \left(1+\frac{4\sigma_\gamma^2}{1+2\sigma^2}\right)^n\right\}. \tag{S214}$$

Substituting $2\sigma_\gamma^2 = 0.99\kappa$ completes the proof of Proposition S3.

□

S4. GAUSSIAN TAIL EFFECT

In this section, we find the condition that the effect of truncating a multivariate normal distribution is smaller than 0.5, which is used to derive the lower bound for entanglement-free schemes. Consider a multivariate normal distribution:

$$q(\boldsymbol{x}) = \left(\frac{1}{2\pi\sigma^2}\right)^n \exp\left(-\frac{|\boldsymbol{x}|^2}{2\sigma^2}\right), \tag{S215}$$

where $\boldsymbol{x} \in \mathbb{R}^{2n}$. Note that in the main text, while we consider $\gamma \in \mathbb{C}^n$, they are equivalent. Now, we consider a truncated distribution with $|\boldsymbol{x}|^2 \leq R^2$ with a given R:

$$\begin{aligned}\int_{|\boldsymbol{x}|\leq R} d\boldsymbol{x} q(\boldsymbol{x}) &= \int_{|\boldsymbol{x}|\leq R} d\boldsymbol{x} \left(\frac{1}{2\pi\sigma^2}\right)^n \exp\left(-\frac{|\boldsymbol{x}|^2}{2\sigma^2}\right) &\text{(S216)}\\ &= \left(\frac{1}{2\pi\sigma^2}\right)^n \int_0^R dr \int d\Omega_{2n} r^{2n-1} \exp\left(-\frac{r^2}{2\sigma^2}\right) &\text{(S217)}\\ &= 1 - \frac{\Gamma\left(n, \frac{R^2}{2\sigma^2}\right)}{\Gamma(n)}. &\text{(S218)}\end{aligned}$$

where we have used the following integrals:

$$\int d\Omega_n = \frac{2\pi^{n/2}}{\Gamma(n/2)}, \qquad \int_0^R dr r^{2n-1} \exp\left(-\frac{r^2}{2\sigma^2}\right) = 2^{n-1}\sigma^{2n}\left[\Gamma(n) - \Gamma\left(n, \frac{R^2}{2\sigma^2}\right)\right], \tag{S219}$$

and

$$\Gamma(n,x) = \int_x^\infty t^{n-1} e^{-t} dt \tag{S220}$$

is the (upper) incomplete gamma function and $\Gamma(n) = \Gamma(n,0)$. Therefore, the tail probability is given by $\Gamma\left(n, \frac{R^2}{2\sigma^2}\right)/\Gamma(n)$. In the main text and the proof of sample complexity lower bound of entanglement-free schemes, we choose $2\sigma^2 = 0.99\kappa$ and $R^2 = \kappa n$. For our purpose, it suffices to show that $\frac{\Gamma(n,n/0.99)}{\Gamma(n)} \leq 0.5$. To see this, we use the following inequality [14]:

$$\frac{\Gamma(n,kn)}{\Gamma(n)} \leq (ke^{1-k})^n, \quad \forall\ k > 1. \tag{S221}$$

First notice that for $k = 1/0.99$ and $n = 14000$, $(ke^{1-k})^n \leq 0.492$. Now, for every $n < 14000$, one can numerically verify $\frac{\Gamma(n,n/0.99)}{\Gamma(n)} \leq 0.5$ (see Fig. S5); For $n > 14000$, the upper bound $(ke^{1-k})^n$ monotonically decreases with n, so we also have $\frac{\Gamma(n,n/0.99)}{\Gamma(n)} \leq 0.492$. Combining these two cases completes the proof.

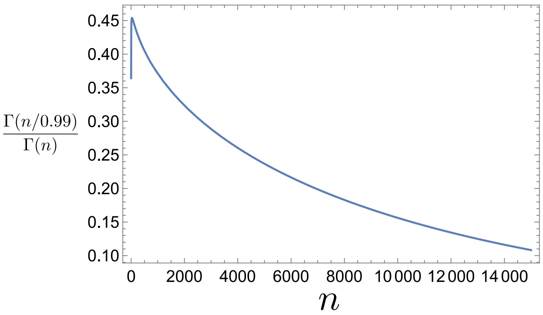


FIG. S5. Numerical verification that the Gaussian tail probability is upper bounded by 0.5 for n up to 14000.

[1] A. Ferraro, S. Olivares, and M. G. Paris, Gaussian states in continuous variable quantum information, arXiv preprint quant-ph/0503237 (2005).

[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Reviews of Modern Physics **84**, 621 (2012).

[3] A. Serafini, *Quantum continuous variables: a primer of theoretical methods* (CRC press, 2017).

[4] H.-Y. Huang, R. Kueng, and J. Preskill, Information-theoretic bounds on quantum advantage in machine learning, Physical Review Letters **126**, 190505 (2021).

[5] D. Aharonov, J. Cotler, and X.-L. Qi, Quantum algorithmic measurement, Nature communications **13**, 1 (2022).

[6] S. Chen, S. Zhou, A. Seif, and L. Jiang, Quantum advantages for pauli channel estimation, Phys. Rev. A **105**, 032435 (2022).

[7] S. Chen, C. Oh, S. Zhou, H.-Y. Huang, and L. Jiang, Tight bounds on pauli channel learning without entanglement, arXiv preprint arXiv:2309.13461 (2023).

[8] S. Chen and W. Gong, Futility and utility of a few ancillas for pauli channel learning, arXiv preprint arXiv:2309.14326 (2023).

[9] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Quantum advantage in learning from experiments, Science **376**, 1182 (2022).

[10] K. Kornelson and D. Larson, Rank-one decomposition of operators and construction of frames, Contemporary Mathematics **345**, 203 (2004).

[11] K. R. Castleman, *Digital image processing* (Prentice Hall Press, 1996).

[12] S. Barnett and P. M. Radmore, *Methods in theoretical quantum optics*, Vol. 15 (Oxford University Press, 2002).

[13] C. M. Caves and K. Wódkiewicz, Fidelity of gaussian channels, Open Systems & Information Dynamics **11**, 309 (2004).

[14] M. Ghosh, Exponential tail bounds for chisquared random variables, Journal of Statistical Theory and Practice **15**, 1 (2021).

Quantum Coherence and Distinguishability: A Resource-Theoretic Perspective on Wave-Particle Duality

Zhiping Liu[1 2] Chengkai Zhu[2] Hua-Lei Yin[3 1] Xin Wang[2]

[1]*Nanjing University, Nanjing 210093, China*
[2] *The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511453, China*
[3] *Renmin University of China, Beijing 100872, China*

Abstract. Wave-particle duality, the cornerstone of quantum mechanics, illustrates essential trade-offs between two complementary aspects of quantum systems. In this work, from the perspective of coherence resource manipulation, we uncover a novel duality relation between quantum coherence and distinguishability in ensembles of mutually orthogonal pure states, treating them as two complementary resources. We demonstrate that the sum of 'co-bits', coherence preserved after discrimination, and classical bits, distinguishability extracted through perfect discrimination is bounded. One cannot simultaneously extract all classical information and preserve coherence. Such duality relation exposes an inherent trade-off between quantum coherence and classical distinguishability resources. Our findings offer a fresh perspective and advance our understanding of the intrinsic complementary relationship between quantum and classical resources. Note: A technical version of this work is attached.

Keywords: Quantum coherence, wave-particle duality, quantum resource theory, quantum state discrimination.

Background. Wave-particle duality, a fundamental principle in quantum mechanics, deeply relates with foundational phenomena such as uncertainty relations [1–3] and Wheeler's delayed-choice experiments [4], as well as to innovative quantum imaging techniques [5, 6]. It reveals an inherent trade-off relation between the display of wave and particle behavior in a single quantum particle. Such duality relation is typically demonstrated in interference experiments [7–10]. In a two-path interferometer experiment, a particle behavior is characterized by path information acquired by a which-path detector, while wave behavior is determined by the visibility of the interference pattern. Quantitative statements of wave-particle duality in two-path interferometer experiments [11, 12], such as the famous inequality by Englert [13] and Jaeger *et al.* [14], are formulated as

$$D^2 + V^2 \leq 1, \tag{1}$$

where D measures path distinguishability, characterizing particle behavior, and V is the visibility of the interference fringe, determining wave behavior.

Furthermore, in extending wave-particle duality relation to multipath interferometers [15, 16], such relation has been reformulated in the context of quantum information theory. These reformulations [17–20] leverage resource theory of coherence [21–24] and quantum state discrimination (QSD) [25], a fundamental quantum information task. By entangling particle and detector states within an interferometer, Eq. (1) was formulated by a duality relation between some coherence measure [26], which substitutes visibility to identify wave properties, and the distinguishability among detector states providing which-path information.

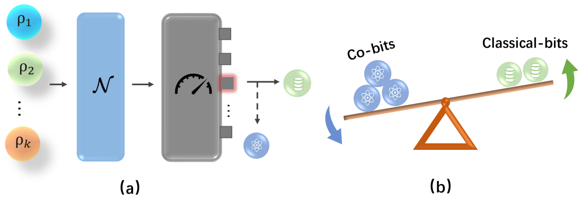


Figure 1: (a) Quantum state discrimination via free operations. The discrimination procedure consists of applying a free operation $\mathcal{N}$ w.r.t. a quantum resource theory and measuring the state in a computational basis. (b) Coherence-distinguishability duality relation. There is an inherent trade-off between the quantum coherence resource ('co-bits') and the classical distinguishability resource ('c-bits').

Coherence stands as a typical quantum resource generating quantum superposition promoting quantum computation algorithms [27, 28] and intrinsic randomness vital in quantum cryptography [29–31]. While distinguishability, contrasted with coherence, acts as a classical resource revealing deterministic classical information encoded in quantum systems [32–34]. The above reformulation caught a glimpse of the deep complementary correlation between quantum and classical resources.

Following up this quantum information perspective, wave-particle duality has been extended into quantum many-body systems [35–37]. An operational meaning of wave-particle duality has also been demonstrated [38]. However, all of these investigations are rooted in interference scenarios. Can we further discern a similar duality relationship between coherence and distinguishability resources in broader and more fundamental quantum scenarios, transcending typical interference experiments? Such inquiry aids in elucidating the intrinsic connection between these two resources themselves from a theoretical perspective for quantum foundations.

Overview of results: This work aims to investigate the manipulation of coherence resources within the context of quantum state discrimination (QSD), offering a fresh perspective on wave-particle duality through the lens of quantum resource theory. Specifically, we establish the following:

1. We propose a general paradigm for quantum state discrimination via quantum channels, enabling the exploration of **quantum resource manipulation** within QSD.

2. We reveal a **coherence-distinguishability duality relation**, quantitatively captured by a bounded sum of 'co-bits' (preserved coherence) and classical bits (extracted distinguishability). This relation highlights a **resource-theoretic nature** of wave-particle duality.

3. We analyze **extreme cases** in this coherence-distinguishability duality relation. First, we show that this duality relation is **tight** by a special case. Secondly, we demonstrate that One cannot simultaneously extract all classical bits and preserve coherence. These observations hint again at the underlying **wave-particle duality relationship** between coherence and distinguishability resource.

Quantum state discrimination via free operations: Our first contribution is to propose a general quantum state discrimination paradigm via quantum channels, which contributes to explore quantum resource manipulation within QSD.

Recall that for the minimum-error state discrimination, one aims to find a Positive Operator-Valued Measure (POVM) $\{E_j\}_{j=0}^{k-1}$ to maximize the average success probability of discriminating a state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ with $\sum_{j=0}^{k-1} p_j = 1, \rho_j \in \mathcal{D}(\mathcal{H}_A)$:

$$P_{\mathrm{suc}}(\Omega) = \max_{\{E_j\}_j} \sum_j p_j \operatorname{Tr}(E_j \rho_j). \tag{2}$$

To investigate the quantum resource manipulation in QSD, we reconsider a general paradigm for discriminating $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ as the following steps in order: (I) Receive an unknown state ρ_j with prior probability p_j. (II) Apply a quantum channel $\mathcal{N}_{A\to BA'}$ to ρ_j, yielding $\omega_{BA'}^{(j)} = \mathcal{N}_{A\to BA'}(\rho_j)$ where $A' \cong A$ and $\dim \mathcal{H}_B = k$. (III) Measure $\omega_{BA'}^{(j)}$ on the subsystem B in computational basis. If the outcome is i, decide the received state is ρ_i.

We call the above quantum channel $\mathcal{N}_{A\to BA'}$ a *discrimination channel.* This paradigm provides an intuitive approach to evaluate the 'resourcefulness' of the discrimination channel, which is crucial for understanding resource dynamics and manipulation within a discrimination task. Specifically, for a given quantum resource theory $(\mathcal{F}, \mathcal{O})$, we introduce the optimal average success probability by free operations as follows.

$$\begin{aligned}\widetilde{P}_{\mathrm{suc},\mathcal{O}}(\Omega) = &\max \sum_{j=0}^{k-1} p_j \operatorname{Tr}[\mathcal{N}_{A\to BA'}(\rho_j)(|j\rangle\langle j|_B \otimes I_{A'})]\\ &\text{s.t. } \mathcal{N}_{A\to BA'} \in \mathcal{O}\end{aligned}$$

Furthermore, we denote $\widetilde{P}_{\mathrm{suc}}(\Omega)$ as the maximal average success probability attainable through operations $\mathcal{N}_{A\to BA'}$ without constraints on their availability. Note if there is an optimal $\mathcal{N}_{A\to BA'} \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_{BA'})$ such that $\widetilde{P}_{\mathrm{suc}}(\Omega) = P_{\mathrm{suc}}(\Omega)$, we say $\mathcal{N}_{A\to BA'}$ can optimally discriminate Ω.

Proposition 1 *For a d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, the optimal discrimination probability $P_{\mathrm{suc}}(\Omega)$ can be achieved by incoherent operations.*

Proposition 1 reveals that the process of optimally discriminating an ensemble Ω does not consume additional quantum coherence. This pivotal finding aligns with the intuition from the wave-particle duality relation that distinguishability cannot increase with an increase in coherence, where they are complementary.

Coherence-distinguishability duality: Our second contribution is to reveal an inherent trade-off between preserved coherence and achievable perfect distinguishability within ensembles of mutually

	Wave-Particle Duality	**Coherence-Distinguishability Duality**
Scenario	Multi-interference experiment	Coherence resource manipulation in QSD
Quantitative Relation	$D^2 + V^2 \leq 1$	$\mathbf{C}_{\text{MIO}}(\Omega) + \mathbf{S}(\Omega) \leq \log d$
Particle behavior	D: Path distinguishability	$\mathbf{S}(\Omega)$: Classical distinguishability bits
Wave behavior	V: Interference fringe visibility	$\mathbf{C}_{\text{MIO}}(\Omega)$: Post-discrimination 'co-bits'
Extreme Case	Perfect path distinguishability $D = 1$ $\Longrightarrow$ No interference $V = 0$	Full classical bit extraction $\mathbf{S}(\Omega) = \log d$ $\Longrightarrow$ No 'co-bits' preserved $\mathbf{C}_{\text{MIO}}(\Omega) = 0$
Equality holding condition	Pure detector states	Maximally coherent states

Table 1: Comparison between Wave-Particle Duality (Eq. (1)) and Coherence-Distinguishability Duality ((Eq. (3))

orthogonal pure states, highlighting the resource-theoretic nature of wave-particle duality.

For coherence analysis, we consider the maximum relative entropy of coherence $C_{\max}(\rho)$ as a coherence measure [22, 39, 40]. The maximal possible value of $C_{\max}(\cdot)$ for a d-dimensional state is achieved by Ψ_d with $C_{\max}(\Psi_d) = \log d$ [41], corresponding with $\log d$ coherent bits (co-bits) [42]. Then, we introduce the *post-disrimination coherence* as the maximum average *co-bits* that can be preserved after a perfect discrimination procedure.

Definition 2 (Post-discrimination coherence) *For a mutually orthogonal d-dimensional state ensemble* $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, *the post-discrimination coherence under maximally incoherent operations is defined as* $\mathbf{C}_{\text{MIO}}(\Omega) := \log(1+\eta)$ *where*

$$\eta = \max\left\{\sum_{j=0}^{k-1} p_j C_R(\sigma_j) : \mathcal{M}(\rho_j) = |j\rangle\langle j| \otimes \sigma_j, \right.$$
$$\left. \sigma_j \in \mathcal{D}(\mathcal{H}_d),\, \forall j,\, \mathcal{M} \in \text{MIO}\right\}.$$

Proposition 1 indicates that there is always a feasible MIO $\mathcal{M}$ for $\mathbf{C}_{\text{MIO}}(\Omega)$.

We recall that the distinguishability emerges from a pure state ensemble $\Omega = \{(p_j, |\psi_j\rangle)\}_{j=0}^{k-1}$ can be characterized by the von-Neumann entropy defined on it [32], i.e., $\mathbf{S}(\Omega) := S(\hat{\omega})$ where $S(\cdot)$ is the von-Neumann entropy of a state and $\hat{\omega} = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ denotes the average state of Ω. In Theorem 3, we demonstrate the duality relation between these two quantities $\mathbf{S}(\Omega)$ and $\mathbf{C}_{\text{MIO}}(\Omega)$.

Theorem 3 (Coherence-distinguishability duality) *For a mutually orthogonal d-dimensional pure-state ensemble* $\Omega = \{(1/k, |\psi_j\rangle)\}_{j=0}^{k-1}$,

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}(\Omega) \leq \log d. \tag{3}$$

Theorem 3 gives a novel wave-particle duality relation through the lens of quantum resource theory. It reveals an intriguing fact that the more classical bits ('c-bits') you want to decode, the fewer 'co-bits' can be preserved after extracting all classical information.

Boundary cases of duality relation: Our third contribution is to analyze extreme cases of this duality relation. We demonstrate the tightness of Eq. (3) and the fact that one cannot simultaneously extract all classical information and preserve coherence.

Proposition 4 *Let* $|\phi_j\rangle = HX^j|0\rangle$ *where* H, X *are the d-dimensional Hadamard gate and generalized Pauli X gate. For* $\Omega = \{(1/k, |\phi_j\rangle)\}_{j=0}^{k-1}$, $k \leq d$,

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}(\Omega) = \log d. \tag{4}$$

Proposition 4 shows that an ensemble of k mutually orthogonal maximally coherent states exactly achieves the upper bound in Eq. (3), which identifies the tightness of this trade-off relation. This finding underscores a novel role for maximally coherent states beyond their established status as golden resources within the quantum resource theory of coherence.

Furthermore, as another boundary case of Theorem 3, we note that when the cardinality of the set Ω is equal to the dimension d, $\mathbf{C}_{\text{MIO}}(\Omega)$ vanishes, indicating that no coherence resource could be preserved after perfect discrimination. The total similarity comparisons between Wave-Particle Duality (Eq. (1)) and Coherence-Distinguishability Duality ((Eq. (3)) are shown in Table 1.

Concluding remarks: In this work, we explore the quantum coherence manipulation within quantum state discrimination and uncover a significant duality relation between quantum coherence and classical distinguishability resources. Our result opens a new avenue for studying wave-particle duality and the uncertainty principle through the lens of quantum resource theories, offering insights to both quantum foundations and quantum information theory.

References

[1] Howard Percy Robertson. The uncertainty principle. *Phys. Rev.*, 34(1):163, 1929. URL https://journals.aps.org/pr/abstract/10.1103/PhysRev.34.163.

[2] Hans Maassen and Jos BM Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60(12):1103, 1988. URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.60.1103.

[3] Patrick J. Coles, Jedrzej Kaniewski, and Stephanie Wehner. Equivalence of wave–particle duality to entropic uncertainty. *Nat. Commun.*, 5(1), December 2014. ISSN 2041-1723. URL http://dx.doi.org/10.1038/ncomms6814.

[4] Xiao-song Ma, Johannes Kofler, and Anton Zeilinger. Delayed-choice gedanken experiments and their realizations. *Rev. Mod. Phys.*, 88(1), March 2016. ISSN 1539-0756. URL http://dx.doi.org/10.1103/RevModPhys.88.015005.

[5] A Gatti, Enrico Brambilla, and LA Lugiato. Entangled imaging and wave-particle duality: from the microscopic to the macroscopic realm. *Phys. Rev. Lett.*, 90(13):133603, 2003. URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.90.133603.

[6] Yiquan Yang, Hong Liang, Xiaze Xu, Lijian Zhang, Shining Zhu, and Xiao-song Ma. Interaction-free, single-pixel quantum imaging with undetected photons. *npj Quantum Inf.*, 9(2), January 2023. ISSN 2056-6387. URL http://dx.doi.org/10.1038/s41534-022-00673-6.

[7] Ralf Menzel, Dirk Puhlmann, Axel Heuer, and Wolfgang P Schleich. Wave-particle dualism and complementarity unraveled by a different mode. *Proc. Natl. Acad. Sci. U.S.A.*, 109(24):9314–9319, 2012. URL https://www.pnas.org/doi/abs/10.1073/pnas.1201271109.

[8] Xingan Wang and Xueming Yang. A molecular double-slit experiment. *Science*, 374(6570):938–939, 2021. URL https://www.science.org/doi/full/10.1126/science.abm5536.

[9] Tai Hyun Yoon and Minhaeng Cho. Quantitative complementarity of wave-particle duality. *Sci. Adv.*, 7(34):eabi9268, 2021. URL https://www.science.org/doi/full/10.1126/sciadv.abi9268.

[10] Dong-Xu Chen, Yu Zhang, Jun-Long Zhao, Qi-Cheng Wu, Yu-Liang Fang, Chui-Ping Yang, and Franco Nori. Experimental investigation of wave-particle duality relations in asymmetric beam interference. *npj Quantum Inf.*, 8(1):101, 2022. URL https://www.nature.com/articles/s41534-022-00610-7.

[11] William K Wootters and Wojciech H Zurek. Complementarity in the double-slit experiment: Quantum nonseparability and a quantitative statement of bohr's principle. *Phys. Rev. D*, 19(2):473, 1979. URL https://journals.aps.org/prd/abstract/10.1103/PhysRevD.19.473.

[12] Daniel M Greenberger and Allaine Yasin. Simultaneous wave and particle knowledge in a neutron interferometer. *Phys. Rev. A*, 128(8):391–394, 1988. URL https://www.sciencedirect.com/science/article/abs/pii/0375960188901144.

[13] Berthold-Georg Englert. Fringe visibility and which-way information: An inequality. *Phys. Rev. Lett.*, 77(11):2154, 1996. URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.77.2154.

[14] Gregg Jaeger, Abner Shimony, and Lev Vaidman. Two interferometric complementarities. *Phys. Rev. A*, 51(1):54, 1995. URL https://journals.aps.org/pra/abstract/10.1103/PhysRevA.51.54.

[15] Stephan Dürr. Quantitative wave-particle duality in multibeam interferometers. *Phys. Rev. A*, 64(4):042113, 2001. URL https://journals.aps.org/pra/abstract/10.1103/PhysRevA.64.042113.

[16] G Bimonte and Renato Musto. Comment on “quantitative wave-particle duality in multibeam interferometers”. *Phys. Rev. A*, 67(6):066101, 2003. URL https://journals.aps.org/pra/abstract/10.1103/PhysRevA.67.066101.

[17] Manabendra Nath Bera, Tabish Qureshi, Mohd Asad Siddiqui, and Arun Kumar Pati. Duality of quantum coherence and path distinguishability. *Phys. Rev. A*, 92

(1), July 2015. ISSN 1094-1622. URL https://journals.aps.org/pra/abstract/10.1103/PhysRevA.92.012118.

[18] Emilio Bagan, János A. Bergou, Seth S. Cottrell, and Mark Hillery. Relations between coherence and path information. *Phys. Rev. Lett.*, 116(16), April 2016. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.116.160406.

[19] Tabish Qureshi and Mohd Asad Siddiqui. Wave–particle duality in n-path interference. *Ann. Phys.*, 385:598–604, 2017. URL http://dx.doi.org/10.1016/j.aop.2017.08.015.

[20] Keerthy K. Menon and Tabish Qureshi. Wave-particle duality in asymmetric beam interference. *Phys. Rev. A*, 98(2), August 2018. ISSN 2469-9934. URL http://dx.doi.org/10.1103/PhysRevA.98.022130.

[21] Andreas Winter and Dong Yang. Operational resource theory of coherence. *Phys. Rev. Lett.*, 116(12), March 2016. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.116.120404.

[22] Carmine Napoli, Thomas R. Bromley, Marco Cianciaruso, Marco Piani, Nathaniel Johnston, and Gerardo Adesso. Robustness of coherence: An operational and observable measure of quantum coherence. *Phys. Rev. Lett.*, 116 (15), apr 2016. URL https://doi.org/10.1103%2Fphysrevlett.116.150502.

[23] Bartosz Regula, Kun Fang, Xin Wang, and Gerardo Adesso. One-shot coherence distillation. *Phys. Rev. Lett.*, 121(1), jul 2018. URL https://doi.org/10.1103%2Fphysrevlett.121.010401.

[24] Kun Fang, Xin Wang, Ludovico Lami, Bartosz Regula, and Gerardo Adesso. Probabilistic distillation of quantum coherence. *Phys. Rev. Lett.*, 121(7), aug 2018. URL https://doi.org/10.1103%2Fphysrevlett.121.070404.

[25] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *J. Phys. A*, 48(8):083001, 2015. URL https://iopscience.iop.org/article/10.1088/1751-8113/48/8/083001/meta.

[26] T. Baumgratz, M. Cramer, and M.B. Plenio. Quantifying coherence. *Phys. Rev. Lett.*, 113(14), September 2014. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.113.140401.

[27] Lov K Grover. Synthesis of quantum superpositions by quantum computation. *Phys. Rev. Lett.*, 85(6):1334, 2000. URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.1334.

[28] Felix Ahnefeld, Thomas Theurer, Dario Egloff, Juan Mauricio Matera, and Martin B. Plenio. Coherence as a resource for shor's algorithm. *Phys. Rev. Lett.*, 129(12), September 2022. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.129.120501.

[29] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, March 1995. ISSN 1094-1622. URL http://dx.doi.org/10.1103/PhysRevA.51.1863.

[30] Xiao Yuan, Hongyi Zhou, Zhu Cao, and Xiongfeng Ma. Intrinsic randomness as a measure of quantum coherence. *Phys. Rev. A*, 92(2), August 2015. ISSN 1094-1622. URL http://dx.doi.org/10.1103/PhysRevA.92.022124.

[31] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Inf.*, 2(1): 16021, 2016. URL https://www.nature.com/articles/npjqi201621.

[32] Richard Jozsa and Jürgen Schlienz. Distinguishability of states and von Neumann entropy. *Phys. Rev. A*, 62(1), June 2000. ISSN 1094-1622. URL http://dx.doi.org/10.1103/PhysRevA.62.012301.

[33] Paul Hausladen, Richard Jozsa, Benjamin Schumacher, Michael Westmoreland, and William K Wootters. Classical information capacity of a quantum channel. *Phys. Rev. A*, 54(3):1869, 1996. URL https://journals.aps.org/pra/abstract/10.1103/PhysRevA.54.1869.

[34] Barbara M. Terhal, David P. DiVincenzo, and Debbie W. Leung. Hiding bits in bell states. *Phys. Rev. Lett.*, 86:5807–5810, Jun 2001. URL https://link.aps.org/doi/10.1103/PhysRevLett.86.5807.

[35] Christoph Dittel, Gabriel Dufour, Gregor Weihs, and Andreas Buchleitner. Wave-particle duality of many-body quantum states. *Phys. Rev. X*, 11(3), August 2021. ISSN 2160-3308. URL http://dx.doi.org/10.1103/PhysRevX.11.031041.

[36] Adrian J. Menssen, Alex E. Jones, Benjamin J. Metcalf, Malte C. Tichy, Stefanie Barz, W. Steven Kolthammer, and Ian A. Walmsley. Distinguishability and many-particle interference. *Phys. Rev. Lett.*, 118(15), April 2017. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.118.153603.

[37] Eric Brunner, Lukas Pausch, Edoardo G. Carnio, Gabriel Dufour, Alberto Rodríguez, and Andreas Buchleitner. Many-body interference at the onset of chaos. *Phys. Rev. Lett.*, 130(8), February 2023. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.130.080401.

[38] Emilio Bagan, John Calsamiglia, János A. Bergou, and Mark Hillery. Duality games and operational duality relations. *Phys. Rev. Lett.*, 120(5), January 2018. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.120.050402.

[39] Kaifeng Bu, Uttam Singh, Shao-Ming Fei, Arun Kumar Pati, and Junde Wu. Maximum relative entropy of coherence: An operational coherence measure. *Phys. Rev. Lett.*, 119(15), October 2017. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.119.150405.

[40] Wenqiang Zheng, Zhihao Ma, Hengyan Wang, Shao-Ming Fei, and Xinhua Peng. Experimental demonstration of observability and operability of robustness of coherence. *Phys. Rev. Lett.*, 120(23):230504, 2018. URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.230504.

[41] Marco Piani, Marco Cianciaruso, Thomas R. Bromley, Carmine Napoli, Nathaniel Johnston, and Gerardo Adesso. Robustness of asymmetry and coherence of quantum states. *Phys. Rev. A*, 93(4), April 2016. ISSN 2469-9934. URL http://dx.doi.org/10.1103/PhysRevA.93.042107.

[42] Eric Chitambar and Min-Hsiu Hsieh. Relating the resource theories of entanglement and quantum coherence. *Phys. Rev. Lett.*, 117(2), July 2016. ISSN 1079-7114. URL http://dx.doi.org/10.1103/PhysRevLett.117.020402.

Quantum Coherence and Distinguishability: A Resource-Theoretic Perspective on Wave-Particle Duality

Zhiping Liu,[1,2,*] Chengkai Zhu,[2,*] Hua-Lei Yin,[3,1] and Xin Wang[2,†]

[1]*National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*
[2]*Thrust of Artificial Intelligence, Information Hub, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511453, China*
[3]*Department of Physics and Beijing Key Laboratory of Opto-electronic Functional Materials and Micro-nano Devices, Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China*

(Dated: May 20, 2024)

Wave-particle duality, a fundamental principle of quantum mechanics, encapsulates the complementary relationship between the wave and particle behaviors of quantum systems. In this paper, we uncover a novel manifestation of this duality by establishing a trade-off between quantum coherence and classical distinguishability through the lens of quantum state discrimination under incoherent operations. We prove that in an ensemble of mutually orthogonal pure states, the sum of 'co-bits', quantifying the coherence preserved under incoherent free operations, and classical bits, representing the distinguishability extracted via quantum state discrimination, is bounded. This coherence-distinguishability duality relation exposes an inherent limitation on the simultaneous preservation of a system's quantum coherence (wave-like property) and extraction of its classical distinguishability (particle-like property). Our findings provide a fresh perspective on wave-particle duality through the paradigm of quantum resource theories, offering fundamental insights into the manipulation of quantum and classical resources, with implications for quantum foundations and quantum technologies.

Introduction.— Can all physical observables of a system be sharply determined simultaneously, or say is there any trade-off relation among them? Heisenberg answered this pivotal question with his famous uncertainty principle [1]. This fundamental principle states that the more accurately one measures the position of a particle, the less accurately one can measure its momentum, and vice versa. Uncertainty principles deeply reveal an inherent knowledge trade-off between two complementary observables of a quantum system [2]. Under a modern formulation in terms of entropy [3–5], uncertainty relation is further shown to be equivalent to another intriguing and fundamental phenomenon in quantum mechanics, namely wave-particle duality.

Wave-particle duality stated by Bohr's complementarity principle [6] also reveals an inherent trade-off relation between two conjugate properties of a quantum object. This describes a competition phenomenon between the display of wave and particle behavior for a single quantum particle. Such duality relation is typically demonstrated in interference experiments [7–10], such as the double-slit experiment or two-path interferometer. In such experiments, a particle behavior is characterized by path information acquired by a which-path detector, while wave behavior is determined by the visibility of the interference pattern. Quantitative statements of wave-particle duality [11, 12], such as the famous inequality by Englert [13] and Jaeger *et al.* [14], are formulated as

$$D^2 + V^2 \leq 1, \tag{1}$$

where D represents path distinguishability and V denotes visibility of the interference fringe. Perfect path distinguishability ($D = 1$) corresponds to complete particle behavior, thus no interference pattern will exhibit ($V = 0$).

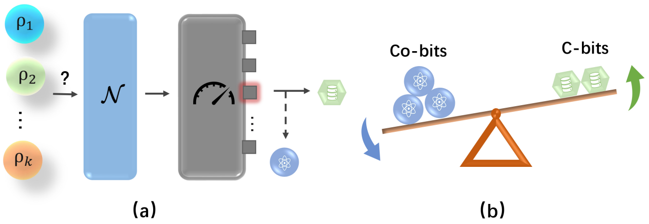


Fig 1. (a) Quantum state discrimination via free operations. The discrimination procedure consists of applying a free operation $\mathcal{N}$ w.r.t. a quantum resource theory and measuring the state on a computational basis. (b) Coherence-distinguishability duality relation. There is a trade-off between the quantum coherence resource ('co-bits') and the classical distinguishability resource ('c-bits').

Furthermore, in extending wave-particle duality relation to multipath interferometers [15, 16], such relation has been reformulated within the context of quantum information theory. These reformulations [17–20] leverage the resource theory of coherence [21–24] and quantum state discrimination (QSD) [25], a fundamental task in quantum information theory. By entangling particle and detector states within an interferometer, Eq. (1) was formulated by a duality relation between some coherence measure [26] replacing visibility to identifying wave property, and the distinguishability among detector states providing which-path information. In this context, perfect distinguishability of mutually orthogonal detector states implies full path information and the absence of coherence.

Coherence stands as a typical quantum resource generating quantum superposition promoting quantum computation

[*] Zhiping Liu and Chengkai Zhu contributed equally to this work.
[†] felixxinwang@hkust-gz.edu.cn

algorithms [27, 28] and intrinsic randomness vital in quantum cryptography [29–31]. While distinguishability, contrasted with coherence, acts as a classical resource revealing deterministic classical information encoded in quantum systems [32–34]. The above reformulation caught a glimpse of the deep complementary correlation between quantum and classical resources.

Following up this quantum information perspective, wave-particle duality has been extended into complicated quantum many-body systems [35–37]. An operational meaning of wave-particle duality has also been demonstrated within discrimination games [38]. However, all of these investigations are rooted in interference scenarios, where the path of particles is entangled with corresponding detector states within an interferometer. Can we further discern a similar duality relationship between coherence and distinguishability resources in broader and more fundamental quantum scenarios, transcending typical interference experiments? Such inquiry aids in elucidating the intrinsic connection between these two resources themselves from a theoretical perspective for quantum foundations.

In this work, we uncover a novel coherence-distinguishability duality relation within mutually orthogonal pure-state ensembles. Different from supposing a multipath interferometer scenario as previous works, our discovery stems from exploring coherence resource manipulation by introducing a new paradigm for QSD via free operations (see Fig. 1(a)). This duality relation shows that the more one extracts classical information by discriminating states in the ensemble, the less one can preserve the coherence, and vice versa. It unveils an inherent trade-off between the coherence resource preserved after discrimination and the achievable perfect distinguishability within these ensembles (see Fig. 1(b)).

In particular, we present two intriguing cases derived from our coherence-distinguishability duality relation. Firstly, we reveal that our duality relation is tight. When considering mutually orthogonal maximally coherent states, the sum of the maximum co-bits left and the classical bits we can extract achieves the bound $\log d$. Secondly, we demonstrate that in discriminating a complete orthonormal basis of a d-dimensional Hilbert space, no coherence can be preserved while extracting $\log d$ classical bits. This is a mutually exclusive extreme situation within our duality relation. Our work establishes a profound connection between coherence and distinguishability as fundamental resources, generalizing the wave-particle duality relation into a new scenario within the realm of quantum resource theory.

Quantum state discrimination via free operations.— We begin with an introduction to quantum resource theories and quantum state discrimination. Let $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ denote the set of linear operations from a d_A-dimensional Hilbert space $\mathcal{H}_A$ to $\mathcal{H}_B$. Let $\mathcal{D}(\mathcal{H}_A)$ be the set of density operators acting on $\mathcal{H}_A$, and $\mathcal{N}_{A\to B}$ be a quantum operation from system A to B which is a completely positive and trace-preserving map. A quantum resource theory of states is defined as a tuple $(\mathcal{F}, \mathcal{O})$ where $\mathcal{F}$ is the set of free states; $\mathcal{O}$ is the set of free operations that preserve free states, i.e., $\mathcal{N}(\rho) \in \mathcal{F}, \forall \mathcal{N} \in \mathcal{O}, \forall \rho \in \mathcal{F}$. For $(\mathcal{F}, \mathcal{O})$, a reasonable resource measure $\mathcal{R}(\rho) \in \mathbb{R}, \forall \rho \in \mathcal{D}(\mathcal{H}_A)$ satisfies monotonicity $\mathcal{R}(\mathcal{N}(\rho)) \le \mathcal{R}(\rho)$ and positivity $\mathcal{R}(\rho) \ge 0, \forall \rho \in \mathcal{D}(\mathcal{H}_A), \forall \mathcal{N} \in \mathcal{O}$. Such a quantum resource theory intuitively arises when there is a restricted set of operations $\mathcal{O}$ that are significantly easier to implement than the others, e.g., local operations and classical communication (LOCC) in entanglement theory [39], Clifford operations in the quantum resource theory of magic states [40, 41].

For coherence, we start by fixing the incoherent basis as the computational basis $\{|i\rangle\}_i$ when considering circuit-based quantum computation, since the encoding and decoding of the information will be reduced to the classical application of stochastic matrices onto probability vectors if there is no coherence involved. We denote by $\mathcal{I}$ the set of incoherent states, i.e., those diagonal in $\{|i\rangle\}_i$. For a given dimension d, we denote $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle$ as the maximally coherent state, and denote $\Psi_d = |\Psi_d\rangle\langle\Psi_d|$. The maximal set of operations that map incoherent states to incoherent states is called the maximally incoherent operations (MIO) [42]. Other common free operations include incoherent operations (IO) [26], dephasing-covariant incoherent operations (DIO) [43, 44] and strictly incoherent operations (SIO) [21]. There are hierarchies among these free operations: SIO $\subsetneq$ IO $\subsetneq$ MIO, SIO $\subsetneq$ DIO $\subsetneq$ MIO [43]. More details about QRT of coherence can be found in the appendix.

Recall that for the minimum-error state discrimination, one aims to find a Positive Operator-Valued Measure (POVM) $\{E_j\}_{j=0}^{k-1}$ to maximize the average success probability of discriminating a state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ with $\sum_j p_j = 1, \rho_j \in \mathcal{D}(\mathcal{H}_A)$:

$$P_{\rm suc}(\Omega) = \max_{\{E_j\}_j} \sum_j p_j \operatorname{Tr}(E_j \rho_j). \tag{2}$$

Numerous studies have been carried out to understand the limits of such a task when measurements are restricted to different classes, including POVMs with locality constraints [45–53] (i.e., LOCC, separable, PPT POVMs), incoherent [54], stabilizer measurement [55], all of which are considered within the context of different quantum resource theories.

To investigate the quantum resource manipulation in QSD, we reconsider a general paradigm for discriminating $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ as the following steps in order: (I) Receive an unknown state ρ_j with prior probability p_j. (II) Apply a quantum channel $\mathcal{N}_{A\to BA'}$ to ρ_j, yielding $\omega_{BA'}^{(j)} = \mathcal{N}_{A\to BA'}(\rho_j)$ where $A' \cong A$ and $\dim \mathcal{H}_B = k$. (III) Measure $\omega_{BA'}^{(j)}$ on the subsystem B in computational basis. If the outcome is i, decide the received state is ρ_i.

We call the above quantum channel $\mathcal{N}_{A\to BA'}$ a *discrimination channel*. This paradigm provides an intuitive approach to evaluate the 'resourcefulness' of the discrimination channel, which is crucial for understanding resource dynamics and manipulation within a discrimination task. Specifically, for a given quantum state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ and a quantum resource theory $(\mathcal{F}, \mathcal{O})$, we introduce the optimal average success probability by free operations as follows.

$$\widetilde{P}_{\text{suc},\mathcal{O}}(\Omega) = \max \sum_{j=0}^{k-1} p_j \operatorname{Tr}[\mathcal{N}_{A\to BA'}(\rho_j)(|j\rangle\langle j|_B \otimes I_{A'})]$$
$$\text{s.t. } \mathcal{N}_{A\to BA'} \in \mathcal{O}$$

Furthermore, we denote $\widetilde{P}_{\text{suc}}(\Omega)$ as the maximal average success probability attainable through operations $\mathcal{N}_{A\to BA'}$ without constraints on their availability. It is worth noting that $\widetilde{P}_{\text{suc},\mathcal{O}}(\Omega)$ can be equivalently characterized by optimization over operations $\mathcal{N}_{A\to B} \in \mathcal{O}$, since discarding the subsystem A' typically constitutes a free operation. However, the inclusion of the reference system A' facilitates a comprehensive examination of resource dynamics during the discrimination process. This concept is elaborated further in Theorem 2. Note if there is an optimal $\mathcal{N}_{A\to BA'} \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_{BA'})$ such that $\widetilde{P}_{\text{suc}}(\Omega) = P_{\text{suc}}(\Omega)$, we say $\mathcal{N}_{A\to BA'}$ can optimally discriminate Ω.

Coherence manipulation in state discrimination.— Now, in the context of quantum coherence manipulation in QSD, we present our first result that the process of optimally discriminating an ensemble Ω does not necessitate the consumption of additional quantum coherence. We establish this by demonstrating that the optimal average success probability, typically associated with unrestricted general POVMs, can be realized through free operations within the prescribed paradigm of a discrimination process.

Proposition 1 *For a d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, the optimal discrimination probability $P_{\text{suc}}(\Omega)$ can be achieved by incoherent operations.*

Proposition 1 is established by proving $P_{\text{suc}}(\Omega) = \widetilde{P}_{\text{suc,IO}}(\Omega) = \widetilde{P}_{\text{suc,MIO}}(\Omega)$, with the detailed proof deferred to appendix. The wave-particle duality relation reminds us that an increase in visibility pattern always implies a decrease in path discrimination. This pivotal finding aligns with the intuition from the wave-particle duality relation that distinguishability cannot increase with an increase in coherence, where they are complementary.

This result also highlights the importance of exploring QSD tasks within the context of dynamical quantum resources, as proposed in our paradigm, rather than focusing solely on restrictions on POVMs. From the perspective of resource theories of measurements [54, 56–58], the 'free measurements' for coherence are previously considered as incoherent measurements, which are diagonal in the fixed basis $\{|i\rangle\}_i$. However, this characterization yields a limited understanding of QSD tasks in the context of resource theories. We establish that QSD performed by incoherent measurements is merely equivalent to our aforementioned process with a discrimination channel belonging to DIO (SIO), a strict subset of MIO (IO), as shown in the appendix. Hence, incoherent measurements generally fall short of achieving optimal discrimination by Proposition 1. This analysis suggests that MIO possesses an intrinsic advantage over DIO in the task of coherent state discrimination, which can be quantified by the generalized robustness of incoherent measurements [54, 56]. This insight establishes a strict hierarchy between MIO and DIO on the optimal discrimination of coherent states.

When optimal discrimination associated with global POVMs is not achievable through free measurements alone, it is intuitive to consider employing ancillary resource states to enhance discrimination capabilities [59–61]. In this way, the resource cost for a QSD task is quantified by the minimal number of copies of the resource state required for reaching optimal global discrimination. However, examining the resource cost of QSD via DIO (SIO), which is tantamount to performing incoherent measurements, reveals a subtlety. For any optimal channel $\mathcal{N} \in \mathcal{O}$ that attains $\widetilde{P}_{\text{suc},\mathcal{O}}(\Omega)$, applying the dephasing channel Δ before or after $\mathcal{N}$ yields the same outcome when $\mathcal{N}$ is DIO (SIO), i.e., $\Delta \circ \mathcal{N}(\rho \otimes \Psi_d) = \mathcal{N} \circ \Delta(\rho \otimes \Psi_d), \forall \rho$. Thus, Ψ_d does not assist in simulating any more powerful discrimination channel through DIO (SIO). This insight implies a no-go case for reaching optimal global discrimination via DIO (SIO) in discriminating general coherent state ensembles.

Coherence-distinguishability duality.— Given that optimal discrimination does not involve additional consumption of coherence, it is reasonable to postulate that the process may consume the coherence present within the state ensemble itself, owing to the decoherence effect of the discrimination task. Then it prompts intriguing questions: how much coherence can be maximally preserved after a discrimination process? By characterizing this maximally preserved coherence, can we establish a duality relation between the distinguishability and coherence resources?

To address this question, we start with the problem of discriminating an ensemble of mutually orthogonal pure states. For coherence analysis, we consider the maximum relative entropy of coherence as a coherence measure [62]. It is denoted as $C_{\max}(\rho) = \log(1 + C_R(\rho))$ where $C_R(\rho) = \min_{\sigma\in\mathcal{D}(\mathcal{H}_d)}\{s \geq 0 | \frac{\rho+s\sigma}{1+s} := \tau \in \mathcal{I}\}$ is the robustness of coherence [22, 63]. The logarithm is taken under the base of two throughout the paper. The maximal value of $C_{\max}(\cdot)$ for a d-dimensional state is achieved by Ψ_d with $C_{\max}(\Psi_d) = \log d$ [64], corresponding with $\log d$ coherent bits (co-bits) [65]. Then, we introduce the *post-disrimination coherence* as the maximum average *co-bits* that can be preserved after a perfect discrimination procedure.

Definition 1 (Post-discrimination coherence) *For a mutually orthogonal d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, the post-discrimination coherence under maximally incoherent operations is defined as $\mathbf{C}_{\text{MIO}}(\Omega) := \log(1+\eta)$ where*

$$\eta = \max\Big\{\sum_{j=0}^{k-1} p_j C_R(\sigma_j) : \mathcal{M}(\rho_j) = |j\rangle\langle j| \otimes \sigma_j,$$
$$\sigma_j \in \mathcal{D}(\mathcal{H}_d),\ \forall j,\ \mathcal{M} \in \text{MIO}\Big\}.$$

It is worth noting that, by Proposition 1, there is always a feasible maximally incoherent operation $\mathcal{M}$ for $\mathbf{C}_{\text{MIO}}(\Omega)$.

The constraint $\mathcal{M}(\rho_j) = |j\rangle\langle j| \otimes \sigma_j$ corresponds to the criterion for perfect discrimination of a mutually orthogonal state ensemble, wherein $\{\sigma_j\}_{j=0}^{k-1}$ act as memory states that restore coherence. This quantity evaluates the average resource retained in the quantum states after a discrimination process by maximally incoherent operations. Notably, it can be efficiently computed by semidefinite programming (SDP), which is a powerful tool in quantum information theory [66, 67].

To characterize the distinguishability, we recall that the distinguishability emerges from a pure state ensemble $\Omega = \{(p_j, |\psi_j\rangle)\}_{j=0}^{k-1}$ can be characterized by the von-Neumann entropy defined on it [32], i.e., $\mathbf{S}(\Omega) := S(\hat{\omega})$ where $S(\cdot)$ is the von-Neumann entropy of a state and $\hat{\omega} = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ denotes the average state of Ω. We are now ready to present our main result of the relationship between these two quantities $\mathbf{S}(\Omega)$ and $\mathbf{C}_{\text{MIO}}(\Omega)$, for a mutually orthogonal pure-state ensemble Ω.

Theorem 2 (Coherence-distinguishability duality) *For a mutually orthogonal d-dimensional pure-state ensemble $\Omega = \{(1/k, |\psi_j\rangle)\}_{j=0}^{k-1}$,*

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}(\Omega) \leq \log d. \tag{3}$$

Notice that from the state ensemble Ω, one can distill $\mathbf{S}(\Omega)$ bits of classical information by perfectly discriminating any given unknown state within the ensemble. For such a fixed state ensemble Ω, the maximum number of co-bits that can be left after perfect discrimination has an upper bound directly related to the von-Neunman entropy of Ω. Moreover, this theorem reveals an intriguing and crucial fact that the more classical bits (‘c-bits’) you want to decode, the fewer ‘co-bits’ can be preserved after extracting all classical information. The proof of Theorem 2 is deferred to the appendix.

We note that Theorem 2 is not entirely a prior unexpected, as a discrimination procedure appears to introduce decoherence. However, remarkably, this quantitative relationship gives a novel wave-particle duality relation as the following. Since we are dealing with a d-dimensional Hilbert space, we can further normalize the post-discrimination coherence $\mathbf{C}_{\text{MIO}}(\Omega)$ and the von-Neunman entropy $\mathbf{S}(\Omega)$ of an ensemble at the same time by $\widetilde{V}^2 = \mathbf{C}_{\text{MIO}}(\Omega)/\log d$ and $\widetilde{D}^2 = \mathbf{S}(\Omega)/\log d$. Thus, we uncover a wave-particle duality-like relation as follows.

$$\widetilde{V}^2 + \widetilde{D}^2 \leq 1, \tag{4}$$

which is akin to the form of Eq. (1). This relation is an inherent duality property of a state ensemble containing mutually orthogonal pure states prepared with equal probability.

More generally, we can extend this duality relation into the state ensemble with non-uniform distribution. If we characterize the distinguishability with the min-entropy of $\mathbf{S}_{\min}(\Omega) := -H_{\max}(\hat{\omega}||\mathbb{I}) = \mathbf{S}_{\min}(\hat{\omega})$, where $\hat{\omega}$ denotes the average state of Ω and $\mathbf{S}_{\min}(\hat{\omega}) = -\log p_{\max}$ is the min-entropy of $\hat{\omega}$ [68], then for a mutually orthogonal d-dimensional pure-state ensemble $\Omega = \{(p_j, |\psi_j\rangle)\}_{j=0}^{k-1}$,

$$\mathbf{C}_{\text{MIO}}(\Omega) + \mathbf{S}_{\min}(\Omega) \leq \log d. \tag{5}$$

The relative proof remains in the appendix. This duality relation reveals that the sum of ‘co-bits’ maximally preserved and ‘c-bits’ at least gained is also bounded, although this bound is not generally tight.

Boundary cases of duality.— To deepen our understanding of the coherence-distinguishability duality relation, we explore two specific instances illuminating its fundamental aspects. Firstly, analogous to how squeezed coherent states in quantum optics reach the Heisenberg uncertainty limit [69], we identify a particular state ensemble that makes the equality in Eq. (3) hold. Let H denote the d-dimensional Hadamard gate, given by $H = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{kj} |k\rangle\langle j|$ where $\omega = e^{i2\pi/d}$, and X denote the d-dimensional generalized Pauli X gate, given by $X = \sum_{i=0}^{d-1} |i+1\rangle\langle i|$. Then we have the following.

Proposition 3 *Let $|\phi_j\rangle = HX^j|0\rangle$ where H, X are the d-dimensional Hadamard gate and generalized Pauli X gate. For $\Omega = \{(1/k, |\phi_j\rangle)\}_{j=0}^{k-1}$, $k \leq d$,*

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}(\Omega) = \log d. \tag{6}$$

Proposition 3 shows that an ensemble of k mutually orthogonal maximally coherent states exactly achieves the upper bound in Eq. (3), which identifies the tightness of this trade-off relation. The proof is provided in the appendix. This finding underscores a novel role for maximally coherent states beyond their established status as golden resources within the quantum resource theory of coherence. It is also interesting to seek other non-trivial ensemble cases saturating the coherence-distinguishability duality relation. A necessary condition for those ensembles to achieve the upper bound can be found in the appendix.

Furthermore, as another boundary case of Theorem 2, we note that when the cardinality of the set Ω is equal to the dimension d, $\mathbf{C}_{\text{MIO}}(\Omega)$ vanishes, indicating that no coherence could be preserved after perfect discrimination. Equivalently, this states that if a quantum channel $\mathcal{N} \in$ MIO exists such that $\mathcal{N}(|\psi_j\rangle\langle\psi_j|) = |j\rangle\langle j| \otimes \sigma_j$, $\sigma_j \in \mathcal{H}_d$ for each $j = 0, 1, ..., d-1$, then each σ_j must be an incoherent state. It illustrates an extreme case in which it is inherently unfeasible to completely extract all c-bits encoded in a complete orthonormal basis of the Hilbert space through MIO while concurrently maintaining any co-bit. This scenario reveals a mutual exclusion between coherence and distinguishability within the ensemble of mutually orthogonal pure states, analogous to the situation described by $D = 1$ and $V = 0$ in Eq. (1). Another extreme situation arises when the ensemble Ω contains only one state ρ, where no distinguishability can be obtained and the coherence of ρ remains completely preserved, as $\mathbf{C}_{\text{MIO}}(\Omega) = C_{\max}(\rho)$. These observations hint again at an underlying wave-particle duality relationship within these ensembles.

Concluding remarks.— In this work, we explore the manipulation of quantum coherence within quantum state discrimination by proposing a general QSD paradigm via quantum operations. Leveraging this new paradigm of QSD, we treat coherence and distinguishability as two complementary resources and then uncover a significant coherence-distinguishability duality relation. This relation emerges from a mutually orthogonal pure-state ensemble where free operations cannot simultaneously accomplish the extraction of all c-bits and the preservation of the co-bits.

Note that the seminal work [17] also established a duality between coherence and path distinguishability via unambiguous state discrimination, focusing on extending the wave-particle duality to multipath interference. In their setting, the particle states and path detector states are entangled within the interferometer forming a total system state. Coherence is quantified with tracing out the detector states, while distinguishability arises from an ensemble of detector states that allow unambiguous discrimination. Orthogonal detector states signify complete distinguishability and the absence of coherence. Our work, however, derives a duality relation from orthogonal state ensembles, presenting a fresh perspective on resource manipulation that contrasts with the interference scenarios addressed in prior research.

We anticipate that our paradigm for QSD may be applied to advance the understanding of the interplay between classical distinguishability and other quantum resources, such as entanglement, magic, thermodynamics [70, 71] and imaginarity [72]. There is a possibility of exploring other duality relations between every two potential complementary resources. Furthermore, it is interesting to study if there is any uncertainty relation formulation of our coherence-distinguishability duality relation, considering that wave-particle duality relation is a special case of uncertainty relation.

Acknowledgments.– We thank Bartosz Regula for the suggestion of extending the duality relation into a pure state ensemble with non-uniform distribution and for other helpful discussions. We also thank Ranyiliu Chen, Kun Wang, and Benchi Zhao for their helpful comments. This work was partially supported by the Start-up Fund (No. G0101000151) from HKUST (Guangzhou), the Guangdong Provincial Quantum Science Strategic Initiative (No. GDZX2303007), the National Key R&D Program of China (No.2024YFE0102500), and the Education Bureau of Guangzhou Municipality. Z.L. acknowledges the support from National Natural Science Foundation of China (No. 12274223).

[1] W. Heisenberg, Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik, Zeitschrift für Physik **43**, 172 (1927).

[2] H. P. Robertson, The uncertainty principle, Phys. Rev. **34**, 163 (1929).

[3] H. Maassen and J. B. Uffink, Generalized entropic uncertainty relations, Phys. Rev. Lett. **60**, 1103 (1988).

[4] P. J. Coles, J. Kaniewski, and S. Wehner, Equivalence of waveparticle duality to entropic uncertainty, Nat. Commun. **5** (2014).

[5] P. J. Coles, Entropic framework for wave-particle duality in multipath interferometers, Phys. Rev. A **93** (2016).

[6] N. Bohr *et al.*, *The quantum postulate and the recent development of atomic theory*, Vol. 3 (Printed in Great Britain by R. & R. Clarke, Limited, 1928).

[7] R. Menzel, D. Puhlmann, A. Heuer, and W. P. Schleich, Wave-particle dualism and complementarity unraveled by a different mode, Proc. Natl. Acad. Sci. U.S.A. **109**, 9314 (2012).

[8] X. Wang and X. Yang, A molecular double-slit experiment, Science **374**, 938 (2021).

[9] T. H. Yoon and M. Cho, Quantitative complementarity of wave-particle duality, Sci. Adv. **7**, eabi9268 (2021).

[10] D.-X. Chen, Y. Zhang, J.-L. Zhao, Q.-C. Wu, Y.-L. Fang, C.-P. Yang, and F. Nori, Experimental investigation of wave-particle duality relations in asymmetric beam interference, npj Quantum Inf. **8**, 101 (2022).

[11] W. K. Wootters and W. H. Zurek, Complementarity in the double-slit experiment: Quantum nonseparability and a quantitative statement of bohr's principle, Phys. Rev. D **19**, 473 (1979).

[12] D. M. Greenberger and A. Yasin, Simultaneous wave and particle knowledge in a neutron interferometer, Phys. Rev. A **128**, 391 (1988).

[13] B.-G. Englert, Fringe visibility and which-way information: An inequality, Phys. Rev. Lett. **77**, 2154 (1996).

[14] G. Jaeger, A. Shimony, and L. Vaidman, Two interferometric complementarities, Phys. Rev. A **51**, 54 (1995).

[15] S. Dürr, Quantitative wave-particle duality in multibeam interferometers, Phys. Rev. A **64**, 042113 (2001).

[16] G. Bimonte and R. Musto, Comment on quantitative wave-particle duality in multibeam interferometers, Phys. Rev. A **67**, 066101 (2003).

[17] M. N. Bera, T. Qureshi, M. A. Siddiqui, and A. K. Pati, Duality of quantum coherence and path distinguishability, Phys. Rev. A **92** (2015).

[18] E. Bagan, J. A. Bergou, S. S. Cottrell, and M. Hillery, Relations between coherence and path information, Phys. Rev. Lett. **116** (2016).

[19] T. Qureshi and M. A. Siddiqui, Wave–particle duality in n-path interference, Ann. Phys. **385**, 598 (2017).

[20] K. K. Menon and T. Qureshi, Wave-particle duality in asymmetric beam interference, Phys. Rev. A **98** (2018).

[21] A. Winter and D. Yang, Operational resource theory of coherence, Phys. Rev. Lett. **116** (2016).

[22] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, Robustness of coherence: An operational and observable measure of quantum coherence, Phys. Rev. Lett. **116** (2016).

[23] B. Regula, K. Fang, X. Wang, and G. Adesso, One-shot coherence distillation, Phys. Rev. Lett. **121** (2018).

[24] K. Fang, X. Wang, L. Lami, B. Regula, and G. Adesso, Probabilistic distillation of quantum coherence, Phys. Rev. Lett. **121** (2018).

[25] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications, J. Phys. A **48**, 083001 (2015).

[26] T. Baumgratz, M. Cramer, and M. Plenio, Quantifying coherence, Phys. Rev. Lett. **113** (2014).

[27] L. K. Grover, Synthesis of quantum superpositions by quantum computation, Phys. Rev. Lett. **85**, 1334 (2000).

[28] F. Ahnefeld, T. Theurer, D. Egloff, J. M. Matera, and M. B. Plenio, Coherence as a resource for shors algorithm, Phys. Rev. Lett. **129** (2022).

[29] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 18631869 (1995).

[30] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Intrinsic randomness as a measure of quantum coherence, Phys. Rev. A **92** (2015).

[31] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Inf. **2**, 16021 (2016).

[32] R. Jozsa and J. Schlienz, Distinguishability of states and von Neumann entropy, Phys. Rev. A **62** (2000).

[33] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Classical information capacity of a quantum channel, Phys. Rev. A **54**, 1869 (1996).

[34] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Hiding bits in bell states, Phys. Rev. Lett. **86**, 5807 (2001).

[35] C. Dittel, G. Dufour, G. Weihs, and A. Buchleitner, Wave-particle duality of many-body quantum states, Phys. Rev. X **11** (2021).

[36] A. J. Menssen, A. E. Jones, B. J. Metcalf, M. C. Tichy, S. Barz, W. S. Kolthammer, and I. A. Walmsley, Distinguishability and many-particle interference, Phys. Rev. Lett. **118** (2017).

[37] E. Brunner, L. Pausch, E. G. Carnio, G. Dufour, A. Rodríguez, and A. Buchleitner, Many-body interference at the onset of chaos, Phys. Rev. Lett. **130** (2023).

[38] E. Bagan, J. Calsamiglia, J. A. Bergou, and M. Hillery, Duality games and operational duality relations, Phys. Rev. Lett. **120** (2018).

[39] E. Chitambar, D. Leung, L. Maninska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), Commun. Math. Phys. **328**, 303326 (2014).

[40] V. Veitch, S. A. Hamed Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New J. Phys. **16**, 013009 (2014).

[41] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, New J. Phys. **14**, 113011 (2012).

[42] J. Aberg, Quantifying superposition (2006), arXiv:quant-ph/0612146 [quant-ph].

[43] E. Chitambar and G. Gour, Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence, Phys. Rev. Lett. **117**, 030401 (2016).

[44] I. Marvian and R. W. Spekkens, How to quantify coherence: Distinguishing speakable and unspeakable notions, Phys. Rev. A **94** (2016).

[45] S. Bandyopadhyay, S. Halder, and M. Nathanson, Entanglement as a resource for local state discrimination in multipartite systems, Phys. Rev. A **94** (2016).

[46] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, A framework for bounding nonlocality of state discrimination, Commun. Math. Phys. **323**, 1121 (2013).

[47] S. Bandyopadhyay, More nonlocality with less purity, Phys. Rev. Lett. **106**, 210402 (2011).

[48] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Strong quantum nonlocality without entanglement, Phys. Rev. Lett. **122** (2019).

[49] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local distinguishability of multipartite orthogonal quantum states, Phys. Rev. Lett. **85**, 4972 (2000).

[50] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Phys. Rev. A **59**, 1070 (1999).

[51] E. Chitambar, R. Duan, and M.-H. Hsieh, When do local operations and classical communication suffice for two-qubit state discrimination?, IEEE Trans. Inf. Theory **60**, 1549 (2013).

[52] E. Chitambar and M.-H. Hsieh, Revisiting the optimal detection of quantum information, Phys. Rev. A **88**, 020302 (2013).

[53] C. Zhu, C. Zhu, Z. Liu, and X. Wang, Entanglement cost of discriminating quantum states under locality constraints (2024), arXiv:2402.18446 [quant-ph].

[54] M. Oszmaniec and T. Biswas, Operational relevance of resource theories of quantum measurements, Quantum **3**, 133 (2019).

[55] C. Zhu, Z. Liu, C. Zhu, and X. Wang, Limitations of classically-simulable measurements for quantum state discrimination (2023), arXiv:2310.11323 [quant-ph].

[56] R. Takagi and B. Regula, General resource theories in quantum mechanics and beyond: Operational characterization via discrimination tasks, Phys. Rev. X **9** (2019).

[57] R. Takagi, B. Regula, K. Bu, Z.-W. Liu, and G. Adesso, Operational advantage of quantum resources in subchannel discrimination, Phys. Rev. Lett. **122**, 140402 (2019).

[58] A. F. Ducuara and P. Skrzypczyk, Operational interpretation of weight-based resource quantifiers in convex quantum resource theories, Phys. Rev. Lett. **125** (2020).

[59] S. Bandyopadhyay, G. Brassard, S. Kimmel, and W. K. Wootters, Entanglement cost of nonlocal measurements, Phys. Rev. A **80**, 012313 (2009).

[60] N. Yu, R. Duan, and M. Ying, Distinguishability of quantum states by positive operator-valued measures with positive partial transpose, IEEE Trans. Inf. Theory **60**, 20692079 (2014).

[61] S. Bandyopadhyay and V. Russo, Entanglement cost of discriminating noisy bell states by local operations and classical communication, Phys. Rev. A **104** (2021).

[62] K. Bu, U. Singh, S.-M. Fei, A. K. Pati, and J. Wu, Maximum relative entropy of coherence: An operational coherence measure, Phys. Rev. Lett. **119** (2017).

[63] W. Zheng, Z. Ma, H. Wang, S.-M. Fei, and X. Peng, Experimental demonstration of observability and operability of robustness of coherence, Phys. Rev. Lett. **120**, 230504 (2018).

[64] M. Piani, M. Cianciaruso, T. R. Bromley, C. Napoli, N. Johnston, and G. Adesso, Robustness of asymmetry and coherence of quantum states, Phys. Rev. A **93** (2016).

[65] E. Chitambar and M.-H. Hsieh, Relating the resource theories of entanglement and quantum coherence, Phys. Rev. Lett. **117** (2016).

[66] X. Wang, Semidefinite optimization for quantum information, PhD thesis (2018).

[67] P. Skrzypczyk and D. Cavalcanti, Semidefinite Programming in Quantum Information Science, arXiv preprint arXiv:2306.11637 (2023).

[68] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 43374347 (2009).

[69] D. F. Walls, Squeezed states of light, Nature **306**, 141 (1983).

[70] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Yunger Halpern, The resource theory of informational nonequilibrium in thermodynamics, Phys. Rep. **583**, 158 (2015).

[71] G. Chiribella, F. Meng, R. Renner, and M.-H. Yung, The nonequilibrium cost of accurate information processing, Nat. Commun. **13**, 7155 (2022).

[72] K.-D. Wu, T. V. Kondra, S. Rana, C. M. Scandolo, G.-Y. Xiang, C.-F. Li, G.-C. Guo, and A. Streltsov, Resource theory of imaginarity: Quantification and state conversion, Phys. Rev. A **103** (2021).

[73] A. Streltsov, G. Adesso, and M. B. Plenio, Colloquium: Quantum coherence as a resource, Rev. Mod. Phys. **89**, 041003 (2017).

[74] B. Zhao, K. Ito, and K. Fujii, Probabilistic channel simulation using coherence, arXiv preprint arXiv:2404.06775 (2024).

[75] M. G. Díaz, K. Fang, X. Wang, M. Rosati, M. Skotiniotis, J. Calsamiglia, and A. Winter, Using and reusing coherence to realize quantum processes, Quantum **2**, 100 (2018).

[76] G. Gour, Resources of the quantum world, arXiv preprint arXiv:2402.05474 (2024).

Supplemental Material for: **Quantum Coherence and Distinguishability: A Resource-Theoretic Perspective on Wave-Particle Duality**

In this Supplemental Material, we offer detailed proofs of the theorems and propositions in the manuscript "Quantum Coherence and Distinguishability: A Resource-Theoretic Perspective on Wave-Particle Duality". In Appendix I, we demonstrate two paradigms of quantum state discrimination via free operations and free POVMs respectively. In Appendix II, we cover the basics of the quantum resource theory of coherence. In Appendix III, we first present the detailed proofs for Proposition 1 and Proposition S2, which characterize the capability difference of different classes of incoherent free operations in state discrimination tasks, respectively. In Appendix IV, we provide detailed proofs of Theorem 2 and Proposition 3, which reveal the coherence-distinguishability duality relation and demonstrate its tightness with a special case. Additionally, we present a necessary condition for the duality relation to achieve equality.

I. QUANTUM STATE DISCRIMINATION VIA FREE OPERATIONS

Given a quantum state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ where $\sum_j p_j = 1, \rho_j \in \mathcal{D}(\mathcal{H}_A)$, $d_A = d$ and $k \leq d$, and a free states set $\mathcal{F}$ with corresponding free operations set $\mathcal{O}$, we introduce the *quantum state discrimination via channel*

1. Receive an unknown state ρ_j with prior probability p_j.
2. Apply a quantum operation $\mathcal{N}_{A\to A'B}$ to ρ_j yielding $\tau_{A'B}^{(j)} = \mathcal{N}_{A\to A'B}(\rho_j)$ where $A' \cong A$ and $\dim \mathcal{H}_B = k$.
3. Measure $\tau_{A'B}^{(i)}$ on subsystem B in basis $\{|i\rangle\}_{i=0}^{k-1}$. If the outcome is i, decide the received state is ρ_i.

POVM

$$P_{\text{suc}}(\Omega) = \max_{\{E_j\}} \sum_{j=0}^{k-1} p_j \operatorname{Tr}(\rho_j E_j)$$
$$\text{s.t.} \quad \sum_{j=0}^{k-1} E_j = I, E_j \geq 0, \forall j,$$

Quantum channel

$$\widetilde{P}_{\text{suc}}(\Omega) = \max \sum_{j=0}^{k-1} p_j \operatorname{Tr}[\mathcal{N}_{A\to BA'}(\rho_j)(|j\rangle\langle j|_B \otimes I_{A'})]$$
$$\text{s.t.} \quad \mathcal{N}_{A\to BA'} \in \text{CPTP}.$$

We call $\mathcal{N}_{A\to BA'}$ the *discrimination channel*, where subsystem A' is introduced to further investigate the resource left after discrimination process. When $\mathcal{N}_{A\to BA'}$ is chosen from a set of free operation $\mathcal{O}$ of some quantum resource theory, we call this task *quantum state discrimination via free operations*. And we denote the optimal average success probability via free operations with $\widetilde{P}_{\text{suc},\mathcal{O}}(\Omega)$. In the following, we discard the subsystem A' and consider $\mathcal{N}_{A\to B} \in \mathcal{O}$ without affecting the attainment of $\widetilde{P}_{\text{suc},\mathcal{O}}(\Omega)$.

Besides, we denote a set of restricted resourceless POVMs with $\mathcal{M}_{\mathcal{F}}$, when $\mathbf{E} = \{E_j\}_j \in \mathcal{M}_{\mathcal{F}}$ for some resource theory, we call the task *quantum state discrimination via free POVMs* and denote the optimal average success probability via free POVMs with $P_{\text{suc},\mathcal{M}_{\mathcal{F}}}(\Omega)$.

II. QUANTUM RESOURCE THEORY OF COHERENCE

We briefly introduce the quantum resource theory (QRT) of coherence [73, 74]. Throughout this Letter, we denote Hilbert space with d-dimension as $\mathcal{H}_d$. Let $\mathcal{L}(\mathcal{H}_d)$ be the space of linear operators mapping $\mathcal{H}_d$ to itself and $\mathcal{D}(\mathcal{H}_d)$ be the set of density operators acting on $\mathcal{H}_d$. We define dephasing operations Δ as follows:

$$\Delta(\rho) = \sum_{i=0}^{d-1} |i\rangle\langle i|\rho|i\rangle\langle i| \tag{S1}$$

The set of free states in QRT of coherence is defined as $\mathcal{I} := \{\rho \geq 0 | \Delta(\rho) = \rho\}$.

In the following, we introduce several free operations in QRT of coherence. The maximally incoherent operations (MIO) is the largest class of incoherent operations, which map $\mathcal{I}$ onto itself. The incoherent operations (IO) [26] admit a set of Kraus operators $\{K_n\}_n$ such that:

$$\frac{K_n \rho K_n^\dagger}{\mathrm{Tr}[K_n \rho K_n^\dagger]} \in \mathcal{I}, \quad \sum_n K_n^\dagger K_n = \mathbb{I},\ \forall n, \rho \in \mathcal{I} \tag{S2}$$

Dephasing-covariant incoherent operations (DIO) [43, 44] are those quantum operations $\mathcal{E}$ which commute with the dephasing operations Δ for any quantum state ρ such that: $[\Delta, \mathcal{E}] = 0$. The strictly incoherent operations (SIO) [21] fulfill $\langle i|K_n \rho K_n^\dagger|i\rangle = \langle i|K_n \Delta[\rho] K_n^\dagger|i\rangle\ \forall n, i$. There are hierarchies among these free operations: SIO $\subsetneq$ IO $\subsetneq$ MIO, SIO $\subsetneq$ DIO $\subsetneq$ MIO [43]. In a d-dimensional Hilbert space $\mathcal{H}_d$, a maximally coherent state is:

$$|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle. \tag{S3}$$

We denote $|\Psi_d\rangle\langle\Psi_d|$ with Ψ_d in the following.

A good coherence measure is expected to satisfy the following three conditions under MIO:

- $C(\rho) = 0\ \forall \rho \in \mathcal{I}$;
- $C(\rho) \geq C(\mathcal{T}(\rho))$ for all incoherent CPTP maps $\mathcal{T}$;
- Convexity: $\sum_j p_j C(\rho_j) \geq C(\sum_j p_j \rho_j)$, which is not necessary.

Definition S1 *(Robustness of coherence [22, 75]) The robustness of coherence of a quantum state $\rho \in \mathcal{D}(\mathcal{H}_d)$ is defined as:*

$$C_R(\rho) = \min_{\tau \in \mathcal{D}(\mathcal{H}_d)} \left\{ s \geq 0 \,\middle|\, \frac{\rho + s\tau}{1+s} := \delta \in \mathcal{I} \right\}, \tag{S4}$$

which can be transformed into a simple semidefinite program (SDP) [22]:

$$\begin{aligned} C_R(\rho) = \max\ & \mathrm{Tr}(W\rho) && \text{(S5)}\\ \text{s.t.}\ & \Delta(W) \leq 0, && \text{(S6)}\\ & W \geq -I, && \text{(S7)} \end{aligned}$$

where the Hermitian operator $M = -W$ fulfills $M \geq 0$ if and only if $\mathrm{Tr}(\rho M) = \mathrm{Tr}(\rho \Delta(M))$ for all incoherent states $\rho \in \mathcal{I}$. Such an observable M serves as a coherence witness, where $\mathrm{Tr}(\rho M) \leq 0$ indicates coherence in the state ρ. Robustness of coherence is multiplicative under the tensor product of states:

$$1 + C_R(\rho_1 \otimes \rho_2) = (1 + C_R(\rho_1))(1 + C_R(\rho_2)) \tag{S8}$$

Another main advantage of the robustness of coherence is that it can be estimated in the laboratory as an expected value of observable M with respect to ρ. An operational interpretation of the robustness of coherence is that: it quantifies the advantage enabled by a quantum state in a *phase discrimination task*.

Another equivalent primal standard form of the above SDP [75] is:

$$1 + C_R(\rho) = \min \left\{ \lambda \,|\, \rho \leq \lambda\sigma, \sigma \in \mathcal{I} \right\} \tag{S9}$$

and the dual form is given by

$$1 + C_R(\rho) = \max \left\{ \mathrm{Tr}(\rho S) \,|\, S \geq 0, S_{ii} = 1,\ \forall i \right\} \tag{S10}$$

Definition S2 *(Maximum relative entropy of coherence) [62] The maximum relative entropy of coherence of a state ρ is defined as:*

$$C_{\max}(\rho) = \min_{\sigma \in \mathcal{I}} D_{\max}(\rho||\sigma), \tag{S11}$$

where $\mathcal{I}$ is the set of incoherent states in $\mathcal{D}(\mathcal{H}_d)$ and $D_{\max}(\rho||\sigma)$ denotes the maximum relative entropy of ρ with respect to σ and $D_{\max}(\rho||\sigma) := \min\{\lambda \,|\, \rho \leq 2^\lambda \sigma\}$.

It is obvious that $D_{\max}(\rho||\sigma)$ is the upper bound of the maximum relative entropy of coherence. Note that $2^{C_{\max}(\rho)} = 1 + C_R(\rho)$.

III. COHERENCE MANIPULATION WITHIN QSD

Lemma S1 *For a d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$ and a resource theory of states $(\mathcal{F}, \mathcal{O})$, there exist quantum-classical channels $\mathcal{N}^{qc} \in \mathcal{O}$ achieving the optimal discrimination probability via free operations $\widetilde{P}_{\mathrm{suc},\mathcal{O}}(\Omega)$.*

Proof We consider QSD via free operations in some quantum resource theory with $\mathcal{N} \in \mathcal{O}$. Suppose $\mathcal{N}$ is the optimal channel achieving $\widetilde{P}_{\mathrm{suc},\mathcal{O}}(\Omega)$. It follows

$$\widetilde{P}_{\mathrm{suc},\mathcal{O}}(\Omega) = \sum_{j=0}^{k-1} p_j \operatorname{Tr}(\mathcal{N}(\rho_j)|j\rangle\langle j|) \tag{S12a}$$

$$= \sum_{j=0}^{k-1} p_j \operatorname{Tr}\left(\mathcal{N}(\rho_j)\Delta(|j\rangle\langle j|)\right) \tag{S12b}$$

$$= \sum_{j=0}^{k-1} p_j \operatorname{Tr}(\Delta \circ \mathcal{N}(\rho_j)|j\rangle\langle j|), \tag{S12c}$$

where we use the fact that the adjoint map of a fully dephasing channel $\Delta(\cdot)$ is itself. Note that $\mathcal{N} \in \mathcal{O}$ is a free operation in some resource theory, it holds that $\mathcal{N}(\rho) \in \mathcal{F}$, $\forall \rho \in \mathcal{F}$, where $\mathcal{F}$ denotes the set of free states. Obviously, we have $\Delta \circ \mathcal{N}(\rho) \in \mathcal{F}$, $\forall \rho \in \mathcal{F}$. Thus, it holds $\Delta \circ \mathcal{N} \in \mathcal{O}$. Then we conclude that $\Delta \circ \mathcal{N}$ is also an optimal free channel achieving $\widetilde{P}_{\mathrm{suc},\mathcal{O}}(\Omega)$. Then we show that $\Delta \circ \mathcal{N}$ is a quantum-classical channel. We express $J_{\mathcal{N}} = \sum_{i,i'} |i\rangle\langle i'| \otimes \mathcal{N}(|i\rangle\langle i'|)$ and deduce that

$$J_{\Delta\circ\mathcal{N}} = \sum_{i,i'} |i\rangle\langle i'| \otimes \Delta \circ \mathcal{N}(|i\rangle\langle i'|) \tag{S13a}$$

$$= \sum_{i,i',q} p_{i,i',q}|i\rangle\langle i'| \otimes |q\rangle\langle q|) \tag{S13b}$$

$$= \sum_{q} Q_q \otimes |q\rangle\langle q| \tag{S13c}$$

Then we express the Choi operator of $\Delta \circ \mathcal{N}$ as $J_{\Delta\circ\mathcal{N}} = \sum_q Q_q \otimes |q\rangle\langle q|$, where $Q_q = \sum_{i,i'} p_{i,i',q}|i\rangle\langle i'|$, $\sum_q Q_q = I$ and $Q_q \geq 0$ due to $\Delta \circ \mathcal{N}$ is a CPTP map. We can choose $Q_q = M_q^T$ and conclude $\{M_q\}_{q=0}^{k-1}$ is a POVM. Thus, $\Delta \circ \mathcal{N}$ is a quantum-classical channel $\mathcal{N}^{\mathrm{qc}}$. Such conclusion also holds when $\mathcal{N} \in$ CPTP without considering any resource theory, and indicates that $\widetilde{P}_{\mathrm{suc}}(\Omega) \leq P_{\mathrm{suc}}(\Omega)$. ■

Proposition 1 *For a d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, the optimal discrimination probability $P_{\mathrm{suc}}(\Omega)$ can be achieved by quantum state discrimination via incoherent operations.*

Proof We prove this proposition by demonstrating that $P_{\mathrm{suc}}(\Omega) = \widetilde{P}_{\mathrm{suc,IO}}(\Omega)$. First, we will show $P_{\mathrm{suc}}(\Omega) \leq \widetilde{P}_{\mathrm{suc,IO}}(\Omega)$. Suppose the optimal POVM for $P_{\mathrm{suc}}(\Omega)$ is $\{E_j\}_{j=0}^{k-1}$. We can obtain a quantum-classical channel

$$\mathcal{M}_{A\to B}(\rho_A) = \sum_{j=0}^{k-1} \operatorname{Tr}(\rho_A E_j)|j\rangle\langle j|. \tag{S14}$$

In the following, we show that quantum-classical channel $\mathcal{M}_{A\to B}$ is an IO. Suppose the spectral decomposition of E_q is

$$E_q = \sum_{i=1}^{r_q} \lambda_i^q |\psi_i^q\rangle\langle\psi_i^q|, \tag{S15}$$

where r_q is the rank of E_q. Then we can express the Kraus operators of the quantum-classical channel as $K_i^q = \sqrt{\lambda_i^q}|q\rangle\langle\psi_i^q|$. We can check that for any $|j\rangle$:

$$K_i^q|j\rangle\langle j|(K_i^q)^\dagger = \lambda_i^q|q\rangle\langle\psi_i^q|j\rangle\langle j|\psi_i^q\rangle\langle q| = \lambda_i^q|\langle j|\psi_i^q\rangle|^2|q\rangle\langle q|. \tag{S16}$$

$K_i^q|j\rangle\langle j|(K_i^q)^\dagger \in \mathcal{I}$. Thus, we can conclude that $\mathcal{M}_{A\to A'} \in$ IO. Then we have

$$\widetilde{P}_{\text{suc,IO}}(\Omega) \geq \sum_{j=0}^{k-1} p_j \operatorname{Tr}(\mathcal{M}(\rho_j)|j\rangle\langle j|) = \sum_{j=0}^{k-1} p_j \operatorname{Tr}(\rho_j E_j) = P_{\text{suc}}(\Omega). \tag{S17}$$

Second, we are going to prove $P_{\text{suc}}(\Omega) \geq \widetilde{P}_{\text{suc,IO}}(\Omega)$. Recall that $\widetilde{P}_{\text{suc,IO}}(\Omega)$ can always be achieved by a quantum-classical channel $\mathcal{N}'$ according to the Lemma S1. Note that we have shown that the quantum-classical channel is an IO. Suppose that $J_{N'} = \sum_q M_q^T \otimes |q\rangle\langle q|$ and we can conclude that $\widetilde{P}_{\text{suc,IO}}(\Omega)$ is equivalently achieved by a POVM $\{M_q\}_0^{k-1}$. Thus, $P_{\text{suc}}(\Omega) \geq \widetilde{P}_{\text{suc,IO}}(\Omega)$.

In conclusion, we have $P_{\text{suc}}(\Omega) = \widetilde{P}_{\text{suc,IO}}(\Omega)$, which means optimal discrimination probability via free operations can be achieved with IO. The result also holds for MIO because IO $\subsetneq$ MIO. ■

Definition S3 *(Incoherent measurement [54]) A d-dimentional POVM $\{E_m\}_{m=0}^{k-1}$ is called an incoherent measurement if $\Delta(E_m) = E_m$ for all m.*

Incoherent measurements can be regarded as POVMs analog of incoherent states, which are diagonal in the fixed basis and can be expressed as $E_m = \sum_{i=0}^{d-1} p(m|i)|i\rangle\langle i|$. We denote the set of incoherent measurements as $\mathcal{M}_{\mathcal{I}}$.

Proposition S2 *For a d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, we have*

$$P_{\text{suc},\mathcal{M}_{\mathcal{I}}}(\Omega) = \widetilde{P}_{\text{suc,SIO}}(\Omega). \tag{S18}$$

Proof First, we show that $P_{\text{suc},\mathcal{M}_{\mathcal{I}}}(\Omega) \geq \widetilde{P}_{\text{suc,DIO}}(\Omega)$. Recall that the discrimination channel $\mathcal{N} \in$ DIO reaching $\widetilde{P}_{\text{suc,DIO}}(\Omega)$ can be a quantum-classical channel. We denote the quantum-classical channel $\mathcal{N}$ by $\mathcal{N}(\cdot) = \sum_{j=0}^{k-1} \operatorname{Tr}(E_j \cdot)|j\rangle\langle j|$, where $\{E_j\}_{j=0}^{k-1}$ is the corresponding POVM. Note that $\mathcal{N} \in$ DIO and $\forall \rho$, we have

$$\mathcal{N}(\rho) = \Delta \circ \mathcal{N}(\rho) = \mathcal{N} \circ \Delta(\rho) = \sum_{j=0}^{k-1} \operatorname{Tr}(E_j \Delta(\rho))|j\rangle\langle j| = \sum_{j=0}^{k-1} \operatorname{Tr}(\Delta(E_j)\rho)|j\rangle\langle j|. \tag{S19}$$

Obviously, $\{\Delta(E_j)\}_{j=0}^{k-1}$ is an incoherent measurement with $\sum_{j=0}^{k-1} \Delta(E_j) = I$ and $\Delta(E_j) \geq 0$. Thus, we can directly let $E_j = \sum_i p_{i,j}|i\rangle\langle i|$ and $\{E_j\}_{j=0}^{k-1} \in \mathcal{M}_{\mathcal{I}}$. Thus, we conclude that $P_{\text{suc},\mathcal{M}_{\mathcal{I}}}(\Omega) \geq \widetilde{P}_{\text{suc,DIO}}(\Omega)$.

Conversely, if we distinguish Ω via incoherent measurements, and the optimal discrimination probability under such constraints is achieved by an incoherent measurement $\{E_j\}_{j=0}^{d-1}$, where $E_j = \sum_i p_{i,j}|i\rangle\langle i|$. We can construct a channel $\widetilde{\mathcal{N}} \in$ DIO with its Choi operator being $J_{\widetilde{\mathcal{N}}} == \sum_j E_j \otimes |j\rangle\langle j| = \sum_{i,j} p_{i,j}|i\rangle\langle i| \otimes |j\rangle\langle j|$, which means $P_{\text{suc},\mathcal{M}_{\mathcal{I}}}(\Omega) \leq \widetilde{P}_{\text{suc,DIO}}(\Omega)$. We can further reduce the DIO into SIO. We have shown that the Choi operator of the quantum-classical channel of incoherent measurements can be expressed as $J_{\widetilde{\mathcal{N}}} = \sum_{i,j} p_{i,j}|i\rangle\langle i| \otimes |j\rangle\langle j|$ with $E_j = \sum_j p_{i,j}|i\rangle\langle i|$. Then we can express the Kraus operators of $J_{\widetilde{\mathcal{N}}}$ as $K_i^j = \sqrt{p_{i,j}}|j\rangle\langle i|$. We can check that

$$K_i^j|q\rangle\langle q'|(K_i^j)^\dagger = p_{i,j}|j\rangle\langle i|q\rangle\langle q'|i\rangle\langle j| = p_{i,j}\delta_{i,q}\delta_{i,q'}|j\rangle\langle j| \tag{S20a}$$

If $q = q'$, we obtain that $K_i^j|q\rangle\langle q|(K_i^j)^\dagger = p_{i,j}\delta_{i,q}|j\rangle\langle j|$; and if $q \neq q'$, we obtain that $K_i^j|q\rangle\langle q'|(K_i^j)^\dagger = 0$. Thus $\widetilde{\mathcal{N}}$ discussed above belongs to SIO. Thus, we have $P_{\text{suc},\mathcal{M}_{\mathcal{I}}}(\Omega) = \widetilde{P}_{\text{suc,SIO}}(\Omega)$. It also holds for $P_{\text{suc},\mathcal{M}_{\mathcal{I}}}(\Omega) = \widetilde{P}_{\text{suc,DIO}}(\Omega)$. ■

Remark 1 Until now, we have demonstrated the significant difference between MIO and DIO in QSD tasks. Using the paradigm of QSD via free operations, we can implement the global optimal POVMs equivalently through MIO (IO), but only achieve the incoherent measurements equivalently through DIO (SIO). Thus, we can argue that MIO (IO) provides a maximal advantage over DIO (SIO) in the QSD task, as discussed in Ref. [54, 56]. This advantage is fully identified by the quantifier called robustness for incoherent measurements $\mathcal{R}_{\mathcal{M}_{\mathcal{I}}}$ as follows:

$$\mathcal{R}_{\mathcal{M}_{\mathcal{I}}}(\mathbf{M}) = \max_{\Omega_0} \frac{p_{\text{suc}}(\Omega_0, \mathbf{M})}{\max_{\mathbf{N}\in\mathcal{M}_{\mathcal{I}}} p_{\text{suc}}(\Omega_0, \mathbf{N})} - 1, \tag{S21}$$

where $p_{\text{suc}}(\Omega_0, \mathbf{E}) = \sum_j p_j \operatorname{Tr}(E_j \rho_j)$ with $\mathbf{E} = \{E_j\}_{j=0}^{k-1}$, $\mathbf{M}$ is a global POVM, $\mathbf{N}$ is an incoherent measurement, and $\Omega_0 = \{p_j, \rho_j\}_{j=0}^{k-1}$ denotes a quantum state ensemble. Note that $\mathcal{R}_{\mathcal{M}_{\mathcal{I}}}(\mathbf{M}) \geq 0$ and when $\mathbf{M} \nsubseteq \mathcal{M}_{\mathcal{I}}$, $\exists\, \Omega_0$ let $\mathcal{R}_{\mathcal{M}_{\mathcal{I}}}(\mathbf{M}) > 0$. We can conclude that QSD via free operation in the QRT of coherence can identify a strict hierarchy between MIO and DIO on the optimal discrimination probability.

IV. COHERENCE-DISTINGUISHABILITY DUALITY RELATION

Lemma S3 *For a mutually orthogonal d-dimensional state ensemble $\Omega = \{(p_j, \rho_j)\}_{j=0}^{k-1}$, if the post-discrimination coherence under maximally incoherent operations $\mathbf{C}_{\text{MIO}}(\Omega)$ is achieved by some MIO $\mathcal{N}$, then $\mathbf{C}_{\text{MIO}}(\Omega) = C_{\max}(\mathcal{N}(\hat{\omega}))$ with $\hat{\omega} = \sum_{j=0}^{k-1} p_j \rho_j$.*

Proof According to the definition, the MIO $\mathcal{N}$ achieving $\mathbf{C}_{\text{MIO}}(\Omega)$ satisfies $\mathcal{N}(\rho_j) = |j\rangle\langle j| \otimes \sigma_j, \forall \rho_j \in \Omega$. Then we have

$$\begin{align}
\mathbf{C}_{\text{MIO}}(\Omega) &= \log[1+\eta] \tag{S22a}\\
&= \log[1 + \sum_{j=0}^{k-1} p_j C_R(\sigma_j)] \tag{S22b}\\
&= \log[1 + \sum_{j=0}^{k-1} p_j C_R(|j\rangle\langle j| \otimes \sigma_j)] \tag{S22c}\\
&= \log\left[1 + C_R\Big(\sum_{j=0}^{k-1} p_j |j\rangle\langle j| \otimes \sigma_j\Big)\right] \tag{S22d}\\
&= \log\left[1 + C_R\Big(\sum_{j=0}^{k-1} p_j \mathcal{N}(\rho_j)\Big)\right] \tag{S22e}\\
&= \log[1 + C_R(\mathcal{N}(\hat{\omega})], \tag{S22f}
\end{align}$$

where $\hat{\omega} = \sum_{j=0}^{k-1} p_j \rho_j$. We drive Eq. (S22c) from Eq. (S22b) because robustness of coherence is multiplicative under the tensor product of states. And Eq. (S22d) is driven from Eq. (S22c) because the robustness of coherence is convex linear on classical-quantum states [76]. ■

Theorem S4 *For a mutually orthogonal d-dimensional pure-state ensemble $\Omega = \{(p_i, |\psi_i\rangle)\}_{i=0}^{k-1}$,*

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}_{\min}(\Omega) \leq \log d, \tag{S23}$$

Proof Denote by $\mathcal{E} = \{|\psi_i\rangle\}_{i=0}^{d-1}$ an orthogonal basis of $\mathcal{H}_A$ with $d_A = k$, and $\mathcal{N}(|\psi_i\rangle\langle\psi_i|) = |i\rangle\langle i| \otimes \sigma_i$, where $|i\rangle\langle i| \in \mathcal{D}(\mathcal{H}_B)$, $d_B = k$ and $i = 0, \cdots, k-1$. For these states $|\psi_j\rangle, j = k, \cdots, d-1$, i.e., $|\psi_j\rangle \in \mathcal{E}$ but $|\psi_j\rangle \notin \Omega$, we directly assume:

$$\mathcal{N}(|\psi_j\rangle\langle\psi_j|) = \left(\sum_{n=0}^{k-1} q_n^j |n\rangle\langle n|\right) \otimes \rho_j, \quad j = k, \cdots d-1, \tag{S24}$$

where $\sum_{n=0}^{k-1} q_n^j = 1$, $\rho_j \in \mathcal{D}(\mathcal{H}_{A'})$ and $d_{A'} = d$, and we use the conclusion that $(\Delta \otimes I) \circ \mathcal{N}$ is also the optimal channel achieving $\mathbf{C}_{\text{MIO}}(\Omega)$. Then we have,

$$\begin{aligned}
\mathcal{N}\left(\frac{I}{d}\right) &= \mathcal{N}\left(\frac{1}{d}\sum_{i=0}^{d-1} |\psi_i\rangle\langle\psi_i|\right)\\
&= \frac{1}{d}\left(\sum_{i=0}^{k-1} \mathcal{N}(|\psi_i\rangle\langle\psi_i|) + \sum_{j=k}^{d-1} \mathcal{N}(|\psi_j\rangle\langle\psi_j|)\right)\\
&= \frac{1}{d}\left(\sum_{i=0}^{k-1} |i\rangle\langle i| \otimes \sigma_i + \sum_{j=k}^{d-1}\left(\sum_{n=0}^{k-1} q_n^j |n\rangle\langle n|\right) \otimes \rho_j\right)\\
&= \frac{1}{d}\left(\sum_{i=0}^{k-1} |i\rangle\langle i| \otimes \left(\sigma_i + \sum_{j=k}^{d-1} q_i^j \rho_j\right)\right)
\end{aligned} \tag{S25}$$

Notice that $\mathcal{N}$ is a MIO which yields $\mathcal{N}\left(\frac{I}{d}\right)$ is incoherent. Thus, we have $\sigma_i + \sum_{j=k}^{d-1} q_i^j \rho_j$ is an incoherent state (unnormalized) for $i = 0, \cdots, k-1$. We can conclude that $C_R(\sigma_i) \leq \sum_{j=k}^{d-1} q_i^j$. Therefore,

$$\eta = \sum_{i=0}^{k-1} p_i C_R(\sigma_i) \leq \max \sum_{i=0}^{k-1} p_i \sum_{j=k}^{d-1} q_i^j. \tag{S26}$$

If each $|\psi_i\rangle$ in Ω is given with probability p_i, we have $\sum_{i=0}^{k-1}\sum_{j=k}^{d-1} p_i q_i^j \leq \sum_{j=k}^{d-1}\sum_{i=0}^{k-1} p_{\max} q_i^j \leq (d-k)p_{\max}$, where $p_{\max} = \max\{p_0, p_1, ..., p_{k-1}\}$). Thus, we have $\mathbf{C}_{\mathrm{MIO}}(\Omega) = \log(1+\eta) \leq \log[(d-k)p_{\max}+1] \leq \log d + \log(p_{\max})$ and conclude

$$\mathbf{C}_{\mathrm{MIO}}(\Omega) + \mathbf{S}_{\min}(\Omega) \leq \log d, \tag{S27}$$

where $\mathbf{S}_{\min}(\Omega)$ is defined as the min-entropy of the average state of Ω with $\hat{\omega} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and $\mathbf{S}_{\min}(\Omega) = \mathbf{S}_{\min}(\hat{\omega}) = -\log(p_{\max})$.

■

Theorem 2 *For a mutually orthogonal d-dimensional pure-state ensemble $\Omega = \{(1/k, |\psi_i\rangle)\}_{i=0}^{k-1}$,*

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}(\Omega) \leq \log d, \tag{S28}$$

Proof Note that for the $\Omega = \{(1/k, |\psi_i\rangle)\}_{i=0}^{k-1}$, $\mathbf{S}(\Omega) = \mathbf{S}_{\min}(\Omega) = \log k$, we arrive the conclusion immediately, combined with the Theorem S4. ■

This bound can be achieved in the following example.

Proposition 3 *Let $|\phi_i\rangle = HX^i|0\rangle$ where H, X are the d-dimensional Hadamard gate and generalized Pauli X gate. For $\Omega = \{(1/k, |\phi_i\rangle)\}_{i=0}^{k-1}$, $k \leq d$,*

$$\mathbf{C}_{MIO}(\Omega) + \mathbf{S}(\Omega) = \log d. \tag{S29}$$

Proof We construct an MIO channel $\mathcal{N}$ to show the equality sign can be achieved in Eq. (S26) for this ensemble containing k mutually orthogonal maximally coherent states. Here, d-dimensional Hadamard gate H and d-dimensional Pauli X gate are defined as $H = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}\omega^{kj}|k\rangle\langle j|$ and $X = \sum_{i=0}^{d-1}|i+1\rangle\langle i|$ respectively, where $\{|i\rangle\}_{i=0}^{d-1}$ denotes computational basis and $\omega = e^{i2\pi/d}$. We denote $|\phi_i\rangle\langle\phi_i|$ with Ψ_i in the following, and construct the MIO channel $\mathcal{N}$ as follows:

$$\mathcal{N}(\rho) = \sum_{i=0}^{k-1}\mathrm{Tr}(\Psi_i\rho)|i\rangle\langle i| \otimes \mathcal{D}_p(Z^{\dagger i}\rho Z^i) + \sum_{j=k}^{d-1}\mathrm{Tr}(\Psi_j\rho)\Pi \otimes [(Z^{\dagger j}\rho Z^j)\circ U], \quad \forall\rho, \tag{S30}$$

where $\Pi = 1/k\sum_{i=0}^{k-1}|i\rangle\langle i|$, Z denotes d-dimensional Pauli Z operator with $Z = \sum_{j=0}^{d-1}\omega^j|j\rangle\langle j|$, $U = I + \frac{1}{d-1}\sum_{i<j}(e^{i\pi}|i\rangle\langle j| + e^{-i\pi}|j\rangle\langle i|)$ and $\tau \circ U$ is the Hadamard product with $(\tau\circ U)_{ij} = -\tau_{ij}/(d-1)$, for $i \neq j$ and a given state τ. Note that $\tau \to \tau\circ U$ is also an MIO. And $\mathcal{D}_p(\rho) = (1-p)\rho + p\frac{I}{d}$ denotes the p-depolarizing channel, with $p = 1 - \frac{d-k}{k(d-1)}$. First, we can check $\mathcal{N}$ is a MIO with $\mathcal{N}(|m\rangle\langle m|) = \Delta[\mathcal{N}(|m\rangle\langle m|)]$ with $m = 0, \cdots, k-1$. Then we can check that:

$$\mathcal{N}(\Psi_i) = |i\rangle\langle i| \otimes \sigma, \quad i = 0, \cdots, k-1, \tag{S31}$$

where $\sigma = I/d + \sum_{m\neq n}\frac{d-k}{k(d-1)d}|m\rangle\langle n|$. Thus, $\mathbf{C}_{\mathrm{MIO}}(\Omega) \geq \sum_{i=0}^{k-1} C_R(\sigma)/k = (d-k)/k$. Combined with the upper bound provided by the Theorem 2, we can conclude that $\mathbf{C}_{\mathrm{MIO}}(\Omega) = (d-k)/k$ and $\mathbf{C}_{\mathrm{MIO}}(\Omega) = \log(d/k) = \log d - \mathbf{S}(\Omega)$. ■

Proposition S5 *For a mutually orthogonal d-dimensional pure-state ensemble $\Omega = \{(1/k, |\psi_i\rangle)\}_{i=0}^{k-1}$ with $k < d$, the necessary condition for Ω to saturate the coherence-distinguishability duality relation is*

$$C_{\max}(\hat{\omega}) + S(\hat{\omega}) \geq \log d, \tag{S32}$$

where $\hat{\omega} = \sum_{i=0}^{k-1} 1/k|\psi_i\rangle\langle\psi_i|$.

Proof Saturating the coherence-distinguishability duality relation with a given Ω means $\mathbf{C}_{\mathrm{MIO}}(\Omega) + \mathbf{S}(\Omega) = \log d$. Note that we restrict $k < d$ and avoid the trivial case of extracting all $\log d$ c-bits from Ω, namely $\mathbf{S}(\Omega) = \log d$. Suppose the MIO achieving $\mathbf{C}_{\mathrm{MIO}}(\Omega)$ is $\mathcal{N}$, combined with Lemma S3, if $C_{\max}(\hat{\omega}) + S(\hat{\omega}) < \log d$, we have

$$\begin{aligned}
\mathbf{C}_{\mathrm{MIO}}(\Omega) + \mathbf{S}(\Omega) &= C_{\max}(\mathcal{N}(\hat{\omega})) + \mathbf{S}(\Omega) && \text{(S33)}\\
&= C_{\max}(\mathcal{N}(\hat{\omega})) + S(\hat{\omega}) && \text{(S34)}\\
&\leq C_{\max}(\hat{\omega}) + S(\hat{\omega}) && \text{(S35)}\\
&< \log d. && \text{(S36)}
\end{aligned}$$

Then it is impossible for Ω to saturate the coherence-distinguishability duality relation. Thus, we conclude that $C_{\max}(\hat{\omega}) + S(\hat{\omega}) \geq \log d$ is the necessary condition. ■

Nonlocality-driven certification without locality requirements

Ivan Supic[1] *

[1] *Sorbonne University*

Abstract. In recent years, quantum technologies have experienced rapid growth and maturation. As quantum devices become capable of specific tasks, ensuring their proper functioning is crucial, necessitating reliable certification techniques. Certification became one of the most important topics in the field as it addresses concerns related to noise and decoherence, ensuring that devices align effectively with blueprints. In this talk I will discuss possible answers to the question: How can certification methods, which rely on the robustness of quantum correlations, be applied to quantum computing platforms? Self-testing as the most important primitive for device-independent certification is constructed within the framework of the Bell scenario, which entails two or more spatially separated parties. While this setup is advantageous for demonstrating foundational proofs of quantumness, its application to computing platforms poses challenges due to the inherent integrality of such platforms, making them incompatible with Bell-type scenarios. I will describe two approaches to dealing with this problem. In the first one I give some answers stemming from using quantum homomorphic encryption to bypass the locality requirement. In the second one I describe plethora of self-testing results that can be proven in the case when some amount of communication is allowed among the parties.

*ivan.supic@lip6.fr

Self-testing: Capabilities and Limitations

Laura Mančinska[1] *

[1] *QMATH, University of Copenhagen*

Abstract. In this talk, I will introduce the concept of self-testing, which aims to address the fundamental question of how can we certify the proper functioning of black-box quantum devices. Self-testing represents the strongest form of quantum functionality certification, enabling a classical user to infer the quantum state and measurements used to produce the observed measurement statistics.

I will survey key self-testing results and discuss outstanding questions in the field. As an example, we will examine a recent protocol that allows for self-testing of arbitrary real projective measurements in the simplest two-party Bell scenario.

Regarding limitations, I will highlight common assumptions in existing self-testing results, pointing out their potential weaknesses, especially in the context of cryptographic applications. To address these limitations, I will present a general theorem that promotes most existing self-testing results to their assumption-free variants. However, we will also see that in some scenarios assumptions cannot be lifted. To illustrate this point, I will present a simple quantum correlation that qualifies as a self-test only under certain assumptions.

*mancinska@math.ku.dk

Quantum communication on the bosonic loss-dephasing channel

Francesco Anna Mele[1] * Farzin Salek[2] † Vittorio Giovannetti[1] ‡ Ludovico Lami[4] §

[1] *NEST, Scuola Normale Superiore and Istituto Nanoscienze, Consiglio Nazionale delle Ricerche, Piazza dei Cavalieri 7, IT-56126 Pisa, Italy*

[2] *Department of Mathematics, Technical University of Munich, Boltzmannstrasse 3, 85748 Garching, Germany*

[3] *QuSoft, Science Park 123, 1098 XG Amsterdam, the Netherlands*

Abstract. Quantum optical platforms, essential for quantum communication and computation, are typically affected by photon loss and dephasing noise. Our paper addresses the crucial problem of determining for which regime of loss and dephasing the noise can be corrected. Our results, refuting a known conjecture, show that quantum error correction and reliable quantum communication are impossible in a large region of parameter space of loss and dephasing. On the positive side, however, we prove that if the sender and the receiver are assisted by two-way classical communication, then reliable quantum communication becomes possible even for arbitrarily high levels of loss and dephasing.

Keywords: Continuous-variable systems, Bosonic loss-dephasing channel, Quantum Shannon Theory

1 Introduction

Quantum optical platforms play a crucial role in both quantum communication and quantum computation. However, one of the most serious problems plaguing these platforms is the presence of noise due to *photon loss* and *bosonic dephasing* [1, 2, 3], which have been both extensively analysed separately [4, 5, 6, 7]. Loss dissipates energy, whereas dephasing works to transform coherent superpositions into probabilistic mixtures. Although loss and dephasing sources can simultaneously affect bosonic systems [8, 9, 10, 11, 12], the existing literature provides only partial results about their combined effect [12], modelled by the so-called loss-dephasing channel. Understanding the combined effect of loss and dephasing is challenging due to the conflicting behaviours they exhibit: loss takes a simple form when written in the coherent state basis but is complicated to analyse in the Fock basis [13], whereas dephasing demonstrates the opposite pattern, making the analysis of their combined effect quite intricate.

Consider an optical link or a quantum memory affected by both loss and dephasing. Can the overall noise be corrected? In other words, does the corresponding channel have non-zero quantum capacity? Answering this question is crucial for determining the specific conditions under which quantum communication and quantum computation can be successfully achieved in optical platforms. This question is intimately related to the *anti-degradability* condition in Quantum Shannon Theory: if a noise channel is anti-degradable [14, 15], there are no quantum communication protocols or quantum error-correcting codes capable of overcoming it. Consequently, it is crucial to understand whether the combined effect of loss and dephasing results in an anti-degradable channel. This has been a puzzling problem, to the point that in [12] it was conjectured that the combined loss-dephasing noise results in an anti-degradable channel if and only if the loss is above 50%.

In our paper [16] we refute the above conjecture; specifically, for any value of the photon loss, we explicitly find a *critical value* of the dephasing above which the resulting loss-dephasing channel is anti-degradable. Our result identifies a large region of the loss-dephasing parameter space where correcting the noise and achieving quantum communication is impossible. On the more positive side, however, we also prove that if the sender and the receiver are assisted by two-way classical communication, then quantum communication — and thus quantum key distribution — is always possible, even in scenarios characterised by arbitrarily high levels of loss and dephasing.

On the technical level, **we devise a new method to analyse anti-degradability of bosonic channels**, and we use it to derive the first analytical results characterising the transmission and storage of quantum information in the presence of both loss and dephasing noise. We believe that this constitutes a significant technical as well as conceptual innovation because *all* other known tools to analyse quantum capacities (e.g. degradability [15], PPT-ness [17], teleportation simulability [18, 19], entanglement breaking-ness [15]) **fail completely** for this channel [12, 16]. We are thus confident that our analysis, which is a first of its kind, will be of wide interest to the community interested in quantum communication at large, beyond the specific niche of those interested in bosonic systems.

2 Preliminaries

The *quantum capacity* $Q(\mathcal{N})$ of a channel $\mathcal{N}$ quantifies the efficiency in transmitting qubits reliably across $\mathcal{N}$ [14, 15]. The condition $Q(\mathcal{N}) = 0$ implies that there exist neither reliable quantum communication protocols across $\mathcal{N}$ nor codes capable of correcting the errors induced by $\mathcal{N}$. By definition, $\mathcal{N}$ is anti-degradable if there exists a channel $\mathcal{A}$ — called the *anti-degrading map* — such that $\mathcal{A} \circ \mathcal{N}^{\mathrm{c}} = \mathcal{N}$, where $\mathcal{N}^{\mathrm{c}}$ is a complementary channel of $\mathcal{N}$ [14]. Importantly, if $\mathcal{N}$ is *anti-degradable*

*francesco.mele@sns.it

†farzin.salek@gmail.com

‡vittorio.giovannetti@sns.it

§ludovico.lami@gmail.com

then $Q(\mathcal{N}) = 0$ [14].

The phenomenon of photon loss can be modelled by the well-known *pure-loss channel* $\mathcal{E}_\lambda$ of transmissivity $\lambda \in [0, 1]$ [13, 20]. When $\lambda = 1$ the pure-loss channel is noiseless, while when $\lambda = 0$ it is completely noisy. It is known that $\mathcal{E}_\lambda$ is anti-degradable for $\lambda \in [0, \frac{1}{2}]$ [21, 22, 23, 24]. The phenomenon of bosonic dephasing can be described by the *bosonic dephasing channel* $\mathcal{D}_\gamma$ [12, 7, 25], which maps the state $\rho = \sum_{m,n=0}^{\infty} \rho_{mn} |m\rangle\langle n|$, written in the Fock basis, to $\mathcal{D}_\gamma(\rho) := \sum_{m,n=0}^{\infty} \rho_{mn}\, e^{-\frac{\gamma}{2}(m-n)^2} |m\rangle\langle n|$, resulting in a reduction in magnitude of the off-diagonal elements. When $\gamma = 0$, the bosonic dephasing channel is noiseless. In contrast, when $\gamma \to \infty$, it completely annihilates all off-diagonal components of the input density matrix, reducing it to an incoherent probabilistic mixture of Fock states. Moreover, $\mathcal{D}_\gamma$ is never anti-degradable [25].

Consider an optical system undergoing simultaneous loss and dephasing over a time interval. At each instant, the system is susceptible to both an infinitesimal pure-loss channel and an infinitesimal bosonic dephasing channel. Hence, the overall channel, which describes the simultaneous effect of loss and dephasing, results in a suitable composition of numerous concatenations between infinitesimal pure-loss and bosonic dephasing channels. However, given that (i) the pure-loss channel and the bosonic dephasing channel commute, $\mathcal{E}_\lambda \circ \mathcal{D}_\gamma = \mathcal{D}_\gamma \circ \mathcal{E}_\lambda$; (ii) the composition of pure-loss channels is a pure-loss channel, $\mathcal{E}_{\lambda_1} \circ \mathcal{E}_{\lambda_2} = \mathcal{E}_{\lambda_1\lambda_2}$; and (iii) the composition of bosonic dephasing channels is a bosonic dephasing channel, $\mathcal{D}_{\gamma_1} \circ \mathcal{D}_{\gamma_2} = \mathcal{D}_{\gamma_1+\gamma_2}$; it follows that the combined effect of loss and dephasing can be modelled by the composition $\mathcal{N}_{\lambda,\gamma} := \mathcal{E}_\lambda \circ \mathcal{D}_\gamma$, which we will refer to as the *bosonic loss-dephasing channel.*

3 Results

Prior to this work, the only result on the anti-degradability of the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ was that it is anti-degradable if the transmissivity λ is below $\frac{1}{2}$ [12]. (This result trivially follows from the anti-degradability of $\mathcal{E}_\lambda$ for $\lambda \leq \frac{1}{2}$). Notably, in the regime $\lambda > \frac{1}{2}$, it was an open question to understand whether $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable for some values of the dephasing γ, and in [12] the answer was conjectured to be negative. However, in the forthcoming Theorem 1, we show that the latter conjecture is incorrect.

Theorem 1 *The bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable if the transmissivity λ and the dephasing γ fall within one of the following regions: (i) $\lambda \in [0, \frac{1}{2}]$ and $\gamma \geq 0$; (ii) $\lambda \in (\frac{1}{2}, 1)$ and γ such that $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}$, where $\theta(x, y) := \sum_{n=0}^{\infty} x^{n^2} y^n$. A weaker but simpler condition that implies anti-degradability is $\lambda \leq \max\left(\frac{1}{2}, \frac{1}{1+9e^{-\gamma}}\right)$.*

Proof. [Proof sketch] A single-mode channel $\mathcal{N}$ is anti-degradable if and only if its generalised Choi state is *two-extendible* [26, 27], i.e. there exists a tripartite state $\rho_{AB_1B_2}$ such that the reduced states on AB_1 and AB_2 both coincide with the generalised Choi state: $\mathrm{Tr}_{B_2}[\rho_{AB_1B_2}] = \mathrm{Tr}_{B_1}[\rho_{AB_1B_2}] = C_{AB}(\mathcal{N}) := \mathrm{Id}_A \otimes \mathcal{N}_{A'\to B}(\Psi_{AA'})$, with $\Psi_{AA'}$ being a two-mode squeezed vacuum state [13]. The crux of our proof is to find a two-extension of $C_{AB}(\mathcal{N}_{\lambda,\gamma})$ in the region identified by condition (ii). We do this in two steps.

First, after scrutinising $C_{AB}(\mathcal{N}_{\lambda,\gamma})$ in the Fock basis, we construct a tripartite state $\tau_{AB_1B_2}$ such that the reduced states on AB_1 and AB_2 have the same diagonal as $C_{AB}(\mathcal{N}_{\lambda,\gamma})$, and the same pattern of vanishing off-diagonal entries. We construct $\tau_{AB_1B_2}$ by applying several channels — namely, beam splitter unitaries, squeezing unitary, partial trace, and a three mode controlled-add-add isometry — to a 4-mode vacuum state.

The second step consists in transforming $\tau_{AB_1B_2}$ into a two-extension of $C_{AB}(\mathcal{N}_{\lambda,\gamma})$ by tweaking its off-diagonal entries. This is done by using the toolbox of *Hadamard maps* [15], whose employment here constitutes **one of our main technical innovations**. For any matrix $A := (a_{mn})_{m,n\in\mathbb{N}}$, the associated Hadamard map $H^{(A)}$ is defined by $H^{(A)}(|m\rangle\langle n|) = a_{mn}|m\rangle\langle n|$ for all m, n [15]. In practice, $H^{(A)}$ acts on the input density matrix by multiplying each (m, n) entry by the corresponding coefficient a_{mn}. Importantly, $H^{(A)}$ is a quantum channel if and only if A is Hermitian, positive semi-definite, and has all 1's on the main diagonal [15]. The crucial observation is that it is always possible to find an infinite matrix $A_{\lambda,\gamma}$, which is Hermitian and has all 1's on the main diagonal, such that the operator $\mathrm{Id}_A \otimes H_{B_1}^{(A_{\lambda,\gamma})} \otimes H_{B_2}^{(A_{\lambda,\gamma})}(\tau_{AB_1B_2})$ coincides with $C_{AB}(\mathcal{N}_{\lambda,\gamma})$ when tracing out either B_1 or B_2.

This however does not mean that we have found a two-extension of C_{AB}, because the above operator is not necessarily a state — it may fail to be positive semi-definite. It *is* a state, however, whenever $H^{(A_{\lambda,\gamma})}$ is a quantum channel, i.e. when the infinite matrix $A_{\lambda,\gamma}$ is positive semi-definite, in formula $A_{\lambda,\gamma} \geq 0$. Therefore, a sufficient condition on the anti-degradability of $\mathcal{N}_{\lambda,\gamma}$ is that $A_{\lambda,\gamma} \geq 0$. The rest of the proof consists in showing that under condition (ii) one indeed finds $A_{\lambda,\gamma} \geq 0$. This is not straightforward to check, because $A_{\lambda,\gamma}$ is an *infinite* matrix, and it cannot be diagonalised analytically nor numerically. To by-pass this last hurdle we had the idea to employ the **theory of diagonally dominant matrices**, and in particular the statement that if a matrix A is such that $|a_{nn}| - \sum_{m:\, m\mathbb{N}eqn} |a_{mn}| \geq 0$ for all n, then necessarily $A \geq 0$ [28, Chapter 6]. □

Theorem 1 identifies a region of the parameter space (λ, γ), illustrated in Fig. 1, where the channel is anti-degradable, thereby implying the absence of viable error correcting codes for quantum data transfer and storage. In Fig. 1, we plot other relevant regions, e.g. a region where $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable, and another region where the quantum capacity of $\mathcal{N}_{\lambda,\gamma}$ is strictly positive.

As we have just seen, (unassisted) quantum communication is not possible when the combined effects of loss and dephasing are too strong. However, as we show in the technical manuscript, if Alice (the sender) and Bob (the receiver) have access to a *two-way* classical communication line, then quantum communication, entanglement distribution, and quantum-key distribution [29] become again achievable for any value of loss and dephasing, even when Alice's input signals are constrained to have limited energy. In particular, this implies that the bosonic loss-dephasing channel is never entanglement breaking [14, 15].

Let us conclude with a quite shocking observation. Theorem 1 implies that even if $\lambda > \frac{1}{2}$ one can pick γ large enough so that there exists an anti-degrading map achieving the transformation $\mathcal{N}^{c}_{\lambda,\gamma}(|n\rangle\langle n|_F) \longrightarrow \mathcal{N}_{\lambda,\gamma}(|n\rangle\langle n|_F)$, which can be expressed as

$$\mathcal{E}_{1-\lambda}(|n\rangle\langle n|_F) \otimes |\sqrt{\gamma}n\rangle\langle\sqrt{\gamma}n|_C \longrightarrow \mathcal{E}_{\lambda}(|n\rangle\langle n|_F)\,, \qquad (1)$$

where $|n\rangle_F$ denotes the nth Fock state and $|\sqrt{\gamma}n\rangle_C$ denotes a coherent state [13] (see the technical manuscript for an explicit construction of such anti-degrading map). This entails the following remarkable fact: for $\lambda > 1/2$ and large enough γ there exists an *n-independent* strategy to convert the lossy Fock state $\mathcal{E}_{1-\lambda}(|n\rangle\langle n|_F)$ into the less lossy Fock state $\mathcal{E}_{\lambda}(|n\rangle\langle n|_F)$ using the coherent state $|\sqrt{\gamma}n\rangle_C$ as a resource. In other words, one can undo part of the loss on $|n\rangle_F$ if one has a coherent state that contains some information on n, sufficiently amplified so that that information is accessible enough. The nontrivial and somewhat surprising nature of this exact conversion strategy arises from the fact that the coherent states $\{|\sqrt{\gamma}n\rangle_C\}_{n\in\mathbb{N}}$ are not orthogonal, meaning that the strategy that consists in measuring the coherent state, guessing n, and re-preparing $\mathcal{E}_{\lambda}(|n\rangle\langle n|_F)$ cannot succeed with probability 1.

4 Discussion

In our paper, we have provided the first analytical investigation of the quantum communication capabilities of the bosonic loss-dephasing channel, a much more realistic model of noise than dephasing and loss treated separately. Refuting a conjecture put forth in [12], we showed that the bosonic loss-dephasing channel is anti-degradable in a large region of the loss-dephasing parameter space, entailing that neither quantum communication nor quantum error correcting codes are possible in this region. On the positive side, we also showed that if two-way classical communication is suitably exploited, then quantum communication is always achievable, even in scenarios characterised by high levels of loss and dephasing, and even in the presence of stringent energy constraints.

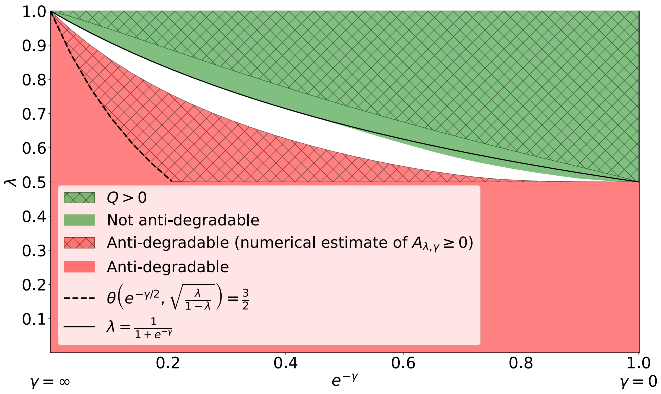


Figure 1: The vertical axis represents the transmissivity λ, while the horizontal axis corresponds to $e^{-\gamma}$, where γ is the dephasing parameter. **1)** In the red region, identified in Theorem 1, the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable, and hence there are neither quantum error correction codes nor quantum communication protocols. **2)** The crossed red region is a numerical estimate of the region where the infinite matrix $A_{\lambda,\gamma}$ is positive semi-definite, implying the anti-degradability of $\mathcal{N}_{\lambda,\gamma}$, as explained in Theorem 1. This estimate is derived by examining the positive semi-definiteness of the $d \times d$ top-left corner of $A_{\lambda,\gamma}$ for large d (increasing d already beyond $d \geq 20$ yields no discernible change in the plot). **3)** In the crossed green region, the quantum capacity of $\mathcal{N}_{\lambda,\gamma}$ is strictly positive, allowing for quantum communication and quantum error correction. We show this by optimising the coherent information [15, 14] over input states of the form $\rho_p := p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$. **4)** In the green region, $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable. This is derived by observing that the action of $\mathcal{N}_{\lambda,\gamma}$ can only subtract and never add any photons. Specifically, if the input state to $\mathcal{N}_{\lambda,\gamma}$ is supported on the span of the first d Fock states, so is the output state. This restriction defines a qu*d*it-to-qu*d*it channel $\mathcal{N}^{(d)}_{\lambda,\gamma}$, analysing which can yield some insights into $\mathcal{N}_{\lambda,\gamma}$ itself. First, if $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is *not* anti-degradable then the same is true of $\mathcal{N}_{\lambda,\gamma}$; secondly, the anti-degradability of $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is equivalent to the *two-extendibility* of the corresponding Choi state [26], and for moderate values of d this latter condition can be efficiently checked numerically via *semi-definite programming* [30, 15]. The restriction $\mathcal{N}^{(6)}_{\lambda,\gamma}$ is anti-degradable if and only if λ and γ fall within the green region, explaining why $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable here. **5)** Interestingly, the qubit restriction $\mathcal{N}^{(2)}_{\lambda,\gamma}$, equivalent to the composition between the amplitude damping channel and the qubit dephasing channel [15], yields the analytical result: *If* $\lambda > \frac{1}{1+e^{-\gamma}}$, *then* $\mathcal{N}_{\lambda,\gamma}$ *is not anti-degradable.*

References

[1] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin. New class of quantum error-correcting codes for a bosonic mode. *Phys. Rev. X*, 6:031006, Jul 2016.

[2] F. Brito, D. P. DiVincenzo, R. H. Koch, and M. Steffen. Efficient one- and two-qubit pulsed gates for an oscillator-stabilized josephson qubit. *New Journal of Physics*, 10(3):033027, mar 2008.

[3] K. H. Wanser. Fundamental phase noise limit in optical fibres due to temperature fluctuations. *Electronics Letters*, 28:53, January 1992.

[4] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang. Performance and structure of single-mode bosonic codes. *Phys. Rev. A*, 97:032346, Mar 2018.

[5] K. Noh, V. V. Albert, and L. Jiang. Quantum capacity bounds of gaussian thermal loss channels and achievable rates with gottesman-kitaev-preskill codes. *IEEE Transactions on Information Theory*, 65(4):2563–2582, 2019.

[6] M. M. Wilde and A. Winter. Strong converse for the classical capacity of the pure-loss bosonic channel. *Problems of Information Transmission*, 50(2):117–132, April 2014.

[7] L. Lami and M. M. Wilde. Exact solution for the quantum and private capacities of bosonic dephasing channels. *Nat. Photonics*, 17(6):525–530, 2023.

[8] P. Campagne-Ibarcq, A. Eickbusch, S. Touzard, E. Zalys-Geller, N. E. Frattini, V. V. Sivak, P. Reinhold, S. Puri, S. Shankar, R. J. Schoelkopf, L. Frunzio, M. Mirrahimi, and M. H. Devoret. Quantum error correction of a qubit encoded in grid states of an oscillator. *Nature*, 584(7821):368–372, August 2020.

[9] Arne L. Grimsmo, Joshua Combes, and Ben Q. Baragiola. Quantum computing with rotation-symmetric bosonic codes. *Phys. Rev. X*, 10:011058, Mar 2020.

[10] M. Reagor, W. Pfaff, C. Axline, R. W. Heeres, N. Ofek, K. Sliwa, E. Holland, C. Wang, J. Blumoff, K. Chou, M. J. Hatridge, L. Frunzio, M. H. Devoret, L. Jiang, and R. J. Schoelkopf. Quantum memory with millisecond coherence in circuit qed. *Phys. Rev. B*, 94:014506, Jul 2016.

[11] S. Rosenblum, P. Reinhold, M. Mirrahimi, L. Jiang, L. Frunzio, and R. J. Schoelkopf. Fault-tolerant detection of a quantum error. *Science*, 361(6399):266–270, July 2018.

[12] P. Leviant, Q. Xu, L. Jiang, and S. Rosenblum. Quantum capacity and codes for the bosonic loss-dephasing channel. *Quantum*, 6:821, sep 2022.

[13] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. CRC Press, Taylor & Francis Group, Boca Raton, USA, 2017.

[14] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2nd edition, 2017.

[15] S. Khatri and M. M. Wilde. Principles of quantum communication theory: A modern approach, 2020.

[16] Francesco Anna Mele, Farzin Salek, Vittorio Giovannetti, and Ludovico Lami. Quantum communication on the bosonic loss-dephasing channel, 2024.

[17] Graeme Smith and John A. Smolin. Detecting incapacity of a quantum channel. *Phys. Rev. Lett.*, 108:230507, Jun 2012.

[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017.

[19] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.

[20] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621–669, 2012.

[21] F. Caruso and V. Giovannetti. Degradability of bosonic gaussian channels. *Physical Review A*, 74:062307, 2006.

[22] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor. Entanglement assisted capacity of the broadband lossy channel. *Physical Review Letters*, 91:047901, 2003.

[23] F. Caruso, V. Giovannetti, and A. S. Holevo. One-mode bosonic Gaussian channels: a full weak-degradability classification. *New Journal of Physics*, 8(12):310–310, 2006.

[24] M. M. Wolf, D. Pérez-García, and G. Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98:130501, 2007.

[25] A. Arqand, L. Memarzadeh, and S. Mancini. Quantum capacity of a bosonic dephasing channel. *Phys. Rev. A*, 102:042413, Oct 2020.

[26] G. O. Myhr and N. Lütkenhaus. Spectrum conditions for symmetric extendible states. *Physical Review A*, 79:062307, 2009.

[27] L. Lami, S. Khatri, G. Adesso, and M. M. Wilde. Extendibility of bosonic Gaussian states. *Physical Review Letters*, 123:050501, 2019.

[28] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1990.

[29] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[30] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

Quantum communication on the bosonic loss-dephasing channel

Francesco Anna Mele,[1,*] Farzin Salek,[2,†] Vittorio Giovannetti,[1,‡] and Ludovico Lami[3,4,5,§]

[1]*NEST, Scuola Normale Superiore and Istituto Nanoscienze,*
Consiglio Nazionale delle Ricerche, Piazza dei Cavalieri 7, IT-56126 Pisa, Italy
[2]*Department of Mathematics, Technical University of Munich, Boltzmannstrasse 3, 85748 Garching, Germany*
[3]*QuSoft, Science Park 123, 1098 XG Amsterdam, the Netherlands*
[4]*Korteweg-de Vries Institute for Mathematics, University of Amsterdam,*
Science Park 105-107, 1098 XG Amsterdam, the Netherlands
[5]*Institute for Theoretical Physics, University of Amsterdam,*
Science Park 904, 1098 XH Amsterdam, the Netherlands

Quantum optical systems are typically affected by two types of noise: photon loss and dephasing. Despite extensive research on each noise process individually, a comprehensive understanding of their combined effect is still lacking. A crucial problem lies in determining the values of loss and dephasing for which the resulting loss-dephasing channel is anti-degradable, implying the absence of codes capable of correcting its effect or, alternatively, capable of enabling quantum communication. A conjecture in [Quantum 6, 821 (2022)] suggested that the bosonic loss-dephasing channel is not anti-degradable if the loss is below 50%. In this paper we refute this conjecture, specifically proving that for any value of the loss, if the dephasing is above a critical value, then the bosonic loss-dephasing channel is anti-degradable. While our result identifies a large parameter region where quantum communication is not possible, we also prove that if two-way classical communication is available, then quantum communication — and thus quantum key distribution — is always achievable, even for high values of loss and dephasing.

Quantum optical platforms are key elements of quantum technologies, contributing significantly to both quantum communication and quantum computation [1–9]. Since the potential benefits of quantum technologies are hindered by the presence of decoherence [10], the investigation of decoherence sources affecting bosonic systems and the development of bosonic quantum error-correcting codes have been extensively analysed in recent years [11–22]. The primary noise processes in bosonic systems that act as dominant sources of decoherence are *photon loss* and *bosonic dephasing* [23–25], which have been both extensively analysed [13, 26–28]. Loss affects the system by causing it to dissipate some of its energy, whereas dephasing works to transform coherent superpositions into probabilistic mixtures. Although loss and dephasing sources can simultaneously affect bosonic systems [15, 29], such as in superconducting systems [30, 31], the existing literature provides only partial results about their combined effect [32]. On a technical level, understanding the combined effect of loss and dephasing is challenging due to the conflicting behaviours they exhibit: the action of loss takes a simple form when written in the coherent state basis but is complicated to analyse in the Fock basis [2], whereas dephasing demonstrates the opposite pattern, making the analysis of their combined effect quite intricate.

Consider an optical link (e.g. an optical fibre or a free-space link) or a quantum memory affected by both loss and dephasing, where the link is used for quantum communication and the memory for quantum computation. A crucial challenge is to determine the conditions under which there exist protocols capable of enabling reliable quantum communication across the optical link or capable of mitigating the combined noise affecting the quantum memory. This problem is closely related to the anti-degradability condition in quantum Shannon theory: if a noise channel is *anti-degradable* [33, 34], there are no quantum communication protocols for reliable information transmission or quantum error-correcting codes capable of overcoming it. Consequently, it is crucial to understand whether the combined effect of loss and dephasing results in an anti-degradable channel. This has been a puzzling problem, to the point that in [32] it was conjectured that the combined loss-dephasing noise does not result in an anti-degradable channel if the loss is below 50%.

In this paper we refute the above conjecture; specifically, we prove that for any value of the photon loss there exists a *critical value* of the dephasing above which the resulting loss-dephasing channel is anti-degradable. Our discovery thus identifies a large region of the loss-dephasing parameter space where correcting the noise and achieving reliable quantum communication is impossible. On the more positive side, however, we also prove that if the sender and the receiver are assisted by two-way classical communication, then reliable quantum communication — and thus quantum key distribution — is always possible, even in scenarios characterised by arbitrarily high levels of loss and dephasing. Ours are the first analytical results to characterise the transmission of quantum information in the presence of both loss and dephasing noise.

***Preliminaries*.**— The *quantum capacity* $Q(\mathcal{N})$ of a quantum channel $\mathcal{N}$ quantifies the efficiency in transmitting qubits reliably across $\mathcal{N}$ [33, 34]. The condition $Q(\mathcal{N}) = 0$ implies that there exist neither reliable quantum communication protocols across $\mathcal{N}$ nor codes capable of correcting the errors induced by $\mathcal{N}$. Accordingly, if $\mathcal{N}$ is *anti-degradable* its quantum capacity vanishes [33]. This underscores the significance of determining whether a channel is anti-degradable, as the noise associated with such a channel cannot be corrected. By definition, a channel $\mathcal{N}$ is anti-degradable if there exists a channel $\mathcal{A}$ — called the *anti-degrading map* — such that $\mathcal{A} \circ \mathcal{N}^{c} = \mathcal{N}$, where $\mathcal{N}^{c}$ denotes a complementary channel of $\mathcal{N}$ [33]. Conversely, a channel $\mathcal{N}$ is degradable if there exists a channel $\mathcal{D}$ such that $\mathcal{D} \circ \mathcal{N} = \mathcal{N}^{c}$. Degradable channels are theoretically important because their quantum capacity can be calculated as the single-letter coherent information of the channel [33–35].

The phenomenon of photon loss is mathematically modelled by the *pure-loss channel* $\mathcal{E}_\lambda$ [2, 4], a single-mode continuous-variable channel that acts on the input state ρ by mixing it with an environmental vacuum state in a beam splitter of transmissivity $\lambda \in [0, 1]$:

$$\mathcal{E}_\lambda(\rho) := \mathrm{Tr}_E \left[U_\lambda \left(\rho_S \otimes |0\rangle\!\langle 0|_E \right) U_\lambda^\dagger \right] , \tag{1}$$

where $U_\lambda := \exp\left[\arccos\!\left(\sqrt{\lambda}\right)(\hat{a}^\dagger \hat{e} - \hat{a}\,\hat{e}^\dagger)\right]$ is the beam splitter unitary, $\hat{a}$ and $\hat{e}$ are the annihilation operators of the input system S and of the environment E, and Tr_E is the partial trace w.r.t. E. When a single photon is fed into $\mathcal{E}_\lambda$, it is transmitted to the output with probability λ, while it is lost to the environment with probability $1 - \lambda$. More generally, if n photons are fed into the channel, the output is given by the binomial probability mixture $\mathcal{E}_\lambda(|n\rangle\!\langle n|) = \sum_{\ell=0}^{n} \binom{n}{l} (1-\lambda)^\ell \lambda^{n-\ell} \, |n-\ell\rangle\!\langle n-\ell|$, where $|n\rangle$ denotes the Fock state with n photons [2]. When $\lambda = 1$ the pure-loss channel is noiseless, while when $\lambda = 0$ it is completely noisy — it maps any state into the vacuum. It is known that the pure-loss channel is anti-degradable for $\lambda \in [0, \frac{1}{2}]$ and degradable for $\lambda \in [\frac{1}{2}, 1]$ [36–39].

The phenomenon of bosonic dephasing is mathematically described by the *bosonic dephasing channel* $\mathcal{D}_\gamma$ [28, 32, 40], which maps the state $\rho = \sum_{m,n=0}^{\infty} \rho_{mn} \, |m\rangle\!\langle n|$, written in the Fock basis, to

$$\mathcal{D}_\gamma(\rho) := \sum_{m,n=0}^{\infty} \rho_{mn} e^{-\frac{\gamma}{2}(m-n)^2} \, |m\rangle\!\langle n| \ , \tag{2}$$

resulting in a reduction in magnitude of the off-diagonal elements. When $\gamma = 0$, the bosonic dephasing channel is noiseless. In contrast, when $\gamma \to \infty$, it completely annihilates all off-diagonal components of the input density matrix, reducing it to an incoherent probabilistic mixture of Fock states. Moreover, the bosonic dephasing channel is never anti-degradable and it is always degradable [40].

Consider an optical system undergoing simultaneous loss and dephasing over a finite time interval. At each instant, the system is susceptible to both an infinitesimal pure-loss channel and an infinitesimal bosonic dephasing channel. Hence, the overall channel, which describes the simultaneous effect of loss and dephasing, results in a suitable composition of numerous concatenations between infinitesimal pure-loss and bosonic dephasing channels. However, given that (i) the pure-loss channel and the bosonic dephasing channel commute, $\mathcal{E}_\lambda \circ \mathcal{D}_\gamma = \mathcal{D}_\gamma \circ \mathcal{E}_\lambda$; (ii) the composition of pure-loss channels is a pure-loss channel, $\mathcal{E}_{\lambda_1} \circ \mathcal{E}_{\lambda_2} = \mathcal{E}_{\lambda_1 \lambda_2}$; and (iii) the composition of bosonic dephasing channels is a bosonic dephasing channel, $\mathcal{D}_{\gamma_1} \circ \mathcal{D}_{\gamma_2} = \mathcal{D}_{\gamma_1 + \gamma_2}$; it follows that the combined effect of loss and dephasing can be modelled by the composition

$$\mathcal{N}_{\lambda,\gamma} := \mathcal{E}_\lambda \circ \mathcal{D}_\gamma \ , \tag{3}$$

which we will refer to as the *bosonic loss-dephasing channel* [41].

Anti-degradability.— Prior to this work, the only result on the anti-degradability of the bosonic loss-dephasing channel was that it is anti-degradable if the transmissivity is below $\frac{1}{2}$ [32]. (This result trivially follows from the anti-degradability of the pure-loss channel for transmissivities below $\frac{1}{2}$, and the fact that the composition of an anti-degradable channel with another channel inherits the property of being anti-degradable [41]). Notably, in the regime $\lambda > \frac{1}{2}$, it was an open question to understand whether or not the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable for some values of the dephasing γ, and in [32] the answer was conjectured to be negative. However, in the forthcoming Theorem 1, we show that the latter conjecture is incorrect, specifically, we prove that for all $\lambda \in [0, 1)$, if γ is sufficiently large, then $\mathcal{N}_{\lambda,\gamma}$ becomes anti-degradable [41, Theorem 27].

Theorem 1. *The bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable if the transmissivity λ and the dephasing γ fall within one of the following regions: (i) $\lambda \in [0, \frac{1}{2}]$ and $\gamma \geq 0$; (ii) $\lambda \in (\frac{1}{2}, 1)$ and γ such that $\theta\!\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}$, where $\theta(x, y) := \sum_{n=0}^{\infty} x^{n^2} y^n$. A weaker but simpler sufficient condition that implies anti-degradability is given by $\lambda \leq \max\!\left(\frac{1}{2}, \frac{1}{1+9e^{-\gamma}}\right)$.*

Proof sketch. Any finite dimensional channel $\mathcal{N}$ is anti-degradable if and only if its Choi state is *two-extendible* [42], meaning that there exists a tripartite state $\rho_{AB_1B_2}$ such that the reduced states on AB_1 and AB_2 both coincide with the Choi state:

$$\begin{aligned} \mathrm{Tr}_{B_2}\left[\rho_{AB_1B_2}\right] &= C_{AB_1}(\mathcal{N}) \, , \\ \mathrm{Tr}_{B_1}\left[\rho_{AB_1B_2}\right] &= C_{AB_2}(\mathcal{N}) \, , \end{aligned} \tag{4}$$

where the Choi state is defined as $C_{AB}(\mathcal{N}) := \mathrm{id}_A \otimes \mathcal{N}_{A' \to B}(\Phi_{AA'})$, with $\Phi_{AA'}$ being the maximally entangled state. Such a characterisation extends to infinite dimension by considering the generalised Choi state

$C^{(r)}_{AB}(\mathcal{N}) := \mathrm{id}_A \otimes \mathcal{N}_{A'\to B}\big(\Psi^{(r)}_{AA'}\big)$ [43], obtained by replacing $\Phi_{AA'}$ by the two-mode squeezed vacuum state $\Psi^{(r)}_{AA'}$ with squeezing parameter $r > 0$ [2]. The crux of our proof is to find a two-extension of $C^{(r)}_{AB}(\mathcal{N}_{\lambda,\gamma})$ in the region identified by condition (ii). We do this in two steps.

First, after scrutinising the matrix $C^{(r)}_{AB}(\mathcal{N}_{\lambda,\gamma})$ written in the Fock basis, we construct a tripartite state $\tau_{AB_1B_2}$ such that the reduced states on AB_1 and AB_2 have the same diagonal as $C^{(r)}_{AB}(\mathcal{N}_{\lambda,\gamma})$, and the same pattern of vanishing off-diagonal entries. The construction of this tripartite state involves applying several channels — namely, beam splitter unitaries, squeezing unitary, partial trace, and a three mode controlled-add-add isometry — to a 4-mode vacuum state.

The second step consists in transforming $\tau_{AB_1B_2}$ into a two-extension of $C^{(r)}_{AB}(\mathcal{N}_{\lambda,\gamma})$ by tweaking its off-diagonal entries. This is done by using the toolbox of *Hadamard maps* [34]. For any matrix $A := (a_{mn})_{m,n\in\mathbb{N}}$, the associated Hadamard map $H^{(A)}$ is defined by

$$H^{(A)}(|m\rangle\!\langle n|) = a_{mn}\,|m\rangle\!\langle n| \tag{5}$$

for all m, n [34]. In practice, $H^{(A)}$ acts on the input density matrix by multiplying each (m, n) entry by the corresponding coefficient a_{mn}. Importantly, $H^{(A)}$ is a quantum channel if and only if A is Hermitian, positive semi-definite, and has all 1's on the main diagonal [34]. The crucial observation is that it is always possible to find an infinite matrix $A_{\lambda,\gamma}$ (possibly not positive semi-definite), which is real, symmetric, and has all 1's on the main diagonal, such that the operator $\mathrm{id}_A \otimes H^{(A_{\lambda,\gamma})}_{B_1} \otimes H^{(A_{\lambda,\gamma})}_{B_2}(\tau_{AB_1B_2})$ coincides with $C^{(r)}_{AB}(\mathcal{N}_{\lambda,\gamma})$ when tracing out either B_1 or B_2.

This however does not mean that we have found a two-extension of $C^{(r)}_{AB}$, because the above operator is not necessarily a state — it may fail to be positive semi-definite. It *is* a state, however, whenever $H^{(A_{\lambda,\gamma})}$ is a quantum channel, i.e. when the infinite matrix $A_{\lambda,\gamma}$ is positive semi-definite, in formula $A_{\lambda,\gamma} \geq 0$. Therefore, a sufficient condition on the anti-degradability of $\mathcal{N}_{\lambda,\gamma}$ is that $A_{\lambda,\gamma} \geq 0$.

The rest of the proof consists in showing that under condition (ii) one indeed finds $A_{\lambda,\gamma} \geq 0$. This is not straightforward to check, because $A_{\lambda,\gamma}$ is an *infinite* matrix, and it cannot be diagonalised analytically nor numerically. To by-pass this last hurdle we employ the theory of diagonally dominant matrices, and in particular the statement that if a matrix A is such that $a_{nn} - \sum_{m:\,m\neq n}|a_{mn}| \geq 0$ for all n, then necessarily $A \geq 0$ [44, Chapter 6]. We demonstrate that if λ and γ satisfy condition (ii), then $A_{\lambda,\gamma}$ satisfies this condition, which establishes that $A_{\lambda,\gamma} \geq 0$ and hence concludes the proof [41]. □

Theorem 1 identifies a region of the parameter space (λ, γ), with λ identifying the transmissivity and γ the dephasing, where the channel is anti-degradable and thus its quantum capacity vanishes, thereby implying the absence of viable error correcting codes for quantum data transfer and storage. This region is illustrated in Fig. 1. Interestingly, Theorem 1 implies that even if $\lambda > \frac{1}{2}$ one can pick γ large enough so that there exists an anti-degrading map achieving the transformation $\mathcal{N}^{\mathrm{c}}_{\lambda,\gamma}(|n\rangle\!\langle n|_F) \longrightarrow \mathcal{N}_{\lambda,\gamma}(|n\rangle\!\langle n|_F)$, which can be expressed as [41, Subsection I G]

$$\mathcal{E}_{1-\lambda}(|n\rangle\!\langle n|_F) \otimes \big|\sqrt{\gamma}n\big\rangle\!\big\langle\sqrt{\gamma}n\big|_C \longrightarrow \mathcal{E}_{\lambda}(|n\rangle\!\langle n|_F)\,, \tag{6}$$

where $|n\rangle_F$ denotes the nth Fock state and $\big|\sqrt{\gamma}n\big\rangle_C$ denotes a coherent state [2] (see [41, Theorem 29] for an explicit construction of such anti-degrading map). This entails the following remarkable fact: for $\lambda > 1/2$ and large enough γ there exists an *n-independent* strategy to convert the lossy Fock state $\mathcal{E}_{1-\lambda}(|n\rangle\!\langle n|_F)$ into the less lossy Fock state $\mathcal{E}_{\lambda}(|n\rangle\!\langle n|_F)$ using the coherent state $\big|\sqrt{\gamma}n\big\rangle_C$ as a resource. In other words, one can undo part of the loss on $|n\rangle_F$ if one has a coherent state that contains some information on n, sufficiently amplified so that that information is accessible enough. The nontrivial and somewhat surprising nature of this exact conversion strategy arises from the fact that the coherent states $\{\big|\sqrt{\gamma}n\big\rangle_C\}_{n\in\mathbb{N}}$ are not orthogonal, meaning that the strategy that consists in measuring the coherent state, guessing n, and re-preparing $\mathcal{E}_{\lambda}(|n\rangle\!\langle n|_F)$ cannot succeed with probability 1.

Theorem 1 does not identify the entire anti-degradability region of $\mathcal{N}_{\lambda,\gamma}$, but only a subset of it. One way to improve this approximation is to determine numerically the region where the infinite matrix $A_{\lambda,\gamma}$ introduced in the proof sketch of Theorem 1 is positive semi-definite. In Fig. 1 we depict a numerical estimate of this region (see the crossed red part of the plot).

So far we have been concerned with inner approximations of the anti-degradability region. To obtain outer approximations, instead, one can start by observing that the action of $\mathcal{N}_{\lambda,\gamma}$ can only subtract and never add any photons. Mathematically, if the input state to $\mathcal{N}_{\lambda,\gamma}$ is supported on the span of the first d Fock states, so is the output state [41]. This restriction defines a qu$d$it-to-qu$d$it channel $\mathcal{N}^{(d)}_{\lambda,\gamma}$, analysing which can yield some insights into $\mathcal{N}_{\lambda,\gamma}$ itself. First, if $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is *not* anti-degradable then the same is true of $\mathcal{N}_{\lambda,\gamma}$ [41]; secondly, as discussed above the anti-degradability of $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is equivalent to the two-extendibility of the corresponding Choi state [42], and for moderate values of d this latter condition can be efficiently checked numerically via *semi-definite programming* [34, 41, 45]. In this way, we can numerically determine a parameter region (see green region of Fig. 1) where $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable. Interestingly, already the qubit restriction $\mathcal{N}^{(2)}_{\lambda,\gamma}$, which coincides with the composition between the amplitude damping channel and the qubit dephasing channel [34], yields the necessary condition $\lambda \leq \frac{1}{1+e^{-\gamma}}$ on the anti-degradability of $\mathcal{N}_{\lambda,\gamma}$, as shown in the forthcoming Theorem 2. Based on the analysis of the qudit restrictions [41], we conjecture that, if γ is sufficiently large, the latter condition $\lambda \leq \frac{1}{1+e^{-\gamma}}$ is not only necessary but also sufficient.

Theorem 2. *If $\lambda > \frac{1}{1+e^{-\gamma}}$ then $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable.*

Proof sketch. A qubit channel $\mathcal{N}$ is anti-degradable if and only if

$$\frac{1}{4}\operatorname{Tr}\left[\mathcal{N}(\mathbb{1}_2)^2\right] \geq \operatorname{Tr}\left[C(\mathcal{N})^2\right] - 4\sqrt{\det[C(\mathcal{N})]}, \qquad (7)$$

where $C(\mathcal{N})$ is the Choi state [42, 46, 47]. When focusing on the qubit restriction $\mathcal{N}^{(2)}_{\lambda,\gamma}$, Eq. (7) is equivalent to the condition $\lambda \leq \frac{1}{1+e^{-\gamma}}$. □

We are interested in the anti-degradability of the loss-dephasing channel because it implies that the quantum capacity vanishes, entailing the impossibility of quantum communication. We now look at the complementary question: when is the quantum capacity $Q(\mathcal{N}_{\lambda,\gamma})$ strictly positive? A simple sufficient condition can be obtained by optimising the coherent information [33, 34] of $\mathcal{N}_{\lambda,\gamma}$ over input states of the form $\rho_p := p\,|0\rangle\!\langle 0| + (1-p)\,|1\rangle\!\langle 1|$. By doing so we identify a region of the (λ,γ) parameter space where $Q(\mathcal{N}_{\lambda,\gamma}) > 0$ (see the crossed green region in Fig. 1). In this region quantum communication and quantum error correction become feasible.

Two-way quantum communication.— As we have just seen, (unassisted) quantum communication is not possible when the combined effects of loss and dephasing are too strong. However, in the forthcoming Theorem 3 we show that if Alice (the sender) and Bob (the receiver) have access to a *two-way* classical communication line, then quantum communication, entanglement distribution, and quantum-key distribution [48] become again achievable for any value of loss and dephasing, even when Alice's input signals are constrained to have limited energy.

In this two-way communication setting the relevant notion of capacity is the *two-way quantum capacity* $Q_2(\mathcal{N})$ [33, 34], defined as the maximum achievable rate of qubits that can be reliably transmitted across $\mathcal{N}$ with the aid of two-way classical communication. Since in practice Alice has only a limited amount of energy to produce her input signals, one usually defines the so-called *energy-constrained* two-way quantum capacity [49, 50], denoted as $Q_2(\mathcal{N}, N_s)$. Here, N_s denotes the mean photon number constraint at the input of the channel. Now, we are ready to state the main result of this section [41, Section III].

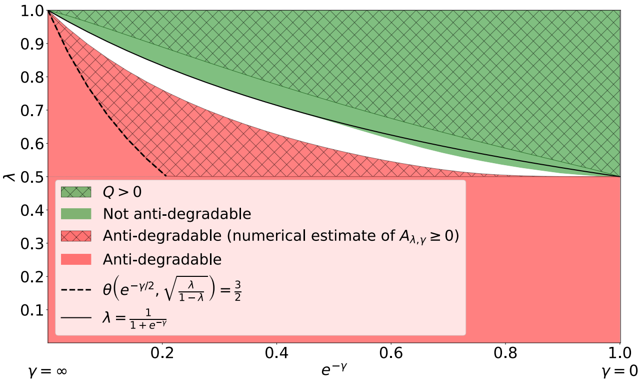


FIG. 1. Summary of results on the anti-degradability of the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$. The vertical axis represents the transmissivity λ, while the horizontal axis corresponds to $e^{-\gamma}$, where γ is the dephasing parameter. In the green region $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable, while in the red region it is anti-degradable. In the crossed green region, the quantum capacity of $\mathcal{N}_{\lambda,\gamma}$ is strictly positive. The crossed red region is a numerical estimate of the region where the infinite matrix $A_{\lambda,\gamma}$ is positive semi-definite, a condition implying that $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable, as explained in the proof sketch of Theorem 1. Such an estimate can be obtained by examining the positive semi-definiteness of the $d \times d$ top-left corner of $A_{\lambda,\gamma}$ for large values of d (here we employ $d = 30$, but increasing d already beyond $d \geq 20$ yields no discernible change in the plot). The restriction $\mathcal{N}^{(6)}_{\lambda,\gamma}$ is anti-degradable if and only if λ and γ fall within the green region, and this is the reason why $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable in the green region. Below the curve $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) = \frac{3}{2}$, the channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable, as stated in Theorem 1. Above the curve $\lambda = \frac{1}{1+e^{-\gamma}}$, the channel is not anti-degradable, as guaranteed by Theorem 2.

Theorem 3. *For all $N_s > 0$, $\lambda \in (0,1]$, and $\gamma \geq 0$, the energy-constrained two-way quantum capacity of the bosonic loss-dephasing channel is strictly positive, i.e. $Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) > 0$. In particular, $\mathcal{N}_{\lambda,\gamma}$ is not entanglement breaking. An explicit lower bound is*

$$Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) \geq \frac{\lambda^N}{k}\left[\log_2\binom{N+k-1}{N} - S\left(\rho_{N,k,\gamma}\right)\right] \qquad (8)$$

for any $N, k \in \mathbb{N}_+$ satisfying $\frac{N}{k} \leq N_s$. Here, $S(\cdot)$ is the von Neumann entropy, $\rho_{N,k,\gamma}$ is a $\binom{N+k-1}{N}$-dimensional state defined by

$$\rho_{N,k,\gamma} := \binom{N+k-1}{N}^{-1} \sum_{p,q \in \Pi(N,k)} e^{-\frac{\gamma}{2}\|p-q\|_2^2}\,|p\rangle\!\langle q|\,, \qquad (9)$$

where $\Pi(N,k) := \left\{p \in \mathbb{N}^k : \sum_{i=1}^{k} p_i = N\right\}$ represents the set of partitions of a set of N elements into k parts, and the vectors $\{|p\rangle\}_{p\in\Pi(N,k)}$ are orthonormal.

Proof sketch. The proof exploits entanglement transmission protected by a particular error correction technique, *rail encoding*. In a k-mode bosonic system, consider the subspace $V_{N,k}$ corresponding to a total photon number N. We can use this subspace, whose dimension is $d_{N,k} := \dim V_{N,k} = \binom{N+k-1}{N}$, as an error correction code that protects against the detrimental action of $\mathcal{N}_{\lambda,\gamma}$. To this end, we prepare a maximally entangled state of dimension $d_{N,k}$ and send one share of it through k copies of the channel $\mathcal{N}_{\lambda,\gamma}$, one per mode. Since under the action of $\mathcal{N}_{\lambda,\gamma}$ photons can only be lost and never added, and each photon has a probability λ of being transmitted, the probability that an N-photon state will retain all of its photons at the output of the channel is exactly λ^N. If this happens to be the case, which — crucially — can be certified by a total photon number measurement at the output, then the input state has been subjected to no loss and only dephasing. The entanglement of the resulting, maximally correlated state can be distilled via an explicit protocol known as the hashing protocol [34, 51], resulting in $\log_2 d_{N,k} - S(\rho_{N,k,\gamma}) > 0$ singlet (a.k.a. ebit, i.e. unit of entanglement) yield. The strict positivity of this yield follows by observing that $\rho_{N,k,\gamma}$ is a $d_{N,k}$-dimensional mixed state that is not maximally mixed [41].

□

Degradability.— The bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is never degradable, except in the simple cases when either $\lambda = 1$ or $\gamma = 0$ and $\lambda \geq 1/2$ [32]. This in turn implies that no single-letter formula for its quantum capacity is known outside of the anti-degradability region studied here, where the capacity vanishes. The failure of degradability has been demonstrated in [32] through a lengthy proof; we are now in position to provide an alternative, much simpler argument. The key ideas are as follows: (i) If the qubit restriction $\mathcal{N}^{(2)}_{\lambda,\gamma}$ is not degradable, then $\mathcal{N}_{\lambda,\gamma}$ is not degradable either [41]; and (ii) if the rank of the Choi state of a qubit channel is greater or equal to 3 than such channel is not degradable [52, Theorem 4]. The result then follows by observing that the rank of the Choi state of the qubit channel $\mathcal{N}^{(2)}_{\lambda,\gamma}$ is exactly 3 (for a detailed proof see [41, Theorem 34]).

Conclusion.— In this paper we have provided the first analytical investigation of the quantum communication capabilities of the bosonic loss-dephasing channel, a much more realistic model of noise than dephasing and loss treated separately. Refuting a conjecture put forth in [32], we showed that the bosonic loss-dephasing channel is anti-degradable in a large region of the loss-dephasing parameter space, entailing that neither quantum communication nor quantum error correcting codes are possible in this region. On the positive side, we also showed that if two-way classical communication is suitably exploited, then quantum communication is always achievable, even in scenarios characterised by high levels of loss and dephasing, and even in the presence of stringent energy constraints.

Two fundamental technical innovations are key to our approach. First, a new method to analyse anti-degradability of bosonic channels, based on a two-stage construction of a symmetric extension of the Choi state. The introduction of this technique is crucial here also on the conceptual level, as *all* other known tools to analyse quantum capacities (e.g. degradability [34], PPT-ness [53], or teleportation simulability [54, 55]) fail completely for the loss-dephasing channel [32]. We envision that our technique could also be applied to other cases, e.g. to analyse the anti-degradability of the composition between the pure-loss channel and a *general* bosonic dephasing channel [41, Section V]. The second innovation we introduce is based on the use of rail encoding to investigate two-way assisted entanglement generation on the loss-dephasing channel. This technique, which we anticipate may be used to study general processes where photon loss is involved, has the additional benefit of yielding an explicit entanglement generation protocol.

Although the capacities of the dephasing channel and the pure-loss channel (separately) have been determined [28, 38, 39, 54, 56–59], the capacities of the channel resulting from their combined action remain unknown. An intriguing open problem is to calculate or approximate these capacities.

Acknowledgements.— FAM and VG acknowledge financial support by MUR (Ministero dell'Istruzione, dell'Università e della Ricerca) through the following projects: PNRR MUR project PE0000023-NQSTI, PRIN 2017 Taming complexity via Quantum Strategies: a Hybrid Integrated Photonic approach (QUSHIP) Id. 2017SRN-BRK, and project PRO3 Quantum Pathfinder. FS is supported by Walter Benjamin Fellowship, DFG project No. 524058134. FAM and LL thank the Freie Universität Berlin for hospitality. FAM thanks the University of Amsterdam for hospitality.

* francesco.mele@sns.it
† farzin.salek@gmail.com
‡ vittorio.giovannetti@sns.it
§ ludovico.lami@gmail.com

[1] M. Hayashi. *Bosonic System and Quantum Optics*, pages 231–262. Springer International Publishing, Cham, 2017.

[2] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. CRC Press, Taylor & Francis Group, Boca Raton, USA, 2017.

[3] C. M. Caves and P. D. Drummond. Quantum limits on bosonic communication rates. *Reviews of Modern Physics*, 66:481–537, 1994.

[4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621–669, 2012.

[5] S. Yokoyama, R. Ukai, S. Armstrong, and et al. Ultra-large-

scale continuous-variable cluster states multiplexed in the time domain. *Nat. Photo*, 7:982–986, 2013.

[6] M. H. Devoret and R. J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science*, 339(6124):1169–1174, 2013.

[7] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi. Hardware-efficient autonomous quantum memory protection. *Phys. Rev. Lett.*, 111:120501, Sep 2013.

[8] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, 536(7617):441–445, 2016.

[9] X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi. Quantum information with gaussian states. *Physics Reports*, 448(1):1–111, 2007.

[10] M. Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Rev. Mod. Phys.*, 76:1267–1305, Feb 2005.

[11] C. Vuillot, H. Asasi, Y. Wang, L. P. Pryadko, and B. M. Terhal. Quantum error correction with the toric gottesman-kitaev-preskill code. *Phys. Rev. A*, 99:032344, Mar 2019.

[12] B. M. Terhal, J. Conrad, and C. Vuillot. Towards scalable bosonic quantum error correction. *Quantum Science and Technology*, 5(4):043001, jul 2020.

[13] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang. Performance and structure of single-mode bosonic codes. *Phys. Rev. A*, 97:032346, Mar 2018.

[14] A. Denys and A. Leverrier. The $2T$-qutrit, a two-mode bosonic qutrit. *Quantum*, 7:1032, June 2023.

[15] Arne L. Grimsmo, Joshua Combes, and Ben Q. Baragiola. Quantum computing with rotation-symmetric bosonic codes. *Phys. Rev. X*, 10:011058, Mar 2020.

[16] K. Noh and C. Chamberland. Fault-tolerant bosonic quantum error correction with the surface–gottesman-kitaev-preskill code. *Phys. Rev. A*, 101:012316, Jan 2020.

[17] D. S. Schlegel, F. Minganti, and V. Savona. Quantum error correction using squeezed schrödinger cat states. *Phys. Rev. A*, 106:022431, Aug 2022.

[18] T. Hillmann and F. Quijandría. Quantum error correction with dissipatively stabilized squeezed-cat qubits. *Phys. Rev. A*, 107:032423, Mar 2023.

[19] F. A. Mele, L. Lami, and V. Giovannetti. Maximum tolerable excess noise in CV-QKD and improved lower bound on two-way capacities. *Preprint arXiv:2303.12867*, 2023.

[20] F. A. Mele, L. Lami, and V. Giovannetti. Restoring quantum communication efficiency over high loss optical fibers. *Physical Review Letters*, 129:180501, 2022.

[21] F. A. Mele, L. Lami, and V. Giovannetti. Quantum optical communication in the presence of strong attenuation noise. *Physical Review A*, 106:042437, 2022.

[22] F. A. Mele, G. De Palma, M. Fanizza, V. Giovannetti, and L. Lami. Optical fibres with memory effects and their quantum communication capacities, 2023.

[23] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin. New class of quantum error-correcting codes for a bosonic mode. *Phys. Rev. X*, 6:031006, Jul 2016.

[24] F. Brito, D. P. DiVincenzo, R. H. Koch, and M. Steffen. Efficient one- and two-qubit pulsed gates for an oscillator-stabilized josephson qubit. *New Journal of Physics*, 10(3):033027, mar 2008.

[25] K. H. Wanser. Fundamental phase noise limit in optical fibres due to temperature fluctuations. *Electronics Letters*, 28:53, January 1992.

[26] K. Noh, V. V. Albert, and L. Jiang. Quantum capacity bounds of gaussian thermal loss channels and achievable rates with gottesman-kitaev-preskill codes. *IEEE Transactions on Information Theory*, 65(4):2563–2582, 2019.

[27] M. M. Wilde and A. Winter. Strong converse for the classical capacity of the pure-loss bosonic channel. *Problems of Information Transmission*, 50(2):117–132, April 2014.

[28] L. Lami and M. M. Wilde. Exact solution for the quantum and private capacities of bosonic dephasing channels. *Nat. Photonics*, 17(6):525–530, 2023.

[29] P. Campagne-Ibarcq, A. Eickbusch, S. Touzard, E. Zalys-Geller, N. E. Frattini, V. V. Sivak, P. Reinhold, S. Puri, S. Shankar, R. J. Schoelkopf, L. Frunzio, M. Mirrahimi, and M. H. Devoret. Quantum error correction of a qubit encoded in grid states of an oscillator. *Nature*, 584(7821):368–372, August 2020.

[30] M. Reagor, W. Pfaff, C. Axline, R. W. Heeres, N. Ofek, K. Sliwa, E. Holland, C. Wang, J. Blumoff, K. Chou, M. J. Hatridge, L. Frunzio, M. H. Devoret, L. Jiang, and R. J. Schoelkopf. Quantum memory with millisecond coherence in circuit qed. *Phys. Rev. B*, 94:014506, Jul 2016.

[31] S. Rosenblum, P. Reinhold, M. Mirrahimi, L. Jiang, L. Frunzio, and R. J. Schoelkopf. Fault-tolerant detection of a quantum error. *Science*, 361(6399):266–270, July 2018.

[32] P. Leviant, Q. Xu, L. Jiang, and S. Rosenblum. Quantum capacity and codes for the bosonic loss-dephasing channel. *Quantum*, 6:821, sep 2022.

[33] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2nd edition, 2017.

[34] S. Khatri and M. M. Wilde. Principles of quantum communication theory: A modern approach, 2020.

[35] I. Devetak and P. W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun. Math. Phys.*, 256(2):287–303, 2005.

[36] F. Caruso and V. Giovannetti. Degradability of bosonic gaussian channels. *Physical Review A*, 74:062307, 2006.

[37] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor. Entanglement assisted capacity of the broadband lossy channel. *Physical Review Letters*, 91:047901, 2003.

[38] F. Caruso, V. Giovannetti, and A. S. Holevo. One-mode bosonic Gaussian channels: a full weak-degradability classification. *New Journal of Physics*, 8(12):310–310, 2006.

[39] M. M. Wolf, D. Pérez-García, and G. Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98:130501, 2007.

[40] A. Arqand, L. Memarzadeh, and S. Mancini. Quantum capacity of a bosonic dephasing channel. *Phys. Rev. A*, 102:042413, Oct 2020.

[41] The Supplemental Material provides detailed derivations and additional results concerning the bosonic loss-dephasing channel for interested readers.

[42] G. O. Myhr and N. Lütkenhaus. Spectrum conditions for symmetric extendible states. *Physical Review A*, 79:062307, 2009.

[43] L. Lami, S. Khatri, G. Adesso, and M. M. Wilde. Extendibility of bosonic Gaussian states. *Physical Review Letters*, 123:050501, 2019.

[44] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge

University Press, 1990.

[45] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[46] C. Paddock and J. Chen. A characterization of antidegradable qubit channels, 2017.

[47] J. Chen, Z. Ji, D. Kribs, N. Lutkenhaus, and B. Zeng. Symmetric extension of two-qubit states. *Physical Review A*, 90(3), sep 2014.

[48] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[49] N. Davis, M. E. Shirokov, and M. M. Wilde. Energy-constrained two-way assisted private and quantum capacities of quantum channels. *Physical Review A*, 97:062310, 2018.

[50] M. M. Wilde and H. Qi. Energy-constrained private and quantum capacities of quantum channels. *IEEE Transactions on Information Theory*, 64(12):7802–7827, 2018.

[51] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. Royal Soc. A*, 461(2053):207–235, 2005.

[52] T. S. Cubitt, M. B. Ruskai, and G. Smith. The structure of degradable quantum channels. *J. Math. Phys.*, 49(10):102104, 2008.

[53] Graeme Smith and John A. Smolin. Detecting incapacity of a quantum channel. *Phys. Rev. Lett.*, 108:230507, Jun 2012.

[54] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017.

[55] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.

[56] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63:032312, 2001.

[57] M. M. Wilde, P. Hayden, and S. Guha. Quantum trade-off coding for bosonic communication. *Physical Review A*, 86:062306, 2012.

[58] M. M. Wilde and H. Qi. Energy-constrained private and quantum capacities of quantum channels. *IEEE Transactions on Information Theory*, 64(12):7802–7827, 2018.

[59] K. Noh, V. V. Albert, and L. Jiang. Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes. *IEEE Transactions on Information Theory*, 65(4):2563–2582, 2019.

Supplemental material: Quantum communication on the bosonic loss-dephasing channel

CONTENTS

I. PRELIMINARIES AND NOTATION

A. Quantum states and Channels

In this subsection, we present a summary of the notation and fundamental properties used in the paper, drawing from the conventions established in standard quantum information theory textbooks [1–4]. Every quantum system is associated with a separable complex Hilbert space $\mathcal{H}$ whose dimension is denoted by $|\mathcal{H}|$. We use subscripts to denote the system associated to a Hilbert space and also systems on which the operators act. The composite quantum systems A and B exist within the tensor product of their individual Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$ which is also denoted by $\mathcal{H}_{AB}$.

We shall use $\mathbb{1}$ to denote the identity operator on $\mathcal{H}$. The operator norm of a linear operator $\Theta : \mathcal{H} \longrightarrow \mathcal{H}$ is defined as

$$\|\Theta\|_\infty := \sup_{|\psi\rangle\in\mathcal{H}:\, \langle\psi|\psi\rangle=1} \sqrt{\langle\psi|\Theta^\dagger\Theta|\psi\rangle}\,. \tag{S1}$$

An alternative (but equivalent) definition of the operator norm is as follows:

$$\|\Theta\|_\infty := \sup_{|v\rangle,|w\rangle\in\mathcal{H},\, \langle v|v\rangle=\langle w|w\rangle=1} |\langle v|\,\Theta\,|w\rangle|\ . \tag{S2}$$

An operator is called bounded if its operator norm is bounded, i.e. $\|\Theta\|_\infty < \infty$. A bounded operator Θ is positive semi-definite if $\langle\psi|\,\Theta\,|\psi\rangle \geq 0, \forall\, |\psi\rangle \in \mathcal{H}$, while it is positive definite if $\langle\psi|\,\Theta\,|\psi\rangle > 0,\, \forall\, |\psi\rangle \in \mathcal{H}$. The trace norm of a linear operator $\Theta : \mathcal{H} \to \mathcal{H}$ is defined as $\|\Theta\|_1 := \mathrm{Tr}\,\sqrt{\Theta^\dagger\Theta}$. The set of trace class operators, denoted as $\mathcal{T}(\mathcal{H})$, is the set of all the linear operators on $\mathcal{H}$ such that their trace norm is finite, i.e. $\|\Theta\|_1 < \infty$. The operator and trace norm satisfy $\|\Theta\|_\infty \leq \|\Theta\|_1$. The set of quantum states (density operators), denoted as $\mathcal{P}(\mathcal{H})$, is the set of positive semi-definite trace class operators on $\mathcal{H}$ with unit trace. The *fidelity* between two quantum states $\rho, \sigma \in \mathcal{P}(\mathcal{H})$ is defined as $F(\rho,\sigma) := \mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]$.

A superoperator is a linear map between spaces of linear operators. The identity superoperator will be denoted as id. Quantum channels are completely-positive trace-preserving (cptp) superoperators. In this paper, we will use two different representations of a quantum channel that are known as Stinespring and Choi–Jamiołkowski representation. A quantum channel $\mathcal{N}_{A'\to B}$ can be represented in Stinespring representation as

$$\mathcal{N}_{A'\to B}(\cdot) = \mathrm{Tr}_E\left[U_{A'E\to BE}(\cdot \otimes |0\rangle\langle 0|_E)U^\dagger_{A'E\to BE}\right].$$

Here, E is an environment system, $|0\rangle_E$ is a pure state of the environment, and $U_{A'E\to BE}$ is an isometry that takes as input the systems A' and E and outputs the systems B, E. The associated complementary channel $\mathcal{N}^{\mathrm{c}}_{A'\to B}$ is given by

$$\mathcal{N}^{\mathrm{c}}_{A'\to E}(\cdot) = \mathrm{Tr}_B\left[U_{A'E\to BE}(\cdot \otimes |0\rangle\langle 0|_E)U^\dagger_{A'E\to BE}\right].$$

A channel $\mathcal{N}$ is called degradable if there exist a quantum channel $\mathcal{J}$, such that when is used after $\mathcal{N}$, we get back to the complementary channel $\mathcal{N}^{\mathrm{c}}$, i.e. $\mathcal{J} \circ \mathcal{N} = \mathcal{N}^{\mathrm{c}}$. On the other hand, a channel is called anti-degradable if there is another quantum channel $\mathcal{A}$, such that using it after the complementary channel, gives back the original channel, i.e. $\mathcal{A} \circ \mathcal{N}^{\mathrm{c}} = \mathcal{N}$. The channels $\mathcal{J}$ and $\mathcal{A}$ are usually called the degrading map and the anti-degrading map of $\mathcal{N}$, respectively.

The Choi–Jamiołkowski representation of the channel $\mathcal{N}_{A'\to B}$ is the operator $C(\mathcal{N}) \in \mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_B)$ that is defined as

$$C(\mathcal{N}) := \mathrm{id}_A \otimes \mathcal{N}_{A'\to B}(|\Phi\rangle\langle\Phi|_{AA'}), \tag{S3}$$

where $|\Phi\rangle = \frac{1}{\sqrt{|\mathcal{H}_A|}}\sum_{i=0}^{|\mathcal{H}_A|-1} |i\rangle_A \otimes |i\rangle_{A'}$ is a maximally entangled state of schmidt rank $|\mathcal{H}_A|$, the set of states $\{|i\rangle\}_{i=0,\ldots,|\mathcal{H}_A|-1}$ forms a basis for $\mathcal{H}_A$, and $\mathcal{H}_A = \mathcal{H}_{A'}$. It is a well-established fact that the superoperator $\mathcal{N}$ is a quantum channel if and only if $C(\mathcal{N}) \geq 0$ and $\mathrm{Tr}_B\, C(\mathcal{N}) = \mathbb{1}_A/|\mathcal{H}_A|$ [2].

Definition 1. *A bipartite state ρ_{AB} is symmetric two-extendible on B if there exists a tripartite state $\tau_{AB_1B_2}$ such that*

- $F_{B_1B_2}\tau_{AB_1B_2}F^\dagger_{B_1B_2} = \tau_{AB_1B_2}$
- $\mathrm{Tr}_{B_1}\,\tau_{AB_1B_2} = \rho_{AB}$,

where B_1 and B_2 are two copies of the system B, the operator $F_{B_1B_2} := \sum_{i,j} |i\rangle\langle j|_{B_1} \otimes |j\rangle\langle i|_{B_2}$ denotes the swap unitary, and $\{|i\rangle_{B_1}\}_i$ and $\{|i\rangle_{B_2}\}_i$ form an orthonormal basis. The state $\tau_{AB_1B_2}$ is called a symmetric two-extension of ρ_{AB} on B.

Definition 2. *A bipartite state ρ_{AB} is called two-extendible on B if there exists a tripartite state $\tau_{AB_1B_2}$ such that*

$$\mathrm{Tr}_{B_1}\,\tau_{AB_1B_2} = \mathrm{Tr}_{B_2}\,\tau_{AB_1B_2} = \rho_{AB}\,, \tag{S4}$$

where B_1 and B_2 are two copies of the system B.

Lemma 3 [5]**.** *A bipartite state ρ_{AB} is two-extendible on B if and only if it is symmetric two-extendible on B .*

Proof. First, assume ρ_{AB} is symmetric two-extendible on B. Since $F_{B_1B_2}\tau_{AB_1B_2}F^\dagger_{B_1B_2} = \tau_{AB_1B_2}$, it holds that $\mathrm{Tr}_{B_2}\,\tau_{AB_1B_2} = \mathrm{Tr}_{B_1}\,\tau_{AB_1B_2}$. This implies that ρ_{AB} is two-extendible on B. Second, let ρ_{AB} be two-extendible on B. One can easily check that the state $1/2(\tau_{AB_1B_2} + F_{B_1B_2}\tau_{AB_1B_2}F^\dagger_{B_1B_2})$ is a symmetric two-extension of ρ_{AB}. □

It has been demonstrated that a quantum channel is anti-degradable if and only if its Choi state is two-extendible on the output system [6]. This equivalence leads to a simple necessary and sufficient condition for the anti-degradability of qubit channels:

Lemma 4. *[7, Corollary 4](See also [6, 8]) Any qubit quantum channel $\mathcal{N}$ is anti-degradable if and only if it satisfies*

$$\mathrm{Tr}\left[\left(\mathcal{N}\left(\frac{\mathbb{1}_2}{2}\right)\right)^2\right] \geq \mathrm{Tr}\left[(C(\mathcal{N}))^2\right] - 4\sqrt{\det(C(\mathcal{N}))},$$

where $\mathbb{1}_2$ denotes the identity operator on the qubit Hilbert space.

B. Bosonic systems

In this subsection, we will provide an overview of relevant definitions and properties concerning quantum information with continuous variable systems; refer to [9] for detailed explanations. A single-mode of electromagnetic radiation with definite frequency and polarisation is represented by the Hilbert space $L^2(\mathbb{R})$, which comprises all square-integrable complex-valued functions over $\mathbb{R}$. Let $\mathbb{N}_+$ be the set of strictly positive integers and let $\mathbb{N} := \{0\} \cup \mathbb{N}_+$. For any $n \in \mathbb{N}$, the construction of the *Fock state* $|n\rangle$ (the quantum state with n photons) involves the application of the bosonic creation operator $\hat{a}^\dagger$ to the *vacuum state* $|0\rangle$:

$$|n\rangle := \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n |0\rangle \, . \tag{S5}$$

The Fock states $\{|n\rangle\}_{n\in\mathbb{N}}$ form an orthonormal basis of $L^2(\mathbb{R})$. The bosonic annihilation operator $\hat{a}$ and creation operator $\hat{a}^\dagger$ satisfy the well-known canonical commutation relation $[\hat{a}, \hat{a}^\dagger] = \mathbb{1}$.

Let $\mathbb{C}$ be the set of complex numbers. For any $\alpha \in \mathbb{C}$, let $D(\alpha) := e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$ be the displacement operator. A coherent state of parameter α, denoted by $|\alpha\rangle$, is defined by applying the displacement operator $D(\alpha)$ to the vacuum state, i.e. $|\alpha\rangle := D(\alpha)|0\rangle$. The overlap between coherent states is given by

$$\langle\alpha|\beta\rangle = e^{-\frac{1}{2}(|\alpha|^2+|\beta|^2-2\alpha^*\beta)} \, . \tag{S6}$$

Quantum channels acting on bosonic systems are sometimes called bosonic channels. Similar to finite-dimensional channels, bosonic channels admit a Choi–Jamiołkowski representation, usually referred to as *generalised* Choi–Jamiołkowski representation [10, 11]. Consider isomorphic Hilbert spaces $\mathcal{H}_A, \mathcal{H}_{A'}$ which are possibly infinite dimensional. Let $|\psi\rangle_{AA'}$ be a pure state satisfying $\mathrm{Tr}_{A'}\left[|\psi\rangle\langle\psi|_{AA'}\right] > 0$ (See [12, Lemma 26]). The generalised Choi state is constructed by applying the channel to the subsystem A' of $|\psi\rangle_{A'A}$ (see Lemma 49 in the Appendix): $\mathrm{id}_A \otimes \mathcal{N}_{A'\to B}(|\psi\rangle\langle\psi|_{AA'})$. The construction of the generalised Choi state usually utilises the two-mode squeezed vacuum state with squeezing parameter $r > 0$, defined as follows [9]:

$$|\psi(r)\rangle_{AA'} := \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} \tanh^n(r) \, |n\rangle_A \, |n\rangle_{A'} \, . \tag{S7}$$

The equivalence between anti-degradability of a channel and two-extendibility of its Choi state extends to the infinite-dimensional channels [13]. We provide a detailed proof of this equivalence in Lemma 50 in the Appendix as it helps us in developing our intuition in inventing an explicit example of an anti-degrading map of the bosonic loss-dephasing channel.

C. Hadamard maps

Let $A = (a_{mn})_{m,n\in\mathbb{N}}$, $a_{mn} \in \mathbb{C}$, be an infinite matrix of complex numbers. Consider the superoperator H on $\mathcal{T}\left(L^2(\mathbb{R})\right)$, recognised as the *Hadamard map*, whose action on rank one operator $|m\rangle\langle n|$ is defined as follows:

$$H(|m\rangle\langle n|) = a_{mn} \, |m\rangle\langle n| \, , \quad \forall \, m, n \in \mathbb{N} \, .$$

In Section IV A in the Appendix, we provide an overview of relevant properties of Hadamard maps. In particular, by combining known results about Hadamard maps and matrix analysis, in Lemma 47 in the Appendix, we show that given an infinite matrix $A = (a_{mn})_{m,n\in\mathbb{N}}$, $a_{mn} \in \mathbb{C}$, the associated Hadamard map is a quantum channel if

- A is Hermitian
- $a_{nn} = 1, \forall n \in \mathbb{N}$
- A is diagonally dominant, i.e. $\sum_{\substack{m=0 \\ m\neq n}}^{\infty} |a_{mn}| \leq 1, \, \forall \, n \in \mathbb{N} \, .$

D. Beam splitter

A beam splitter serves as a linear optical tool employed for creating quantum entanglement between two modes, referred to as the *system* mode (denoted as S) and the *environment* mode (denoted as E). A depiction of a beam splitter is reported in Fig 1.

Definition 5. *Let $\mathcal{H}_S, \mathcal{H}_E := L^2(\mathbb{R})$. Let $\hat{a}$ and $\hat{e}$ denote the annihilation operator of $\mathcal{H}_S$ and $\mathcal{H}_E$, respectively. For all $\lambda \in [0,1]$, the beam splitter unitary of transmissivity λ is given by*

$$U_\lambda^{SE} := \exp\left[\arccos\sqrt{\lambda}\left(\hat{a}^\dagger\hat{e} - \hat{a}\,\hat{e}^\dagger\right)\right] . \tag{S8}$$

Lemma 6. *For all $\lambda \in [0,1]$, it holds that*

$$\begin{aligned}(U_\lambda^{SE})^\dagger \hat{a}\, U_\lambda^{SE} &= \sqrt{\lambda}\,\hat{a} + \sqrt{1-\lambda}\,\hat{e}\,,\\ U_\lambda^{SE}\hat{a}\,(U_\lambda^{SE})^\dagger &= \sqrt{\lambda}\,\hat{a} - \sqrt{1-\lambda}\,\hat{e}\,,\\ (U_\lambda^{SE})^\dagger \hat{e}\, U_\lambda^{SE} &= -\sqrt{1-\lambda}\,\hat{a} + \sqrt{\lambda}\,\hat{e}\,,\\ U_\lambda^{SE}\hat{e}\,(U_\lambda^{SE})^\dagger &= \sqrt{1-\lambda}\,\hat{a} + \sqrt{\lambda}\,\hat{e}\,.\end{aligned} \tag{S9}$$

Proof. These identities can be readily proved by applying the Baker-Campbell-Hausdorff formula. For an alternative proof see [14, Lemma A.2]. □

Lemma 7. *For all $\lambda \in [0,1]$ and all $n \in \mathbb{N}$, it holds that*

$$U_\lambda^{SE}\,|n\rangle_S \otimes |0\rangle_E = \sum_{l=0}^{n}(-1)^l\sqrt{\binom{n}{l}}\lambda^{\frac{n-l}{2}}(1-\lambda)^{\frac{l}{2}}\,|n-l\rangle_S \otimes |l\rangle_E\ , \tag{S10}$$

$$U_\lambda^{SE}\,|0\rangle_S \otimes |n\rangle_E = \sum_{l=0}^{n}\sqrt{\binom{n}{l}}(1-\lambda)^{\frac{l}{2}}\lambda^{\frac{n-l}{2}}\,|l\rangle_S \otimes |n-l\rangle_E\ . \tag{S11}$$

Proof. Thanks to Lemma (6), we have that $U_\lambda^{SE}\hat{a}\left(U_\lambda^{SE}\right)^\dagger = \sqrt{\lambda}\hat{a} - \sqrt{1-\lambda}\hat{e}$. Consequently, it holds that

$$\begin{aligned}U_\lambda^{SE}\,|n\rangle_S \otimes |0\rangle_E &= \frac{1}{\sqrt{n!}}U_\lambda^{SE}(a^\dagger)^n\,|0\rangle_S \otimes |0\rangle_E\\ &= \frac{1}{\sqrt{n!}}\left(U_\lambda^{SE}a^\dagger\left(U_\lambda^{SE}\right)^\dagger\right)^n |0\rangle_S \otimes |0\rangle_E\\ &= \frac{1}{\sqrt{n!}}\left(\sqrt{\lambda}a^\dagger - \sqrt{1-\lambda}b^\dagger\right)^n |0\rangle_S \otimes |0\rangle_E\\ &= \frac{1}{\sqrt{n!}}\sum_{l=0}^{n}(-1)^l\binom{n}{l}\lambda^{\frac{n-l}{2}}(1-\lambda)^{\frac{l}{2}}(a^\dagger)^{n-l}\,|0\rangle_S \otimes (b^\dagger)^l\,|0\rangle_E\\ &= \sum_{l=0}^{n}(-1)^l\sqrt{\binom{n}{l}}\lambda^{\frac{n-l}{2}}(1-\lambda)^{\frac{l}{2}}\,|n-l\rangle_S \otimes |l\rangle_E\ .\end{aligned} \tag{S12}$$

Analogously, one can show the validity of (S11) by exploiting $U_\lambda^{SE}\hat{e}\,(U_\lambda^{SE})^\dagger = \sqrt{1-\lambda}\,\hat{a} + \sqrt{\lambda}\,\hat{e}$. □

Remark 8. *It is easily seen that Eq.* (S10) *is equivalent to*

$$U_\lambda^{SE}\,|n\rangle_S \otimes |0\rangle_E = (-1)^n\sum_{l=0}^{n}(-1)^l\sqrt{\binom{n}{l}}\lambda^{\frac{l}{2}}(1-\lambda)^{\frac{n-l}{2}}\,|l\rangle_S \otimes |n-l\rangle_E\ .$$

E. Pure-loss channel

In optical platforms, the most common source of noise is photon loss, which is modelled by the *pure-loss channel* [9]. For any $\lambda \in [0,1]$, the pure-loss channel $\mathcal{E}_\lambda$ of transmissivity λ is a single-mode bosonic channel which acts on the input system by mixing it in a beam splitter of transmissivity λ with an environmental vacuum state; see Fig 1. In this model, the input signal is partially transmitted and partially reflected by the beam splitter, representing the loss of photons (or energy) in the channel. When $\lambda = 1$, the pure-loss channel is noiseless (it equals the identity superoperator). Conversely, when $\lambda = 0$, the pure-loss channel is completely noisy (specifically, it is a constant channel that maps any state in $|0\rangle\langle 0|$).

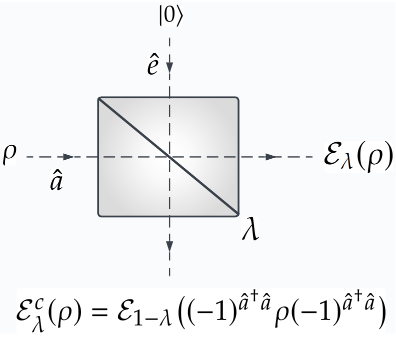

$|0\rangle$
$\hat{e}$
ρ
$\hat{a}$
$\mathcal{E}_\lambda(\rho)$
λ
$\mathcal{E}^c_\lambda(\rho) = \mathcal{E}_{1-\lambda}\big((-1)^{\hat{a}^\dagger\hat{a}}\rho(-1)^{\hat{a}^\dagger\hat{a}}\big)$

FIG. 1. Stinespring representation of the pure-loss channel $\mathcal{E}_\lambda$. The pure-loss channel $\mathcal{E}_\lambda$ acts on the input state ρ by mixing it in a beam splitter of transmissivity λ (represented by the grey box) with an environmental vacuum state $|0\rangle$. Moreover, $\hat{a}$ and $\hat{e}$ are the annihilation operators of the input mode and the environmental mode, respectively. The complementary channel of the pure-loss channel is given by $\mathcal{E}^c_\lambda(\rho) = \mathcal{E}_{1-\lambda}\big((-1)^{\hat{a}^\dagger\hat{a}}\rho(-1)^{\hat{a}^\dagger\hat{a}}\big)$.

Definition 9. *Let $\mathcal{H}_S, \mathcal{H}_E := L^2(\mathbb{R})$. For all $\lambda \in [0,1]$, the pure-loss channel of transmissivity λ is a quantum channel $\mathcal{E}_\lambda : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_S)$ defined as follows:*

$$\mathcal{E}_\lambda(\rho) := \mathrm{Tr}_E\left[U^{SE}_\lambda(\rho_S \otimes |0\rangle\langle 0|_E)(U^{SE}_\lambda)^\dagger\right], \quad \forall\, \rho \in \mathcal{T}(\mathcal{H}_S),$$

where $|0\rangle\langle 0|_E$ denotes the vacuum state of $\mathcal{H}_E$ and U^{SE}_λ denotes the beam splitter unitary defined in (S8)*.*

Lemma 10. *For all $\lambda \in [0,1]$ and all $n, m \in \mathbb{N}$, it holds that*

$$\mathcal{E}_\lambda(|m\rangle\langle n|) = \sum_{\ell=0}^{\min(n,m)} \sqrt{\binom{m}{\ell}\binom{n}{\ell}}\,(1-\lambda)^\ell \lambda^{\frac{n+m}{2}-\ell}\,|m-\ell\rangle\langle n-\ell|\,.$$

Proof. This is a direct consequence of (S10) and of the definition of pure-loss channel. □

Lemma 11. *For all $\lambda \in [0,1]$, a complementary channel $\mathcal{E}^c_\lambda : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_E)$ of the pure-loss channel $\mathcal{E}_\lambda : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_S)$ is given by*

$$\mathcal{E}^c_\lambda(\rho) := \mathrm{Tr}_S\left[U^{SE}_\lambda(\rho_S \otimes |0\rangle\langle 0|_E)\left(U^{SE}_\lambda\right)^\dagger\right] = \mathcal{E}_{1-\lambda} \circ \mathcal{R}(\rho), \qquad \forall\, \rho \in \mathcal{T}(\mathcal{H}_S), \tag{S13}$$

where $\mathcal{R}(\cdot) := V \cdot V^\dagger$ with $V := (-1)^{\hat{a}^\dagger\hat{a}}$.

Proof. By linearity, it suffices to show the identity in (S13) for rank-one Fock operators of the form $|m\rangle\langle n|$ for any $n, m \in \mathbb{N}$, i.e.

$$\mathrm{Tr}_S\left[U^{SE}_\lambda(\,|m\rangle\langle n|_S \otimes |0\rangle\langle 0|_E\,)\left(U^{SE}_\lambda\right)^\dagger\right] = \mathcal{E}_{1-\lambda} \circ \mathcal{R}(|m\rangle\langle n|)\,. \tag{S14}$$

This follows directly from (S10). □

Proposition 12. *[15, 16] The pure-loss channel $\mathcal{E}_\lambda$ is degradable if and only if $\lambda \in [\frac{1}{2}, 1]$, and it is anti-degradable if and only if $\lambda \in [0, \frac{1}{2}]$.*

Lemma 13. *[14, Lemma A.7] For all $\lambda_1, \lambda_2 \in [0,1]$ it holds that $\mathcal{E}_{\lambda_1} \circ \mathcal{E}_{\lambda_2} = \mathcal{E}_{\lambda_1\lambda_2}$.*

F. Bosonic dephasing channel

Another main source of noise in optical platforms is bosonic dephasing, which serves as a prominent example of a non-Gaussian channel [17, 18].

Definition 14. *Let $\mathcal{H}_S := L^2(\mathbb{R})$ and let $\hat{a}$ be the corresponding annihilation operator. For all $\gamma \geq 0$, the bosonic dephasing channel $\mathcal{D}_\gamma : \mathcal{T}(\mathcal{H}_S) \longrightarrow \mathcal{T}(\mathcal{H}_S)$ is a quantum channel defined as follows:*

$$\mathcal{D}_\gamma(\rho) := \frac{1}{\sqrt{2\pi\gamma}} \int_{-\infty}^{\infty} \mathrm{d}\phi\, e^{-\frac{\phi^2}{2\gamma}}\, e^{i\phi \hat{a}^\dagger \hat{a}}\, \rho\, e^{-i\phi\hat{a}^\dagger\hat{a}}, \quad \forall\, \rho \in \mathcal{T}(\mathcal{H}_S)\,.$$

In other words, $\mathcal{D}_\gamma$ is a convex combination of phase space rotations $\rho \longmapsto e^{i\phi\hat{a}^\dagger\hat{a}}\, \rho\, e^{-i\phi\hat{a}^\dagger\hat{a}}$, where the random variable ϕ follows a centered Gaussian distribution with a variance of γ.

Lemma 15. *For all $\gamma \geq 0$ and all $n, m \in \mathbb{N}$, it holds that*

$$\mathcal{D}_\gamma(|m\rangle\!\langle n|) = e^{-\frac{1}{2}\gamma(n-m)^2}\, |m\rangle\!\langle n|\,.$$

Proof. This result follows from the Fourier transform of the Gaussian function:

$$\frac{1}{\sqrt{2\pi\gamma}} \int_{-\infty}^{\infty} \mathrm{d}\phi\, e^{-\frac{\phi^2}{2\gamma}} e^{i\phi k} = e^{-\frac{1}{2}\gamma k^2}, \quad \forall\, k \in \mathbb{R}\,. \tag{S15}$$

□

When $\gamma = 0$, the bosonic dephasing channel is noiseless. In contrast, when $\gamma \longrightarrow \infty$ it annihilates all off-diagonal components of the input density matrix, reducing it to an incoherent probabilistic mixture of Fock states. We now present a Stinespring dilation of the bosonic dephasing channel.

Lemma 16. *Let $\mathcal{H}_S = \mathcal{H}_E := L^2(\mathbb{R})$ and let $\hat{a}$ and $\hat{e}$ be annihilation operators on $\mathcal{H}_S$ and $\mathcal{H}_E$, respectively. For all $\gamma > 0$, the bosonic dephasing channel $\mathcal{D}_\gamma : \mathcal{T}(\mathcal{H}_S) \longrightarrow \mathcal{T}(\mathcal{H}_S)$ can be expressed in Stinespring representation as*

$$\mathcal{D}_\gamma(\rho) = \mathrm{Tr}_E\left[V_\gamma^{SE}(\rho_S \otimes |0\rangle\!\langle 0|_E)(V_\gamma^{SE})^\dagger\right], \qquad \forall\, \rho \in \mathcal{T}(\mathcal{H}_S)\,, \tag{S16}$$

where V_γ^{SE} denotes the conditional displacement unitary defined by

$$V_\gamma^{SE} := \exp\left[\sqrt{\gamma}\, \hat{a}^\dagger\hat{a} \otimes (\hat{e}^\dagger - \hat{e})\right] = \sum_{n=0}^{\infty} |n\rangle\!\langle n|_S \otimes D(\sqrt{\gamma}n). \tag{S17}$$

Proof. For any $n, m \in \mathbb{N}$ it holds that

$$\begin{aligned} &\mathrm{Tr}_E\left[V_\gamma^{SE}(\,|m\rangle\!\langle n|_S \otimes |0\rangle\!\langle 0|_E\,)(V_\gamma^{SE})^\dagger\right] \\ &\overset{\text{(i)}}{=} \mathrm{Tr}_E\left[|m\rangle\!\langle n|_S \otimes \left|\sqrt{\gamma}n\right\rangle\!\left\langle\sqrt{\gamma}m\right|_E\right] \\ &\overset{\text{(ii)}}{=} e^{-\frac{\gamma}{2}(n-m)^2}\, |m\rangle\!\langle n| \\ &\overset{\text{(iii)}}{=} \mathcal{D}_\gamma(|m\rangle\!\langle n|)\,. \end{aligned} \tag{S18}$$

Here, in (i) we used that $V_\gamma^{SE}\,|n\rangle_S \otimes |0\rangle_E = |n\rangle_S \otimes \left|\sqrt{\gamma}n\right\rangle_E$, where $\left|\sqrt{\gamma}n\right\rangle_E$ denotes the coherent state with parameter $\sqrt{\gamma}n$. In (ii), we exploited the formula for the overlap between coherent states provided in (S6), and in (iii) we used Lemma 15. The proof is completed by linearity. □

Remark 17. *A different approach to dilating the bosonic dephasing channel, as outlined in the existing literature [17, 19, 20], is as follows:*

$$\tilde{V}_\gamma^{SE} = \exp\left[-i\sqrt{\gamma}\, \hat{a}^\dagger\hat{a}\,(\hat{e}^\dagger + \hat{e})\right].$$

This unitary transformation is achieved by rotating the environmental mode of the unitary operator V_γ^{SE} in (S17) *by $\frac{\pi}{2}$, that is $\tilde{V}_\gamma^{SE} = e^{i\frac{\pi}{2}\hat{e}^\dagger\hat{e}} V_\gamma^{SE} e^{-i\frac{\pi}{2}\hat{e}^\dagger\hat{e}}$. These dilations yield the same dephasing channel, as all dilations are equivalent up to unitary transformations.*

Proposition 18 [21]**.** *The bosonic dephasing channel $\mathcal{D}_\gamma$ is degradable for all $\gamma \geq 0$.*

Proposition 19 [21]**.** *The bosonic dephasing channel $\mathcal{D}_\gamma$ is never anti-degradable.*

Lemma 20. *For all $\gamma_1, \gamma_2 \geq 0$, the composition of bosonic dephasing channels is given by $\mathcal{D}_{\gamma_1} \circ \mathcal{D}_{\gamma_2} = \mathcal{D}_{\gamma_1+\gamma_2}$.*

Proof. This can be shown by leveraging Lemma 15. □

G. Bosonic loss-dephasing channel

Consider an optical system undergoing simultaneous loss and dephasing over a finite time interval. At each instant, the system is susceptible to both an infinitesimal pure-loss channel and an infinitesimal bosonic dephasing channel. Hence, the overall channel describing the simultaneous effect of loss and dephasing results in a suitable composition of numerous concatenations between infinitesimal pure-loss and bosonic dephasing channels. However, given that:

- The pure-loss channel and the bosonic dephasing channel commute, i.e. $\mathcal{E}_\lambda \circ \mathcal{D}_\gamma = \mathcal{D}_\gamma \circ \mathcal{E}_\lambda$, as implied by Lemma 10 and Lemma 15;
- The composition of pure-loss channels is a pure-loss channel, $\mathcal{E}_{\lambda_1} \circ \mathcal{E}_{\lambda_2} = \mathcal{E}_{\lambda_1 \lambda_2}$ (Lemma 13);
- The composition of bosonic dephasing channels is a bosonic dephasing channel, $\mathcal{D}_{\gamma_1} \circ \mathcal{D}_{\gamma_2} = \mathcal{D}_{\gamma_1+\gamma_2}$ (Lemma 20);

it follows that the combined effect of loss and dephasing can be modelled by the composition between pure-loss channel and bosonic dephasing channel,

$$\mathcal{N}_{\lambda,\gamma} := \mathcal{E}_\lambda \circ \mathcal{D}_\gamma \,, \tag{S19}$$

dubbed the *bosonic loss-dephasing channel*.

Definition 21. *For all $\gamma \geq 0$ and $\lambda \in [0,1]$, the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is a quantum channel defined by the composition between pure-loss channel and bosonic dephasing channel: $\mathcal{N}_{\lambda,\gamma} := \mathcal{D}_\gamma \circ \mathcal{E}_\lambda$.*

Lemma 22. *For all $\lambda \in [0,1]$ and $\gamma \geq 0$, it holds that $\mathcal{N}_{\lambda,\gamma} := \mathcal{D}_\gamma \circ \mathcal{E}_\lambda = \mathcal{E}_\lambda \circ \mathcal{D}_\gamma$. Moreover, for all $n, m \in \mathbb{N}$ it holds that*

$$\begin{aligned}\mathcal{N}_{\lambda,\gamma}(|m\rangle\!\langle n|) &= e^{-\frac{1}{2}\gamma(n-m)^2}\mathcal{E}_\lambda(|m\rangle\!\langle n|)\\ &= e^{-\frac{1}{2}\gamma(n-m)^2}\sum_{\ell=0}^{\min(n,m)}\sqrt{\binom{n}{\ell}\binom{m}{\ell}}(1-\lambda)^\ell\lambda^{\frac{n+m}{2}-\ell}\,|m-\ell\rangle\!\langle n-\ell| \,.\end{aligned}$$

Proof. It follows from Lemma 10 and Lemma 15. □

Lemma 23. *Let $\mathcal{H}_S, \mathcal{H}_{E_1}, \mathcal{H}_{E_2} := L^2(\mathbb{R})$. For all $\lambda \in [0,1]$ and all $\gamma \geq 0$, the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_S)$ admits the following Stinespring representation:*

$$\mathcal{N}_{\lambda,\gamma}(\rho) = \mathrm{Tr}_{E_1E_2}\left[U_\lambda^{SE_1}V_\gamma^{SE_2}(\rho_S\otimes|0\rangle\!\langle 0|_{E_1}\otimes|0\rangle\!\langle 0|_{E_2})\left(U_\lambda^{SE_1}V_\gamma^{SE_2}\right)^\dagger\right], \qquad \forall\,\rho\in\mathcal{T}(\mathcal{H}_S),$$

The associated complementary channel $\mathcal{N}^c_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_{E_1}\otimes\mathcal{H}_{E_2})$ is defined as follows:

$$\mathcal{N}^c_{\lambda,\gamma}(\rho) := \mathrm{Tr}_S\left[U_\lambda^{SE_1}V_\gamma^{SE_2}(\rho_S\otimes|0\rangle\!\langle 0|_{E_1}\otimes|0\rangle\!\langle 0|_{E_2})\left(U_\lambda^{SE_1}V_\gamma^{SE_2}\right)^\dagger\right], \qquad \forall\,\rho\in\mathcal{T}(\mathcal{H}_S).$$

In particular,

$$\mathcal{N}^c_{\lambda,\gamma}(|m\rangle\!\langle n|) = (-1)^{m-n}\mathcal{E}_{1-\lambda}\left(|m\rangle\!\langle n|_{E_1}\right)\otimes\left|\sqrt{\gamma}m\right\rangle\!\left\langle\sqrt{\gamma}n\right|_{E_2}, \qquad \forall\, m,n\in\mathbb{N}\,, \tag{S20}$$

where $\left|\sqrt{\gamma}n\right\rangle_{E_2}$ denotes the coherent state with parameter $\sqrt{\gamma}n$.

Proof. The Eq. (S20) is derived by first applying (S13) and subsequently utilising the dilation of the bosonic dephasing channel. Finally, the non-environment mode of the bosonic dephasing channel is traced out. □

Lemma 24. *Consider the Hilbert spaces $\mathcal{H}_S$, $\mathcal{H}_{E_1}$, and $\mathcal{H}_{E_2}$, all isomorphic to $L^2(\mathbb{R})$. Let $\lambda \in [0,1]$ and $\gamma \geq 0$. The bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_S)$ exhibits anti-degradability if and only if there exists a quantum channel $\mathcal{A}_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_{E_{out}}) \to \mathcal{T}(\mathcal{H}_S)$ satisfying the following condition:*

$$\mathcal{A}_{\lambda,\gamma}\circ\mathcal{N}^c_{\lambda,\gamma}(|m\rangle\!\langle n|) = \mathcal{N}_{\lambda,\gamma}(|m\rangle\!\langle n|), \quad \forall\, m,n\in\mathbb{N}\,, \tag{S21}$$

where $\mathcal{N}^c_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_{E_{out}})$ denotes the complementary channel reported in (S20)*, and $\mathcal{H}_{E_{out}} \subset \mathcal{H}_{E_1}\otimes\mathcal{H}_{E_2}$ is defined in* (S42)*. Moreover, the condition in* (S21) *is equivalent to*

$$\mathcal{A}_{\lambda,\gamma}\left(\mathcal{E}_{1-\lambda}\left(|m\rangle\!\langle n|\right)\otimes\left|\sqrt{\gamma}m\right\rangle\!\left\langle\sqrt{\gamma}n\right|\right) = (-1)^{m-n}e^{-\frac{\gamma}{2}(m-n)^2}\mathcal{E}_\lambda(|m\rangle\!\langle n|), \quad \forall\, m,n\in\mathbb{N}\,, \tag{S22}$$

where $\left|\sqrt{\gamma}n\right\rangle$ denotes the coherent state with parameter $\sqrt{\gamma}n$.

Proof. $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable if and only if there exists a quantum channel $\mathcal{A}_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_{E_{\text{out}}}) \to \mathcal{T}(\mathcal{H}_S)$ such that

$$\mathcal{A}_{\lambda,\gamma} \circ \mathcal{N}^{\text{c}}_{\lambda,\gamma}(\rho) = \mathcal{N}_{\lambda,\gamma}(\rho), \qquad \forall\, \rho \in \mathcal{T}(\mathcal{H}_S)\,. \tag{S23}$$

By linearity, it suffices to show the condition in (S21), i.e. which corresponds to the condition in (S23) restricted to rank-one Fock operators of the form $\rho = |m\rangle\!\langle n|$ with $m, n \in \mathbb{N}$. Moreover, by exploiting Lemma 22 and S20, the condition in (S21) is equivalent to (S22). □

Lemma 25. *For all $\gamma_1, \gamma_2 \geq 0$ and all λ_1, λ_2 it holds that $\mathcal{N}_{\lambda_1,\gamma_1} \circ \mathcal{N}_{\lambda_2,\gamma_2} = \mathcal{N}_{\lambda_1\lambda_2\,,\,\gamma_1+\gamma_2}$.*

Proof. This can be shown by exploiting Lemma 13 and Lemma 20. □

H. Preliminaries on capacities of quantum channels

Quantum channels can be suitably exploited in order to transfer information from their input port to a possibly distant output port, a crucial task in quantum information theory [1, 3]. In particular, quantum Shannon theory [2, 4] primarily helps us understand the fundamental limits of quantum communication using a quantum channel $\mathcal{N}$. These limits are called *capacities* and tell us the ultimate amount of information we can send through the channel when we use it many times [2, 4]. Different capacities are defined based on the type of information that is being sent down the channel. For example, classical and quantum capacities of a quantum channel correspond to its ultimate capability of transmission of classical and quantum information, respectively. A channel can also be used to generate secret bits and the relevant capacity in this context is the so-called secret-key capacity. Each of the above-mentioned capacities might be endowed with other resources such as initial shared entanglement between the sender and the receiver or (possibly interactive) classical communication over a noiseless but public channel. This latter scenario gives rise to the notion of two-way capacities.

Specifically, the *quantum capacity* $Q(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is the maximum rate at which qubits can be reliably transmitted through $\mathcal{N}$ [4]. We can further assume that both the sender, Alice, and the receiver, Bob, have free access to a public, noiseless two-way classical channel. In this two-way communication setting, the relevant notion of capacities are the *two-way quantum capacity* $Q_2(\mathcal{N})$ and the *secret-key capacity* $K(\mathcal{N})$ [2, 4], defined as the maximum achievable rate of qubits and secret-key bits, respectively, that can be reliably transmitted across $\mathcal{N}$ with the aid of two-way classical communication. Since an ebit (i.e. a maximally entangled state of Schmidt rank 2) can always be used to generate one bit of secret key [22], a trivial bound relates these capacities: $Q_2(\mathcal{N}) \leq K(\mathcal{N})$.

In practical scenarios, it is important to consider that the input state prepared by Alice can not have unlimited energy and it adheres to specific energy constraints. In bosonic systems, it is common to limit the average photon number of any input state ρ as $\mathrm{Tr}\left[\hat{a}^\dagger\hat{a}\rho\right] \leq N_s$, where $N_s > 0$ is a given energy constraint. For any $N_s > 0$, the energy-constrained (EC) two-way capacities for transmitting qubits and secret-key bits, denoted as $Q_2(\mathcal{N}, N_s)$ and $K(\mathcal{N}, N_s)$ respectively, are defined similarly to the unconstrained capacities with the difference that now the optimisation is performed over those strategies that exploit input states that adhere to the specified energy constraint. As in the unconstrained scenario, the relation between EC two-way capacities continue to hold, i.e. $Q_2(\mathcal{N}, N_s) \leq K(\mathcal{N}, N_s)$. Moreover, the unconstrained capacities are upper bounds for the corresponding energy constrained capacities and they become equal in the limit $N_s \to \infty$.

Two-way capacities of a quantum channel are closely related to another important information-processing task, namely, entanglement distillation over a quantum channel. Suppose Alice generates n copies of a state $\rho_{A'A}$ and sends the A' subsystems to Bob using the channel $\mathcal{N}$ for n times. Now, Alice and Bob share n copies of the state $\rho'_{AB} := \mathrm{id}_A \otimes \mathcal{N}_{A'\to B}(\rho_{AA'})$. The task of an entanglement distillation protocol concerns identifying the largest number m of ebits that can be extracted using n copies of ρ'_{AB} via LOCC (Local Operations and Classical Communication) operations. The rate of an entanglement distillation protocol is defined by the ratio m/n. The distillable entanglement $E_d(\rho'_{AB})$ of ρ'_{AB} is defined as the maximum rate over all the possible entanglement distillation protocols [23] [4, Chapter 8]. Note that without extra classical communication, entanglement distillation is not possible [24]. The following lemma establishes a link between the two-way quantum capacity, secret-key capacity, and distillable entanglement.

Lemma 26. *Let $\mathcal{H}_A, \mathcal{H}_{A'}, \mathcal{H}_B := L^2(\mathbb{R})$. Let $\mathcal{N} : \mathcal{H}_{A'} \to \mathcal{H}_B$ be a quantum channel. Let $N_s > 0$ be the energy constaint, and let $\rho_{A'A} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_{A'})$ be a two-mode state satisfying the energy constraint $\mathrm{Tr}\left[(\hat{a}^\dagger\hat{a} \otimes \mathrm{id}_A)\rho_{A'A}\right] \leq N_s$, where $\hat{a}$ denotes the annihilation operator on $\mathcal{H}_{A'}$. Then, it holds that*

$$K(\mathcal{N}, N_s) \geq Q_2(\mathcal{N}, N_s) \geq E_d(\mathrm{id}_A \otimes \mathcal{N}(\rho_{AA'}))\ , \tag{S24}$$

where $K(\mathcal{N}, N_s)$ denotes the energy-constrained secret-key capacity of $\mathcal{N}$, $Q_2(\mathcal{N}, N_s)$ denotes the energy-constrained two-way quantum capacity of $\mathcal{N}$, and $E_d(\mathrm{id}_A \otimes \mathcal{N}(\rho_{AA'}))$ denotes the distillable entanglement of the state $\mathrm{id}_A \otimes \mathcal{N}(\rho_{AA'})$.

The proof idea of the above lemma is the following. Suppose that Alice produces n copies of a state $\rho_{AA'}$ such that the energy constraint is satisfied. Then, she can use the channel n times to send all subsystems A' to Bob. Then, Alice and Bob share n copies of $\mathrm{id}_A \otimes \mathcal{N}(\rho_{AA'})$, which can now be used to generate $\approx n\, E_d(\mathrm{id}_A \otimes \mathcal{N}(\rho_{AA'}))$ ebits by means of a suitable entanglement distillation protocol. The ebit rate of this protocol is thus $E_d(\mathrm{id}_A \otimes \mathcal{N}(\rho_{AA'}))$, which provides a lower bound on $Q_2(\mathcal{N}, N_s)$ thanks to quantum teleportation [25]. In addition, it holds that $K(\mathcal{N}, N_s) \geq Q_2(\mathcal{N}, N_s)$ because an ebit can generate a secret-key bit [22]. Consequently, (S24) holds.

II. ANTI-DEGRADABILITY AND DEGRADABILITY OF BOSONIC LOSS-DEPHASING CHANNEL

This section is split into two parts based on the observation that if the input state to the bosonic loss-dephasing channel is chosen from a finite-dimensional subspace, the bosonic loss-dephasing channel effectively becomes a finite-dimensional channel, a fact we show in Lemma 33. This property allows us to apply established insights about the finite-dimensional channels to the bosonic loss-dephasing channel. In subsection II A, we present our study of the bosonic loss-dephasing channel when the input resides in the entire infinite-dimensional space, while subsection II B is dedicated to the findings resulting from analysis of finite-dimensional restrictions of the bosonic loss-dephasing channel.

A. Sufficient condition on anti-degradability

It is known that the bosonic dephasing channel $\mathcal{D}_\gamma$ is degradable across all dephasing parameter range $\gamma \geq 0$ and also it is never anti-degradable [17]. The pure-loss channel $\mathcal{E}_\lambda$ displays the peculiar characteristic of being anti-degradable for transmissivity values within the range $\lambda \in [0, \frac{1}{2}]$ and degradable for $\lambda \in [\frac{1}{2}, 1]$ [15, 16]. It turns out that when an anti-degradable channel is concatenated with another channel, the resulting channel inherits the property of being anti-degradable (see Lemma 51). This implies the following: if $\lambda \in [0, \frac{1}{2}]$ and $\gamma \geq 0$, then the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable [21]. The authors of [21] left as an open question to understand whether or not the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable in the region $\lambda \in (\frac{1}{2}, 1]$. In particular, they conjecture that $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable for all transmissivity values $\lambda \in (\frac{1}{2}, 1]$ and for all $\gamma \geq 0$. In the following theorem, we refute this conjecture by explicitly finding values of $\lambda \in (\frac{1}{2}, 1]$ and $\gamma \geq 0$ where the channel is anti-degradable. Our approach also yields an explicit expression for an anti-degrading map of the bosonic loss-dephasing channel.

Theorem 27. *Each of the following is a sufficient condition for the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ to exhibit anti-degradability:*

(i) $\lambda \in [0, \frac{1}{2}]$ and $\gamma \geq 0$.

(ii) $\lambda \in (\frac{1}{2}, 1)$ and $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}$, where θ is defined as $\theta(x, y) := \sum_{n=0}^{\infty} x^{n^2} y^n$, $\forall\, x, y \in [0, 1)$.

In particular, $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable if $\lambda \leq \max\left(\frac{1}{2}, \frac{1}{1+9e^{-\gamma}}\right)$.

Proof. The proof of the sufficient condition (i) follows directly from the observation that the composition of a pure-loss channel with transmissivity $\lambda \in [0, \frac{1}{2}]$ with any other channel inherits the anti-degradability from the pure-loss channel (see Lemma 51).

The proof of the sufficient condition (ii) is more involved, and it is the main technical contribution of our work. We rely on the equivalence between anti-degradability of a quantum channel and the two-extendibility of its Choi state [6, 13]. To provide a comprehensive and intuitive understanding of this idea and to aid in the construction of an anti-degrading map of the bosonic loss-dephasing channel, we present this equivalence in Lemma 50 within the Appendix.

Assume $\lambda \in (\frac{1}{2}, 1)$ and $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}$. Let $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_{B_1}, \mathcal{H}_{B_2} = L^2(\mathbb{R})$ and suppose that the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is a quantum channel from the system A' to B. We want to show that the generalised Choi state of $\mathcal{N}_{\lambda,\gamma}$ is two-extendible on B. In other words, we want to show that there exists a tripartite state $\rho_{AB_1B_2}$ such that

$$\begin{aligned} \mathrm{Tr}_{B_2}\left[\rho_{AB_1B_2}\right] &= \tau_{AB_1}\,, \\ \mathrm{Tr}_{B_1}\left[\rho_{AB_1B_2}\right] &= \tau_{AB_2}\,, \end{aligned} \tag{S25}$$

where $\tau_{AB} := \mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\psi(r)\rangle\langle\psi(r)|_{AA'})$ is the generalised Choi state of $\mathcal{N}_{\lambda,\gamma}$, and $|\psi(r)\rangle_{AA'}$ is the two-mode squeezed vacuum state with squeezing parameter $r > 0$ defined in (S7). By Lemma (22), the generalised Choi state of the bosonic loss-dephasing channel can be expressed as follows:

$$\tau_{AB} = \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell=0}^{\min(m,n)} (\tanh(r))^{m+n} e^{-\frac{\gamma}{2}(m-n)^2} \sqrt{\mathcal{B}_\ell(m,1-\lambda)\,\mathcal{B}_\ell(n,1-\lambda)}\, |m\rangle\langle n|_A \otimes |m-\ell\rangle\langle n-\ell|_B \;, \tag{S26}$$

where $\mathcal{B}_\ell(n,\lambda) := \binom{n}{\ell}\lambda^\ell(1-\lambda)^{n-\ell}$. We observe that τ_{AB} is a linear combination of $|m\rangle\langle n|\otimes|j_1\rangle\langle j_2|$, where $m,n,j_1,j_2 \in \mathbb{N}$, $j_1 \le n_1$, $j_2 \le n$, and $m-n = j_1 - j_2$. This insight leads to the following educated guess about the structure of a potential two-extension:

$$\tilde{\rho}_{AB_1B_2} = \sum_{m,n=0}^{\infty} \sum_{\ell_1=0}^{m} \sum_{\ell_2=0}^{n} \sum_{k=0}^{\min(m-\ell_1,n-\ell_2)} c(m,n,\ell_1,\ell_2,k)\, |m\rangle\langle n|_A \otimes |m-\ell_1\rangle\langle n-\ell_2|_{B_1} \otimes |\ell_1+k\rangle\langle \ell_2+k|_{B_2} \;, \tag{S27}$$

where $\{c(m,n,\ell_1,\ell_2,k)\}_{m,n,\ell_1,\ell_2,k}$ are some suitable coefficients. The soundness of this guess is confirmed by the fact that both $\mathrm{Tr}_{B_2}[\tilde{\rho}_{AB_1B_2}]$ and $\mathrm{Tr}_{B_1}[\tilde{\rho}_{AB_1B_2}]$ are linear combinations of $|m\rangle\langle n|\otimes|j_1\rangle\langle j_2|$ with $m,n,j_1,j_2 \in \mathbb{N}$, $j_1 \le m$, $j_2 \le n$, and $m-n = j_1 - j_2$, similar to the generalised Choi state τ_{AB} in (S26).

At this point, one could try to define the coefficients $\{c(m,n,\ell_1,\ell_2,k)\}_{m,n,\ell_1,\ell_2,k}$ so as to satisfy the required conditions of the extendibility. However, the resulting tripartite operator may not qualify as a quantum state. In order to ensure that we obtain a quantum state, our approach consists in producing the operator $\tilde{\rho}_{AB_1B_2}$ via a physical process that consists in applying a sequence of quantum channels to a quantum state.

We begin by constructing a quantum state that has the same operator structure as the operator $\tilde{\rho}_{AB_1B_2}$ in (S27). This means that at this initial stage, we only aim to build a tripartite state consisting of a linear combination of operators $|m\rangle\langle n|_A \otimes |m-\ell_1\rangle\langle n-\ell_2|_{B_1} \otimes |\ell_1+k\rangle\langle\ell_2+k|_{B_2}$ with the summation limits identical to those in (S27). This ensures that the coefficients equal to zero coincide in the two operators.

We now illustrate on each step of this construction. For a fixed $n \in \mathbb{N}$, consider the state $|n\rangle_A \otimes |n\rangle_{B_1}$. We introduce two auxiliary single-mode systems B_2 and C initially in vacuum states: $|n\rangle_A \otimes |n\rangle_{B_1} \otimes |0\rangle_{B_2} \otimes |0\rangle_C$. We next send the systems B_2 and B_1 through the ports of a beam splitter, resulting in a superposition of $|n\rangle_A \otimes |n-\ell\rangle_{B_1} \otimes |\ell\rangle_{B_2} \otimes |0\rangle_C$ for $\ell = 0,1,\ldots,n$, as implied by Lemma (7). We repeat this for systems B_1 and C, thus obtaining a superposition of $|n\rangle_A \otimes |n-\ell-k\rangle_{B_1} \otimes |\ell\rangle_{B_2} \otimes |k\rangle_C$, with $k = 0,1,\ldots,n-\ell$ and $\ell = 0,1,\ldots,n$. Consider now the isometry $W^{CB_1B_2}$ defined by

$$W^{CB_1B_2}\, |n\rangle_{B_1} \otimes |m\rangle_{B_2} \otimes |k\rangle_C = |n+k\rangle_{B_1} \otimes |m+k\rangle_{B_2} \otimes |k\rangle_C \,, \quad \forall\, n,m,k \in \mathbb{N}\,, \tag{S28}$$

dubbed *controlled-add-add isometry* (mode C is the control mode). By applying this isometry to the superposition we created by using beam splitters, we obtain a superposition of $|n\rangle_A \otimes |n-\ell\rangle_{B_1} \otimes |\ell+k\rangle_{B_2} \otimes |k\rangle_C$ with $k = 0,1,\ldots,n-\ell$ and $\ell = 0,1,\ldots,n$. Finally, by tracing out system C, we obtain the same operator structure of the operator $\tilde{\rho}_{AB_1B_2}$ in (S27). Having focused on the operator structure, we have not considered the transmissivities of the two beam splitters so far. We will see that these transmissivities can be chosen carefully such that the diagonal elements of the operator at hand becomes equal to those of the Choi state.

We now apply the outlined construction to the two-mode squeezed vacuum state with two vacuum states appended to it, i.e. $|\psi(r)\rangle_{AB_1} \otimes |0\rangle_{B_2} \otimes |0\rangle_C$. For reasons that will become clear in a moment, we choose the two beam splitter transmissivities to be λ (for the beam splitter acting on B_2B_1) and $\frac{1-\lambda}{\lambda}$ (for the one acting on CB_1). By doing so we obtain the state

$$\begin{aligned} \left|\phi\right\rangle_{AB_1B_2C} &:= W^{C,B_1B_2} U^{CB_1}_{\frac{1-\lambda}{\lambda}} U^{B_2B_1}_{\lambda}\, |\psi(r)\rangle_{AB_1} \otimes |0\rangle_{B_2} \otimes |0\rangle_C \\ &= \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} \sum_{\ell=0}^{n} \sum_{k=0}^{n-\ell} \tanh^n(r) \sqrt{\mathcal{B}_\ell(n,1-\lambda)\, \mathcal{B}_k\!\left(n-\ell, \frac{2\lambda-1}{\lambda}\right)}\, |n\rangle_A \otimes |n-\ell\rangle_{B_1} \otimes |\ell+k\rangle_{B_2} \otimes |k\rangle_C \;, \end{aligned} \tag{S29}$$

where we used (S7) and Lemma 7. Note that the transmissivities of the beam splitters $U^{CB_1}_{\frac{1-\lambda}{\lambda}}$ and $U^{B_2B_1}_{\lambda}$ are chosen such that the diagonal elements of $\mathrm{Tr}_{B_2C}\left[\,|\phi\rangle\langle\phi|_{AB_1B_2C}\,\right]$ and $\mathrm{Tr}_{B_1C}\left[\,|\phi\rangle\langle\phi|_{AB_1B_2C}\,\right]$ both coincide with those of the

Choi state τ_{AB} in (S26). To verify this, let us calculate the state $\mathrm{Tr}_C\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right]$:

$$\mathrm{Tr}_C\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right] = \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell_1=0}^{m} \sum_{\ell_2=0}^{n} \sum_{k=0}^{\min(m-\ell_1,n-\ell_2)} (\tanh(r))^{m+n} \sqrt{\mathcal{B}_{\ell_1}(m,1-\lambda)\,\mathcal{B}_{\ell_2}(n,1-\lambda)}$$
$$\left[\sqrt{\mathcal{B}_k\!\left(m-\ell_1,\frac{2\lambda-1}{\lambda}\right)\,\mathcal{B}_k\!\left(n-\ell_2,\frac{2\lambda-1}{\lambda}\right)}\right] |m\rangle\!\langle n|_A \otimes |m-\ell_1\rangle\!\langle n-\ell_2|_{B_1} \otimes |\ell_1+k\rangle\!\langle \ell_2+k|_{B_2}\,.$$

Notably, the structure of the state $\mathrm{Tr}_C\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right]$ mirrors that of (S27) with specific coefficients $c(m,n,\ell_1,\ell_2,k)$. Moreover, it holds that

$$\mathrm{Tr}_{B_2C}\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right] = \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell=0}^{\min(m,n)} (\tanh(r))^{m+n} \sqrt{\mathcal{B}_{\ell}(m,1-\lambda)\,\mathcal{B}_{\ell}(n,1-\lambda)}$$
$$\left[\sum_{k=0}^{\min(m-\ell,n-\ell)} \sqrt{\mathcal{B}_k\!\left(m-\ell,\frac{2\lambda-1}{\lambda}\right)\,\mathcal{B}_k\!\left(n-\ell,\frac{2\lambda-1}{\lambda}\right)}\right] |m\rangle\!\langle n|_A \otimes |m-\ell\rangle\!\langle n-\ell|_{B_1} \tag{S30}$$

and that

$$\mathrm{Tr}_{B_1C}\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right] = \mathrm{Tr}_{B_2C}\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right]. \tag{S31}$$

In order to prove (S31), observe that

$$\begin{aligned}
\mathrm{Tr}_{B_1C}\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right] &= \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell_1=\max(m-n,0)}^{m} \sum_{k=0}^{m-\ell_1} (\tanh(r))^{m+n} \sqrt{\mathcal{B}_{\ell_1}(m,1-\lambda)\,\mathcal{B}_{n-m+\ell_1}(n,1-\lambda)} \\
&\qquad \mathcal{B}_k\!\left(m-\ell_1,\frac{2\lambda-1}{\lambda}\right) |m\rangle\!\langle n|_A \otimes |\ell_1+k\rangle\!\langle n-m+\ell_1+k|_{B_2} \\
&= \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell_1=\max(m-n,0)}^{m} \sum_{\ell=0}^{m-\ell_1} (\tanh(r))^{m+n} \sqrt{\mathcal{B}_{\ell_1}(m,1-\lambda)\,\mathcal{B}_{n-m+\ell_1}(n,1-\lambda)} \\
&\qquad \mathcal{B}_{m-\ell_1-\ell}\!\left(m-\ell_1,\frac{2\lambda-1}{\lambda}\right) |m\rangle\!\langle n|_A \otimes |m-\ell\rangle\!\langle n-\ell|_{B_2} \\
&= \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell=0}^{\min(m,n)} (\tanh(r))^{m+n} \sum_{\ell_1=\max(m-n,0)}^{m-\ell} \sqrt{\mathcal{B}_{\ell_1}(m,1-\lambda)\,\mathcal{B}_{n-m+\ell_1}(n,1-\lambda)} \\
&\qquad \mathcal{B}_{m-\ell_1-\ell}\!\left(m-\ell_1,\frac{2\lambda-1}{\lambda}\right) |m\rangle\!\langle n|_A \otimes |m-\ell\rangle\!\langle n-\ell| \\
&= \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell=0}^{\min(m,n)} (\tanh(r))^{m+n} \sum_{k=0}^{\min(n-\ell,m-\ell)} \sqrt{\mathcal{B}_{m-\ell-k}(m,1-\lambda)\,\mathcal{B}_{n-\ell-k}(n,1-\lambda)} \\
&\qquad \mathcal{B}_k\!\left(k+\ell,\frac{2\lambda-1}{\lambda}\right) |m\rangle\!\langle n|_A \otimes |m-\ell\rangle\!\langle n-\ell| \\
&\overset{\text{(i)}}{=} \frac{1}{\cosh^2(r)} \sum_{m,n=0}^{\infty} \sum_{\ell=0}^{\min(m,n)} (\tanh(r))^{m+n} \sqrt{\mathcal{B}_{\ell}(m,1-\lambda)\,\mathcal{B}_{\ell}(n,1-\lambda)} \\
&\qquad \left[\sum_{k=0}^{\min(m-\ell,n-\ell)} \sqrt{\mathcal{B}_k\!\left(m-\ell,\frac{2\lambda-1}{\lambda}\right)\,\mathcal{B}_k\!\left(n-\ell,\frac{2\lambda-1}{\lambda}\right)}\right] |m\rangle\!\langle n|_A \otimes |m-\ell\rangle\!\langle n-\ell|_{B_2} \\
&\overset{\text{(ii)}}{=} \mathrm{Tr}_{B_2C}\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right]
\end{aligned} \tag{S32}$$

Here, in (i), we used the identity

$$\begin{aligned}&\sqrt{\mathcal{B}_{m-\ell-k}(m,1-\lambda)\,\mathcal{B}_{n-\ell-k}(n,1-\lambda)}\mathcal{B}_k\left(k+\ell,\frac{2\lambda-1}{\lambda}\right)\\&\quad=\sqrt{\mathcal{B}_\ell(m,1-\lambda)\,\mathcal{B}_\ell(n,1-\lambda)}\sqrt{\mathcal{B}_k\left(m-\ell,\frac{2\lambda-1}{\lambda}\right)\,\mathcal{B}_k\left(n-\ell,\frac{2\lambda-1}{\lambda}\right)}\,,\end{aligned}\tag{S33}$$

which can be easily proved by substituting the definition $\mathcal{B}_\ell(n,\lambda) := \binom{n}{\ell}\lambda^\ell(1-\lambda)^{n-\ell}$ and by leveraging the binomial identity

$$\binom{n}{l+k}\binom{l+k}{k}=\binom{n}{l}\binom{n-l}{k}.\tag{S34}$$

Moreover, in (ii), we exploited (S30).

Note that the off-diagonal terms of the state in (S30) are not equal to those of the Choi state τ_{AB} in (S26). Specifically, the points of difference with the Choi state τ_{AB} are the presence of the term inside the square brackets and the absence of the dephasing exponent. To address these additional terms, let us use the toolbox of *Hadamard maps*. Let H be the Hadamard map, introduced in Sec. I C, associated with the infinite matrix $A := (a_{mn})_{m,n\in\mathbb{N}}$ defined as follows:

$$a_{mn} := \frac{e^{-\frac{\gamma}{2}(n-m)^2}}{\sum_{j=0}^{\min(n,m)}\sqrt{\mathcal{B}_j\left(n,\frac{2\lambda-1}{\lambda}\right)\,\mathcal{B}_j\left(m,\frac{2\lambda-1}{\lambda}\right)}}\,,\qquad\forall\, n,m\in\mathbb{N}\,.\tag{S35}$$

By construction, we have that

$$\begin{aligned}&\mathrm{id}_A\otimes H_{B_1}\left(\mathrm{Tr}_{B_2C}\left[\,|\phi\rangle\!\langle\phi|_{AB_1B_2C}\,\right]\right)\\&=\frac{1}{\cosh^2(r)}\sum_{m,n=0}^{\infty}\sum_{\ell=0}^{\min(m,n)}(\tanh(r))^{m+n}\sqrt{\mathcal{B}_\ell(m,1-\lambda)\,\mathcal{B}_\ell(n,1-\lambda)}\\&\quad\left[\sum_{k=0}^{\min(m-\ell,n-\ell)}\sqrt{\mathcal{B}_k\left(m-\ell,\frac{2\lambda-1}{\lambda}\right)\,\mathcal{B}_k\left(n-\ell,\frac{2\lambda-1}{\lambda}\right)}\right]a_{m-\ell,n-\ell}\ |m\rangle\!\langle n|_A\otimes|m-\ell\rangle\!\langle n-\ell|_{B_1}\\&=\frac{1}{\cosh^2(r)}\sum_{m,n=0}^{\infty}\sum_{\ell=0}^{\min(m,n)}(\tanh(r))^{m+n}e^{-\frac{\gamma}{2}(n-m)^2}\sqrt{\mathcal{B}_\ell(m,1-\lambda)\,\mathcal{B}_\ell(n,1-\lambda)}\,|m\rangle\!\langle n|_A\otimes|m-\ell\rangle\!\langle n-\ell|_{B_1}\\&=\tau_{AB_1}\,.\end{aligned}\tag{S36}$$

This means that the operator

$$\rho_{AB_1B_2} := \mathrm{id}_A\otimes H_{B_1}\otimes H_{B_2}\left(\mathrm{Tr}_C\left[|\phi\rangle\!\langle\phi|_{AB_1B_2C}\right]\right)\tag{S37}$$

satisfies the extendibility conditions in (S25). All that remains to prove is that $\rho_{AB_1B_2}$ is in fact a quantum state. We will do this by showing that the superoperator H is a quantum channel. In Sec. I C, we establish that a Hadamard map is a quantum channel if its defining infinite matrix is Hermitian, has diagonal elements equal to one, and is diagonally dominant. The first two properties are trivially satisfied by the infinite matrix A defined in (S35). We only need to demonstrate that for the parameter region $\lambda > \frac{1}{2}$ and $\theta\left(e^{-\gamma/2},\sqrt{\frac{\lambda}{1-\lambda}}\right)\le\frac{3}{2}$, the infinite matrix A is diagonally dominant. We recall that, by definition, A is diagonally dominant if it holds that $\sum_{\substack{m=0\\m\neq n}}^{\infty}|a_{mn}|\le 1$, $\forall\, n\in\mathbb{N}$. Note that for any $n, m \in \mathbb{N}$ we have that

$$
\begin{aligned}
|a_{nm}| &= \frac{e^{-\frac{\gamma}{2}(n-m)^2}}{\sum_{j=0}^{\min(n,m)} \sqrt{\binom{n}{j}\binom{m}{j}\left(\frac{1-\lambda}{\lambda}\right)^{n+m-2j}\left(\frac{2\lambda-1}{\lambda}\right)^{2j}}} \\
&\leq \frac{e^{-\frac{\gamma}{2}(n-m)^2}}{\sum_{j=0}^{\min(n,m)} \sqrt{\binom{\min(n,m)}{j}^2\left(\frac{1-\lambda}{\lambda}\right)^{n+m-2j}\left(\frac{2\lambda-1}{\lambda}\right)^{2j}}} \\
&= e^{-\frac{\gamma}{2}(n-m)^2}\left(\frac{\lambda}{1-\lambda}\right)^{\frac{|n-m|}{2}} .
\end{aligned}
\tag{S38}
$$

Consequently, if λ and γ are such that $\lambda > \frac{1}{2}$ and $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}$, for any $n \in \mathbb{N}$ we have that

$$
\begin{aligned}
\sum_{\substack{m=0\\ m\neq n}}^{\infty} |a_{mn}| &\leq \sum_{\substack{m=0\\ m\neq n}}^{\infty} e^{-\frac{\gamma}{2}(m-n)^2}\left(\frac{\lambda}{1-\lambda}\right)^{\frac{|m-n|}{2}} \\
&= \sum_{k=1}^{\infty} e^{-\frac{\gamma}{2}k^2}\left(\frac{\lambda}{1-\lambda}\right)^{\frac{k}{2}} + \sum_{k=1}^{n} e^{-\frac{\gamma}{2}k^2}\left(\frac{\lambda}{1-\lambda}\right)^{\frac{k}{2}} \\
&\leq 2\sum_{k=1}^{\infty} e^{-\frac{\gamma}{2}k^2}\left(\frac{\lambda}{1-\lambda}\right)^{\frac{k}{2}} \\
&= 2\,\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) - 2 \\
&\leq 1 .
\end{aligned}
\tag{S39}
$$

Therefore, the infinite matrix A is diagonally dominant if $\lambda > \frac{1}{2}$ and $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}$. This establishes that H_{B_1} and H_{B_2} are valid quantum channels in this parameter range, implying that $\rho_{AB_1B_2}$ is a valid two-extension of the Choi state of $\mathcal{N}_{\lambda,\gamma}$, and in turn entailing that $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable. Finally, note that if $\lambda > \frac{1}{2}$ the condition

$$
\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \leq \frac{3}{2}
\tag{S40}
$$

is implied by $\lambda \leq \frac{1}{1+9e^{-\gamma}}$. Indeed,

$$
\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) := \sum_{k=0}^{n} e^{-\frac{\gamma}{2}k^2}\left(\sqrt{\frac{\lambda}{1-\lambda}}\right)^{k} \leq \sum_{k=0}^{\infty}\left(\frac{e^{-\gamma}\lambda}{1-\lambda}\right)^{k/2} = \frac{1}{1-\sqrt{\frac{e^{-\gamma}\lambda}{1-\lambda}}} \leq \frac{3}{2},
$$

where the last inequality follows from $\frac{e^{-\gamma}\lambda}{1-\lambda} \leq \frac{1}{9}$, which is implied by $\lambda \leq \frac{1}{1+9e^{-\gamma}}$. □

Expanding the anti-degradability region numerically

Note that Theorem 27 does not identify the entire anti-degradability region of the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$. In fact, from the above argument it becomes clear that a way to obtain a better inner approximation of this region is to check for which values of the parameters the infinite matrix A defined by (S35) is positive semi-definite. This is established in the following theorem.

Theorem 28. *Let $\ell^2(\mathbb{N})$ be the space of square-summable complex-valued sequences (defined by* (S83) *below). For any $\lambda \in (\frac{1}{2}, 1)$ and $\gamma > 0$, let $A = (a_{mn})_{m,n\in\mathbb{N}}$ be the infinite matrix whose components are defined by* (S35)*. If $A \geq 0$ is positive semi-definite as an operator on $\ell^2(\mathbb{N})$, then the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable.*

Proof. In the proof of Theorem 27 we have seen that the bosonic loss-dephasing channel is anti-degradable if the Hadamard map associated with the infinite matrix A (given in (S35)) is a quantum channel. Since the diagonal elements of A are equal to one, from Lemma 46 we deduce that the Hadamard map associated to A is a quantum channel if and only if A is positive semi-definite. This concludes the proof. □

In Theorem 27, we showed that the above-mentioned infinite matrix A is positive semi-definite if $\theta\left(e^{-\gamma/2}, \sqrt{\lambda/(1-\lambda)}\right) \leq \frac{3}{2}$, where $\theta(x,y) \coloneqq \sum_{n=0}^{\infty} x^{n^2} y^n$. This identifies just a portion of the full region of parameters of λ and γ where the infinite matrix A is positive semi-definite.

To analyse the positive semi-definiteness of the infinite matrix A further, let $A^{(d)}$ denote its $d \times d$ top-left corner. Note that it is well-known that an infinite matrix is positive semi-definite if and only if its $d \times d$ top-left corner is positive semi-definite for all $d \in \mathbb{N}$. For modest values of d, we can numerically determine the parameter region where $A^{(d)}$ is positive semi-definite. To achieve this, we plot in Fig. 2 the quantity

$$\eta_d(\gamma) \coloneqq \max\left(\lambda \in \left(\frac{1}{2}, 1\right] : \; A^{(d)} \text{ is positive semi-definite}\right) , \tag{S41}$$

with respect to $e^{-\gamma}$ for various values of d. This quantity is relevant because $A^{(d)}$ is positive semi-definite if and only if $\lambda \leq \eta_d(\gamma)$. Moreover, the quantity $\eta_d(\gamma)$ monotonically decreases in d and converges to some $\bar{\eta}(\gamma)$ as $d \longrightarrow \infty$. Notably, the condition $\lambda \leq \bar{\eta}(\gamma)$ is necessary and sufficient for positive semi-definiteness of the infinite matrix A, and also a sufficient condition for the anti-degradability of the the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$. Our numerical investigation seems to suggest that when d is approximately 20, the quantity $\eta_d(\gamma)$ has already reached its limiting value $\bar{\eta}(\gamma)$, which can be approximated, for instance, by considering, the curve $\eta_{30}(\gamma)$.

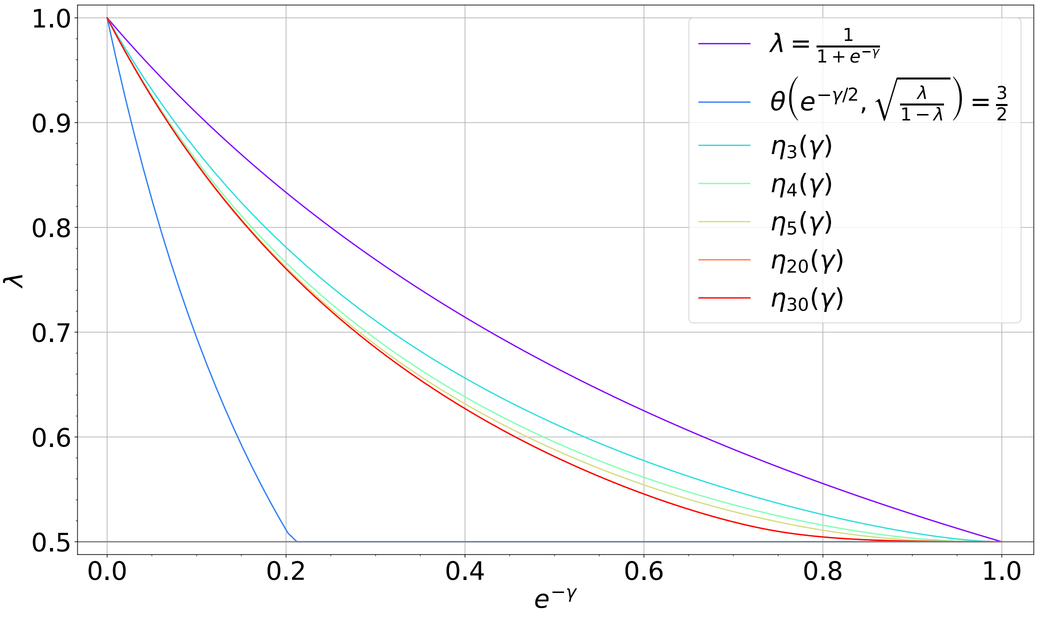


FIG. 2. Numerical estimation of the anti-degradability of the loss-dephasing channel. The horizontal axis shows the quantity $e^{-\gamma}$, varying from 0 to 1 as dephasing parameter γ decreases from ∞ to 0, while the vertical axis corresponds to the transmissivity λ. Theorem 27 establishes that below the region defined by the blue curve, corresponding to the condition $\theta(e^{-\gamma/2}, \sqrt{\lambda/(1-\lambda)}) = 3/2$, the bosonic loss-dephasing channel is anti-degradable. Moreover, Theorem 35 establishes that above the region defined by the purple curve, corresponding to $\lambda = \frac{1}{1+e^{-\gamma}}$, the bosonic loss-dephasing channel is not anti-degradable. The other curves depict the quantity $\eta_d(\gamma)$, which is defined in (S41) as the maximum value of the transmissivity where $A^{(d)}$ is positive semi-definite, for various values of d. Our numerical analysis seems to indicate that in the region below the red curve, corresponding to $\lambda \leq \eta_{30}(\gamma)$, the bosonic loss-dephasing channel is anti-degradable. Here, we employ $d = 30$, as increasing d beyond $d \geq 20$ yields no discernible change in the plot.

Theorem 27 discovers parameter regions of transmissivity λ and dephasing γ in which the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable. Although the proof of this theorem ensures the existence of anti-degrading maps for $\mathcal{N}_{\lambda,\gamma}$ within these parameter regions, it does not offer explicit constructions of such anti-degrading maps. In the forthcoming Theorem 29, we present such explicit constructions. Note that, thanks to Lemma 23, the output operators of the complementary channel $\mathcal{N}^{\mathrm{c}}_{\lambda,\gamma}$ reside within the space $\mathcal{T}(\mathcal{H}_{E_{\mathrm{out}}})$, where $\mathcal{H}_{E_{\mathrm{out}}}$ is the following subspace of the two-mode Hilbert space $\mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2} = L^2(\mathbb{R}) \otimes L^2(\mathbb{R})$:

$$\mathcal{H}_{E_{\mathrm{out}}} := \mathrm{Span}\left\{ |\ell\rangle_{E_1} \otimes \left|\sqrt{\gamma} n\right\rangle_{E_2} :\ \ell \le n \text{ with } \ell, n \in \mathbb{N} \right\}, \tag{S42}$$

where $|n\rangle$ represents the nth Fock state, and $\left|\sqrt{\gamma} n\right\rangle$ denotes the coherent state with a parameter of $\sqrt{\gamma} n$. These states correspond to the environmental modes of the pure-loss and dephasing channels, respectively (we shall maintain this notation throughout).

Theorem 29. *Anti-degrading maps corresponding to each parameter region in Theorem 27 can be defined as follows. In the region (i), i.e. $\lambda \in \left[0, \frac{1}{2}\right]$ and $\gamma \ge 0$, an anti-degrading map is given by*

$$\mathcal{A}_{\lambda,\gamma} = \left(\mathcal{E}_{\frac{\lambda}{1-\lambda}} \circ \mathcal{R}_{E_1} \right) \otimes \mathrm{Tr}_{E_2}, \tag{S43}$$

where $\mathcal{R}_{E_1}(\cdot) := (-1)^{\hat{e}_1^\dagger \hat{e}_1} \cdot (-1)^{\hat{e}_1^\dagger \hat{e}_1}$, with $\hat{e}_1$ as the annihilation operator of the output mode of the pure-loss channel E_1.

In the region (ii), i.e. $\lambda \in (\frac{1}{2}, 1)$ and γ such that $\theta\left(e^{-\gamma/2}, \sqrt{\frac{\lambda}{1-\lambda}}\right) \le \frac{3}{2}$, an anti-degrading map $\mathcal{A}_{\lambda,\gamma} : \mathcal{T}(\mathcal{H}_{E_{out}}) \to \mathcal{T}(\mathcal{H}_B)$, with $\mathcal{H}_{E_{out}}$ given by (S42)*, is defined as follows. For all $\ell_1, \ell_2, n_1, n_2 \in \mathbb{N}$ with $\ell_1 \le n_1$ and $\ell_2 \le n_2$, it holds that*

$$\mathcal{A}_{\lambda,\gamma}\left(|\ell_1\rangle\langle\ell_2| \otimes \left|\sqrt{\gamma} n_1\right\rangle\left\langle\sqrt{\gamma} n_2\right|\right) := \sum_{k=0}^{\min(n_1-\ell_1, n_2-\ell_2)} c_k^{(\ell_1,\ell_2,n_1,n_2)} \, |k+\ell_1\rangle\langle k+\ell_2| \ , \tag{S44}$$

where for all $k \in \{0, 1, \ldots, \min(n_1 - \ell_1, n_2 - \ell_2)\}$ the coefficients $c_k^{(\ell_1,\ell_2,n_1,n_2)}$ are defined as

$$c_k^{(\ell_1,\ell_2,n_1,n_2)} := (-1)^{\ell_1-\ell_2} \sqrt{\mathcal{B}_k\left(n_1 - \ell_1, \frac{2\lambda - 1}{\lambda}\right) \mathcal{B}_k\left(n_2 - \ell_2, \frac{2\lambda - 1}{\lambda}\right)} \, a_{n_1-\ell_1 n_2-\ell_2} \, a_{k+\ell_1 k+\ell_2} \ , \tag{S45}$$

where $\mathcal{B}_l(n, \lambda) := \binom{n}{l} \lambda^l (1-\lambda)^{n-l}$, and a_{mn} is defined in (S35)*.*

Proof of Theorem 29. Let us suppose that λ and γ fall within the parameter region (i). A complementary channel of the pure-loss channel $\mathcal{E}_\lambda$ is given by $\mathcal{E}_\lambda^{\mathrm{c}} = \mathcal{E}_{1-\lambda} \circ \mathcal{R}$. Consequently, Lemma 13 implies that $\left(\mathcal{E}_{\frac{\lambda}{1-\lambda}} \circ \mathcal{R} \right) \circ \mathcal{E}_\lambda^{\mathrm{c}} = \mathcal{E}_\lambda$, i.e. the channel $\mathcal{E}_{\frac{\lambda}{1-\lambda}} \circ \mathcal{R}$ is an anti-degrading map of the pure-loss channel. The general construction detailed in the proof of Lemma 51 for the anti-degrading map of the composition between an anti-degradable channel and another channel demonstrates that the map given in (S43) is an anti-degrading map of $\mathcal{N}_{\lambda,\gamma}$.

Let us now suppose that λ and γ fall within the parameter region (ii). To come up with the anti-degrading map defined in (S44), we drew intuition from the proof of Lemma 50, which demonstrates the equivalence between two-extendibility of the Choi state and the existence of an anti-degrading map, while also considering the two-extension of the Choi state of $\mathcal{N}_{\lambda,\gamma}$ explicitly found in (S37). In order to show that the map $\mathcal{A}_{\lambda,\gamma}$ in (S44) is an anti-degrading map of $\mathcal{N}_{\lambda,\gamma}$, we need to show that it is a quantum channel satisfying $\mathcal{A}_{\lambda,\gamma} \circ \mathcal{N}^{\mathrm{c}}_{\lambda,\gamma} = \mathcal{N}_{\lambda,\gamma}$. We begin by proving that $\mathcal{A}_{\lambda,\gamma}$ is trace preserving. By linearity, it suffices to show that for any $\ell_1, \ell_2, n_1, n_2 \in \mathbb{N}$ with $\ell_1 \le n_1$ and $\ell_2 \le n_2$ it holds that

$$\mathrm{Tr}\left[\mathcal{A}_{\lambda,\gamma}\left(|\ell_1\rangle\langle\ell_2|_{E_1} \otimes \left|\sqrt{\gamma} n_1\right\rangle\left\langle\sqrt{\gamma} n_2\right|_{E_2} \right) \right] = \mathrm{Tr}\left[|\ell_1\rangle\langle\ell_2|_{E_1} \otimes \left|\sqrt{\gamma} n_1\right\rangle\left\langle\sqrt{\gamma} n_2\right|_{E_2} \right] \ . \tag{S46}$$

Indeed, we obtain

$$
\begin{aligned}
\mathrm{Tr}\left[\mathcal{A}_{\lambda,\gamma}\left(|\ell_1\rangle\!\langle\ell_2|_{E_1}\otimes\left|\sqrt{\gamma}m\right\rangle\!\left\langle\sqrt{\gamma}n\right|_{E_2}\right)\right] &= \delta_{\ell_1,\ell_2}\sum_{k=0}^{\min(m-\ell_1,n-\ell_1)} c_k^{(\ell_1,\ell_1,m,n)} \\
&= \delta_{\ell_1,\ell_2}\sum_{k=0}^{\min(m-\ell_1,n-\ell_1)} \sqrt{\mathcal{B}_k\left(m-\ell_1,\frac{2\lambda-1}{\lambda}\right)\mathcal{B}_k\left(n-\ell_1,\frac{2\lambda-1}{\lambda}\right)}a_{m-\ell_1,n-\ell_1}\,a_{k+\ell_1,k+\ell_1} \\
&= \delta_{\ell_1,\ell_2}e^{-\frac{\gamma}{2}(m-n)^2} \\
&= \mathrm{Tr}\left[|\ell_1\rangle\!\langle\ell_2|_{E_1}\otimes\left|\sqrt{\gamma}n_1\right\rangle\!\left\langle\sqrt{\gamma}n_2\right|_{E_2}\right]\,,
\end{aligned}
$$

where δ_{ℓ_1,ℓ_2} denotes the kronecker delta and where we have exploited the formula for the overlap between coherent states provided in (S6). Now, let us show that $\mathcal{A}_{\lambda,\gamma}$ is completely positive. To achieve this, we need to find a pure state Ψ on $\mathcal{H}_{\mathrm{anc}}\otimes\mathcal{H}_{E_{\mathrm{out}}}$, where $\mathcal{H}_{\mathrm{anc}}$ in an auxiliary reference, such that $\mathrm{Tr}_{\mathrm{anc}}[|\Psi\rangle\!\langle\Psi|]>0$ and $(\mathrm{id}_{\mathrm{anc}}\otimes\mathcal{A}_{\lambda,\gamma})(|\Psi\rangle\!\langle\Psi|)\geq 0$ [10, 11, 26]. Let $\mathcal{H}_{\mathrm{anc}}:=\mathcal{H}_A\otimes\mathcal{H}_{B_1}=L^2(\mathbb{R})\otimes L^2(\mathbb{R})$ and let us construct the pure state $|\Psi\rangle_{AB_1E_1E_2}\in\mathcal{H}_{\mathrm{anc}}\otimes\mathcal{H}_{E_{\mathrm{out}}}$ as follows:

$$
\begin{aligned}
|\Psi\rangle_{AB_1E_1E_2} &:= U_\lambda^{B_1E_1}V_\gamma^{B_1E_2}\,|\psi(r)\rangle_{AB_1}\,|0\rangle_{E_1}\,|0\rangle_{E_2} \\
&= \frac{1}{\cosh(r)}\sum_{n=0}^{\infty}\sum_{\ell=0}^{n}(-1)^{\ell}\tanh^n(r)\sqrt{\mathcal{B}_l(n,1-\lambda)}\,|n\rangle_A\,|n-\ell\rangle_{B_1}\,|\ell\rangle_{E_1}\left|\sqrt{\gamma}n\right\rangle_{E_2}\,,
\end{aligned}
\tag{S47}
$$

where $U_\lambda^{B_1E_1}$ is the beam splitter unitary, $V_\gamma^{B_1E_2}$ is the conditional displacement unitary, and $|\psi(r)\rangle_{AB_1}$ is the two-mode squeezed vacuum state with squeezing $r>0$. Let us now show that $\mathrm{Tr}_{AB_1}\left[|\Psi\rangle\!\langle\Psi|_{AB_1E_1E_2}\right]$ is positive definite on $\mathcal{H}_{E_{\mathrm{out}}}$. Let $\left|\phi\right\rangle_{E_1E_2}\in\mathcal{H}_{E_{\mathrm{out}}}$. Since there exists $\bar{\ell},\bar{n}\in\mathbb{N}$ with $\bar{l}\leq\bar{n}$ such that $\left\langle\phi\right|_{E_1E_2}\left|\bar{\ell}\right\rangle_{E_1}\otimes\left|\sqrt{\gamma}\bar{n}\right\rangle_{E_2}\neq 0$, (S47) implies that

$$
\begin{aligned}
\left\langle\phi\right|_{E_1E_2}\mathrm{Tr}_{AB_1}\left[|\Psi\rangle\!\langle\Psi|_{AB_1E_1E_2}\right]\left|\phi\right\rangle_{E_1E_2} &= \frac{1}{\cosh^2(r)}\sum_{n=0}^{\infty}\sum_{l=0}^{n}\tanh^{2n}(r)\,\mathcal{B}_\ell\left(n,1-\lambda\right)\left|\left\langle\phi\right|_{E_1E_2}|\ell\rangle_{E_1}\otimes\left|\sqrt{\gamma}n\right\rangle_{E_2}\right|^2 \\
&\geq \frac{1}{\cosh^2(r)}\tanh^{2\bar{n}}(r)\,\mathcal{B}_{\bar{l}}\left(\bar{n},1-\lambda\right)\left|\left\langle\phi\right|_{E_1E_2}\left|\bar{\ell}\right\rangle_{E_1}\otimes\left|\sqrt{\gamma}\bar{n}\right\rangle_{E_2}\right|^2 \\
&>0\,.
\end{aligned}
$$

We next show that $\mathrm{id}_{AB_1}\otimes\mathcal{A}_{\lambda,\gamma}(|\Psi\rangle\!\langle\Psi|)$ is positive semi-definite. Let B_2 denote the output system of $\mathcal{A}_{\lambda,\gamma}$. Note that

$$
\begin{aligned}
\mathrm{id}_{AB_1}\otimes\mathcal{A}_{\lambda,\gamma}(|\Psi\rangle\!\langle\Psi|_{AB_1E_1E_2}) &\overset{\text{(i)}}{=} \frac{1}{\cosh^2(r)}\sum_{m,n=0}^{\infty}\sum_{\ell_1=0}^{m}\sum_{\ell_2=0}^{n}(-1)^{\ell_1+\ell_2}[\tanh(r)]^{m+n}\sqrt{\mathcal{B}_{\ell_1}(m,1-\lambda)\mathcal{B}_{\ell_2}(n,1-\lambda)} \\
&\qquad |m\rangle\!\langle n|_A\otimes|m-\ell_1\rangle\!\langle n-\ell_2|_{B_1}\otimes\mathcal{A}_{\lambda,\gamma}\left(|\ell_1\rangle\!\langle\ell_2|_{E_1}\otimes\left|\sqrt{\gamma}m\right\rangle\!\left\langle\sqrt{\gamma}n\right|_{E_2}\right) \\
&\overset{\text{(ii)}}{=} \frac{1}{\cosh^2(r)}\sum_{m,n=0}^{\infty}\sum_{\ell_1=0}^{m}\sum_{\ell_2=0}^{n}\sum_{k=0}^{\min(m-\ell_1,n-\ell_2)}[\tanh(r)]^{m+n} \\
&\qquad \sqrt{\mathcal{B}_{\ell_1}(m,1-\lambda)\,\mathcal{B}_{\ell_2}(n,1-\lambda)\,\mathcal{B}_k\left(m-\ell_1,\frac{2\lambda-1}{\lambda}\right)\mathcal{B}_k\left(n-\ell_2,\frac{2\lambda-1}{\lambda}\right)} \\
&\qquad a_{m-\ell_1,n-\ell_2}\,a_{k+\ell_1,k+\ell_2}\,|n_1\rangle\!\langle n|_A\otimes|m-\ell_1\rangle\!\langle n-\ell_2|_{B_1}\otimes|k+\ell_1\rangle\!\langle k+\ell_2|_{B_2} \\
&\overset{\text{(iii)}}{=} \rho_{AB_1B_2}\,.
\end{aligned}
\tag{S48}
$$

Here, in (i) we used the definition of $|\Psi\rangle_{AB_1E_1E_2}$ given in (S47); in (ii) we utilised the definition of the map $\mathcal{A}_{\lambda,\gamma}$ from (S44); and in (iii) we recognised the tripartite operator $\rho_{AB_1B_2}$ defined in (S37), which is a quantum state provided that λ and γ satisfy $\theta\left(e^{-\gamma/2},\sqrt{\frac{\lambda}{1-\lambda}}\right)\leq\frac{3}{2}$. Therefore, in such a parameter region, $\mathrm{id}_{AB_1}\otimes\mathcal{A}_{\lambda,\gamma}(|\Psi\rangle\!\langle\Psi|_{AB_1E_1E_2})$

is positive semi-definite, and thus $\mathcal{A}_{\lambda,\gamma}$ is a quantum channel. Let us now verify that $\mathcal{A}_{\lambda,\gamma} \circ \mathcal{N}^{\mathrm{c}}_{\lambda,\gamma} = \mathcal{N}_{\lambda,\gamma}$. To show this, note that

$$\begin{aligned}\mathrm{id}_A \otimes \left(\mathcal{A}_{\lambda,\gamma} \circ \mathcal{N}^{\mathrm{c}}_{\lambda,\gamma}\right)(|\psi(r)\rangle\!\langle\psi(r)|_{AB_1}) &\overset{\text{(iv)}}{=} \mathrm{Tr}_{B_1}\left[\mathrm{id}_{AB_1} \otimes \mathcal{A}_{\lambda,\gamma}(|\Psi\rangle\!\langle\Psi|_{AB_1E_1E_2})\right] \\ &\overset{\text{(v)}}{=} \mathrm{Tr}_{B_1}\left[\rho_{AB_1B_2}\right] \\ &\overset{\text{(vi)}}{=} \mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}\left(|\psi(r)\rangle\!\langle\psi(r)|_{AB_2}\right),\end{aligned} \tag{S49}$$

Here, in (iv) we employed (S47); in (v) we exploited (S48); and in (vi) we used that $\rho_{AB_1B_2}$ is a two-extension of $\mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\psi(r)\rangle\!\langle\psi(r)|)$, as established in the proof of Theorem 27. Finally, since the two-mode squeezed vacuum state $|\psi(r)\rangle_{AB}$ satisfies $\mathrm{Tr}_B[|\psi(r)\rangle\!\langle\psi(r)|_{AB}] > 0$, we conclude $\mathcal{A}_{\lambda,\gamma} \circ \mathcal{N}^{\mathrm{c}}_{\lambda,\gamma} = \mathcal{N}_{\lambda,\gamma}$. □

B. Analysis of the bosonic loss-dephasing channel via its finite-dimensional restrictions

Definition 30. *Let $d \in \mathbb{N}$ and let $\mathcal{H}_d := \mathrm{Span}(\{|n\rangle\}_{n=0,\ldots,d-1})$ be the subspace spanned by the first d Fock states. The qudit restriction of the bosonic loss-dephasing channel $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is a quantum channel defined by*

$$\mathcal{N}^{(d)}_{\lambda,\gamma}(\Theta) := \mathcal{N}_{\lambda,\gamma}(\Theta) \qquad \forall\, \Theta \in \mathcal{T}(\mathcal{H}_d) \tag{S50}$$

Lemma 31. *Let $\mathcal{H}_A, \mathcal{H}_B := L^2(\mathbb{R})$. Let $\mathcal{N} : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ be a quantum channel and let $\mathcal{N}^{(d)}$ be its qudit restriction, defined by*

$$\mathcal{N}^{(d)}(\Theta) := \mathcal{N}(\Theta) \qquad \forall\, \Theta \in \mathcal{T}(\mathcal{H}_d)\,. \tag{S51}$$

If $\mathcal{N}$ is (anti-)degradable, then its qudit restriction $\mathcal{N}^{(d)}$ is (anti-)degradable.

Proof. Let $\mathcal{N}(\cdot) = \mathrm{Tr}_E[V_{A\to BE}(\cdot)V^\dagger_{A\to BE}]$ be a Stinespring representation of $\mathcal{N}$, and let $\mathcal{N}^{\mathrm{c}}(\cdot) = \mathrm{Tr}_B[V_{A\to BE}(\cdot)V^\dagger_{A\to BE}]$ be the associated complementary channel. Note that the isometry $V_{A\to BE}$ provides a Stinespring representation also for the qudit restriction $\mathcal{N}^{(d)}$. Hence, the qudit restriction of the complementary channel $\mathcal{N}^{\mathrm{c}}$ is a complementary channel of the qudit restriction $\mathcal{N}^{(d)}$, i.e.

$$(\mathcal{N}^{(d)})^{\mathrm{c}}(\Theta) = \mathcal{N}^{\mathrm{c}}(\Theta) \qquad \forall\, \Theta \in \mathcal{T}(\mathcal{H}_d)\,. \tag{S52}$$

Moreover, note that any degrading or anti-degrading map of $\mathcal{N}$ is effective for all input states, including those restricted to $\mathcal{H}_d$. Consequently, an (anti-)degrading map of $\mathcal{N}$ is also an (anti-)degrading map of its qudit restriction $\mathcal{N}^{(d)}$. □

Corollary 32. *If the qudit restriction $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is not (anti)-degradable, then the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is also not (anti)-degradable.*

The following lemma shows that qudit restriction $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is a qu*d*it-to-qu*d*it channel, mapping the space spanned by $\{|n\rangle\}_{n=0,\ldots,d-1}$ into itself.

Lemma 33. *If the input state to the bosonic loss-dephasing channel is confined into the finite-dimensional subspace spanned by $\{|n\rangle\}_{n=0,\ldots,d-1}$, the resulting output state will similarly be confined to this subspace.*

Proof. Examining Lemma 22 reveals that the operator $|m\rangle\!\langle n|$, when acted on by the bosonic loss-dephasing channel, is transformed into linear combinations of operators $\{|\ell\rangle\!\langle k|\}_{\ell\le m, k\le n}$. This means that if the input state to the bosonic loss-dephasing channel is restricted to the d-dimensional subspace $\{|n\rangle\}_{n=0,\ldots,d-1}$, the output of the channel will reside within the same subspace. □

The qubit restriction $\mathcal{N}^{(2)}_{\lambda,\gamma}$ of the bosonic loss-dephasing channel coincides with the composition between the amplitude damping channel and the qubit dephasing channel [2, 4], which we dub *amplitude-phase damping channel*. Theorems 34 and 35 utilise the amplitude-phase damping channel $\mathcal{N}^{(2)}_{\lambda,\gamma}$ to find that the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is never degradable and, additionally, it is not anti-degradabile for $\lambda > \frac{1}{1+e^{-\gamma}}$, respectively.

The bosonic loss-dephasing channel is never degradable

The bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is never degradable, except when it coincides with either the bosonic dephasing channel ($\gamma > 0$ and $\lambda = 1$) or the degradable pure-loss channel ($\gamma = 0$ and $\lambda \geq \frac{1}{2}$), thereby complicating the derivation of its quantum capacity [21]. This result has been previously demonstrated in [21] through pages-long proof; however, here we provide a significantly simpler proof of this result.

Theorem 34. *Let $\lambda \in [0,1]$ and $\gamma \geq 0$. The bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is degradable if and only if one of the following conditions is satisfied:*

- $\gamma = 0$ *and* $\lambda \in [\frac{1}{2}, 1]$
- $\gamma \geq 0$ *and* $\lambda = 1$

Proof. Thanks to Corollary 32, a necessary condition for $\mathcal{N}_{\lambda,\gamma}$ to be degradable is the degradability of the amplitude-phase damping channel $\mathcal{N}^{(2)}_{\lambda,\gamma}$. We now apply [27, Theorem 4], which establishes a necessary condition on the degradability of any qubit channel. Specifically, the rank of the Choi state of a degradable qubit channel is necessarily less or equal to 2. By using the notation used in (S3), the matrix associated with the Choi state of the amplitude-phase damping channel $C\left(\mathcal{N}^{(2)}_{\lambda,\gamma}\right)$ in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is given by:

$$\frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \sqrt{e^{-\gamma}\lambda} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\lambda & 0 \\ \sqrt{e^{-\gamma}\lambda} & 0 & 0 & \lambda \end{pmatrix}. \tag{S53}$$

One can easily see that its rank is equal to 3 for $\gamma > 0$ and $\lambda \in (0,1)$. In addition, for $\lambda = 1$ the bosonic loss-dephasing channel coincides with the bosonic dephasing channel, $\mathcal{N}_{1,\gamma} = \mathcal{D}_\gamma$, which is degradable for any value of $\gamma \geq 0$ [17]. Finally, for $\gamma = 0$ the bosonic loss-dephasing channel coincides with the pure-loss channel, $\mathcal{N}_{\lambda,0} = \mathcal{E}_\lambda$, which is degradable if and only if $\lambda \in [\frac{1}{2}, 1]$ [15, 16]. □

Necessary condition on anti-degradability via qubit restriction

The next theorem establishes the parameter range where the bosonic loss-dephasing channel is not anti-degradable. We provide three different proofs for this theorem.

Theorem 35. *Let $\gamma \geq 0$. If $\lambda > \frac{1}{1+e^{-\gamma}}$, then the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable.*

Proof 1. Assume that $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable; then substituting $m = 0$ and $n = 1$ in (S22) yields

$$\mathcal{A}_{\lambda,\gamma}\left(\mathcal{E}_{1-\lambda}(|0\rangle\langle 1|) \otimes |0\rangle\langle\sqrt{\gamma}|\right) = -e^{-\frac{1}{2}\gamma}\mathcal{E}_\lambda(|0\rangle\langle 1|). \tag{S54}$$

By exploiting $\mathcal{E}_\lambda(|0\rangle\langle 1|) = \sqrt{\lambda}\,|0\rangle\langle 1|$, we have

$$\mathcal{A}_{\lambda,\gamma}\left(|0\rangle\langle 1| \otimes |0\rangle\langle\sqrt{\gamma}|\right) = -\sqrt{\frac{e^{-\gamma}\lambda}{1-\lambda}}\,|0\rangle\langle 1| \,.$$

Using Lemma 48 in the Appendix, we find $\sqrt{\frac{e^{-\gamma}\lambda}{1-\lambda}} \leq 1$, or $\lambda \leq \frac{1}{1+e^{-\gamma}}$. □

Proof 2. Assume that $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable. As a consequence of (S22) and of the data-processing inequality for the fidelity [1], we find

$$F\left(\mathcal{E}_\lambda(|0\rangle\langle 0|), \mathcal{E}_\lambda(|1\rangle\langle 1|)\right) \geq F\left(\mathcal{E}_{1-\lambda}(|0\rangle\langle 0|) \otimes |0\rangle\langle 0|\,, \mathcal{E}_{1-\lambda}(|1\rangle\langle 1|) \otimes |\sqrt{\gamma}\rangle\langle\sqrt{\gamma}|\right). \tag{S55}$$

Furthermore, we obtain

$$\begin{aligned}\sqrt{1-\lambda} &= F\big(\,|0\rangle\!\langle 0|\,,\lambda\,|1\rangle\!\langle 1| + (1-\lambda)\,|0\rangle\!\langle 0|\,\big)\\ &\overset{\text{(i)}}{=} F\big(\mathcal{E}_\lambda(|0\rangle\!\langle 0|),\mathcal{E}_\lambda(|1\rangle\!\langle 1|)\big)\\ &\overset{\text{(ii)}}{\geq} F\big(\,|0\rangle\!\langle 0|\,,\big|\sqrt{\gamma}\big\rangle\!\big\langle\sqrt{\gamma}\big|\,\big)\, F\big(\mathcal{E}_{1-\lambda}(|0\rangle\!\langle 0|),\mathcal{E}_{1-\lambda}(|1\rangle\!\langle 1|)\big)\\ &\overset{\text{(iii)}}{\geq} F\big(\,|0\rangle\!\langle 0|\,,\big|\sqrt{\gamma}\big\rangle\!\big\langle\sqrt{\gamma}\big|\,\big)\,F\big(\,|0\rangle\!\langle 0|\,, \lambda\,|0\rangle\!\langle 0| + (1-\lambda)\,|1\rangle\!\langle 1|\,\big)\\ &\overset{\text{(iv)}}{=} \sqrt{e^{-\gamma}\lambda}\,.\end{aligned} \tag{S56}$$

Here, (i) follows from Lemma 10, (ii) follows from (S55) and from the fact that the fidelity is multiplicative under tensor product [1], (iii) uses Lemma 10 again, and in (iv) we exploited that $|\,\langle 0|\sqrt{\gamma}\rangle\,| = \sqrt{e^{-\gamma}}$. This yields $\sqrt{1-\lambda} \geq \sqrt{e^{-\gamma}\lambda}$, or $\lambda \leq \frac{1}{1+e^{-\gamma}}$. □

Proof 3. By exploiting Lemma 4 and the Choi matrix of the qubit channel $\mathcal{N}^{(2)}_{\lambda,\gamma}$ reported in (S53), one can easily obtain that $\mathcal{N}^{(2)}_{\lambda,\gamma}$ is anti-degradable if and only if $\lambda \leq \frac{1}{1+e^{-\gamma}}$. Consequently, thanks to Corollary 32, the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable for $\lambda > \frac{1}{1+e^{-\gamma}}$. □

Necessary condition on anti-degradability via qudit restrictions

Let us introduce the following quantity for any $d \in \mathbb{N}$ and $\gamma \geq 0$:

$$\lambda_d(\gamma) := \max\left(\lambda \in [0,1] :\ \mathcal{N}^{(d)}_{\lambda,\gamma} \text{ is anti-degradable}\right)\,. \tag{S57}$$

This quantity is relevant since it allows us to find parameter region where the bosonic loss-dephasing channel is not anti-degradable. Specifically, for $\lambda > \lambda_d(\gamma)$ the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is not anti degradable, as established by Corollary 32. Thanks to the Proof 3 of Theorem 35, it follows that for $d = 2$ we have that $\lambda_2(\gamma) = \frac{1}{1+e^{-\gamma}}$, thereby establishing that $\mathcal{N}_{\lambda,\gamma}$ is not anti degradable for $\lambda > \frac{1}{1+e^{-\gamma}}$. Through an examination of larger values of d, we aim to identify an extended parameter region where the channel is not anti-degradable (see Fig. 3). We begin by proving some useful properties of the quantity $\lambda_d(\gamma)$.

Lemma 36. *For any $\gamma \geq 0$ and $d \in \mathbb{N}, d \geq 2$, the following facts hold:*

- *Fact 1: The qudit restriction of the bosonic loss-dephasing channel $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is anti-degradable if and only if $\lambda \leq \lambda_d(\gamma)$*
- *Fact 2: The quantity $\lambda_d(\gamma)$ is monotonically increasing in γ*
- *Fact 3: For $d = 2$, it precisely holds that $\lambda_2(\gamma) = \frac{1}{1+e^{-\gamma}}$*
- *Fact 4: The quantity $\lambda_d(\gamma)$ is monotonically non-increasing in d*
- *Fact 5: It holds that $\frac{1}{2} \leq \lambda_d(\gamma) \leq \frac{1}{1+e^{-\gamma}}$*
- *Fact 6: When $d = 3$ and $e^{-\gamma} \leq \sqrt{2} - 1$ (or $\gamma \geq 0.881$), it exactly holds that $\lambda_3(\gamma) = \frac{1}{1+e^{-\gamma}}$*

Proof. Fact 1. It suffices to show that for any $\gamma \geq 0$ and $\lambda, \lambda' \in [0,1]$ with $\lambda' < \lambda$, if $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is anti-degradable, then so is $\mathcal{N}^{(d)}_{\lambda',\gamma}$. To show this, we exploit the composition rule

$$\mathcal{E}_{\lambda_1} \circ \mathcal{N}_{\lambda_2,\gamma} = \mathcal{N}_{\lambda_1\lambda_2,\gamma} \qquad \forall\, \lambda_1, \lambda_2 \in [0,1]\,, \tag{S58}$$

as established by Lemma 25, implying that the channel $\mathcal{N}^{(d)}_{\lambda',\gamma}$ can be written as the composition between $\mathcal{N}^{(d)}_{\lambda,\gamma}$ and another channel. Consequently, Lemma 51 concludes the proof.

Fact 2. Analogously to Fact 1, it suffices to show that for any $\lambda \in [0,1]$ and for any $\gamma' \geq \gamma \geq 0$, if $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is anti-degradable, then so is $\mathcal{N}^{(d)}_{\lambda,\gamma'}$. This follows from the composition rule

$$\mathcal{D}_{\gamma_1} \circ \mathcal{N}_{\lambda,\gamma_2} = \mathcal{N}_{\lambda,\gamma_1+\gamma_2} \qquad \forall\, \gamma_1, \gamma_2 \geq 0\,, \tag{S59}$$

as proved in Lemma 25. Furthermore, Lemma 51 concludes the proof.

Fact 3. This has already been proved in the Proof 3 of Theorem 35.

Fact 4. This follows from the observation that for all $d' \geq d$, if $\mathcal{N}^{(d')}_{\lambda,\gamma}$ is anti-degradable, then so is $\mathcal{N}^{(d)}_{\lambda,\gamma}$.

Fact 5. The upper bound $\lambda_d(\gamma) \leq \frac{1}{1+e^{-\gamma}}$ follows from Fact 3 and Fact 4. Moreover, since the pure-loss channel $\mathcal{E}_\lambda$ is anti-degradable if and only if $\lambda \leq \frac{1}{2}$, Fact 4 implies that $\lambda_d(0) \geq \frac{1}{2}$ (more specifically, one can also show that $\lambda_d(0) = \frac{1}{2}$). Consequently, Fact 2 concludes the proof.

Fact 6. This proof relies on the equivalence between anti-degradability of a channel and two-extendibility of its Choi state, as established in Lemma 50. Let λ and γ be such that $\lambda = \frac{1}{1+e^{-\gamma}}$ and $e^{-\gamma} \leq \sqrt{2}-1$, implying that $\lambda \geq \frac{1}{\sqrt{2}}$. By using Lemma 22, we obtain the Choi state of $\mathcal{N}^{(3)}_{\lambda,\gamma}$ as follows:

$$\mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\Phi_3\rangle\!\langle\Phi_3|) = \frac{1}{3}\sum_{m=0}^{2}\sum_{n=0}^{2}\sum_{\ell=0}^{\min(m,n)} e^{-\frac{\gamma}{2}(m-n)^2}\sqrt{\binom{m}{\ell}\binom{n}{\ell}}\,\lambda^{\frac{m+n}{2}-\ell}(1-\lambda)^l\, |m\rangle\!\langle n|_A \otimes |m-\ell\rangle\!\langle n-\ell|_B\,,$$

where Φ_3 is the maximally entangled state of Schmidt rank 3. We define a two-extension $\tilde{\rho}_{AB_1B_2}$ of the Choi state by the following conditions. First, $\tilde{\rho}_{AB_1B_2}$ satisfies the following $B_1 \leftrightarrow B_2$ symmetry for all $i_1, i_2, i_3, j_1, j_2, j_3 \in \{0,1,2\}$:

$$\begin{aligned} \langle j_1|_A \langle j_2|_{B_1} \langle j_3|_{B_2}\, \tilde{\rho}_{AB_1B_2}\, |i_1\rangle_A |i_2\rangle_{B_1} |i_3\rangle_{B_2} &= \langle j_1|_A \langle j_3|_{B_1} \langle j_2|_{B_2}\, \tilde{\rho}_{AB_1B_2}\, |i_1\rangle_A |i_2\rangle_{B_1} |i_3\rangle_{B_2} \\ \langle j_1|_A \langle j_2|_{B_1} \langle j_3|_{B_2}\, \tilde{\rho}_{AB_1B_2}\, |i_1\rangle_A |i_2\rangle_{B_1} |i_3\rangle_{B_2} &= \langle j_1|_A \langle j_2|_{B_1} \langle j_3|_{B_2}\, \tilde{\rho}_{AB_1B_2}\, |i_1\rangle_A |i_3\rangle_{B_1} |i_2\rangle_{B_2}\ . \end{aligned} \tag{S60}$$

Furthermore, if $i_1 < \max(i_2, i_3)$ or $j_1 < \max(j_2, j_3)$, or if $i_1 > i_2+i_3$ or $j_1 > j_2+j_3$, then $\langle j_1|_A \langle j_2|_{B_1} \langle j_3|_{B_2}\, \tilde{\rho}_{AB_1B_2}\, |i_1\rangle_A |i_2\rangle_{B_1} |i_3\rangle_{B_2} = 0$. We can thus define $\tilde{\rho}_{AB_1B_2}$ by writing only the matrix elements with respect the set $\{|i_1\rangle_A |i_2\rangle_{B_1} |i_3\rangle_{B_2}\}$ with $2 \geq i_1 \geq i_2 \geq i_3 \geq 0$ such that $i_2 + i_3 \geq i_1$. Hence, in order to fully define $\tilde{\rho}_{AB_1B_2}$, it suffices to write the matrix elements of $\tilde{\rho}_{AB_1B_2}$ with respect to the set $\{\ |0\rangle_A |0\rangle_{B_1} |0\rangle_{B_2}, |1\rangle_A |0\rangle_{B_1} |0\rangle_{B_2}, |1\rangle_A |1\rangle_{B_1} |1\rangle_{B_2}, |2\rangle_A |1\rangle_{B_1} |1\rangle_{B_2}\ , |2\rangle_A |2\rangle_{B_1} |0\rangle_{B_2}, |2\rangle_A |2\rangle_{B_1} |1\rangle_{B_2}\ , |2\rangle_A |2\rangle_{B_1} |2\rangle_{B_2}\ \}$. This gives rise to the following 7×7 matrix:

$$\begin{array}{c|ccccccc}
 & 0_A0_{B_1}0_{B_2} & 1_A1_{B_1}0_{B_2} & 1_A1_{B_1}1_{B_2} & 2_A1_{B_1}1_{B_2} & 2_A2_{B_1}0_{B_2} & 2_A2_{B_1}1_{B_2} & 2_A2_{B_1}2_{B_2} \\
\hline
0_A0_{B_1}0_{B_2} & 1 & \sqrt{1-\lambda} & 0 & \sqrt{2}(1-\lambda) & \frac{(1-\lambda)^2}{\lambda} & 0 & 0 \\
1_A1_{B_1}0_{B_2} & \sqrt{1-\lambda} & 1-\lambda & 0 & \sqrt{2(1-\lambda)^3} & \sqrt{\frac{(1-\lambda)^5}{\lambda^2}} & 0 & 0 \\
1_A1_{B_1}1_{B_2} & 0 & 0 & 2\lambda-1 & 0 & 0 & \frac{2\lambda-1}{\lambda}\sqrt{1-\lambda} & 0 \\
2_A1_{B_1}1_{B_2} & \sqrt{2}(1-\lambda) & \sqrt{2(1-\lambda)^3} & 0 & 2(1-\lambda)^2 & \sqrt{2}\frac{(1-\lambda)^3}{\lambda} & 0 & 0 \\
2_A2_{B_1}0_{B_2} & \frac{(1-\lambda)^2}{\lambda} & \sqrt{\frac{(1-\lambda)^5}{\lambda^2}} & 0 & \sqrt{2}\frac{(1-\lambda)^3}{\lambda} & (1-\lambda)^2 & 0 & 0 \\
2_A2_{B_1}1_{B_2} & 0 & 0 & \frac{2\lambda-1}{\lambda}\sqrt{1-\lambda} & 0 & 0 & 2(1-\lambda)(2\lambda-1) & 0 \\
2_A2_{B_1}2_{B_2} & 0 & 0 & 0 & 0 & 0 & 0 & (2\lambda-1)^2
\end{array}$$

One can show by direct calculation that this matrix is positive semi-definite if and only $\lambda \geq \frac{1}{\sqrt{2}}$. Note that the matrix is positive semi-definite if and only if $\tilde{\rho}_{AB_1B_2}$ is positive semi-definite. The latter follows from the following two simple facts: (i) A $n \times n$ symmetric matrix with a duplicate column is positive semi-definite if and only if the

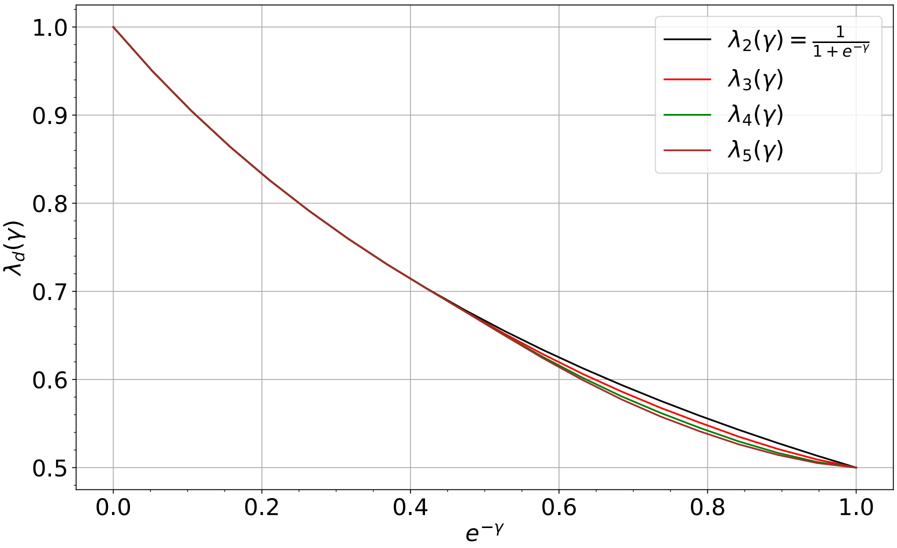


FIG. 3. Each curve indicates necessary and sufficient conditions where the qu*d*it restriction $\mathcal{N}^{(d)}_{\lambda,\gamma}$ of the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable. In the region above the curve $\lambda_5(\gamma)$, the bosonic loss-dephasing channel is never anti-degradable.

$(n-1)\times(n-1)$ matrix obtained by deleting one of the two equal column and the corresponding row is positive semi-definite, and (ii) A $n\times n$ symmetric matrix with a zero column is positive semi-definite if and only if the $(n-1)\times(n-1)$ matrix obtained by deleting such a column and the corresponding row is positive semi-definite. One can also verify $\mathrm{Tr}_{B_1}\,\tilde{\rho}_{AB_1B_2} = \mathrm{Tr}_{B_2}\,\tilde{\rho}_{AB_1B_2}$, and they are equal to the Choi state of the qutrit restriction with $\lambda = \frac{1}{1+e^{-\gamma}}$. We therefore conclude that the curve $\lambda = \frac{1}{1+e^{-\gamma}}$ provides a necessary and sufficient condition for the anti-degradability of the qutrit channel $\mathcal{N}^{(3)}_{\lambda,\gamma}$ when $\lambda \geq \frac{1}{\sqrt{2}}$, or equivalently when $e^{-\gamma} \leq \sqrt{2}-1$. □

To numerically compute the quantity $\lambda_d(\gamma)$ given in (S57), we utilise the equivalence between anti-degradability of a channel and two-extendibility of its Choi state [6]. Specifically, for small values of d, we can determine necessary and sufficient conditions for the anti-degradability of $\mathcal{N}^{(d)}_{\lambda,\gamma}$ by numerically solving the following *semi-definite program*:

$$\begin{aligned} &\min_{\rho_{AB_1B_2}} 1 \\ \text{s.t. } &\rho_{AB_1B_2} \geq 0\,, \\ &\mathrm{Tr}[\rho_{AB_1B_2}] = 1, \\ &\mathrm{Tr}_{B_2}[\rho_{AB_1B_2}] = \mathrm{id}_A \otimes \mathcal{N}^{(d)}_{\lambda,\gamma}(|\Phi_d\rangle\langle\Phi_d|_{AA'})\,, \\ &\mathrm{Tr}_{B_1}[\rho_{AB_1B_2}] = \mathrm{id}_A \otimes \mathcal{N}^{(d)}_{\lambda,\gamma}(|\Phi_d\rangle\langle\Phi_d|_{AA'})\,. \end{aligned} \tag{S61}$$

where $|\Phi_d\rangle$ is the maximally entangled state of schmidt rank d. The channel $\mathcal{N}^{(d)}_{\lambda,\gamma}$ is anti-degradable if and only if the semi-definite program admits a feasible solution. We compute the quantity $\lambda_d(\gamma)$ defined in (S57) by numerically solving the semi-definite program. The results are plotted with respect to $e^{-\gamma}$ for various values of d in Fig. 3, showcasing the dependence of $\lambda_d(\gamma)$ on γ for small values of d. Our numerical analysis reveals that when γ is sufficiently large, i.e. $e^{-\gamma} \lesssim 0.41$ or $\gamma \gtrsim 0.89$, the value of $\lambda_d(\gamma)$ consistently equals $\frac{1}{1+e^{-\gamma}}$ for all examined values of d. In particular, this seems to suggest that within this range of the dephasing parameter, $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable if and only if $\lambda \leq \frac{1}{1+e^{-\gamma}}$. Based on this numerical exploration, we propose the following conjecture:

Conjecture 37. *If γ is sufficiently large ($\gamma \gtrsim 0.89$), then the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is anti-degradable if and only if $\lambda \leq \frac{1}{1+e^{-\gamma}}$.*

Notably, from Fig. 3 we observe that if λ and γ satisfy $\lambda = \frac{1}{1+e^{-\gamma}}$ with $e^{-\gamma} \gtrsim 0.41$ (or $\gamma \lesssim 0.89$), then $\mathcal{N}_{\lambda,\gamma}$ is not anti-degradable.

III. COHERENCE PRESERVATION OF THE BOSONIC LOSS-DEPHASING CHANNEL

In this section we use the notation introduced in Section I H.

Theorem 38. *Let $\gamma \geq 0$ and $\lambda \in (0,1]$. For any energy constraint $N_s > 0$, the energy-constrained two-way quantum and secret-key capacities of the bosonic loss-dephasing channel are strictly positive, $K(\mathcal{N}_{\lambda,\gamma}, N_s) \geq Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) > 0$.*

Proof. We begin by assuming $N_s \in (0,1)$ and defining the two-mode state

$$|\Psi_{N_s}\rangle_{AA'} := \sqrt{1-N_s}\,|00\rangle_{AA'} + \sqrt{N_s}\,|11\rangle_{AA'}\ , \tag{S62}$$

where the mean photon number of A' system is equal to N_s. By exploiting Lemma 22, one can observe that the state

$$\rho_{AB} := \mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'}) \tag{S63}$$

is effectively a two-qubit state and its matrix with respect to the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is given by:

$$\rho_{AB} = \begin{pmatrix} 1-N_s & 0 & 0 & \sqrt{(1-N_s)N_s e^{-\gamma}\lambda} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & (1-\lambda)N_s & 0 \\ \sqrt{(1-N_s)N_s e^{-\gamma}\lambda} & 0 & 0 & \lambda N_s \end{pmatrix}.$$

If we perform partial transpose with respect to the system B, we find the matrix

$$(\rho_{AB})^{\intercal_B} = \begin{pmatrix} 1-N_s & 0 & 0 & 0 \\ 0 & 0 & \sqrt{(1-N_s)N_s e^{-\gamma}\lambda} & 0 \\ 0 & \sqrt{(1-N_s)N_s e^{-\gamma}\lambda} & (1-\lambda)N_s & 0 \\ 0 & 0 & 0 & \lambda N_s \end{pmatrix},$$

whose eigenvalues are not all positive, i.e. the state ρ_{AB} is not PPT [28]. By exploiting the fact that any two-qubit state is distillable if and only if it is not PPT [28], it follows that $E_d\left(\mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})\right) > 0$, where E_d is the distillable entanglement. On the other hand, from Lemma 26 we have that

$$K(\mathcal{N}_{\lambda,\gamma}, N_s) \geq Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) \geq E_d\big(\mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})\big)\ . \tag{S64}$$

This concludes the proof for $N_s \in (0,1)$. Since the energy-constrained capacities are monotonically non-decreasing in the energy constraint N_s, the proof follows for any $N_s > 0$. □

Since the state $\mathrm{id}_A \otimes \mathcal{N}_{\lambda,\gamma}(|\Psi_{N_s}\rangle\!\langle\Psi_{N_s}|_{AA'})$ in (S63) is always entangled, it follows that the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is never entanglement breaking [2]. We state this formally in the following theorem.

Theorem 39. *For all $\gamma \geq 0$ and all $\lambda \in (0,1]$, the bosonic loss-dephasing channel $\mathcal{N}_{\lambda,\gamma}$ is not entanglement breaking.*

In the following subsection we will find an explicit strictly positive lower bound on the two-way capacities of the bosonic loss-dephasing channel.

A. Multi-rail multi-photon encoding

Let $\Pi(N,k)$ be the set of partitions of N objects into k (possibly empty) parts. It is well known that $|\Pi(N,k)| = \binom{N+k-1}{k-1} = \binom{N+k-1}{N}$. Clearly, we can think of each $p \in \Pi(N,k)$ as a vector in $\mathbb{N}_+^k$, also denoted by p, with the constraint that $\sum_{\ell=1}^{k} p_\ell = N$. For each $p \in \Pi(N,k)$, define the associate k-mode Fock state as

$$\left|\psi_p\right\rangle := |p_1\rangle \dots |p_k\rangle\ . \tag{S65}$$

Note that for $p, q \in \Pi(N,k)$, we have that $\langle \psi_p | \psi_q \rangle = \delta_{p,q}$. Let us call

$$P_{N,k} := \sum_{p\in\Pi(N,k)} \psi_p \tag{S66}$$

the projector onto the k-mode subspace of total photon number N. Note that the bosonic dephasing channel satisfies that

$$\mathcal{D}_\gamma^{\otimes k}\left(|\psi_p\rangle\!\langle\psi_q|\right) = e^{-\frac{\gamma}{2}\sum_\ell (p_\ell - q_\ell)^2} |\psi_p\rangle\!\langle\psi_q| = e^{-\frac{\gamma}{2}\|p-q\|^2} |\psi_p\rangle\!\langle\psi_q| = (K_{N,k,\gamma})_{pq} |\psi_p\rangle\!\langle\psi_q| \,, \tag{S67}$$

where $K_{N,k,\gamma}$ is the $\binom{N+k-1}{N} \times \binom{N+k-1}{N}$ matrix with entries

$$(K_{N,k,\gamma})_{pq} := e^{-\frac{\gamma}{2}\|p-q\|^2}. \tag{S68}$$

For any $\binom{N+k-1}{N}$-dimensional state σ, let us denote as $\overline{\sigma}$ the following isometrically equivalent state

$$\overline{\sigma} := \sum_{p,q\in\Pi(N,k)} \sigma_{pq} |\psi_p\rangle\!\langle\psi_q| \,. \tag{S69}$$

The state $\overline{\sigma}$, which is termed as the *rail encoding* of σ, is supported on the subspace of k modes with total photon number equal to N. Now, let ρ be a $\binom{N+k-1}{N}$-dimensional state and let us calculate the output of $\mathcal{D}_\gamma^{\otimes k}$ when the input is $\overline{\rho}$:

$$\mathcal{D}_\gamma^{\otimes k}(\overline{\rho}) = \sum_{p,q\in\Pi(N,k)} \rho_{pq}(K_{N,k,\gamma})_{pq} |\psi_p\rangle\!\langle\psi_q| = \overline{K_{N,k,\gamma} \circ \rho} = \overline{\Theta_{N,k,\gamma}(\rho)} \,, \tag{S70}$$

where the operation $\circ$ denotes the element-wise product between matrices and where we have introduced the following Hadamard channel:

$$\Theta_{N,k,\gamma}(X) := K_{N,k,\gamma} \circ X \,, \tag{S71}$$

Since $\mathcal{D}_\gamma^{\otimes k}$ is a (completely) positive map, this in particular shows that $K_{N,k,\gamma} \geq 0$. (This latter statement can also be proved directly with techniques similar to that in the proof of [29, Lemma 15].) In practice, the k-fold application of the bosonic dephasing channel on the k-mode N-photon code space behaves as a new Hadamard channel $\Theta_{N,k,\gamma}$ with associated matrix $K_{N,k,\gamma}$.

Lower bound on the two-way capacity of the bosonic loss-dephasing channel

Since under the action of $\mathcal{N}_{\lambda,\gamma}$ photons can only be lost and never added, and each photon has a probability λ of being transmitted, the probability that an N-photon state will retain N photons at the output of the channel is exactly λ^N. *If that happens*, then the state in the code space is effectively left untouched by the loss and only dephased under the action of the Hadamard channel $\Theta_{N,k,\gamma}$.

More formally, from the Kraus representation

$$\mathcal{E}_\lambda(X) = \sum_{n=0}^{\infty} \frac{1}{n!}(1-\lambda)^n \lambda^{\frac{a^\dagger a}{2}} a^n X (a^\dagger)^n \lambda^{\frac{a^\dagger a}{2}} \tag{S72}$$

it is easy to deduce the handy identity

$$\mathcal{E}_\lambda^{\otimes k}(\overline{\rho}) = \lambda^N \overline{\rho} + \left(1 - \lambda^N\right) \delta_{N,k,\lambda} \,, \tag{S73}$$

valid for all $\binom{N+k-1}{N}$-dimensional states ρ, with the notation of (S69). Here, $\delta_{N,k,\lambda}$ is a suitable k-mode state supported on the subspace of total photon number at most $N-1$, and thus $\overline{\rho}\delta_{N,k,\lambda} = \delta_{N,k,\lambda}\overline{\rho} = 0$. In turn, the above identity implies that

$$\mathcal{N}_{\lambda,\gamma}^{\otimes k}(\overline{\rho}) = \lambda^N\, \overline{K_{N,k,\gamma} \circ \rho} + \left(1 - \lambda^N\right) \delta'_{N,k,\lambda,\gamma} = \lambda^N\, \overline{\Theta_{N,k,\gamma}(\rho)} + \left(1 - \lambda^N\right) \delta'_{N,k,\lambda,\gamma} \,, \tag{S74}$$

where once again $\delta'_{N,k,\lambda,\gamma}$ is a suitable k-mode state supported on the subspace of total photon number at most $N-1$.

Therefore, we can use the channel $\mathcal{N}_{\lambda,\gamma}^{\otimes k}$ to simulate $\Theta_{N,k,\gamma}$ *probabilistically*, with probability λ^N. The simulation works as follows:

(i) The input state ρ is encoded in the k-mode N-photon subspace according to the mapping $\rho \mapsto \overline{\rho}$.

(ii) The k-mode state $\overline{\rho}$ is sent across $\mathcal{N}_{\lambda,\gamma}^{\otimes k}$, via k uses of the bosonic loss-dephasing channel.

(iii) The total photon number is measured at the output. If N photons are found then the simulation is successful, otherwise the protocol is aborted.

A wealth of operational resource inequalities can be deduced from the above considerations. Here we limit ourselves to the observation that the two-way quantum capacity must satisfy

$$Q_2(\mathcal{N}_{\lambda,\gamma}) \overset{\text{(i)}}{\geq} \frac{\lambda^N}{k}\, Q_2(\Theta_{N,k,\gamma})\,. \tag{S75}$$

Consequently, it holds that

$$\begin{aligned} Q_2(\mathcal{N}_{\lambda,\gamma}) &\geq \frac{\lambda^N}{k}\, Q_2(\Theta_{N,k,\gamma}) \\ &\overset{\text{(i)}}{\geq} \frac{\lambda^N}{k}\, I_{\text{coh}}\left(\text{id}\otimes\Theta_{N,k,\gamma}(|\Psi\rangle\!\langle\Psi|)\right) \\ &\overset{\text{(iii)}}{=} \frac{\lambda^N}{k}\left[\log_2\binom{N+k-1}{N} - S\left(\binom{N+k-1}{N}^{-1} K_{N,k,\gamma}\right)\right]. \end{aligned} \tag{S76}$$

Here, in (ii), we used the fact that the two-way quantum capacity of a channel can be lower bounded in terms of the coherent information [2, 4] and we introduced the two-qu$d$it maximally entangled state $|\Psi\rangle$ of dimension $d = \binom{N+k-1}{N}$. In (iii), we used the definition of coherent information $I_{\text{coh}}(\rho_{AB}) := S(\rho_B) - S(\rho_{AB})$, with $S(\cdot)$ being the von Neumann entropy, and the fact that

$$\begin{aligned} \text{id}\otimes\Theta_{N,k,\gamma}(|\Psi\rangle\!\langle\Psi|) &= \frac{1}{\binom{N+k-1}{N}} \sum_{p,q\in\Pi(N,k)} |p\rangle\!\langle q| \otimes \Theta_{N,k,\gamma}(|p\rangle\!\langle q|) \\ &= \frac{1}{\binom{N+k-1}{N}} \sum_{p,q\in\Pi(N,k)} (K_{N,k,\gamma})_{pq}\, |p\rangle\!\langle q| \otimes |p\rangle\!\langle q|\ , \end{aligned} \tag{S77}$$

which implies that the spectrum of $\text{id}\otimes\Theta_{N,k,\gamma}(|\Psi\rangle\!\langle\Psi|)$ coincides with the spectrum of the matrix $\binom{N+k-1}{N}^{-1} K_{N,k,\gamma}$. Consequently, we have that

$$Q_2(\mathcal{N}_{\lambda,\gamma}) \geq \max_{N,k\in\mathbb{N}_+} \frac{\lambda^N}{k}\left[\log_2\binom{N+k-1}{N} - S\left(\binom{N+k-1}{N}^{-1} K_{N,k,\gamma}\right)\right]. \tag{S78}$$

One can obtain a lower bound on the energy-constrained two-way quantum capacity $Q_2(\mathcal{N}_{\lambda,\gamma}, N_s)$ by restricting the optimisation to the values of N and k such that $\frac{N}{k} \leq N_s$. Indeed, note that the rail-encoded state $\bar{\rho}$ satisfies the energy constraint as its mean photon number per mode is $\frac{N}{k}$. In formula, we have that

$$Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) \geq \max_{N,k\in\mathbb{N}_+:\ \frac{N}{k}\leq N_s} \frac{\lambda^N}{k}\left[\log_2\binom{N+k-1}{N} - S\left(\binom{N+k-1}{N}^{-1} K_{N,k,\gamma}\right)\right]. \tag{S79}$$

Note that $\log_2\binom{N+k-1}{N} - S\left(\binom{N+k-1}{N}^{-1} K_{N,k,\gamma}\right)$ is always positive because $\binom{N+k-1}{N}^{-1} K_{N,k,\gamma}$ is a $\binom{N+k-1}{N}$-dimensional, non-maximally mixed, state and thus its von Neumann entropy is strictly smaller than by $\log_2\binom{N+k-1}{N}$. Consequently, we have the following theorem.

Theorem 40. *Let $\gamma \geq 0$ and $\lambda \in (0,1]$. For any energy constraint $N_s > 0$, the energy-constrained two-way quantum and secret-key capacities of the bosonic loss-dephasing channel are lower bounded by*

$$K(\mathcal{N}_{\lambda,\gamma}, N_s) \geq Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) \geq \max_{\substack{N,k\in\mathbb{N}_+ \\ \frac{N}{k}\leq N_s}} \frac{\lambda^N}{k}\left[\log_2\binom{N+k-1}{N} - S\left(\rho_{N,k,\gamma}\right)\right] > 0\,. \tag{S80}$$

Here, $S(\cdot)$ is the von Neumann entropy, $\rho_{N,k,\gamma}$ is a $\binom{N+k-1}{N}$-dimensional state defined by

$$\rho_{N,k,\gamma} := \binom{N+k-1}{N}^{-1} \sum_{p,q\in\Pi(N,k)} e^{-\frac{\gamma}{2}\|p-q\|_2^2} |p\rangle\!\langle q| \, , \tag{S81}$$

where $\Pi(N,k) := \left\{p \in \mathbb{N}^k : \sum_{i=1}^k p_i = N\right\}$ represents the set of partitions of a set of N elements into k parts, and the vectors $\{|p\rangle\}_{p\in\Pi(N,k)}$ are orthonormal. In particular,

$$K(\mathcal{N}_{\lambda,\gamma}, N_s) \geq Q_2(\mathcal{N}_{\lambda,\gamma}, N_s) > \max_{N,k\in\mathbb{N}_+} \frac{\lambda^N}{k}\left[\log_2\binom{N+k-1}{N} - S\left(\rho_{N,k,\gamma}\right)\right] > 0\, . \tag{S82}$$

IV. APPENDIX

A. Hadamard maps

Given an infinite matrix $A = (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$, we can introduce a superoperator H, recognised as the *Hadamard map*, whose action is defined as $H(|m\rangle\!\langle n|) = a_{n,m}\, |m\rangle\!\langle n|$ for all $n, m \in \mathbb{N}$. We are interested in establishing requirements for an infinite matrix A to ensure that the associated Hadamard map H is a quantum channel. We begin with some preliminaries. Let $\ell^2(\mathbb{N})$ be the space of square-summable complex-valued sequences defined as

$$\ell^2(\mathbb{N}) := \left\{ x := \{x_n\}_{n\in\mathbb{N}}, x_n \in \mathbb{C} : \|x\| := \sqrt{\sum_{n=0}^{\infty} |x_n|^2} < \infty \right\}\, . \tag{S83}$$

An infinite matrix $A := (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$ defines a linear operator on $\ell^2(\mathbb{N})$. The operator norm of A is defined as follows:

$$\|A\|_\infty := \sup_{\substack{x\in\ell^2(\mathbb{N})\\ \|x\|=1}} \|Ax\| = \sup_{\substack{\{x_n\}_{n\in\mathbb{N}}, x_n\in\mathbb{C}\\ \sum_{n=0}^\infty |x_n|^2=1}} \sqrt{\sum_{m=0}^{\infty}\left|\sum_{n=0}^{\infty} a_{mn}x_n\right|^2}\, .$$

A is said to be bounded if $\|A\|_\infty < \infty$. The following lemma, referred to as *Schur test*, gives a sufficent condition for an infinite matrix to be bounded (e.g. [30, Page 24, Problem 45]).

Lemma 41. *Let $A := (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$, be an infinite matrix. Suppose that there exist $\{p_n\}_{n\in\mathbb{N}}, p_n \in \mathbb{R}_{>0}$ and $\{q_m\}_{m\in\mathbb{N}}, q_m \in \mathbb{R}_{>0}$, and $\beta > 0$, and $\gamma > 0$ such that*

$$\sum_{m=0}^{\infty} |a_{mn}|p_m \leq \beta q_n \quad \text{and} \quad \sum_{n=0}^{\infty} |a_{mn}|q_n \leq \gamma p_m\, , \quad \forall\, m, n \in \mathbb{N}\, .$$

Then the matrix A satisfies $\|A\|_\infty \leq \beta\gamma$. In particular, A is bounded.

By choosing $p_n = q_n = 1$ and $\gamma = \beta = \sup_{n\in\mathbb{N}} \sum_{m=0}^\infty |a_{mn}|$, we obtain the following corollary:

Corollary 42. *Let $A = (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$, be an infinite Hermitian matrix. If $\sup_{n\in\mathbb{N}} \sum_{m=0}^\infty |a_{mn}|$ is finite, then A is bounded.*

Lemma 43. *Let $A = (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$, be a bounded Hermitian infinite matrix. Then A is positive semi-definite as an operator on $\ell^2(\mathbb{N})$ if and only if $A^{(d)} := (a_{mn})_{m,n=0,1,\ldots,d-1}$ is positive semi-definite for all $d \in \mathbb{N}$, where $A^{(d)}$ is the $d \times d$ top left corner of A.*

Proof. Assume that $A^{(d)}$ is positive semi-definite for all $d \in \mathbb{N}$. Let us pick an arbitrary $x \in \ell^2(\mathbb{N})$. It is known that for any $\varepsilon > 0$, there exists $d \in \mathbb{N}$ and $y^{(d)} := (y_n^{(d)})_{n\in\mathbb{N}}, y_n^{(d)} \in \mathbb{C}$, with $y_n^{(d)} = 0$ for all $n > d$, such that $\|x - y^{(d)}\| < \varepsilon$. Note that

$$\begin{aligned} x^\dagger A x &= \left(x - y^{(d)}\right)^\dagger A\, x + \left(y^{(d)}\right)^\dagger A\,(x - y^{(d)}) + \left(y^{(d)}\right)^\dagger A y^{(d)} \\ &\overset{\text{(i)}}{\geq} -\|x - y^{(d)}\|\, \|A\|_\infty \left(\|x\| + \|y^{(d)}\|\right) + \left(y^{(d)}\right)^\dagger A^{(d)}\, y^{(d)} \\ &\overset{\text{(ii)}}{\geq} -\varepsilon\, \|A\|_\infty\, (2\|x\| + \varepsilon)\ , \end{aligned}$$

where in (i) we applied Cauchy-Schwarz inequality twice and the definition of infinity norm as follows

$$|(x-y^{(d)})^{\dagger}A\,x| \leq \|x-y^{(d)}\|\|A\,x\| \leq \|x-y^{(d)}\|\|A\|_{\infty}\|x\|\,,$$
$$|(y^{(d)})^{\dagger}A\,(x-y^{(d)})| \leq \|y^{(d)}\|\|A\,(x-y^{(d)})\| \leq \|y^{(d)}\|\|A\|_{\infty}\|x-y^{(d)}\|\,,$$

and, in (ii), we exploited triangular inequality to derive

$$\|y^{(d)}\| \leq \|y^{(d)}-x\| + \|x\| \leq \varepsilon + \|x\|\,, \tag{S84}$$

together with the fact that $A^{(d)}$ is positive semi-definite. Hence, since $\varepsilon > 0$ is arbitrary, we conclude that $x^{\dagger}Ax \geq 0$, meaning that A is positive semi-definite as an operator on $\ell^2(\mathbb{N})$. □

A square matrix is said to be diagonally dominant if

$$\sum_{m\neq n} |a_{mn}| \leq |a_{nn}|, \quad \forall n.$$

In words, a square matrix is said to be diagonally dominant if for every row of the matrix, the absolute value of the diagonal entry in a row is larger than or equal to the sum of the absolute values of all the other (non-diagonal) entries in that row. Note that for Hermitian matrices one can exchange row with column in this definition. We proceed to state a sufficient condition for a matrix A to be positive semi-definite as an operator on $\ell^2(\mathbb{N})$. While the following sufficient condition is usually stated for finite matrices, it can be generalised to infinite matrices as per Lemma 43.

Lemma 44. *[31, Chapter 6] For any $d \in \mathbb{N}$, let $A = (a_{mn})_{m,n=0,1,\ldots,d-1}, a_{mn} \in \mathbb{C}$, be a $d \times d$ Hermitian matrix with $a_{nn} \in \mathbb{R}_{\geq 0}$ for all $n \in \{0,\ldots,d-1\}$. A is positive semi-definite if it is diagonally dominant.*

Lemma 45. *Let $A = (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$ be an infinite Hermitian matrix with $a_{nn} \in \mathbb{R}_{\geq 0}, \forall n \in \mathbb{N}$. Assume that $\sup_{n\in\mathbb{N}} a_{nn}$ is finite and that A is diagonally dominant. Then A is bounded and positive semi-definite when seen as an operator on $\ell^2(\mathbb{N})$.*

Proof. Since

$$\sup_{n\in\mathbb{N}} \sum_{m=0}^{\infty} |a_{mn}| \leq 2 \sup_{n\in\mathbb{N}} a_{n,n} < \infty\,,$$

Corollary 42 implies that A is bounded. The fact that A is positive semi-definite as an operator on $\ell^2(\mathbb{N})$ follows from Lemma 44 together with Lemma 43. □

We now present a lemma from the literature that establishes necessary and sufficient conditions for an infinite matrix A to ensure that the associated Hadamard map H is a quantum channel. We then use it to derive an explicit sufficient condition for an infinite matrix A to give rise to a cptp Hadamard map.

Lemma 46. *[18, Lemma S4] Let $A := (a_{mn})_{m,n\in\mathbb{N}}, a_{mn} \in \mathbb{C}$ be a bounded infinite matrix. The following requirements establish the necessary and sufficient conditions for the associated Hadamard map H to qualify as a quantum channel:*

(i) $a_{nn} = 1$, $\forall n \in \mathbb{N}$;

(ii) A is positive semi-definite as on operator on $\ell^2(\mathbb{N})$.

As a consequence of Lemma 46 and Lemma 45, we obtain:

Lemma 47. *Let $A := (a_{mn})_{m,n\in\mathbb{N}}$ be an infinite Hermitian matrix that is diagonally dominant with $a_{n,n} = 1$ for all $n \in \mathbb{N}$. In this case, its associated Hadamard map H is a quantum channel.*

B. Miscellaneous Lemmas

Lemma 48. *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces and let $\mathcal{N} : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ be a quantum channel. For all normalised states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_A$ and $|\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}_B$ it holds that*

$$\left|\langle\phi_1|\mathcal{N}(|\psi_1\rangle\!\langle\psi_2|)\,|\phi_2\rangle\right| \leq 1\,. \tag{S85}$$

Proof. It holds that

$$\begin{aligned} \left|\langle\phi_1\right|\mathcal{N}(|\psi_1\rangle\!\langle\psi_2|)\left|\phi_2\rangle\right| &\overset{\text{(i)}}{\le} \|\mathcal{N}(|\psi_1\rangle\!\langle\psi_2|)\|_\infty \\ &\overset{\text{(ii)}}{\le} \|\mathcal{N}(|\psi_1\rangle\!\langle\psi_2|)\|_1 \\ &\overset{\text{(iii)}}{\le} \|\,|\psi_1\rangle\!\langle\psi_2|\,\|_1 \\ &= 1\,. \end{aligned} \tag{S86}$$

Here, in (i), we exploited one of the definition of the operator norm in (S2). In (ii), we exploited that the trace norm is always an upper bound on the operator norm. Finally, in (iii), we leveraged the monotonicity of the trace norm under quantum channels [1]. □

Lemma 49 [10, 11]. *Let $\mathcal{H}_A, \mathcal{H}_{A'}$ be isomorphic Hilbert spaces, possibly infinite dimensional. Let $|\psi\rangle_{A'A}$ be a pure state that satisfies $\mathrm{Tr}_{A'}\left[|\psi\rangle\!\langle\psi|_{AA'}\right] > 0$. The generalised Choi–Jamiołkowski matrix defines an isomorphism between the set of quantum channels from $\mathcal{H}_{A'}$ to $\mathcal{H}_B$ and the set of bipartite states $\sigma_{AB} \in \mathcal{P}(\mathcal{H}_{AB})$ such that $\mathrm{Tr}_B\,\sigma_{AB} = \mathrm{Tr}_{A'}\left[|\psi\rangle\!\langle\psi|_{AA'}\right]$. Specifically, for any quantum channel $\mathcal{N}_{A'\to B} : \mathcal{T}(\mathcal{H}_{A'}) \to \mathcal{T}(\mathcal{H}_B)$, it holds that*

$$\mathcal{N}_{A'\to B}(|e_i\rangle\!\langle e_j|) = \frac{1}{\sqrt{\lambda_i\lambda_j}}\,\mathrm{Tr}_A\left[\left(|e_j\rangle\!\langle e_i|_A \otimes \mathbb{1}_B\right)\sigma_{AB}\right], \quad \forall\, i,j \in \mathbb{N}, \tag{S87}$$

where $(|e_i\rangle)_{i\in\mathbb{N}}$ and $(\lambda_i)_{i\in\mathbb{N}}$ form a spectral decomposition of $\mathrm{Tr}_{A'}\left[|\psi\rangle\!\langle\psi|_{AA'}\right]$, i.e. $\mathrm{Tr}_{A'}\left[|\psi\rangle\!\langle\psi|_{AA'}\right] = \sum_i \lambda_i\,|e_i\rangle\!\langle e_i|_A$, and where the state $\sigma_{AB} := \mathrm{id}_A \otimes \mathcal{N}_{A'\to B}(|\psi\rangle\!\langle\psi|_{AA'})$ is called the generalised Choi state of $\mathcal{N}$. Eq. S87 is enough to specify the channel $\mathcal{N}_{A'\to B}$ completely, as the linear span of the operators $\left(|e_i\rangle\!\langle e_j|\right)_{i,j\in\mathbb{N}}$ (i.e. the set of finite-rank operators) is dense in $\mathcal{T}(\mathcal{H}_{A'})$.

Lemma 50 [6]. *Let $\mathcal{H}_A, \mathcal{H}_{A'}, \mathcal{H}_B$ be isomorphic Hilbert spaces, possibly infinite dimensional. Let $\mathcal{N}_{A'\to B} : \mathcal{T}(\mathcal{H}_{A'}) \to \mathcal{T}(\mathcal{H}_B)$ be a quantum channel. Let $|\psi\rangle_{A'A} \in \mathcal{H}_A \otimes \mathcal{H}_{A'}$ be a pure state such that the reduced state $\mathrm{Tr}_{A'}[|\psi\rangle\!\langle\psi|_{AA'}]$ is positive definite. Then, $\mathcal{N}_{A'\to B}$ is anti-degradable if and only if the state $\mathrm{id}_A \otimes \mathcal{N}_{A'\to B}(|\psi\rangle\!\langle\psi|_{AA'})$ is two-extendible on B, meaning that there exists a state $\rho_{AB_1B_2} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2})$ such that*

$$\begin{aligned} \mathrm{Tr}_{B_2}\left[\rho_{AB_1B_2}\right] &= \mathrm{id}_A \otimes \mathcal{N}_{A'\to B_1}(|\psi\rangle\!\langle\psi|_{AA'})\,, \\ \mathrm{Tr}_{B_1}\left[\rho_{AB_1B_2}\right] &= \mathrm{id}_A \otimes \mathcal{N}_{A'\to B_2}(|\psi\rangle\!\langle\psi|_{AA'}), \end{aligned} \tag{S88}$$

where $\mathcal{H}_{B_1}$ and $\mathcal{H}_{B_2}$ are Hilbert spaces that are isomorphic to $\mathcal{H}_B$.

Proof. Let $U_{A'E\to BE}$ be a Stinespring dilation of the channel $\mathcal{N}_{A'\to B}$. Further assume that $\mathcal{N}_{A'\to B}$ is anti-degradable. By definition, there exists a quantum channel $\mathcal{A}_{E\to B}$ such that $\mathcal{A}_{E\to B} \circ \mathcal{N}^{\mathrm{c}}_{A'\to B} = \mathcal{N}_{A'\to B}$. Let us consider the tripartite state $\rho_{AB_1B_2}$, with B_1, B_2 being copies of B, defined as

$$\rho_{AB_1B_2} = \mathrm{id}_A \otimes \mathrm{id}_{B_1} \otimes \mathcal{A}_{E\to B_2}\left(U_{A'E\to B_1E}\left(\,|\psi\rangle\!\langle\psi|_{AA'} \otimes |0\rangle\!\langle 0|_E\,\right)U^\dagger_{A'E\to B_1E}\right)\,. \tag{S89}$$

It holds that

$$\begin{aligned} \mathrm{Tr}_{B_2}\left[\rho_{AB_1B_2}\right] &= \mathrm{Tr}_{B_2}\left[\mathrm{id}_A \otimes \mathrm{id}_{B_1} \otimes \mathcal{A}_{E\to B_2}\left(U_{A'E\to B_1E}\left(\,|\psi\rangle\!\langle\psi|_{AA'} \otimes |0\rangle\!\langle 0|_E\,\right)U^\dagger_{A'E\to B_1E}\right)\right] \\ &= \mathrm{id}_A \otimes \mathrm{Tr}_E\left[U_{A'E\to B_1E}\left(\,|\psi\rangle\!\langle\psi|_{AA'} \otimes |0\rangle\!\langle 0|_E\,\right)U^\dagger_{A'E\to B_1E}\right] \\ &= \mathrm{id}_A \otimes \mathcal{N}_{A'\to B_1}\left(|\psi\rangle\!\langle\psi|_{AA'}\right)\,, \end{aligned}$$

and

$$\begin{aligned} \mathrm{Tr}_{B_1}\left[\rho_{AB_1B_2}\right] &= \mathrm{Tr}_{B_1}\left[\mathrm{id}_A \otimes \mathrm{id}_{B_1} \otimes \mathcal{A}_{E\to B_2}\left(U_{A'E\to B_1E}\left(\,|\psi\rangle\!\langle\psi|_{AA'} \otimes |0\rangle\!\langle 0|_E\,\right)U^\dagger_{A'E\to B_1E}\right)\right] \\ &= \mathrm{id}_A \otimes \mathcal{A}_{E\to B_2}\left(\mathrm{Tr}_{B_1}\left[U_{A'E\to B_1E}\left(\,|\psi\rangle\!\langle\psi|_{AA'} \otimes |0\rangle\!\langle 0|_E\,\right)U^\dagger_{A'E\to B_1E}\right]\right) \\ &= \mathrm{id}_A \otimes \mathcal{A}_{E\to B_2} \circ \mathcal{N}^{\mathrm{c}}_{A'\to B_2}\left(|\psi\rangle\!\langle\psi|_{AA'}\right) \\ &= \mathrm{id}_A \otimes \mathcal{N}_{A'\to B_2}\left(|\psi\rangle\!\langle\psi|_{AA'}\right)\,. \end{aligned}$$

Now, let us establish the converse. Assume that there exists $\rho_{AB_1B_2}$ which satisfies (S88). Let $|\Psi\rangle_{AB_1B_2P} \in \mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2} \otimes \mathcal{H}_P$ be a purification of $\rho_{AB_1B_2}$, with $\mathcal{H}_P$ being the purifying Hilbert space. Note that both $|\Psi\rangle_{AB_1B_2P}$ and $U_{A'E\to B_1E}\left(|\psi\rangle_{AA'} \otimes |0\rangle_E\right)$ are purifications of $\mathrm{id}_A \otimes \mathcal{N}_{A'\to B_1}\left(|\psi\rangle\langle\psi|_{AA'}\right)$, with $\mathcal{H}_{B_2} \otimes \mathcal{H}_P$ and $\mathcal{H}_E$ being their purifying Hilbert spaces, respectively. It follows that [1] there exists an isometry $V_{E\to B_2P} : \mathcal{H}_E \to \mathcal{H}_{B_2} \otimes \mathcal{H}_P$ such that $V_{E\to B_2P}\, U_{A'E\to B_1E}\left(|\psi\rangle_{AA'} \otimes |0\rangle_E\right) = |\Psi\rangle_{AB_1B_2P}$. Hence, the quantum channel $\mathcal{A}_{E\to B_2} : \mathcal{T}(\mathcal{H}_E) \to \mathcal{T}(\mathcal{H}_{B_2})$, defined by $\mathcal{A}_{E\to B_2}(\cdot) = \mathrm{Tr}_P\left[V_{E\to B_2P}(\cdot)V^\dagger_{E\to B_2P}\right]$, satisfies that

$$\begin{aligned}\mathrm{id}_A \otimes \mathcal{A}_{E\to B_2} \circ \mathcal{N}^{\mathrm{c}}_{A'\to B_2}(|\psi\rangle\langle\psi|_{AA'}) &= \mathrm{id}_A \otimes \mathcal{A}_{E\to B_2}\left(\mathrm{Tr}_{B_1}\left[U_{A'E\to B_1E}(|\psi\rangle\langle\psi|_{AA'} \otimes |0\rangle\langle 0|_E)U^\dagger_{A'E\to B_1E}\right]\right)\\ &= \mathrm{Tr}_{B_1P}\left[|\Psi\rangle\langle\Psi|_{AB_1B_2P}\right]\\ &= \mathrm{Tr}_{B_1}\left[\rho_{AB_1B_2}\right]\\ &= \mathrm{id}_A \otimes \mathcal{N}_{A'\to B_2}\left(|\psi\rangle\langle\psi|_{AA'}\right)\,.\end{aligned}$$

Consequently, since the pure state $|\psi\rangle_{A'A}$ satisfies $\mathrm{Tr}_{A'}\left[|\psi\rangle\langle\psi|_{AA'}\right] > 0$, Lemma 49 implies that $\mathcal{A}_{E\to B_2} \circ \mathcal{N}^{\mathrm{c}}_{A'\to B_2} = \mathcal{N}_{A'\to B_2}$, meaning that $\mathcal{N}_{A'\to B_2}$ is anti-degradable. □

Lemma 51. *Let $\mathcal{N}, \mathcal{M} : \mathcal{T}(\mathcal{H}_S) \to \mathcal{T}(\mathcal{H}_S)$ be quantum channels. If either $\mathcal{M}$ or $\mathcal{N}$ is anti-degradable, then the composition $\mathcal{M} \circ \mathcal{N}$ is anti-degradable. Specifically, let E_1 and E_2 be the Stinespring environments of $\mathcal{N}$ and $\mathcal{M}$, respectively. If $\mathcal{N}$ is anti-degradable with anti-degrading map $\mathcal{A}_{E_1\to S}$, then $(\mathcal{M} \circ \mathcal{A}_{E_1\to S}) \otimes \mathrm{Tr}_{E_2}$ is an anti-degrading map of $\mathcal{M} \circ \mathcal{N}$. Analogously, if $\mathcal{M}$ is anti-degradable with anti-degrading map $\mathcal{A}_{E_2\to S}$, then $\mathrm{Tr}_{E_1} \otimes \mathcal{A}_{E_2\to S}$ is an anti-degrading map of $\mathcal{M} \circ \mathcal{N}$.*

Proof. Let $V^{S\to SE_1}$ and $W^{S\to SE_2}$ be Stinespring isometries associated with $\mathcal{N}$ and $\mathcal{M}$, respectively. By considering the following complementary channel of $\mathcal{M} \circ \mathcal{N}$,

$$(\mathcal{M} \circ \mathcal{N})^{\mathrm{c}}(\rho) = \mathrm{Tr}_S\left[W^{S\to SE_2}V^{S\to SE_1}\,\rho\,\left(V^{S\to SE_1}\right)^\dagger\left(W^{S\to SE_2}\right)^\dagger\right], \qquad \forall\,\rho \in \mathcal{T}(\mathcal{H}_S)\,,$$

one can easily check that if $\mathcal{N}$ is anti-degradable with anti-degrading map $\mathcal{A}_{E_1\to S}$, then

$$[(\mathcal{M} \circ \mathcal{A}_{E_1\to S}) \otimes \mathrm{Tr}_{E_2}] \circ (\mathcal{M} \circ \mathcal{N})^{\mathrm{c}} = \mathcal{M} \circ \mathcal{N}\,. \tag{S90}$$

Analogously, one can easily verify that if $\mathcal{M}$ is anti-degradable with anti-degrading map $\mathcal{A}_{E_2\to S}$, then

$$[\mathrm{Tr}_{E_1} \otimes \mathcal{A}_{E_2\to S}] \circ (\mathcal{M} \circ \mathcal{N})^{\mathrm{c}} = \mathcal{M} \circ \mathcal{N}\,. \tag{S91}$$

□

V. GENERALISATION OF OUR METHODS TO GENERAL BOSONIC DEPHASING CHANNELS

In Theorem 27 we introduced a method to analyse anti-degradability of the bosonic loss-dephasing channel. In this section, we show that this method can be applied also to analyse the anti-degradability of the composition between a *general* bosonic dephasing channel and the pure-loss channel channel.

Given a probability distribution $p(\cdot)$ over $\mathbb{R}$, the associated *general bosonic dephasing channel* is given by

$$\mathcal{D}^{(p)}(X) := \int_{-\infty}^{\infty} \mathrm{d}\phi\, p(\phi)\, e^{i\phi\hat{a}^\dagger\hat{a}}\, X\, e^{-i\phi\hat{a}^\dagger\hat{a}}\,. \tag{S92}$$

If $p(\phi)$ is the Gaussian distribution $p(\phi) := \frac{1}{\sqrt{2\pi\gamma}}e^{-\frac{\phi^2}{2\gamma}}$, the general bosonic dephasing channel $\mathcal{D}^{(p)}$ exactly coincides with the bosonic dephasing channel $\mathcal{D}_\gamma$ analysed in this work. The action of $\mathcal{D}^{(p)}$ on operators of the form $|n\rangle\langle m|$ is given by

$$\mathcal{D}^{(p)}(|n\rangle\langle m|) = \tilde{p}(n-m)\,|n\rangle\langle m|\,, \tag{S93}$$

where $\tilde{p}$ is the Fourier transform of the probability distribution p, i.e.

$$\tilde{p}(k) := \int_{-\infty}^{\infty} \mathrm{d}\phi\, p(\phi)\, e^{ik\phi}\,. \tag{S94}$$

Let $\mathcal{N}_\lambda^{(p)}$ be the composition between such a general bosonic dephasing channel $\mathcal{D}^{(p)}$ and the pure-loss channel, i.e.

$$\mathcal{N}_\lambda^{(p)} := \mathcal{D}^{(p)} \circ \mathcal{E}_\lambda = \mathcal{E}_\lambda \circ \mathcal{D}^{(p)} \,. \tag{S95}$$

We can apply the exact same method that we have introduced in the proof of Thereom 27 in order to analyse the anti-degradability of $\mathcal{N}_\lambda^{(p)}$. The key observation is that in the proof of Theorem 27 we did not use the explicit expression of the channel $\mathcal{D}^{(p)}$ before stating (S37). This simple observation allows us to generalise our results to arbitrary bosonic dephasing channels, as stated in the following theorem.

Theorem 52 (Sufficient condition on the anti-degradability of the composition between a general bosonic dephasing channel and pure-loss channel)**.** *Let $\lambda \in [0,1)$ and let $p(\cdot)$ be a probability distribution over $\mathbb{R}$. Let $A = (a_{mn})_{m,n\in\mathbb{N}}$ be the infinite matrix whose components are defined by*

$$a_{mn} := \frac{\tilde{\phi}(n-m)}{\sum_{j=0}^{\min(n,m)} \sqrt{\mathcal{B}_j\left(n, \frac{2\lambda-1}{\lambda}\right)\, \mathcal{B}_j\left(m, \frac{2\lambda-1}{\lambda}\right)}}\,, \qquad \forall\, n,m \in \mathbb{N}\,. \tag{S96}$$

The channel $\mathcal{N}_\lambda^{(p)}$ is anti-degradable as long as either $\lambda \in [0, \frac{1}{2}]$ or the infinite matrix A is positive semi-definite.

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Cambridge, 2010.

[2] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2nd edition, 2017.

[3] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[4] S. Khatri and M. M. Wilde. Principles of quantum communication theory: A modern approach, 2020.

[5] M. L. Nowakowski. The symmetric extendibility of quantum states. *Journal of Physics A: Mathematical and Theoretical*, 49(38):385301, aug 2016.

[6] G. O. Myhr and N. Lütkenhaus. Spectrum conditions for symmetric extendible states. *Physical Review A*, 79:062307, 2009.

[7] C. Paddock and J. Chen. A characterization of antidegradable qubit channels, 2017.

[8] J. Chen, Z. Ji, D. Kribs, N. Lutkenhaus, and B. Zeng. Symmetric extension of two-qubit states. *Physical Review A*, 90(3), sep 2014.

[9] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. CRC Press, Taylor & Francis Group, Boca Raton, USA, 2017.

[10] A. S. Holevo. The Choi–Jamiolkowski forms of quantum Gaussian channels. *J. Math. Phys.*, 52(4):042202, 2011.

[11] A. S. Holevo. On the Choi–Jamiolkowski correspondence in infinite dimensions. *Preprint arXiv:1004.0196*, 2010.

[12] Z. Baghali Khanian and A. Winter. Distributed compression of correlated classical-quantum sources or: The price of ignorance. *IEEE Transactions on Information Theory*, 66(9):5620–5633, 2020.

[13] L. Lami, S. Khatri, G. Adesso, and M. M. Wilde. Extendibility of bosonic Gaussian states. *Physical Review Letters*, 123:050501, 2019.

[14] F. A. Mele, L. Lami, and V. Giovannetti. Quantum optical communication in the presence of strong attenuation noise. *Physical Review A*, 106:042437, 2022.

[15] M. M. Wolf, D. Pérez-García, and G. Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98:130501, 2007.

[16] F. Caruso, V. Giovannetti, and A. S. Holevo. One-mode bosonic Gaussian channels: a full weak-degradability classification. *New Journal of Physics*, 8(12):310–310, 2006.

[17] A. Arqand, L. Memarzadeh, and S. Mancini. Quantum capacity of a bosonic dephasing channel. *Phys. Rev. A*, 102:042413, Oct 2020.

[18] L. Lami and M. M. Wilde. Exact solution for the quantum and private capacities of bosonic dephasing channels. *Nat. Photonics*, 17(6):525–530, 2023.

[19] M. Rexiti, L. Memarzadeh, and S. Mancini. Discrimination of dephasing channels. *Journal of Physics A: Mathematical and Theoretical*, 55(24):245301, may 2022.

[20] S. Dehdashti, J. Nötzel, and P. V. Loock. Quantum capacity of a deformed bosonic dephasing channel, 2022.

[21] P. Leviant, Q. Xu, L. Jiang, and S. Rosenblum. Quantum capacity and codes for the bosonic loss-dephasing channel. *Quantum*, 6:821, sep 2022.

[22] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[23] H. Dür and H. J. Briegel. Entanglement purification and quantum error correction. *Reports on Progress in Physics*, 70(8):1381–1424, 2007.

[24] F. Salek and A. Winter. New protocols for conference key and multipartite entanglement distillation. *Preprint arXiv:2308.01134*, 2023.

[25] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[26] A. S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. Texts and Monographs in Theoretical Physics. De Gruyter, Berlin, Germany, 2nd edition, 2019.

[27] T. S. Cubitt, M. B. Ruskai, and G. Smith. The structure of degradable quantum channels. *J. Math. Phys.*, 49(10):102104, 2008.

[28] M. Horodecki, P. Horodecki, and R. Horodecki. Inseparable two spin-$\frac{1}{2}$ density matrices can be distilled to a singlet form. *Physical Review Letters*, 78:574–577, 1997.

[29] L. Lami, K. K. Sabapathy, and A. Winter. All phase-space linear bosonic channels are approximately Gaussian dilatable. *New Journal of Physics*, 20(11):113012, 2018.

[30] P. R. Halmos. *A Hilbert Space Problem Book*. Graduate Texts in Mathematics. Springer New York, NY, 1982.

[31] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1990.

Bombs and prizes, and the communication power of a single noisy qubit

Saptarshi Roy[1] * Tamal Guha[1] † Sutapa Saha[2] ‡ Giulio Chiribella[1] §

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *Department of Astrophysics and High Energy Physics, S. N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India*

Abstract. A fundamental property of quantum information is that a single qubit, taken in isolation, can carry at most 1 bit. The situation is different if the sender and receiver share entangled particles: in this case, the rate at which classical information can be transmitted through a qubit channel, quantified by its entanglement-assisted capacity, can generally exceed 1 bit. But what if the entanglement-assisted capacity is not more than 1 bit, as it happens for an important class of qubit channels known as entanglement-breaking? Can a noisy entanglement-breaking qubit channel be replaced by a noisy bit channel for the purposes of classical communication? Here we answer the question in the negative. We introduce a game where a player helps another player to find a prize hidden in one of four possible boxes, while avoiding a bomb hidden in one of the remaining three boxes. In this game, the two players cannot be sure to avoid the bomb if they communicate through a noisy bit channel. In contrast, they can avoid the bomb with certainty and find the prize with 1/3 probability if they communicate through an entanglement-breaking qubit channel, known as the universal `NOT` channel. The features of the quantum strategy can be simulated through the transmission of a bit, but this simulation requires the transmission to be a noiseless bit and to be assisted by shared randomness: without shared randomness, even the noiseless transmission of a three-level classical system cannot match the winning probability of the quantum strategy.

Keywords: Classical communication, Entanglement breaking channel, Shared Randomness

Introduction.- A celebrated result by Holevo [1] implies that a d-dimensional quantum system, taken in isolation, can carry at most $\log d$ bits of classical information, where log denotes the base-2 logarithm. This statement was later generalized by Frenkel and Weiner [2], who showed that the set of conditional probability distributions achievable by a sender and a receiver through the transmission of a d-dimensional quantum system coincides with the set of conditional probability distributions achievable through the transmission of a d-dimensional classical system, possibly assisted by correlated random bits shared by the sender and the receiver before the start of the communication protocol. This result implies that, for every possible classical task, the transmission of a d-dimensional quantum system can be replaced by the transmission of a d-dimensional classical system assisted by classical shared randomness.

The situation is different when the sender and receiver pre-share entanglement. In this case, the rate at which bits can be reliably transmitted through a quantum communication channel is quantified by its entanglement-assisted classical capacity [3]. For qubit channels, the entanglement-assisted capacity can generally exceed one bit, as shown by the dense coding protocol [4]. In this case, the transmission of a two-dimensional quantum system is clearly superior to the transmission of a two-dimensional classical system. But what if the entanglement-assisted capacity is not more than one bit? The prototype of qubit channels with entanglement-assisted capacity no more than 1 bit is the class of *entanglement-breaking* channels [5, 6, 7]. In general, the transmission of a d-dimensional quantum system through an entanglement-breaking channel can yield at most $\log d$ bits of classical communication [7]. Hence, a natural question is whether, for the purposes of classical communication, the transmission of a two-dimensional quantum system through a noisy entanglement-breaking channel can be replaced by the transmission of a two-dimensional classical system through a noisy classical channel.

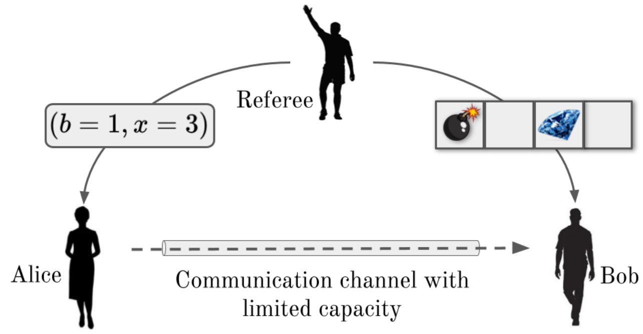


Figure 1: **The bomb and prize game.** A referee puts a prize in one of four possible boxes, labelled as $\{1, 2, 3, 4\}$, and a bomb in one of the three remaining boxes. The referee communicates to Alice the label b of the box containing the bomb and the label x of the box containing the prize. Then, the referee closes the boxes and sends them over to Bob, asking him to open one box. Bob wins if the finds the prize, under the constraint that the bomb is avoided with certainty. In this task, he is assisted by Alice, who communicates classical messages to him through a channel with limited capacity.

*sapsoy@gmail.com
†g.tamal91@gmail.com
‡sutapa.gate@gmail.com
§giulio@cs.hku.hk

Here we answer the above question in the negative: we provide a purely classical communication task that we put in the form of a game where a noisy entanglement-breaking qubit channel is more valuable than any noisy bit channel, even with the assistance of arbitrary amounts of shared randomness between the sender and receiver. In stark contrast, we show that the entanglement-assisted transmission of a qubit through a noisy entanglement-breaking channel allows the task to be accomplished with a finite probability of success. Finally, we analyze the additional classical resources required to achieve the communication task.

The bomb and prize game.– We now provide the precise mathematical formulation of the bomb and prize game illustrated in Figure 1. The location of the bomb and prize is described by a pair (b, x), where $b \in \{1, 2, 3, 4\}$ specifies the position of the bomb and $x \in \{1, 2, 3, 4\} \setminus \{b\}$ specifies the position of the prize. The overall strategy adopted by Alice and Bob can be described by a conditional probability distribution $p(y|b, x)$, where $y \in \{1, 2, 3, 4\}$ is the box opened by Bob. For a given configuration (b, x), the probability of winning the game is $p(x|b, x)$. In the following, we will consider the worst case winning probability

$$p_{\text{worst}}^{\text{prize}} := \min_{b,x} p(x|b, x)\,, \tag{1}$$

under the constraint that the bomb is avoided, corresponding to the condition

$$p_{\text{worst}}^{\text{bomb}} = 0 \quad \text{with} \quad p_{\text{worst}}^{\text{bomb}} := \max_{b,x} p(b|b, x)\,. \tag{2}$$

We now show two key results about classical strategies: *(i)* the bomb-avoiding condition (2) cannot be satisfied by any bit channel with nonmaximal capacity, and *(ii)* if the Alice and Bob do not share randomness, then the winning probability (1) subject to the bomb-avoiding condition (2) is zero even if a noiseless bit channel (or even a noiseless trit channel) is available.

Result *(i)* is established by the following theorem:

Theorem 1 *For every classical strategy using a single-bit channel of capacity $C < 1$ and an arbitrary amount of shared randomness, the worst-case probability of opening the box containing the bomb is lower bounded as*

$$p_{\text{worst}}^{\text{bomb}} \geq \frac{[1 - C]^{\ln 4}}{8}\,. \tag{3}$$

The proof of the theorem is provided in the technical version.

Result *(ii)* is established by the following theorem:

Theorem 2 *In the absence of shared randomness between Alice and Bob, the worst-case winning probability (1) subject to the bomb-avoiding condition (2) is zero for every classical strategy using the transmission of a classical system of dimension $d \leq 3$.*

The detailed proof of the theorem is in the technical version.

It is worth noting that the above theorem provides the best possible result in terms of dimensionality of the transmitted classical system: indeed, if Alice could transmit a 4-dimensional system through a noiseless channel, then she could communicate to Bob the exact location of the prize, thereby trivializing the game.

The quantum strategy. We now show that the transmission of a single qubit through a noisy entanglement-breaking channel allows Bob to avoid the bomb with certainty and to find the prize with a guaranteed probability of 1/3. The quantum strategy uses an entanglement-breaking channel known as the *(approximate) universal* `NOT` *channel* [8] (see also [9] for an extension to $d \geq 2$.) The universal `NOT` channel, hereafter denoted by `UNOT`, acts on an input density matrix ρ as follows:

$$\texttt{UNOT}(\rho) = \frac{2}{3}\,\text{Tr}[\rho]\,I - \frac{1}{3}\,\rho\,. \tag{4}$$

Experimental realizations of this transformation have been demonstrated with photons [10, 11]. The `UNOT` channel is unitarily equivalent to the optimal universal transpose [12, 13], which also has been implemented experimentally [14, 15, 16, 17].

The universal `NOT` channel can be equivalently realized as a uniform mixture of three Bloch sphere rotations about the three Cartesian axes; specifically, one has $\texttt{UNOT}(\rho) = \frac{1}{3}(X\rho X + Y\rho Y + Z\rho Z)$, where, $\{X, Y, Z\}$ are the spin-1/2 Pauli operators along x, y and z directions respectively. Since `UNOT` is a Pauli channel, its entanglement-assisted capacity can be computed via a closed-form expression [3, 18], which yields the value $C_{\text{E}}(\texttt{UNOT}) = 2 - \log 3 \approx 0.415$. Hence, the universal `NOT` channel satisfies the constraint of the bomb game: even with the assistance of quantum correlations, it does not allow Alice to transmit more than one bit per channel use.

On the other hand, the entanglement-assisted transmission of a qubit through the `UNOT` channel can be used to avoid the bomb with certainty and to win the game with a guaranteed probability of 1/3. The protocol that achieves this feature is a "universal `NOT` version" of the dense coding protocol [4].

Protocol 1 (`UNOT` dense coding) *Before the start of the protocol, Alice and Bob share two qubits A and B in the entangled state $|\Phi^+\rangle_{AB} = (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)/\sqrt{2}$. Then, they perform the following operations:*

1. *Alice applies one of the unitary gates $I, X, Y,$ or Z depending on whether the bomb is in box $1, 2, 3,$ or 4, respectively.*

2. *Alice sends qubit A to Bob through the universal* `NOT` *channel.*

3. *Bob measures both qubits A and B in the Bell basis, that is, the orthonormal basis consisting of states $|\Phi_1\rangle := |\Phi^+\rangle$, $|\Phi_2\rangle := (X \otimes I)|\Phi^+\rangle$, $|\Phi_3\rangle := (Y \otimes I)|\Phi^+\rangle$, and $|\Phi_4\rangle := (Z \otimes I)|\Phi^+\rangle$. If the measurement outcome is y, Bob will open the y-th box.*

Checking that the above protocol allows Bob to avoid the bomb is relatively straightforward. If the bomb is in position $b \in \{1,2,3,4\}$, then qubits A and B are in the state $|\Phi_b\rangle$. When qubit A is sent through the UNOT channel, the final state of qubits AB is

$$(\mathtt{UNOT} \otimes \mathcal{I}_B)(|\Phi_b\rangle\langle\Phi_b|) = \frac{1}{3}\, I \otimes I - \frac{1}{3}\,|\Phi_b\rangle\langle\Phi_b| \\ = \frac{1}{3}\sum_{y\neq b} |\Phi_y\rangle\langle\Phi_y| \,. \qquad (5)$$

Hence, when Bob measures the two qubits in the Bell basis, he will obtain an outcome y that is guaranteed to satisfy the condition $y \neq b$. Thanks to this fact, Bob avoids the bomb with certainty. Since the value of y is uniformly random in the set $\{1,2,3,4\} \setminus \{b\}$, Bob is guaranteed to find the prize with probability $p^{\rm prize}_{\rm worst} = 1/3$.

Comparing this result with Theorem 1, we can conclude that the entanglement-assisted transmission of a qubit through the UNOT channel is more valuable than the transmission of a bit through a noisy channel, even in the presence of shared randomness. Note also that the net effect of Protocol 1 is to reproduce the transmission of a *four-dimensional* classical system through the noisy channel specified by the conditional probability distribution

$$p_{\mathtt{NOT}}(y|b) = \begin{cases} 0 & \text{if } y = b \\ \frac{1}{3} & \text{if } y \neq b\,. \end{cases} \qquad (6)$$

This channel, which we call *classical 4-dimensional* NOT *channel*, has capacity $C = 2 - \log_2 3$-bits, exactly equal to the entanglement-assisted capacity of the universal NOT channel. A corollary of Theorem 1 is that the classical 4-dimensional NOT channel cannot be simulated by any noisy bit channel.

The shared randomness requirement. Theorem 2 implies that, in the absence of shared randomness, even the noiseless transmission of a trit cannot match the transmission of a qubit through the UNOT channel. It is then natural to ask how much shared randomness is needed to reproduce the features of the quantum strategy. In the following, we answer this question.

Consider a variant of the bomb and prize game where the referee communicates to Alice only the position of the bomb, without communicating the position of the prize. A general strategy for this variant of the game is described by the conditional probability distribution $p(y|b)$ that Bob opens box y when the bomb is in position b. In this case, the worst-case winning probability is $p^{\rm prize}_{\rm worst} := \min_b \min_{y\neq b} p(y|b)$ and the worst-case probability of opening the bomb is $p^{\rm bomb}_{\rm worst} : \max_b p(b|b)$. With these settings, the maximum of $p^{\rm prize}_{\rm worst}$ over all strategies $p(y|b)$ satisfying the bomb-avoiding condition $p^{\rm bomb}_{\rm worst} = 0$ is 1/3. This maximum winning probability is achieved by one and only one strategy, corresponding to the classical NOT channel $p_{\mathtt{NOT}}(y|b)$ in Eq. (6).

We now show that every classical strategy that simulates the channel $p_{\mathtt{NOT}}(y|b)$ using a noiseless bit channel must be assisted by $\log 3$ bits of shared randomenss. Moreover, this amount of shared randomness is sufficient:

Theorem 3 *The classical 4-dimensional* NOT *channel (6) can be simulated through the transmission of a single bit if and only if the sender and receiver share* $\log 3$ *bits of randomness.*

The proof is provided in the technical version. Note that the amount of shared randomness required by the simulation is more than 1 bit: while the 4-dimensional NOT channel can be simulated with two entangled qubits and a noisy, entanglement-breaking qubit channel, it cannot be simulated with two correlated bits and a noiseless bit channel.

Simulation of the universal NOT *channel.* Quite remarkably, a bit of noiseless classical communication plus $\log 3$ bits of classical shared randomness is also sufficient to simulate the UNOT channel. To this purpose, Alice and Bob can use the following protocol:

Protocol 2 (Simulation of the universal NOT channel) *Before the beginning of the protocol, Alice and Bob share two perfectly correlated trits, with uniformly distributed values.*

1. *If the value of the trit is* $i \in \{1,2,3\}$, *Alice measures the input qubit in the orthonormal basis* $\mathsf{B}_i = \{|\psi^{(i)}_0\rangle, |\psi^{(i)}_1\rangle\}$ *corresponding to the eigenstates of the Pauli matrix* σ_i, *with* $\sigma_1 := X$, $\sigma_2 := Y$, *and* $\sigma_3 := Z$,

2. *Alice uses the classical bit channel to communicate the outcome of her measurement to Bob,*

3. *Upon receiving the measurement outcome* $j \in \{0,1\}$, *Bob prepares the output qubit in the basis state* $|\psi^{(i)}_{(j+1) \bmod 2}\rangle$, *depending on the outcome* j *and on the trit value* i.

On average, Protocol 2 yields the UNOT channel, as shown in the technical version. This result can be further generalized, showing that every entanglement-breaking qubit channel can be simulated by using a noiseless classical bit channel assisted by shared randomness (see the technical version). An interesting open question is whether the result further generalizes to higher dimensions.

Conclusions.- We have shown that the transmission of a qubit through a noisy entanglement-breaking channel cannot, in general, be reproduced by the transmission of a bit through a noisy channel, even if the sender and receiver share arbitrary amounts of randomness. Moreover, we have shown that even if a bit (or a trit) channel with maximal capacity is available, reproducing the transmission of a qubit requires shared randomness. The advantage of the transmission of a noisy qubit can be demonstrated experimentally on a photonic platform.

References

[1] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[2] Péter E Frenkel and Mihály Weiner. Classical information storage in an n-level quantum system. *Communications in Mathematical Physics*, 340(2):563–574, 2015.

[3] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.*, 83:3081–3084, Oct 1999.

[4] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.

[5] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(06):629–641, August 2003.

[6] Mary Beth Ruskai. Qubit entanglement breaking channels. *Reviews in Mathematical Physics*, 15(06):643–662, 2003.

[7] Heng Fan. A note on quantum entropy inequalities and channel capacities. *Journal of Physics A: Mathematical and General*, 36(48):12081–12088, November 2003.

[8] V. Bužek, M. Hillery, and R. F. Werner. Optimal manipulations with qubits: Universal-not gate. *Phys. Rev. A*, 60:R2626–R2629, Oct 1999.

[9] Giulio Chiribella, Matt Wilson, and HF Chau. Quantum and classical data transmission through completely depolarizing channels in a superposition of cyclic orders. *Physical review letters*, 127(19):190502, 2021.

[10] Francesco De Martini, Vladimír Bužek, Fabio Sciarrino, and Carlo Sias. Experimental realization of the quantum universal not gate. *Nature*, 419(6909):815–818, 2002.

[11] M. Ricci, F. Sciarrino, C. Sias, and F. De Martini. Teleportation scheme implementing the universal optimal quantum cloning machine and the universal not gate. *Phys. Rev. Lett.*, 92:047901, Jan 2004.

[12] N. Gisin and S. Popescu. Spin flips and quantum information for antiparallel spins. *Phys. Rev. Lett.*, 83:432–435, Jul 1999.

[13] Paweł Horodecki and Artur Ekert. Method for direct detection of quantum entanglement. *Phys. Rev. Lett.*, 89:127902, Aug 2002.

[14] F. De Martini, V. Bužek, F. Sciarrino, and C. Sias. Experimental realization of the quantum universal not gate. *Nature*, 419(6909):815–818, October 2002.

[15] Hyang-Tag Lim, Yong-Su Kim, Young-Sik Ra, Joonwoo Bae, and Yoon-Ho Kim. Experimental realization of an approximate partial transpose for photonic two-qubit systems. *Phys. Rev. Lett.*, 107:160401, Oct 2011.

[16] Hyang-Tag Lim, Young-Sik Ra, Yong-Su Kim, Joonwoo Bae, and Yoon-Ho Kim. Experimental implementation of the universal transpose operation using the structural physical approximation. *Phys. Rev. A*, 83:020301, Feb 2011.

[17] Hyang-Tag Lim, Yong-Su Kim, Young-Sik Ra, Joonwoo Bae, and Yoon-Ho Kim. Experimental implementation of an approximate partial transpose for two-qubit systems. In *Conference on Lasers and Electro-Optics 2012*, QELS. OSA, 2012.

[18] XIAN-TING LIANG and HONG-YI FAN. ENTANGLEMENT-ASSISTED CLASSICAL CAPACITIES OF SOME SINGLE QUBIT QUANTUM NOISY CHANNELS. *Modern Physics Letters B*, 16(12):441–448, May 2002.

Appendix A: Proof of Theorem 1

The single-bit channel $\mathcal{N}$ available to Alice and Bob can be represented by a conditional probability distribution $p_{\rm chan}(j|i)$, $i,j\in\{0,1\}$, specifying the probability that Bob receives a bit in the state j when Alice sent a bit in the state i.

The bit channel $\mathcal{N}$ has unit capacity if and only if j is an invertible function of i, that is, if and only if $p_{\rm chan}(j|i)=\delta_{j,i}$ or $p_{\rm chan}(j|i)=\delta_{j,i\oplus 1}$, where $\oplus$ denotes addition modulo 2. Hence, the hypothesis that $\mathcal{N}$ has non-unit capacity implies that there exists at least one value j such that $p_{\rm chan}(j|0)>0$ and $p_{\rm chan}(j|1)>0$. We call such an j an "ambiguous output" and denote its minimum probability of the ambiguous output as

$$p_{\rm min}(j):=\min_i p_{\rm chan}(j|i). \tag{A1}$$

Taking the worst case over all ambiguous outputs, we obtain the ambiguous probability

$$p_? := \max_j p_{\rm min}(j)\,. \tag{A2}$$

In the following, we will denote by j_* the value such that $p_{\rm min}(j_*)=p_?$. Since the channel $\mathcal{N}$ has non-unit capacity, the ambiguous probability is nonzero: $p_?>0$.

Let us start by analyzing the setting where Alice and Bob do not share any correlated random bit. In this case, Alice's and Bob's strategy is completely described by an encoding channel $\mathcal{E}$, used by Alice to encode the position of the bomb into the input of channel $\mathcal{C}$, and a decoding channel $\mathcal{D}$, used by Bob to convert the output of channel $\mathcal{C}$ into the decision as to which box Bob should open. The two channels are represented by probability distributions $p_{\rm enc}(i|m)$ and $p_{\rm dec}(n|j)$, with $m,n\in\{1,2,3,4\}$. Hence, the probability that Bob opens box n when the bomb is in box m is

$$\begin{aligned} p_{\rm in/out}(n|m) &:= \sum_{i,j} p_{\rm dec}(n|j)\, p_{\rm chan}(j|i)\, p_{\rm enc}(i|m) \\ &= \sum_j p_{\rm dec}(n|j)\,\mathsf{Prob}(j|m)\,, \end{aligned} \tag{A3}$$

having defined $\mathsf{Prob}(j|m):=\sum_i p_{\rm chan}(j|i)\,p_{\rm enc}(i|m)$.

Now, notice that the ambiguous output j_* has probability lower bounded as $\mathsf{Prob}(j_*|m)\geq p_?$, independently of m. Denoting by $p_{\rm worst}:=\max_n p_{\rm in/out}(n|n)$ the worst-case probability that Bob opens a box containing the bomb, we then have the bound

$$\begin{aligned} p_{\rm worst} &\geq p_{\rm in/out}(n|n) \\ &\geq p_{\rm dec}(n|j_*)\,\mathsf{Prob}(j_*|n) \\ &\geq p_{\rm dec}(n|j_*)\,p_?\,, \qquad \forall n\in\{1,2,3,4\}\,. \end{aligned} \tag{A4}$$

In particular, let $n_{\rm max}$ be the most likely output of Bob's decoder when the output of the transmission channel is j_*, namely $p_{\rm dec}(n_{\rm max}|j_*)\geq p_{\rm dec}(n|j_*)$ for every $n\in\{1,2,3,4\}$. With this definition, we have $p_{\rm dec}(n_{\rm max}|j_*)\geq 1/4$, and the above bound becomes

$$p_{\rm worst}\geq \frac{p_?}{4}\,. \tag{A5}$$

Since the non-unit capacity condition implies $p_?>0$, the probability of opening the box with the bomb is nonzero.

Bound (A5) holds even if Alice and Bob share randomness. If Alice and Bob pick encoding and decoding operations $\mathcal{E}_k$ and $\mathcal{D}_k$ with probability λ_k, then the overall input-output distribution takes the form $p_{\rm in/out}(n|m)=\sum_k \lambda_k\, p^{(k)}_{\rm in/out}(n|m)$, where $p^{(k)}_{\rm in/out}(n|m)$ is the input-output distribution for fixed encoding and decoding operations $\mathcal{E}_k$ and $\mathcal{D}_k$. The worst case probability is then lower bounded as

$$\begin{aligned} p_{\rm worst} &\geq \sum_k \lambda_k\, p^{(k)}_{\rm in/out}(n|n) \\ &\geq \sum_k \lambda_k\, p^{(k)}_{\rm dec}(n|j_*)\,\mathsf{Prob}^{(k)}(j_*|n) \\ &\geq \sum_k \lambda_k\, p^{(k)}_{\rm dec}(n|j_*)\,p_? \\ &= p_{\rm dec}(n|j_*)\,p_?\,, \qquad \forall n\in\{1,2,3,4\}\,, \end{aligned} \tag{A6}$$

having defined $p_{\rm dec}(n|j):=\sum_k \lambda_k\, p^{(k)}_{\rm dec}(n|j)$ to be the average probability that Bob opens box n upon receiving the bit value j. Defining $n_{\rm max}$ to be the value of n that maximizes $p_{\rm dec}(n|j_*)$, we then have the inequality $p_{\rm dec}(n|j_*)\geq 1/4$, which plugged into Eq. (A6) yields Eq. (A5).

To conclude, we provide a lower bound to the r.h.s. of Eq. (A5) in terms of the channel capacity. To this purpose, note that the capacity of channel $\mathcal{N}$ is an upper bound to the capacity of the binary symmetric channel $\mathcal{N}_{\rm sym}=(\mathcal{N}+\mathcal{N}')/2$, where $\mathcal{N}'$ is the channel obtained by pre- and post- composing channel $\mathcal{N}$ with a bit flip (explicitly, channel $\mathcal{N}'$ corresponds to the probability distribution $p'_{\rm chan}(j|i)=p_{\rm chan}(j\oplus 1|i\oplus 1)$). Explicitly, the capacity of the binary symmetric channel $\mathcal{N}_{\rm sym}$ is [1]

$$C(\mathcal{N}_{\rm sym})=1-H(p_{\rm sym})\,, \tag{A7}$$

where $H(p)=-p\log p-(1-p)\log(1-p)$ is the binary entropy, and

$$p_{\rm sym}:=\min\left\{\frac{p(0|0)+p(1|1)}{2},\frac{p(0|1)+p(1|0)}{2}\right\}, \tag{A8}$$

Since the binary entropy satisfies the bound $H(p)\leq[4p(1-p)]^{1/\ln 4}$ [2], we obtain the bound

$$\begin{aligned} 4\,p_{\rm sym}\,(1-p_{\rm sym}) &\geq [1-C(\mathcal{N}_{\rm sym})]^{\ln 4} \\ &\geq [1-C(\mathcal{N})]^{\ln 4}\,, \end{aligned} \tag{A9}$$

which in turn implies the bound

$$p_{\mathrm{sym}} \geq \frac{1-\sqrt{1-[1-C(\mathcal{N})]^{\ln 4}}}{2} \geq \frac{[1-C(\mathcal{N})]^{\ln 4}}{2}. \qquad \text{(A10)}$$

Finally, note that the definition of p_{sym} implies $p_{\mathrm{sym}} \leq p_?$. Hence, Eqs. (A5) and (A10) imply $p_{\mathrm{worst}} \geq p_?/4 \geq p_{\mathrm{sym}}/4 \geq [1-C(\mathcal{N})]^{\ln 4}/8$. ■

Appendix B: Proof of Theorem 2

The most general classical strategy using a classical bit channel and no shared randomness consists of an encoding operation, described by the conditional probability $p_{\mathrm{enc}}(s|b,x)$ that Alice communicates the bit value s if the initial configuration of the boxes is (b,x), and a decoding operation, described by the conditional probability $p_{\mathrm{dec}}(y|s)$ that Bob opens box y upon receiving the bit value s. Without loss of generality, we assume that the communication channel from Alice to Bob is the identity channel, since any other bit channel can be reproduced by appending an additional noisy operation to Bob's decoding. Now, for every $s \in \{0,1,2\}$ we define the sets $\widetilde{\mathsf{A}}_s := \{(b,x) \mid p_{\mathrm{enc}}(s|b,x) \neq 0\}$, $\mathsf{A}_s := \{b \mid \exists x : (b,x) \in \widetilde{\mathsf{A}}_s\}$, and $\mathsf{B}_s := \{y \mid p_{\mathrm{dec}}(y|s) \neq 0\}$. Since Bob opens at least one box with non-zero probability, the set B_s is nonempty for every $s \in \{0,1,2\}$. The constraint that the bomb is avoided with certainty implies the condition $B_0 \cap B_1 \cap B_2 = \emptyset$: indeed, if the intersection were nonempty, there would be a box that has nonzero probability to be opened no matter what value is communicated by Alice, and meaning that there is no way to avoid the bomb with certainty if the bomb is placed into that box.

If the union $B_0 \cup B_1 \cup B_2$ is not the full set $\{1,2,3,4\}$, then there exist a box that has zero probability to be opened, no matter what message Alice sends. Clearly, putting the prize in that box brings the winning probability down to zero. In the following we will assume that $B_0 \cup B_1 \cup B_2 = \{1,2,3,4\}$. Now, there are two possible cases: (1) there exist two indices s and t such that the intersection $B_s \cap B_t$ has cardinality at least 2, (2) the intersection $B_s \cap B_t$ has cardinality at most 1 for every $s,t \in \{0,1,2\}$. Let us consider case (1) first, assuming $s=0$ and $t=1$ without loss of generality. Let y_0 and y_1 be the boxes in the intersection $B_0 \cap B_1$. The condition $B_0 \cap B_1 \cap B_2 = \emptyset$ then implies that neither y_0 nor y_1 is contained in B_2. Hence, placing the bomb in box y_0 forces Alice to communicate the message $s=2$, and placing the prize in box y_1 implies that Bob has zero probability of finding the prize.

Let us now consider the case (2). Since the intersection between any two of the sets B_0, B_1, and B_2 has cardinality at most 1, the set $B := (B_0 \cap B_1) \cup (B_1 \cap B_2) \cup (B_0 \cap B_2)$ has cardinality at most 3. Hence, there exists at least one element y_0 that is not in B. Since $B_0 \cup B_1 \cup B_2 = \{1,2,3,4\}$, the element y_0 should be in one of the three sets B_0, B_1, and B_2. Without loss of generality, let us assume $y_0 \in B_0$. To conclude, we separate two cases: (2a) $|B_0| \geq 2$ and (2b) $|B_0| = 1$. In case (2a), B_0 contains at least another index y_1 in addition to y_0. Hence, putting the bomb in y_1 guarantees that Alice will not communicate the message $s=0$, and putting the prize in y_0 guarantees that Bob has zero probability of finding the prize. In case (2b), the condition $B_0 \cup B_1 \cup B_2 = \{1,2,3,4\}$ implies $B_1 \cup B_2 = \{1,2,3,4,\} \setminus \{y_0\}$. Hence, at least one of the two sets has cardinality 2. Without loss of generality, let us assume that B_2 has cardinality 2. Since the intersection $B_1 \cap B_2$ has cardinality at most 1, B_2 must contain at least one element y_2 that is not contained in B_1, plus another element y_1. Putting the bomb in y_1 guarantees that Alice does not send the message $s=2$, and putting the prize in y_2 guarantees that Bob has zero probability of finding the prize. ■

Appendix C: Proof of Theorem 3

Here we introduce a compact notation of *strategy matrices* for the strategies that can be implemented by limited classical communication. They are characterized by the input-output statistics that the strategy $\mathcal{S}$ induces. Therefore, formally,

Definition 1. *A strategy $\mathcal{S}$ is a 4×4 matrix containing the entire set of input(b)-output(y) conditional probabilities $\{p(y|b)\}$ such that $\mathcal{S}^{by} = p(y|b)$.*

In our work, we will be interested in the scenario when Alice is allowed to communicate a classical two-level system $x \in \{0,1\}$ to Bob, which finally partitioned the full set of output indices $\{1,2,3,4\}$ in two disjoint subsets B_x, $x \in \{0,1\}$. With the condition $B_0 \cup B_1 = \{1,2,3,4\}$ and $B_0 \cap B_1 = \emptyset$, only two possibilities arise: $|B_x| = 1$, $|B_{x\oplus 1}| = 3$ and $|B_x| = |B_{x\oplus 1}| = 2$.

The *first* possibility encapsulates ${}^4C_1 = 4$ differently partitioned subsets each corresponding to a strategy with two independent probability parameters (p,q). As an example, consider a particular partition where $B_0 = \{1\}$ and $B_1 = \{2,3,4\}$, i.e., for $x=0$ communication from Alice, Bob always outputs 1, and for $x=1$, he outputs $\{2,3,4\}$ with the probabilities $(p,q,1-p-q)$ respectively. Then these four strategy matrices which we will henceforth call $1:3$ strategies can be represented as:

$$\mathcal{S}_{(1,1)} := \begin{pmatrix} 0 & p & q & (1-p-q) \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \mathcal{S}_{(1,2)} := \begin{pmatrix} 0 & 1 & 0 & 0 \\ p & 0 & q & (1-p-q) \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

,

$$\mathcal{S}_{(1,3)} := \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ p & q & 0 & (1-p-q) \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } \mathcal{S}_{(1,4)} := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ p & q & (1-p-q) & 0 \end{pmatrix}$$

On the other hand, for the strategy matrices belonging to the *second* class, there are 3 different set partitioning each with the two-parameter probabilities (p, q) denoting three distinct strategies. However, here when Alice communicates $x = 0$ $(x = 1)$, Bob any one index randomly from B_0 (B_1) following a probability distribution $\{p, 1-p\}$ $(\{q, 1-q\})$. Hence under this partitioning possibility, we obtain the following three strategy matrices which from now on will be referred to as $2:2$ strategies:

$$\mathcal{S}_{(2,1)} := \begin{pmatrix} 0 & p & (1-p) & 0 \\ q & 0 & 0 & (1-q) \\ q & 0 & 0 & (1-q) \\ 0 & p & (1-p) & 0 \end{pmatrix}, \mathcal{S}_{(2,2)} := \begin{pmatrix} 0 & p & 0 & (1-p) \\ q & 0 & (1-q) & 0 \\ 0 & p & 0 & (1-p) \\ q & 0 & (1-q) & 0 \end{pmatrix} \text{ and } \mathcal{S}_{(2,3)} := \begin{pmatrix} 0 & 0 & p & (1-p) \\ 0 & 0 & p & (1-p) \\ q & (1-q) & 0 & 0 \\ q & (1-q) & 0 & 0 \end{pmatrix}.$$

In all these strategy matrices $S_{(i,j)}$, $i = 1$ and $i = 2$ correspond respectively the $1:3$ and $2:2$ partitioning and j denotes the particular set partition for the corresponding group $i \in \{1, 2\}$.

A general strategy receives assistance from a shared classically correlated system. The role of any shared correlation (randomness) is to mix these deterministic strategies. Therefore any strategy using shared randomness takes the form

$$\mathcal{S} = \sum_{i=1}^{d} P_i \, \mathcal{S}_{(x_i, y_i)}(p_i, q_i), \text{ where } \sum_i P_i = 1. \quad \text{(C1)}$$

Here d is the local dimension of the shared classically correlated state. Also, d denotes the maximal number of strategies $\mathcal{S}_{(x,y)}$ that can be mixed.

With all these preliminaries we will now move to the question of simulating the classical 4-dimensional `NOT` channel with two-level classical communication and SR. Let us begin with the characterization of the classical 4-dimensional `NOT` gate in terms of a strategy matrix.

Proposition 1. *In the strategy matrix notation, the 4-dimensional* `NOT` *gate takes the form* $\mathcal{S}^* := \frac{1}{3}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

Proof. The proof directly follows from the action of 4-dimensional `NOT` gate, as in Eq. (**??**) of the main manuscript. ■

Evidently, the strategy matrix $\mathcal{S}^*$ cannot be obtained from any particular $\mathcal{S}_{(x,y)}$. Then the objective is to find the min d (as in Eq. (C1)), such that we can have $\mathcal{S} = \mathcal{S}^*$ by optimally choosing the free parameters x_i, y_i, p_i, q_i, and P_i. Our analysis reveals that the minimal dimension of the local subsystem of the classically correlated state to implement the 4-dimensional `NOT` strategy is three $(d = 3)$, a trit. Furthermore, we show that one requires two perfectly correlated trits, i.e., $\log 3$ bits of shared randomness to implement the 4-dimensional `NOT` strategy. We prove this to be a necessary and sufficient condition. This rules out the possibility of using the shared randomness of two classically correlated two-level systems to implement $\mathcal{S}^*$. We give a detailed description of our findings subsequently.

Sharing two $d = 3$ dimensional classical systems implies that the strategies that can be generated are obtained from mixing at most three deterministic strategies listed before into $1:3$ and $2:2$ classes. From Eq. (C1) the most general strategies in this case take the form $\mathcal{S} = \alpha\mathcal{S}_{(x_1,y_1)}(p_1, q_1) + \beta\mathcal{S}_{(x_2,y_2)}(p_2, q_2) + \gamma\mathcal{S}_{(x_3,y_3)}(p_3, q_3)$, where $\alpha + \beta + \gamma = 1$.

Lemma 1. *Mixing three strategies from class* $1:3$ *cannot generate* $\mathcal{S}^*$.

Proof. Let us consider any three strategy matrices $\mathcal{S}_{(1,y_i)}$, $y_i \in \{1,2,3,4\}$ chosen from the $1:3$ classes, such that $\mathcal{S} = \sum_{i=1}^{3} P_i \mathcal{S}_{(1,y_i)}(p_i,q_i)$. A closer inspection reveals that for any three such strategies, there is one row $\bar{y} = \{1,2,3,4\} \setminus \{y_1,y_2,y_3\}$, where two of the non-diagonal elements are zero. This immediately tells that $\mathcal{S}$ can not be identified as $\mathcal{S}^*$. ■

Lemma 2. *Mixing any strategy from class* $1:3$ *with any two strategies from the* $2:2$ *class cannot generate* $\mathcal{S}^*$.

Proof. There are $\binom{3}{2} \times 4 = 12$ ways one can choose such a mixture of strategies. However, all such mixtures are mathematically equivalent. This is because mixing any two class $2:2$ strategies can make all the non-diagonal elements of the effective strategy matrix non-zero. Mixing any class $1:3$ strategy on top of this yields identical equations for generating the optimal strategy matrix $\mathcal{S}^*$. So without loss of generality we mix $\mathcal{S}_{(2,1)}$, $\mathcal{S}_{(2,2)}$, and $\mathcal{S}_{(1,1)}$ and demand the generation of $\mathcal{S}^*$. We have

$$S = \alpha\mathcal{S}_{(2,1)}(p_1,q_1) + \beta\mathcal{S}_{(2,2)}(p_2,q_2) + \gamma\mathcal{S}_{(1,1)}(p_3,q_3), \tag{C2}$$

where we have $\alpha+\beta+\gamma = 1$, and p_is and q_is denote the local randomness parameters. We want to solve for $S = \mathcal{S}^*$, which translates to $S^{ij} = \frac{1-\delta_{ij}}{3}$, where ij denotes the ij^{th} matrix element. Here there are only 8 unknowns but 12 equations making it an overdetermined system. For there to be a consistent solution, we must have

$$S^{01} - S^{21} - S^{31} = -\frac{1}{3} \implies \gamma p_3 = -\frac{1}{3}. \tag{C3}$$

Since $\gamma \geq 0$, for a consistent solution, we need $p_3 < 0$. Being a probability $p_3 \geq 0$ and hence a consistent solution for $S = \mathcal{S}^*$ cannot exist. ■

Lemma 3. $\log 3$ *bits of shared randomness is necessary to generate the optimal strategy matrix* $\mathcal{S}^*$.

Proof. The possible candidates are obtained by mixing three strategies from class $2:2$, and mixing two class $1:3$ strategies with a class $2:2$ strategy.
Case 1. Here we consider mixing three strategies from class $2:2$. When they are mixed with probabilities α, β, and γ we have

$$S = \alpha\mathcal{S}_{(2,1)}(p_1,q_1) + \beta\mathcal{S}_{(2,2)}(p_2,q_2) + \gamma\mathcal{S}_{(2,3)}(p_3,q_3), \tag{C4}$$

where p_i, q_i denote the local randomness that Bob employs for the $(2,i)^{\text{th}}$ strategy. Of course the mixing probabilities sum to unity, $\alpha+\beta+\gamma = 1$. We want to solve for $S = \mathcal{S}^*$. This is equivalent to the condition $S^{ij} = \frac{1-\delta_{ij}}{3}$, where ij in superscript denotes the ij^{th} matrix element. The number of non-trivial relations, as pointed out before, is 12, but the number of unknowns is 8 making it an overdetermined system. For a consistent solution to exist we must have

$$S^{01} + S^{10} + S^{23} + S^{32} = \frac{4}{3} \implies \alpha + \beta = \frac{2}{3},$$
$$S^{12} + S^{21} + S^{03} + S^{30} = \frac{4}{3} \implies \beta + \gamma = \frac{2}{3},$$
$$S^{02} + S^{20} + S^{13} + S^{31} = \frac{4}{3} \implies \alpha + \gamma = \frac{2}{3}.$$

The above equations imply that for a consistent solution to exist we must have $\alpha = \beta = \gamma = \frac{1}{3}$. It corresponds to an initial shared randomness of $\log 3$ bits.
Case 2.
Now we will consider the scenario where two of the 1:3 strategies is combined with one of the 2:2 class strategy. Note that, due to the symmetric structure of each of the individual strategy classes we can choose any two of the $1:3$ class, however, depending upon this choice not all the strategies from $2:2$ classes are equivalent. Let us first consider the following convex combination of strategies:

$$S = \alpha\mathcal{S}_{(1,1)}(p_1,q_1) + \beta\mathcal{S}_{(1,2)}(p_2,q_2) + \gamma\mathcal{S}_{(2,1)}(p_3,q_3),$$

where, $\{p_k, q_k | k \in \{1,2\}\}$ and p_3, q_3 are the local randomness for $(1,k)^{\text{th}}$ and $(2,1)^{\text{th}}$ strategies respectively and α,β,γ denote the same as in Eq. (C4). Using the notation S^{ij} to denote the ij^{th} element of the matrix S and identifying S with $\mathcal{S}^*$, we obtain the following equations:

$$S^{21} = \beta = \frac{1}{3},$$
$$S^{30} = \alpha = \frac{1}{3},$$

which readily implies $\gamma = \frac{1}{3}$. On the other hand, if they choose $\mathcal{S}_{(2,2)}$ instead of $\mathcal{S}_{(2,1)}$, then the similar analysis will again lead to the condition $\alpha = \beta = \gamma = \frac{1}{3}$. However, for choice of $\mathcal{S}_{(2,3)}$ as the $2:2$ class element, both the third and fourth rows will contain zeros other than the input position b. Hence such a strategy will never work to obtain $\mathcal{S}^*$. With a similar analysis, one may argue that for every pair of $1:3$ class strategies, there exists one $2:2$ strategy, combining which lead to a failure in the worst case scenario. In particular, $\mathcal{S}_{(2,1)}$ should be avoided whenever the pair $\{\mathcal{S}_{(1,1)}, \mathcal{S}_{(1,4)}\}$ or, $\{\mathcal{S}_{(1,2)}, \mathcal{S}_{(1,3)}\}$ is chosen and so on. ■

1. Sufficiency of a classical bit and $\log 3$-bit SR to simulate 4-dimensional `NOT` channel

In the following, we will give a strategy to utilize $\log 3$-bits of SR, along with the communication of a two-level classical system to simulate 4-dimensional `NOT` gate. To begin with Alice and Bob have two perfectly correlated trits: the probability p_i that Alice's and Bob's trits are in the state $i \in \{1,2,3\}$ is $1/3$ for every i. Alice can communicate one bit $x_{i,b} \in \{0,1\}$ to Bob which depends on i and the input $b \in \{1,2,3,4\}$. Precisely, $x_{i,b} = 0$ whenever the input variable b to Alice is in the sector $B_{i,0} = \{1, 1+i\} \subset \{1,2,3,4\}$ and $x_{i,b} = 1$ for $b \in B_{i,1} = \{1,2,3,4\} \setminus B_{i,0}$. Finally depending upon i and $x_{i,b}$, Bob produces an output $y \in \{1,2,3,4\}$ with the following probability distribution.

$$\begin{aligned} p\Big(y = B^{1(2)}_{i,x_{i,b}} | i, x_{i,b}\Big) &= \frac{1}{2}, \\ p\Big(y = B^{1(2)}_{i,x_{i,b}\oplus 1} | i, x_{i,b}\Big) &= 0, \end{aligned} \tag{C5}$$

where $B^{1(2)}_{i,k}$ are the respective elements of the set $B_{i,k}$, i.e., $B_{i,k} = \{B^1_{i,k}, B^2_{i,k}\}$.

We are interested in the input-output statistics $p(y|b)$ that the above strategy produces. Formally, we can write

$$p(y|b) = \sum_{i=1}^{3} p_i p(y|i, x_{i,b}) = \frac{1}{3}\sum_{i=1}^{3} p(y|i, x_{i,b}). \tag{C6}$$

Now two distinct cases arise. When $y \neq b$, then there exists a unique $i^* \in \{1,2,3\}$, s.t. $\{y, b\} = B_{i^*,0}$ or $B_{i^*,1}$. Then from (C5), it right away implies $p(y|i^*, x_{i^*,b}) = 0$. Again from Eq. (C5), for all $i \in \{1,2,3\} \setminus i^*$, we have $p(y|i, x_{i,b}) = \frac{1}{2}$. Combining the above findings with (C6), we get

$$p(y \neq b|b) = \frac{1}{3}\sum_{i \neq i^*} p(y|i, x_{i,b}) + \frac{1}{3} p(y|i^*, x_{i^*,b}) = \frac{1}{3}. \tag{C7}$$

For $y = b$, (C5) immediately forces $p(y = b|i, x_{i,b}) = 0$ for all i. Substituting this in (C6) we get $p(y = b|b) = 0$. This along with (C7) demonstrate the simulation of the classical NOT channel (**??**). ■

Appendix D: Simulation of universal NOT channel

We will now prove that the Protocol. 2 in the main manuscript exactly simulates the universal qubit NOT channel.

Note that, Protocol. 2 simulates a qubit channel from $L(\mathcal{H}_A) \to L(\mathcal{H}_B)$ which takes the form

$$\mathcal{N}_{A\to B}(\rho_A) = \sum_{i=1}^{3}\sum_{j=-1}^{1} p_i \langle\psi^{(i)}_j|\,\rho_A\,|\psi^{(i)}_j\rangle\,|\psi^{(i)}_{-j}\rangle\langle\psi^{(i)}_{-j}|_B,$$

where, $|\psi^{(i)}_j\rangle$, $j \in \{\pm 1\}$ are the respective eigenstates of the Pauli matrices σ_i, $i \in \{1,2,3\}$ and $0 \le p_i \le 1$ are the probabilities at which Alice performs the corresponding Pauli measurement. In the following we will drop the subscripts A and B for simplicity. Now, if Alice and Bob share a classically correlated trit system randomly sampled over $\{1,2,3\}$, then for an arbitrary two-level quantum state $\rho = \frac{1}{2}(\mathbb{I} + \vec{n}.\vec{\sigma})$, we obtain

$$\begin{aligned} \mathcal{N}(\rho) &= \frac{1}{3}\sum_{i=1}^{3}\Big(\frac{1 \pm n_i}{2}\Big)|\psi^{(i)}_{\mp 1}\rangle\langle\psi^{(i)}_{\mp 1}| \\ &= \frac{1}{3}\sum_{i=1}^{3}\Big(\frac{1 \pm n_i}{2}\Big)\frac{1}{2}(\mathbb{I} \mp \sigma_i) \\ &= \frac{1}{2}(\mathbb{I} - \frac{1}{3}\vec{n}.\vec{\sigma}) \\ &= \frac{1}{3}\sum_{i=1}^{3}\sigma_i \rho \sigma_i. \end{aligned}$$

Appendix E: Simulation of entanglement-breaking qubit channels

An entanglement-breaking channel Φ_{CQ} is called classical-quantum (CQ) if its action on arbitrary state $\rho \in L(\mathcal{H})$ can be expressed as $\Phi_{CQ}(\rho) = \sum_k R_k \langle\psi_k|\rho|\psi_k\rangle$, where R_ks are arbitrary density matrices and $\{|\psi_k\rangle\}$ constitutes an orthonormal basis. Being a special case, a qubit CQ map $\Phi^{\texttt{qubit}}_{CQ}$ assumes a particularly simple form

$$\Phi^{\texttt{qubit}}_{CQ}(\rho) = R_0\langle\psi|\rho|\psi\rangle + R_1\langle\psi^\perp|\rho|\psi^\perp\rangle. \tag{E1}$$

for all possible $\rho \in L(\mathbb{C}^2)$, where $\mathbb{C}^2$ is the two dimensional complex Hilbert space.

It is known that every extreme point of the set of entanglement-breaking qubit maps is an extreme CQ map $\mathcal{E}^j_{CQ}$. Therefore, the set of entanglement-breaking qubit maps is the convex hull of extreme qubit CQ maps [3, 4]. Hence, every entanglement-breaking qubit map $\Phi^{\texttt{qubit}}$ can be written as

$$\Phi^{\texttt{qubit}}(\rho) = \sum_j p_j \mathcal{E}^j_{CQ}(\rho), \quad \text{with} \quad \sum_j p_j = 1. \tag{E2}$$

Since $\mathcal{E}^j_{CQ}$ is an extreme CQ map, we have $\mathcal{E}^j_{CQ}(\rho) = R^j_0\langle\psi_j|\rho|\psi_j\rangle + R^j_1\langle\psi^\perp_j|\rho|\psi^\perp_j\rangle$, with $R^j_{0(1)} = |\phi^j_{0(1)}\rangle\langle\phi^j_{0(1)}|$ being pure states. Now, two distant parties, one (say Alice) in possession of an arbitrary state ρ, and the other (say Bob) responsible for simulating $\Phi^{\texttt{qubit}}(\rho)$ employ the following protocol.

Protocol 1 (Simulation of a qubit entanglement-breaking channel). *Before the protocol begins, Alice and Bob share a classically correlated random variable k distributed with the same probabilities as in Eq.* (E2).

1. *If the value of the random variable is j, which they obtain with probability p_j, Alice measures the state ρ in her possession in the basis $\{|\psi_j\rangle, |\psi^\perp_j\rangle\}$.*

2. *Alice then communicates a bit* $\{0 \mapsto |\psi_j\rangle, 1 \mapsto |\psi_j^\perp\rangle\}$ *conveying the measurement outcome to Bob.*

3. *Bob prepares* R_0^j *or* R_1^j *when the communicated bit is* 0 *or* 1 *respectively.*

The net effect of the protocol is to simulate every $\mathcal{E}_{CQ}^j$ with a probability p_j, and on average, generates the same map as in Eq. (E2). Therefore, Protocol. 1 demonstrates that every entanglement-breaking qubit channel can be simulated by using a perfect classical bit channel assisted by shared randomness.

[1] T. M. Cover, *Elements of information theory* (John Wiley & Sons, 1999).

[2] F. Topsøe, Bounds for entropy and divergence for distributions over a two-element set., JIPAM. Journal of Inequalities in Pure Applied Mathematics [electronic only] **2**, Paper No. 25, 13 p. (2001).

[3] M. B. Ruskai, Qubit entanglement breaking channels, Reviews in Mathematical Physics **15**, 643 (2003).

[4] M. Horodecki, P. W. Shor, and M. B. Ruskai, Entanglement breaking channels, Reviews in Mathematical Physics **15**, 629 (2003).

Quantum networks boosted by entanglement with a control system

Tamal Guha[1] * Saptarshi Roy[1] † Giulio Chiribella[1 2 3] ‡

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *Department of Computer Science, University of Oxford, Parks Road, Oxford OX1 3QD, United Kingdom*

[3] *Perimeter Institute for Theoretical Physics, Caroline Street, Waterloo, Ontario N2L 2Y5, Canada*

Abstract. Coherent control over the configurations of quantum devices in a network scenario offer promising advantages in quantum information processing. So far such advantages were assuming the control system is uncorrelated with the communicated data. Here, we explore the power of quantum correlation between them, showing two communication tasks that can be accomplished by the information-erasing channels if and only if the sender shares prior entanglement with a third party controlling the network configuration. While the first task considers a-bit of classical communication keeping secret to the controller, the second task is to establish entanglement among a number of distant receivers.

Keywords: Coherent control of path, Indefinite causal order

1 Introduction

A remarkable feature for quantum particles is their ability to undergo multiple evolutions simultaneously, in a coherent superposition [1, 2, 3]. The application of such an interfering evolution to filter out the noise in a quantum channel was first pointed out in [4] and thereafter, recently studied from various information theoretic perspectives both theoretically [5, 6, 7, 8] and experimentally [9, 10]. In a quantum network, such a superposition of multiple evolutions, i.e., the quantum channels, is modelled in presence of a control system, which routes the target system through a particular path.

Alternatively, such a network model, equipped with the control system, also provides an interesting toy model to investigate a new causal structure that could potentially arise in a quantum theory of gravity [11, 12]. A concrete example of such a new causal structure is quantum SWITCH [13, 14], which connects two quantum channels in an order determined by the quantumness of the control and gives rise to causal nonseparability [15, 16]. Over the past decade, quantum SWITCH is found to offer information processing advantages in various tasks [17, 18, 19, 20, 7, 21, 22, 23, 24, 25, 26, 27, 28] and also stimulated several experimental investigations [29, 30, 31, 32, 33, 34].

Previous studies of all coherently controlled networks, including quantum SWITCH, are explored the benefits of quantum superposition by assuming the controller initially uncorrelated with the target system. It is possible, however, to consider a more general situation, in which the control and the target share prior correlations. In this situation, the data processed by the network becomes correlated with its evolution, potentially giving rise to new phenomena that could not be observed in the traditional setting.

Here, we explore the power of quantum correlations between control and target, showing that they enable two communication tasks that are impossible with an uncorrelated control, or even with a classically correlated one. Both the tasks involve an assistance of the controller, who also shares a prior quantum correlation with the sender. The controller, for instance, can be considered as a communication company responsible for the connection between the sender and the receiver, or in general, any third party who has access on the outcomes of the measurement performed on the control system.

Our first task considers perfect communication of the classical information via completely information-erasing channels and also without leaking any information to the controller. The second task is to establish bipartite, or more generally, multipartite entangled network between sender and a number of spatially separated receivers via the same completely information-erasing channels. We show that both the tasks can be accomplished perfectly if and only if the sender and the controller initially shares a maximally entangled state.

2 Basic Framework

The general quantum evolutions are referred as quantum channels acting on the set of quantum states. Mathematically, the action of any quantum channel (say $\mathcal{E}$) on a quantum system (ρ) can be identified with a non-unique set of operators ($\{E_i\}$), namely the Kraus operators, summed up to the identity operator on the system Hilbert space.

Quantum SWITCH, in its simplest form, considers two such quantum channels $\mathcal{E}$ and $\mathcal{F}$ acting on a single target system in a controlled-order fashion and gives rise to a combined channel $\mathcal{S}(\mathcal{E},\mathcal{F})$ acting jointly on the target-control pair. In particular, the target effectively passes through two different quantum channels $\mathcal{E}\circ\mathcal{F}$ or $\mathcal{F}\circ\mathcal{E}$ depending upon whether the control system is in $|0\rangle$ or $|1\rangle$ state. In the present context $\mathcal{E}$ and $\mathcal{F}$ are regarded as completely information erasing *qubit* channels, which we will denote as $\mathcal{E}_0$ and $\mathcal{E}_1$ respectively. Here, $\mathcal{E}_\psi$ represents a channel which produces a fixed quantum state $|\psi\rangle$ independent of the input system. The Kraus opera-

*g.tamal91@gmail.com

†sapsoy@gmail.com

‡giulio@cs.hku.hk

tors for the combined SWITCH channel $\mathcal{S}(\mathcal{E}_0,\mathcal{E}_1)$ can be found in the main manuscript [35], where we have also considered the SWITCH action of d-different completely information erasing *qudit* channels $\{\mathcal{E}_0,\mathcal{E}_1,\cdots,\mathcal{E}_{d-1}\}$.

The control over the choice of the same quantum channels $\mathcal{E}_0$ and $\mathcal{E}_1$ can be described in a similar manner. Here, the target system will pass through the channel $\mathcal{E}_0$ or, $\mathcal{E}_1$, whenever the control is in the state $|0\rangle$ or, $|1\rangle$ respectively. We will denote the combined channel action on the target-control quantum system for the controlled choice configuration as $\mathcal{T}(\mathcal{E}_0,\mathcal{E}_1)$ and the corresponding Kraus operators can be found in our main manuscript [35].

It is important to mention that while the controlled-order configuration (quantum SWITCH) $\mathcal{S}(\mathcal{E}_0,\mathcal{E}_1)$ depends only on the channels, the Kraus operators of controlled-choice configuration $\mathcal{T}(\mathcal{E}_0,\mathcal{E}_1)$ involves a couple of complex parameters, generally referred as vacuum amplitudes from the experimental perspectives [6, 36]. Physically, these externally tunable parameters carry the information of the trivial path, i.e., the path which is *not* used in a particular instance of choice.

In our main manuscript [35], it is shown in detail that for a particular choice of these external parameters, the effective action of $\mathcal{T}(\mathcal{E}_0,\mathcal{E}_1)$ exactly matches with that of the $\mathcal{S}(\mathcal{E}_0,\mathcal{E}_1)$, even when more numbers of orthogonal completely information erasing channels $\{\mathcal{E}_0,\mathcal{E}_1,\cdots,\mathcal{E}_{d-1}\}$ are considered. This, in turn, helps us to continue our analysis only with the controlled-order configuration of these channels, which at the same time holds true for the controlled-choice configuration.

3 Private Classical Communication

Consider a scenario where the sender Alice would like to communicate a bit of classical information to a distant receiver Bob. Unfortunately, they do not have access to clean classical channel, instead connected via a pair of completely information erasing set-reset channels: one of them ($\mathcal{E}_0$) produces the bit "0" and the other ($\mathcal{E}_1$) produces "1" irrespective of any input they fed into the line. However, there is a third party Charlie who has access to a controlling quibt which can rout the sent bit through these channels in any arbitrary order. Still there is no way to establish perfect classical communication between Alice and Bob, keeping Charlie completely ignorant, by probing the channels in a definite causal order. Interestingly, the SWITCH action $\mathcal{S}(\mathcal{E}_0,\mathcal{E}_1)$ has a decoherence free subspace spanned $|0\rangle\otimes|0\rangle$ and $|1\rangle\otimes|1\rangle$ (see our main manuscript [35] for detailed analysis), which contains both states $|\Phi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle \pm |1\rangle\otimes|1\rangle)$. Therefore, if Alice initially shares a maximally entangled state $|\Phi^{+}\rangle$ with Charlie, then she can encode the classical bit $x\in\{0,1\}$ on her qubit by applying nothing or, a σ_x rotation respectively. In either case, the state will be transferred intact after the SWITCH action and Charlie will remain ignorant about the message x since it is impossible distinguish between $|\Phi^{\pm}\rangle$ just by performing measurement on the control qubit. Then Charlie can perform a σ_x measurement on his qubit and communicate the information classically to Bob. Finally, performing again a σ_x measurement on his qubit Bob can decode the bit x perfectly: $x=0$ when Bob's outcome is same with that of Charlie and $x=1$ otherwise (see Fig. 1).It can be shown that the initial maximal entanglement between Alice and Charlie is necessary for the perfect accomplishment of the task. This, along with its d-dimensional generalization, leads us to the following theorem, proof of which is presented in our main manuscript [35].

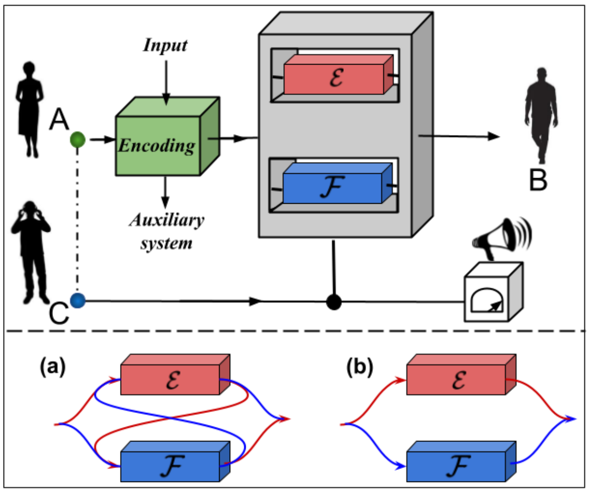


Figure 1: Communication with the assistance of correlations with a control system. Sender A communicates to receiver B through two noisy channels with the assistance of a third party, C, who controls the configuration of the two channels. We focus on the case where the configuration is either the order of the noisy channels (a), or the choice of which channel is used (b). The controller and the sender initially share an entangled state (dotted line on the top left). Then, the sender encodes some input data, by performing local operations on her part of the entangled state. The output of these operations is a signal that is sent through the network, and possibly some auxiliary systems that the sender will keep in her laboratory. After transmission, the controller assists the receiver by providing him classical information extracted from the control system.

Theorem 1 *A classical dit can be communicated, with no leakage to the controller, through d orthogonal information-erasing channels in d coherently controlled configurations if and only if the control and target are initially in a d-dimensional maximally entangled state.*

Theorem 1 also highlights a fundamental difference between protocols using control over the configurations of channel configuration and protocols using the noisy channels in a fixed configuration, while allowing control over operations performed before and after each noisy channel [37]. Such a protocol allow Alice to communication the classical information through the control, in a way which is completely independent of the noisy channels [38]. However, it generally leaks information to Charlie, violating the privacy requirement of the present task (see [35] for detailed analysis).

4 Establishment of Multipartite Entanglement

Our second task is to establish entanglement between the sender (Alice) and an N numbers of spatially separated receivers (Bobs), all of whom are connected via completely information erasing channels to Alice. While the general scenario with an arbitrary N is discussed in our main manuscript [35], here we will consider only $N = 2$ case. Note that, being completely information erasing, such channels acting on one part of a multipartite quantum state, destroy any form of initial correlations the state possessed and hence obviously entanglement-breaking too. This suggests that it is impossible to establish entanglement between sender and receivers via these channels, even in any possible definite causal orderings. However, if Alice is allowed to share a maximally entangled state $|\Phi^+\rangle$ with Charlie, using two ancillary qubit $|0\rangle \otimes |0\rangle$ and applying C-NOT gate on each of them she can prepare a four-partite GHZ state $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes 4} + |1\rangle^{\otimes 4})$. Then keeping the first qubit with her, Alice can send other two qubits via individual SWITCH channels. Interestingly, it transfers the GHZ state unaffected at the receivers end (see our manuscript [35]), which could also be understood intuitively, by recalling the fact that every individual SWITCH line admits a decoherence free subspace. However, the crucial point here is that using a single control qubit and two different transmission lines of completely information erasing channels $\mathcal{E}_0$ and $\mathcal{E}_1$ it is possible to preserve the subspace spanned by $|0\rangle \otimes |0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle \otimes |1\rangle$. Finally, by performing the Fourier measurement on the control qubit, Charlie can communicate the outcome to any of the receivers (say Bob$_1$) and accordingly Bob$_1$ can apply a local unitary to establish a tripartite GHZ state among Alice, Bob$_2$ and himself. In particular, Bob$_1$ will do nothing or apply a σ_x rotation if Charlie communicates + or −, respectively (see Fig 2).

Also, in this case we have proved the necessity of maximal entanglement between target and control system for GHZ distribution [35]. This result and its d-dimensional generalization is contained in the following theorem.

Theorem 2 *Coherent control on the configuration of d orthogonal information-erasing channels enables perfect establishment of d-dimensional GHZ states between the sender and N spatially separated receivers if and only if the sender and controller initially share a d-dimensional maximally entangled state.*

Besides of its various information theoretic applications [39, 40, 41], a distributed GHZ-state can be used to achieve a task, namely Random Receiver Quantum Communication (RRQC) [23], where the goal is to transfer the quantum information to one of many receivers, however, whose identity will only be disclosed after the communication. Strikingly, initial target-control entanglement allows us to accomplish RRQC with completely information erasing channels, while in lack of such entanglement the task can only be achieved with channels which preserve classical information [23].

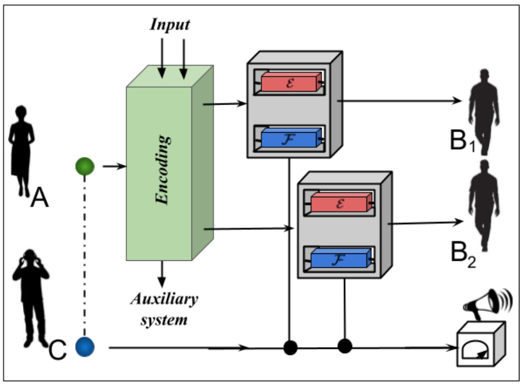


Figure 2: Distribution of entanglement to $N = 2$ spatially separated parties through coherently controlled information-erasing channels. The task can be perfectly achieved with the assistance of shared entanglement between the qubit at the sender's end, and a qubit used to control the configuration of channels between the sender and each receiver.

5 Conclusion

In this work we initiated the exploration of quantum networks whose configuration is entangled with the state of a control system. We focused on applications to quantum communication, identifying two tasks that can be perfectly achieved if and only if the sender and the controller initially share maximal entanglement.

Both the tasks highlights the power of initial target-control quantum correlation in compared to their uncorrelated or even classically correlated configurations. Moreover, the first task points out that the coherent controlled configurations of noisy channels are fundamentally different from those of other protocols where the encoded information bypassed via the controller, avoiding the actual noises. The coherently controlled configurations in our work involves both the coherently controlled order as well as the coherently controlled choice configuration of the completely information erasing channels.

While in this work we focused on quantum communication, we believe that protocols using quantum correlations with the configuration of quantum networks will have significant implications also in other quantum technology, likely including quantum metrology, thermodynamics, and computation. Such protocols are potentially within reach with existing photonic setups, and would mark a new step in the development of a quantum technology of coherent control over the configurations of quantum networks.

References

[1] Yakir Aharonov, Jeeva Anandan, Sandu Popescu, and Lev Vaidman. Superpositions of time evolutions of a quantum system and a quantum time-translation machine. *Phys. Rev. Lett.*, 64:2965–2968, Jun 1990.

[2] Daniel K. L. Oi. Interference of quantum channels. *Phys. Rev. Lett.*, 91:067902, Aug 2003.

[3] Johan Åberg. Operations and single-particle interferometry. *Phys. Rev. A*, 70:012103, Jul 2004.

[4] N. Gisin, N. Linden, S. Massar, and S. Popescu. Error filtration and entanglement purification for quantum communication. *Phys. Rev. A*, 72:012338, Jul 2005.

[5] Alastair A Abbott, Julian Wechs, Dominic Horsman, Mehdi Mhalla, and Cyril Branciard. Communication through coherent control of quantum channels. *Quantum*, 4:333, 2020.

[6] Giulio Chiribella and Hlér Kristjánsson. Quantum shannon theory with superpositions of trajectories. *Proceedings of the Royal Society A*, 475(2225):20180903, 2019.

[7] Nicolas Loizeau and Alexei Grinbaum. Channel capacity enhancement with indefinite causal order. *Physical Review A*, 101(1):012340, 2020.

[8] Hlér Kristjánsson, Wenxu Mao, and Giulio Chiribella. Witnessing latent time correlations with a single quantum particle. *Phys. Rev. Research*, 3:043147, Nov 2021.

[9] L.-P. Lamoureux, E. Brainis, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar. Experimental error filtration for quantum communication over highly noisy channels. *Phys. Rev. Lett.*, 94:230501, Jun 2005.

[10] Giulia Rubino, Lee A. Rozema, Daniel Ebler, Hlér Kristjánsson, Sina Salek, Philippe Allard Guérin, Alastair A. Abbott, Cyril Branciard, Časlav Brukner, Giulio Chiribella, and Philip Walther. Experimental quantum communication enhancement by superposing trajectories. *Phys. Rev. Research*, 3:013093, Jan 2021.

[11] Lucien Hardy. Towards quantum gravity: a framework for probabilistic theories with non-fixed causal structure. *Journal of Physics A: Mathematical and Theoretical*, 40(12):3081–3099, March 2007.

[12] Lucien Hardy. Quantum gravity computers: On the theory of computation with indefinite causal structure. In *The Western Ontario Series in Philosophy of Science*, pages 379–401. Springer Netherlands, 2009.

[13] G. Chiribella, G. M. D′Ariano, P. Perinotti, and B. Valiron. Beyond quantum computers.

[14] Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, and Benoit Valiron. Quantum computations without definite causal structure. *Phys. Rev. A*, 88:022318, Aug 2013.

[15] Ognyan Oreshkov, Fabio Costa, and Časlav Brukner. Quantum correlations with no causal order. *Nature Communications*, 3(1), January 2012.

[16] Mateus Araújo, Cyril Branciard, Fabio Costa, Adrien Feix, Christina Giarmatzi, and Časlav Brukner. Witnessing causal nonseparability. *New Journal of Physics*, 17(10):102001, 2015.

[17] Giulio Chiribella. Perfect discrimination of no-signalling channels via quantum superposition of causal structures. *Phys. Rev. A*, 86:040301, Oct 2012.

[18] Mateus Araújo, Fabio Costa, and Časlav Brukner. Computational advantage from quantum-controlled ordering of gates. *Phys. Rev. Lett.*, 113:250402, Dec 2014.

[19] Daniel Ebler, Sina Salek, and Giulio Chiribella. Enhanced communication with the assistance of indefinite causal order. *Phys. Rev. Lett.*, 120:120502, Mar 2018.

[20] Giulio Chiribella, Manik Banik, Some Sankar Bhattacharya, Tamal Guha, Mir Alimuddin, Arup Roy, Sutapa Saha, Sristy Agrawal, and Guruprasad Kar. Indefinite causal order enables perfect quantum communication with zero capacity channels. *New Journal of Physics*, 23(3):033039, March 2021.

[21] Marcello Caleffi and Angela Sara Cacciapuoti. Quantum switch for the quantum internet: Noiseless communications through noisy channels. *IEEE Journal on Selected Areas in Communications*, 38(3):575–588, 2020.

[22] Nicolas Loizeau and Alexei Grinbaum. Channel capacity enhancement with indefinite causal order. *Phys. Rev. A*, 101:012340, Jan 2020.

[23] Some Sankar Bhattacharya, Ananda G. Maity, Tamal Guha, Giulio Chiribella, and Manik Banik. Random-receiver quantum communication. *PRX Quantum*, 2:020350, Jun 2021.

[24] Sk Sazim, Michal Sedlak, Kratveer Singh, and Arun Kumar Pati. Classical communication with indefinite causal order for n completely depolarizing channels. *Phys. Rev. A*, 103:062610, Jun 2021.

[25] Giulio Chiribella, Matt Wilson, and H. F. Chau. Quantum and classical data transmission through completely depolarizing channels in a superposition of cyclic orders. *Phys. Rev. Lett.*, 127:190502, Nov 2021.

[26] David Felce and Vlatko Vedral. Quantum refrigeration with indefinite causal order. *Phys. Rev. Lett.*, 125:070603, Aug 2020.

[27] Tamal Guha, Mir Alimuddin, and Preeti Parashar. Thermodynamic advancement in the causally inseparable occurrence of thermal maps. *Phys. Rev. A*, 102:032215, Sep 2020.

[28] Kyrylo Simonov, Gianluca Francica, Giacomo Guarnieri, and Mauro Paternostro. Work extraction from coherently activated maps via quantum switch. *Phys Rev A*, 105:032217, 2022.

[29] Lorenzo M Procopio, Amir Moqanaki, Mateus Araújo, Fabio Costa, Irati Alonso Calafell, Emma G Dowd, Deny R Hamel, Lee A Rozema, Časlav Brukner, and Philip Walther. Experimental superposition of orders of quantum gates. *Nature communications*, 6(1):1–6, 2015.

[30] Giulia Rubino, Lee A. Rozema, Adrien Feix, Mateus Araújo, Jonas M. Zeuner, Lorenzo M. Procopio, Časlav Brukner, and Philip Walther. Experimental verification of an indefinite causal order. *Science Advances*, 3(3), March 2017.

[31] K. Goswami, C. Giarmatzi, M. Kewming, F. Costa, C. Branciard, J. Romero, and A. G. White. Indefinite causal order in a quantum switch. *Phys. Rev. Lett.*, 121:090503, Aug 2018.

[32] Kejin Wei, Nora Tischler, Si-Ran Zhao, Yu-Huai Li, Juan Miguel Arrazola, Yang Liu, Weijun Zhang, Hao Li, Lixing You, Zhen Wang, Yu-Ao Chen, Barry C. Sanders, Qiang Zhang, Geoff J. Pryde, Feihu Xu, and Jian-Wei Pan. Experimental quantum switching for exponentially superior quantum communication complexity. *Phys. Rev. Lett.*, 122:120504, Mar 2019.

[33] Yu Guo, Xiao-Min Hu, Zhi-Bo Hou, Huan Cao, Jin-Ming Cui, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, and Giulio Chiribella. Experimental transmission of quantum information using a superposition of causal orders. *Phys. Rev. Lett.*, 124:030502, Jan 2020.

[34] K. Goswami and J. Romero. Experiments on quantum causality. *AVS Quantum Science*, 2(3):037101, October 2020.

[35] Tamal Guha, Saptarshi Roy, and Giulio Chiribella. Quantum networks boosted by entanglement with a control system. *Physical Review Research*, 5(3):033214, 2023.

[36] Augustin Vanrietvelde and Giulio Chiribella. Universal control of quantum processes using sector-preserving channels. *arXiv preprint arXiv:2106.12463*, 2021.

[37] Philippe Allard Guérin, Giulia Rubino, and Časlav Brukner. Communication through quantum-controlled noise. *Phys. Rev. A*, 99:062317, Jun 2019.

[38] Hlér Kristjánsson, Giulio Chiribella, Sina Salek, Daniel Ebler, and Matthew Wilson. Resource theories of communication. *New Journal of Physics*, 22(7):073014, July 2020.

[39] Harry Buhrman, Wim van Dam, Peter Høyer, and Alain Tapp. Multiparty quantum communication complexity. *Physical Review A*, 60(4):2737, 1999.

[40] Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp. Anonymous quantum communication. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 460–473. Springer, 2007.

[41] Anne Broadbent, Paul-Robert Chouha, and Alain Tapp. The ghz state in secret sharing and entanglement simulation. In *2009 Third International Conference on Quantum, Nano and Micro Technologies*, pages 59–62. IEEE, 2009.

Shadow simulation of quantum processes*

Xuanqiang Zhao[1] Xin Wang[2] Giulio Chiribella[1 3 4]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science,
The University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *Thrust of Artificial Intelligence, Information Hub,
The Hong Kong University of Science and Technology (Guangzhou), Guangdong 511453, China*
[3] *Quantum Group, Department of Computer Science,
University of Oxford, Wolfson Building, Parks Road, Oxford, OX1 3QD, United Kingdom*
[4] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada*

Abstract. We introduce the task of shadow process simulation, where the goal is to reproduce the expectation values of arbitrary quantum observables at the output of a target physical process. When the sender and receiver share no-signaling resources, we show that the performance of shadow process simulation exceeds that of conventional process simulation protocols in scenarios including communication, noise simulation, and data compression. Remarkably, shadow simulation provides increased accuracy without any increase in the sampling cost. Overall, shadow simulation provides a unified framework for a variety of quantum protocols, including probabilistic error cancellation and circuit knitting in quantum computing.

Keywords: Quantum Shannon Theory, Quantum Channel Simulation, Quantum Communication

1 Introduction

Quantum channel simulation [1, 2, 3, 4, 5, 6, 7] is a fundamental primitive in quantum Shannon theory. It serves as an abstraction of many practical tasks in quantum computing and quantum information processing, including quantum communication and quantum error correction. The aim of quantum channel simulation is to reproduce the output states of a target channel using an available channel $\mathcal{N}$.

However, in many practical scenarios, what we are interested in is shadow information, *i.e.*, the information about the expectation values of all possible observables. Shadow information unravels many physical properties of a quantum system, and its importance has motivated the invention of protocols such as shadow tomography [8] and classical shadow [9]. In this work, we ask the question that what if we only want to transmit the shadow information through quantum channels? Would it be an easier task than transmitting the quantum state itself?

To answer this question, we introduce a new quantum information processing task called *shadow process simulation*, where the goal is to reproduce the expectation values of all possible observables at the output of a target quantum channel. Shadow process simulation can be regarded as a generalization of quantum channel simulation. This generalization is useful for quantum information processing in the near term, where classical post-processing of expectation values can be used to simulate larger quantum memories [10, 11, 12, 13], probe properties of quantum systems [14, 9, 15], mitigate errors [16, 17, 18, 19, 20, 21], and simulate unphysical operations [22, 23, 24].

We start the investigation under a framework where the two parties involved in this task are allowed to perform local operations assisted by shared classical randomness. In particular, within this framework we establish the following:

- We prove that shared randomness together with post-processing can simulate arbitrary no-signaling resources, providing a complete characterization of randomness-assisted shadow simulation codes.
- We find in several applications that shadow simulation overcomes the limits of conventional channel simulation at the price of an increase in the number of samples needed to accurately estimate the expectation values.
- We also find scenarios where shadow simulation achieves lower error than conventional channel simulation without any sampling overhead, demonstrating a strict advantage of shadow simulation.

Our work challenges a common interpretation of quantum states. While the quantum state is often regarded as an encoding of the expectation values of arbitrary observables, we show that transferring an encoding of all expectation values is a much less demanding task than transmitting the quantum state. In this respect, the quantum state appears to be more than just a catalogue of expectation values.

2 Framework of shadow process simulation

Conventional channel simulation aims to simulate the action of a target channel $\mathcal{M}$ by using an available channel $\mathcal{N}$. To accomplish this simulation, Alice and Bob perform local encoding and decoding channels $\mathcal{E}$ and $\mathcal{D}$, respectively, thus obtaining the new channel $\mathcal{D}\circ\mathcal{N}\circ\mathcal{E} = \mathcal{M}$. In shadow simulation, because the final result is the expectation value of some observable, which is obtained by multiple rounds of measurement, Alice and Bob can sample their local operations $\mathcal{E}$ and $\mathcal{D}$ from sets of channels $\{\mathcal{E}_j\}$ and $\{\mathcal{D}_j\}$ in each round as in Figure 1. We allow

[*] This submission is based on arXiv:2401.14934.

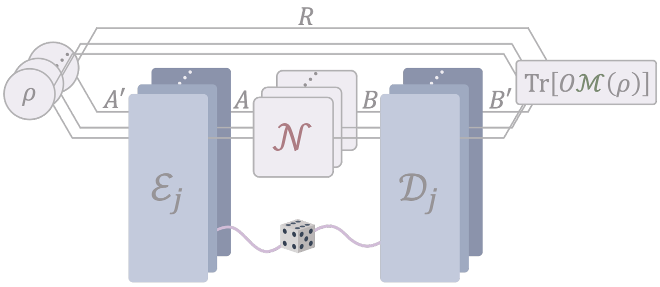


Figure 1: Alice and Bob are connected through a quantum channel $\mathcal{N}$. The task is to enable Bob to estimate the expectation value $\mathrm{Tr}[O\mathcal{M}(\rho)]$ of an arbitrary observable O on the output state $\mathcal{M}(\rho)$ produced by a target channel $\mathcal{M}$ when acting on an arbitrary input state ρ of a reference system R and a system A' in Alice's laboratory.

them to share classical randomness so that they can coordinate their local operations. After the output has been measured, Bob can post-process the measurement statistics, taking arbitrary linear combinations of the outcome probabilities. In this way, Alice and Bob can simulate any linear map of the form

$$\widetilde{\mathcal{S}}(\mathcal{N}) = \sum_j \lambda_j \mathcal{D}_j \circ \mathcal{N} \circ \mathcal{E}_j. \tag{1}$$

The linear map $\widetilde{\mathcal{S}}$ is an example of a supermap [25], that is, a map acting on the vector space spanned by quantum operations. Due to the possible presence of negative coefficients in the set $\{\lambda_j\}$, $\widetilde{\mathcal{S}}$ generally does not transform quantum channels into quantum channels. Instead, it transforms Hermitian-preserving maps into Hermitian-preserving maps, and we call such a supermap a *virtual supermap*.

A virtual supermap $\widetilde{\mathcal{S}}$ of the form (1) represents a *randomness-assisted shadow simulation code*, corresponding to a virtual bipartite process $\widehat{\mathcal{S}} := \sum_j \lambda_j \mathcal{E}_j \otimes \mathcal{D}_j$. It is rather straightforward to see that this virtual process is *no-signaling*, meaning that no information is exchanged between Alice and Bob. The converse is less straightforward but turns out to be true:

Theorem 1 *A virtual supermap $\widetilde{\mathcal{S}}$ is a randomness-assisted shadow simulation code if and only if the corresponding virtual process $\widehat{\mathcal{S}}$ is no-signaling.*

Theorem 1 provides a complete characterization of the randomness-assisted shadow simulation codes and allows us to directly study shadow process simulation with *no-signaling shadow simulation codes*, which are linear combinations of quantum no-signaling codes. Sampling over different quantum codes generally leads to a sampling overhead, meaning that more rounds of data collection are needed to estimate the desired expectation values [22, 23, 24]. We define the *sampling cost* of the code $\widetilde{\mathcal{S}}$ as

$$c_{\mathrm{smp}}\left(\widetilde{\mathcal{S}}\right) := \inf\left\{p_+ + p_- \,\middle|\, \widehat{\mathcal{S}} = p_+\widehat{\mathcal{S}}^+ - p_-\widehat{\mathcal{S}}^-,\ p_\pm \in \mathbb{R}^+,\right.$$
$$\left.\widehat{\mathcal{S}}^\pm \in \mathrm{CPTP} \cap \mathrm{NS}\right\}, \tag{2}$$

where CPTP and NS denote the set of completely positive, trace-preserving maps and the set of no-signaling virtual processes, respectively, and $\mathbb{R}^+$ is the set of non-negative real numbers. Note that every conventional channel simulation protocol has $c_{\mathrm{smp}}\left(\widetilde{\mathcal{S}}\right) = 1$, since the map $\widehat{\mathcal{S}}$ is a no-signaling channel. The sampling cost c_{smp} characterizes the range of post-processed measurement outcomes, and a wider range requires more rounds of measurement to accurately estimate the expectation value.

3 Surpassing the limits of quantum channel simulation

We illustrate the power of shadow simulation in three applications. The first application we consider is communication, which can be viewed as the simulation of an identity channel acting on a given number of qubits. The key quantity to study in communication is capacity, which measures the highest dimension of an identity channel that one can simulate. Here, we define the one-shot γ-cost shadow capacity assisted by no-signaling resources as

$$Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}) := \sup_{d,\widehat{\mathcal{S}}\in\mathrm{NS}} \left\{\log_2 d \,\middle|\, \widetilde{\mathcal{S}}(\mathcal{N}) = \mathrm{id}_d,\ c_{\mathrm{smp}}\left(\widetilde{\mathcal{S}}\right) \le \gamma\right\}, \tag{3}$$

where the dimension d is optimized over positive integers. In the technical version, we provide an explicit semidefinite programming expression for the shadow capacity for every given γ. This expression extends the previously known expression for the one-shot quantum capacity assisted by no-signaling resources [4, 26], which can be retrieved in the special case $\gamma = 1$. For $\gamma > 1$, we show that the one-shot shadow capacity is generally larger than the one-shot quantum capacity. A concrete example is provided below:

Theorem 2 *Let $\mathcal{N}_{\mathrm{depo},p}(\rho) = p\rho + (1-p)\mathbb{1}_2/2$ be a single-qubit depolarizing channel, where $p \in [0,1]$ is a probability and $\mathbb{1}_2$ is the identity operator on $\mathbb{C}^2$. For $\gamma \ge 1$, the one-shot zero-error shadow capacity assisted by no-signaling resources is*

$$Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p}) = \log_2 \left\lfloor \sqrt{2p\gamma + p + 1} \right\rfloor. \tag{4}$$

Theorem 2 shows that a qubit depolarizing channel can be used to transmit the expectation values of all observables on a quantum system of arbitrarily high dimension, at the price of an increased sampling cost, provided that the channel is not completely depolarizing ($p \neq 0$). This fact is interesting because, for $p \le 1/3$, the depolarizing channel is entanglement-breaking [27] and therefore it cannot reliably transmit quantum states, even if infinitely many copies of it are available.

In the technical version, we also show similar results in the dual task to communication, that is, the simulation of a target noisy channel using a noiseless one. In this case, the key quantity is the simulation cost, defined as

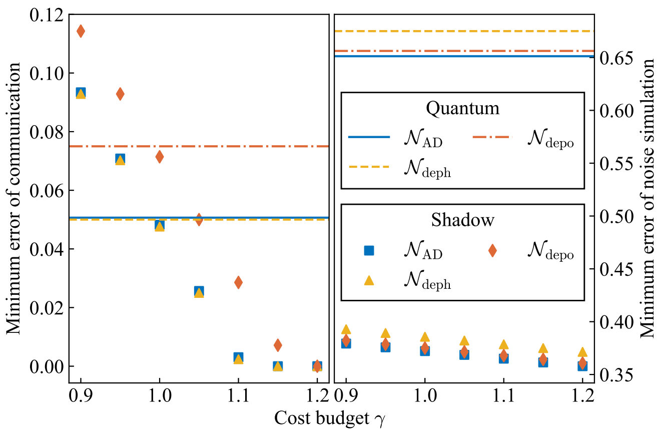


Figure 2: Compared with that of conventional quantum channel simulation (horizontal lines), the minimum error in the shadow simulation case is smaller with the same or even lower cost budget.

the number of noiseless qubits that must be sent from the sender to a receiver. The shadow simulation cost generalizes the quantum simulation cost studied in the conventional scenario [4, 7] and can generally be reduced by increasing the sampling cost.

Besides communication and noisy channel simulation, shadow simulation also allows simulating high-dimensional noiseless channels using low-dimensional ones. This shadow simulation can also be viewed as a form of quantum compression, where the goal is to store the expectation values of all possible observables. Alternatively, one can view this shadow simulation as the simulation of a high-dimensional quantum measurement using a low-dimensional one. In the following theorem, we provide an exact characterization of the minimum sampling cost required for this shadow compression task.

Theorem 3 *Given identity channels* id_d *and* $\mathrm{id}_{d'}$ *with* $d' \geq d \geq 2$, *the minimum sampling cost of an exact shadow simulation of* $\mathrm{id}_{d'}$ *using* id_d *and no-signaling resources is* $2{d'}^2/d^2 - 1$.

This theorem implies that one can perfectly shadow-simulate the transmission of an arbitrarily large number of qubits, and thus any quantum channel, using only a single-qubit identity channel, a task that cannot be achieved in conventional channel simulation. Furthermore, it also implies that every channel with non-zero shadow capacity $Q^{(1)}_{\gamma,\text{NS}}$ for some γ can shadow-simulate every other channel, generalizing the result of Theorem 2 for single-qubit depolarizing channels.

4 Achieving lower error without sampling overhead

In the zero-error scenario, we have seen that the shadow capacity and shadow simulation cost coincide with the conventional capacity and simulation cost for $\gamma = 1$. In stark contrast, we now show that in the approximate scenario, shadow simulation can achieve lower error than conventional channel simulation even if $\gamma = 1$.

In this scenario, our goal is to convert channel $\mathcal{N}$ into an approximation of channel $\mathcal{M}$. We define the minimum error achievable with sampling cost bounded by γ based on the diamond distance:

$$\varepsilon^*_{\gamma,\text{NS}}(\mathcal{N},\mathcal{M}) := \inf_{\widetilde{\mathcal{S}}\in\text{NS}} \left\{ \frac{1}{2}\left\| \widetilde{\mathcal{S}}(\mathcal{N}) - \mathcal{M} \right\|_{\diamond} \;\middle|\; c_{\text{smp}}\left(\widetilde{\mathcal{S}}\right) \leq \gamma \right\}. \tag{5}$$

We use the diamond distance because, as we show in the technical version, it captures the worst case error of measuring observables. Figure 2 presents the minimum errors in both shadow communication and noisy channel simulation at different cost budgets ranging from 0.9 to 1.2 for some commonly used quantum channels. Surprisingly, shadow simulation codes achieve smaller errors at the same or even lower levels of sampling cost compared with quantum simulation codes. This implies that classical post-processing can enhance the transmission of expectation values even if no sampling overhead is involved.

5 Conclusions

In this work, we introduced the task of shadow simulation of quantum channels, showing that transmitting and processing expectation values of arbitrary observables is generally a less demanding task than transmitting and processing quantum states. Besides their foundational interest, our results are relevant to practical applications to NISQ quantum technologies. Our work provides new efficient methods for measuring observables with noisy quantum devices, and new communication protocols for transmitting multiple complementary pieces of information, opening up a systematic way to study new quantum protocols that sample over different transformations of quantum processes.

References

[1] D. Kretschmann and R. F. Werner, “Tema con variazioni: quantum channel capacity,” *New Journal of Physics*, vol. 6, no. 1, p. 26, 2004.

[2] M. Berta, M. Christandl, and R. Renner, “The quantum reverse shannon theorem based on one-shot information theory,” *Communications in Mathematical Physics*, vol. 306, pp. 579–615, 2011.

[3] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, “The quantum reverse shannon theorem and resource tradeoffs for simulating quantum channels,” *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 2926–2959, 2014.

[4] R. Duan and A. Winter, “No-signalling-assisted zero-error capacity of quantum channels and an information theoretic interpretation of the lovász number,” *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 891–914, 2015.

[5] D. Leung and W. Matthews, "On the Power of PPT-Preserving and Non-Signalling Codes," *IEEE Transactions on Information Theory*, vol. 61, pp. 4486–4499, aug 2015.

[6] X. Wang, W. Xie, and R. Duan, "Semidefinite Programming Strong Converse Bounds for Classical Capacity," *IEEE Transactions on Information Theory*, vol. 64, pp. 640–653, jan 2018.

[7] K. Fang, X. Wang, M. Tomamichel, and M. Berta, "Quantum channel simulation and the channel's smooth max-information," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2129–2140, 2019.

[8] S. Aaronson, "Shadow tomography of quantum states," in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 325–338, 2018.

[9] H.-Y. Huang, R. Kueng, and J. Preskill, "Predicting many properties of a quantum system from very few measurements," *Nature Physics*, vol. 16, no. 10, pp. 1050–1057, 2020.

[10] S. Bravyi, G. Smith, and J. A. Smolin, "Trading classical and quantum computational resources," *Physical Review X*, vol. 6, no. 2, p. 021043, 2016.

[11] T. Peng, A. W. Harrow, M. Ozols, and X. Wu, "Simulating large quantum circuits on a small quantum computer," *Physical Review Letters*, vol. 125, no. 15, p. 150504, 2020.

[12] K. Mitarai and K. Fujii, "Overhead for simulating a non-local channel with local channels by quasiprobability sampling," *Quantum*, vol. 5, p. 388, 2021.

[13] C. Piveteau and D. Sutter, "Circuit knitting with classical communication," *IEEE Transactions on Information Theory*, 2023.

[14] F. Buscemi, M. Dall'Arno, M. Ozawa, and V. Vedral, "Direct observation of any two-point quantum correlation function," *arXiv:1312.4240*, 2013.

[15] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, "The randomized measurement toolbox," *Nature Reviews Physics*, vol. 5, no. 1, pp. 9–24, 2023.

[16] Y. Li and S. C. Benjamin, "Efficient variational quantum simulator incorporating active error minimization," *Physical Review X*, vol. 7, no. 2, p. 021050, 2017.

[17] K. Temme, S. Bravyi, and J. M. Gambetta, "Error mitigation for short-depth quantum circuits," *Physical Review Letters*, vol. 119, no. 18, p. 180509, 2017.

[18] C. Piveteau, D. Sutter, S. Bravyi, J. M. Gambetta, and K. Temme, "Error mitigation for universal gates on encoded qubits," *Physical Review Letters*, vol. 127, p. 200505, Nov 2021.

[19] M. Lostaglio and A. Ciani, "Error mitigation and quantum-assisted simulation in the error corrected regime," *Physical Review Letters*, vol. 127, p. 200506, Nov 2021.

[20] Y. Suzuki, S. Endo, K. Fujii, and Y. Tokunaga, "Quantum error mitigation as a universal error reduction technique: Applications from the nisq to the fault-tolerant quantum computing eras," *PRX Quantum*, vol. 3, p. 010345, Mar 2022.

[21] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, "Quantum error mitigation," *arXiv:2210.00921*, 2022.

[22] J. Jiang, K. Wang, and X. Wang, "Physical implementability of linear maps and its application in error mitigation," *Quantum*, vol. 5, p. 600, 2021.

[23] B. Regula, R. Takagi, and M. Gu, "Operational applications of the diamond norm and related measures in quantifying the non-physicality of quantum maps," *Quantum*, vol. 5, p. 522, 2021.

[24] X. Zhao, L. Zhang, B. Zhao, and X. Wang, "Power of quantum measurement in simulating unphysical operations," *arXiv:2309.09963*, 2023.

[25] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Transforming quantum operations: Quantum supermaps," *Europhysics Letters*, vol. 83, no. 3, p. 30004, 2008.

[26] X. Wang and R. Duan, "A semidefinite programming upper bound of quantum capacity," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 1690–1694, IEEE, 2016.

[27] M. Horodecki, P. W. Shor, and M. B. Ruskai, "Entanglement breaking channels," *Reviews in Mathematical Physics*, vol. 15, no. 06, pp. 629–641, 2003.

Shadow simulation of quantum processes

Xuanqiang Zhao,[1, *] Xin Wang,[2, †] and Giulio Chiribella[1, 3, 4, ‡]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *Thrust of Artificial Intelligence, Information Hub, The Hong Kong University of Science and Technology (Guangzhou), Guangdong 511453, China*

[3] *Quantum Group, Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, OX1 3QD, United Kingdom*

[4] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada*

(Dated: May 20, 2024)

We introduce the task of shadow process simulation, where the goal is to reproduce the expectation values of arbitrary quantum observables at the output of a target physical process. When the sender and receiver share no-signaling resources, we show that the performance of shadow process simulation exceeds that of conventional process simulation protocols in a variety of scenarios including communication, noise simulation, and data compression. Remarkably, shadow simulation provides increased accuracy without any increase in the sampling cost. Overall, shadow simulation provides a unified framework for a variety of quantum protocols, including probabilistic error cancellation and circuit knitting in quantum computing.

Introduction.— "What is a quantum state?" is one of the central questions in the foundations of quantum mechanics. A minimal interpretation is that a quantum state is a compact way to represent all expectation values of the possible observable quantities associated to a given system. This interpretation may suggest that transmitting a quantum state from a place to another is equivalent to transferring information about the expectation values of arbitrary observables. In this paper, we show that this equivalence does not hold when the sender and receiver share random bits: in this case, transferring information about all possible expectation values is a much less demanding task than transferring the quantum state. Some instances of this phenomenon can be derived from results on error mitigation [1–3], while other more radical instances emerge from a new task that we name *shadow simulation of quantum processes.*

The settings of shadow simulation are illustrated in Figure 1, and we only consider finite-dimensional quantum systems. A sender, Alice, has access to a quantum communication channel $\mathcal{N}$ that transfers quantum states to a receiver, Bob. Initially, Alice has a quantum system A', which may be entangled with a reference system R and together in an arbitrary state ρ possibly unknown to her. Bob has a device that measures an arbitrary observable O, possibly unknown to him. The goal of shadow simulation is to enable Bob to estimate the expectation value $\mathrm{Tr}[O\mathcal{M}(\rho)]$ for a target quantum channel $\mathcal{M}$. To achieve this goal, Alice and Bob perform pre- and post-processing operations $\mathcal{E}_j$ and $\mathcal{D}_j$, coordinating their actions using shared random bits. To estimate the expectation value $\mathrm{Tr}[O\mathcal{M}(\rho)]$, Bob will perform measurements at the output of the channel $\mathcal{N}$ and perform classical post-processing on the measurement outcomes. The protocol is successful if Bob's estimate deviates from the true value $\mathrm{Tr}[O\mathcal{M}(\rho)]$ by less than a given error tolerance ϵ, for every possible state ρ and for every possible observable O.

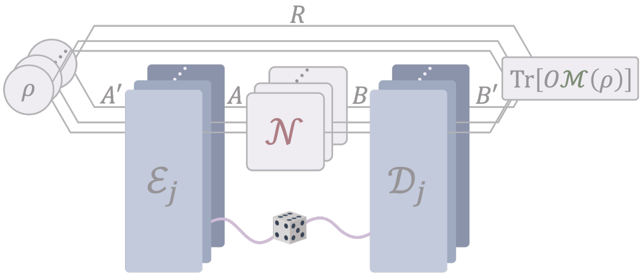


FIG. 1. **Shadow simulation of quantum channels.** A sender (Alice) and a receiver (Bob) are connected through a quantum channel $\mathcal{N}$. The task is to enable Bob to estimate the expectation value $\mathrm{Tr}[O\mathcal{M}(\rho)]$ of an arbitrary observable O on the output state $\mathcal{M}(\rho)$ produced by a target channel $\mathcal{M}$ when acting on an arbitrary input state ρ of a reference system R and a system A' in Alice's laboratory. To achieve this task, Alice and Bob can coordinate their operations $\mathcal{E}_j$ and $\mathcal{D}_j$ by sharing random bits.

Shadow simulation can be viewed as a generalization of the task of quantum channel simulation [4–10]. The crucial difference is that shadow simulation does not aim at reproducing the output states of a target channel, but only their "shadow information" [11, 12], *i.e.*, the information about the expectation values of all possible observables. This generalization is useful for quantum information processing in the noisy intermediate-scale quantum (NISQ) era [13], where classical post-processing of expectation values can be used to simulate larger quantum memories [14–17], probe properties of quantum systems [18–20], mitigate errors [1, 2, 21–24], and simulate unphysical operations [25–27].

Remarkably, we find that shadow simulation is not constrained by the limits of conventional channel simulation. For example, we show that one can perfectly shadow-simulate the transmission of an arbitrarily large number of qubits using only a single-qubit channel, a task that cannot be achieved in conventional channel simulation. In this example, the transmission of a larger number of qubits is simulated at the price of an increase of the number of samples needed to accurately estimate the expectation values. Quite surprisingly, we also find scenarios where shadow simulation achieves lower error than conventional channel simulation without any overhead in sampling cost, provided that Alice and Bob have access to no-signaling quantum resources. Overall, our results reveal that shared classical randomness and classical post-processing are valuable resources for quantum communication and other quantum technologies.

Framework: virtual supermaps. — In conventional quantum channel simulation, the aim is to simulate the action of a target channel $\mathcal{M}$ (with input A' and output B') by using an available channel $\mathcal{N}$ (with input A and output B). To convert channel $\mathcal{N}$ into an approximation of channel $\mathcal{M}$, Alice and Bob perform encoding and decoding channels $\mathcal{E}$ and $\mathcal{D}$ in their local laboratories, respectively, thus obtaining the new channel $\mathcal{D} \circ \mathcal{N} \circ \mathcal{E}$. In shadow simulation, instead, Bob can sample his decoding operation $\mathcal{D}$ from a set of channels $\{\mathcal{D}_j\}$ and, after the output has been measured, he can post-process the measurement statistics, taking arbitrary linear combinations of the outcome probabilities. In this way, Bob can effectively implement a linear map of the form $\widetilde{\mathcal{D}}= \sum_j \lambda_j \mathcal{D}_j$, where $\{\lambda_j\}$ are arbitrary real numbers [1, 18, 25, 28]. Note that in general $\widetilde{\mathcal{D}}$ is not a valid quantum channel (completely positive, trace-preserving map), but rather a virtual channel, described by a Hermitian-preserving and trace-scaling map [11, 29–32].

More generally, Bob may share classical randomness with Alice, and coordinate his local operations with hers, as in Figure 1. Hence, Bob's post-processing gives rise to linear maps of the form

$$\widetilde{\mathcal{S}}(\mathcal{N}) = \sum_j \lambda_j \mathcal{D}_j \circ \mathcal{N} \circ \mathcal{E}_j . \tag{1}$$

The linear map $\widetilde{\mathcal{S}}$ is an example of a supermap [33–35], that is, a map acting on the vector space spanned by quantum operations. Unlike most supermaps considered so far, however, $\widetilde{\mathcal{S}}$ generally does not transform quantum channels into quantum channels due to the possible presence of negative coefficients in the set $\{\lambda_j\}$. Instead, $\widetilde{\mathcal{S}}$ transforms Hermitian-preserving maps into Hermitian-preserving maps, and trace-scaling maps into trace-scaling maps with possibly different scaling factors. We call the supermaps with these two properties *virtual supermaps.*

Any virtual supermap $\widetilde{\mathcal{S}}$ is into one-to-one correspondence with a virtual bipartite processes $\widehat{\mathcal{S}}$ transforming operators on system $A'B$ into operators on system AB'. The correspondence can be made explicit by decomposing the action of the virtual supermap $\widetilde{\mathcal{S}}$ as $\widetilde{\mathcal{S}}(\mathcal{N}) = \sum_k \mathcal{B}_k \circ \mathcal{N} \circ \mathcal{A}_k$, where $\mathcal{A}_k$ and $\mathcal{B}_k$ are suitable linear maps, and by defining $\widehat{\mathcal{S}} := \sum_k \mathcal{A}_k \otimes \mathcal{B}_k$.

A virtual supermap $\widetilde{\mathcal{S}}$ of the special form (1) will be called a *(randomness-assisted) shadow simulation code.* For a shadow simulation code $\widetilde{\mathcal{S}}$, the corresponding virtual bipartite process is $\widehat{\mathcal{S}} := \sum_j \lambda_j \mathcal{E}_j \otimes \mathcal{D}_j$. It is rather straightforward to see that this virtual process is *no-signaling*, meaning that for every pair of operators $\rho_{A'}$ and ρ_B acting on A' and B, respectively, the operator $\mathsf{Tr}_{B'}[\widehat{\mathcal{S}}(\rho_{A'} \otimes \rho_B)]$ is independent of ρ_B, and the operator $\mathsf{Tr}_A[\widehat{\mathcal{S}}(\rho_{A'} \otimes \rho_B)]$ is independent of $\rho_{A'}$. The converse is less straightforward but turns out to be true, yielding a complete characterization of the randomness-assisted shadow simulation codes:

Theorem 1 *A virtual supermap $\widetilde{\mathcal{S}}$ is a randomness-assisted shadow simulation code if and only if the corresponding virtual process $\widehat{\mathcal{S}}$ is no-signaling.*

The proof is provided in Appendix A. An important consequence of Theorem 1 is that shared randomness and classical post-processing can be used to simulate arbitrary no-signaling resources. Explicitly, a no-signaling resource is represented by a quantum no-signaling channel $\widehat{\mathcal{S}}$ [36, 37] with input $A'B$ and output AB'. Using the no-signaling channel $\widehat{\mathcal{S}}$, Alice and Bob can implement the corresponding supermap $\widetilde{\mathcal{S}}$, which can be implemented using only shared randomness and classical post-processing, as guaranteed by Theorem 1. The same conclusion applies to protocols using local operations and shared entanglement, which is a special case of no-signaling resources.

No-signaling assisted shadow simulation.— Quantum no-signaling resources have been extensively studied in quantum Shannon theory [7, 10, 38]. We now extend their study to the task of shadow simulation. While in channel simulation Alice and Bob have the assistance of a fixed no-signaling channel, in shadow simulation they can more generally sample over a set of no-signaling channels $\{\widehat{\mathcal{S}}_j\}$. Using classical post-processing, they can reproduce the virtual supermap $\widetilde{\mathcal{S}} := \sum_j \lambda_j \widetilde{\mathcal{S}}_j$. We call this supermap a *no-signaling shadow simulation code.*

The randomization over different settings generally comes at the price of an increased sampling cost, meaning that more rounds of data collection are needed to estimate the desired expectation values [25–27]. To quantify this price, we define the *sampling cost* of the code $\widetilde{\mathcal{S}}$ as

$$c_{\text{smp}}\left(\widetilde{\mathcal{S}}\right) := \inf\Big\{p_+ + p_- \;\Big|\; \widehat{\mathcal{S}} = p_+ \widehat{\mathcal{S}}^+ - p_- \widehat{\mathcal{S}}^-, \\ p_\pm \in \mathbb{R}^+,\; \widehat{\mathcal{S}}^\pm \in \text{CPTP} \cap \text{NS}\Big\},$$

where CPTP and NS denote the set of completely positive, trace-preserving maps and the set of no-signaling virtual processes, respectively, and $\mathbb{R}^+$ is the set of non-negative real numbers. Note that every conventional channel simulation protocol has $c_{\rm smp}\left(\widetilde{\mathcal{S}}\right) = 1$, since the map $\widehat{\mathcal{S}}$ is a no-signaling channel. The sampling cost $c_{\rm smp}$ characterizes the range of post-processed measurement outcomes. Intuitively, a wider range requires more rounds of measurement to accurately estimate the expectation value. In Appendix A, we rigorously justify the definition of sampling cost using Hoeffding's inequality [39], which confirms this intuition.

To quantify the simulation error, we adopt the diamond-norm distance $\|\widetilde{\mathcal{S}}(\mathcal{N}) - \mathcal{M}\|_\diamond/2 =: p_{\rm err}(\widetilde{\mathcal{S}};\mathcal{N},\mathcal{M})$ [40], which is the same as the worst case error of measuring observables as we show in Appendix A. This error measure applies to conventional and shadow simulation, with the only difference that in the conventional scenario the no-signaling bipartite map $\widehat{\mathcal{S}}$ is completely positive and trace-preserving, while in the shadow simulation scenario $\widehat{\mathcal{S}}$ can be any Hermitian-preserving and trace-scaling map.

The optimal quantum limits to the task of shadow simulation can be quantified by two parameters. One is the minimum error achievable with sampling cost bounded by γ:

$$\varepsilon^*_{\gamma,\rm NS}(\mathcal{N},\mathcal{M}) := \inf_{\widehat{\mathcal{S}}\in \rm NS} \left\{ p_{\rm err}\left(\widetilde{\mathcal{S}};\mathcal{N},\mathcal{M}\right) \;\middle|\; c_{\rm smp}\left(\widetilde{\mathcal{S}}\right) \leq \gamma \right\}.$$

The other is the minimum sampling cost needed to guarantee that the error is below a given error tolerance ε:

$$\gamma^*_{\varepsilon,\rm NS}\left(\mathcal{N},\mathcal{M}\right) := \inf_{\widehat{\mathcal{S}}\in \rm NS} \left\{ c_{\rm smp}\left(\widetilde{\mathcal{S}}\right) \;\middle|\; p_{\rm err}\left(\widetilde{\mathcal{S}};\mathcal{N},\mathcal{M}\right) \leq \varepsilon \right\}.$$

Both quantities can be computed efficiently by semidefinite programs (SDPs) given in Appendix B. In the following, we illustrate the power of shadow simulation in three applications.

Shadow communication.— Quantum communication can be viewed as a special case of channel simulation: the simulation of an identity channel acting on a given number of qubits. Here we consider the zero-error scenario [7, 41–43], corresponding to an exact simulation of the identity channel. We define a zero-error shadow communication code $\widetilde{\mathcal{S}}$ as a supermap satisfying the condition $p_{\rm err}\left(\widetilde{\mathcal{S}};\mathcal{N},{\rm id}_d\right) = 0$, where ${\rm id}_d$ denotes the identity channel on a d-dimensional quantum system. Then, we define the one-shot zero-error shadow capacity assisted by no-signaling resources as

$$Q^{(1)}_{\gamma,\rm NS}(\mathcal{N}) := \sup_{d,\widehat{\mathcal{S}}\in \rm NS} \left\{ \log_2 d \;\middle|\; \widetilde{\mathcal{S}}(\mathcal{N}) = {\rm id}_d,\; c_{\rm smp}\left(\widetilde{\mathcal{S}}\right) \leq \gamma \right\}, \tag{2}$$

where the dimension d is optimized over positive integers. Here the term "one-shot" refers to the fact that the communication protocol only involves quantum operations on the inputs and outputs of a *single* use of channel $\mathcal{N}$. Note that $\widetilde{\mathcal{S}}$ is not a physical operations but a virtual one implemented as the average action across multiple rounds, where each round involves a single use of $\mathcal{N}$.

In Appendix C, we provide an explicit SDP expression for the shadow capacity for every given γ. This expression extends the previously known expression for the one-shot zero-error quantum capacity assisted by no-signaling resources [7, 44], which can be retrieved in the special case $\gamma = 1$.

For $\gamma > 1$, we show that the zero-error shadow capacity is generally larger than the zero-error quantum capacity. A concrete example is provided by the following theorem:

Theorem 2 *Let $\mathcal{N}_{{\rm depo},p}(\rho) = p\rho + (1-p)\mathbb{1}_2/2$ be a single-qubit depolarizing channel, where $p \in [0,1]$ is a probability and $\mathbb{1}_2$ is the identity operator on $\mathbb{C}^2$. For $\gamma \geq 1$, the one-shot zero-error shadow capacity assisted by no-signaling resources is*

$$Q^{(1)}_{\gamma,\rm NS}(\mathcal{N}_{{\rm depo},p}) = \log_2 \left\lfloor \sqrt{2p\gamma + p + 1} \right\rfloor. \tag{3}$$

Eq. (3) shows that the shadow capacity can become arbitrarily large as γ grows, provided that the channel is not completely depolarizing ($p \neq 0$). In other words, a qubit depolarizing channel can be used to transmit the expectation values of all observables on a quantum system of arbitrarily high dimension, at the price of an increased sampling cost.

It is useful to compare the above finding with the existing results about error mitigation. Error mitigation protocols, such as those in Refs. [25, 45], can be used to transmit arbitrary expectation values *on a single-qubit state* through repeated uses of a single-qubit depolarizing channel. This fact is interesting because, for $p \leq 1/3$, the depolarizing channel is entanglement-breaking [46] and therefore it cannot reliably transmit quantum states, even if infinitely many copies of it are available. Theorem 2 takes this observation to a much stronger level: not only can a qubit depolarizing channel transmit all expectation values for a single qubit, but also it can transmit the expectation values on arbitrarily high-dimensional quantum systems.

Now, recall that Theorem 1 guarantees that every no-signaling code can be simulated with local operations and shared classical randomness, generally at the expense of a larger sampling cost. Combining this fact with Theorem 2, we obtain that randomness-assisted shadow simulation codes can have arbitrarily large capacity for sufficiently large values of the sampling cost. The same argument applies to shadow simulation codes assisted by shared entanglement. Remarkably, these phenomena are not limited to the depolarizing channel, but apply in general to every quantum channel achieving at least one non-zero value of the zero-error no-signaling assisted shadow

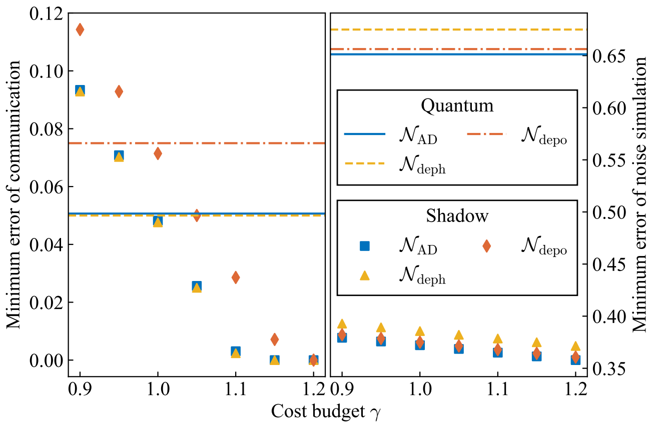


FIG. 2. Minimum error of shadow simulation of common channels under different budgets for sampling cost. The channels we consider here are the amplitude damping channel, the dephasing channel, and the depolarizing channel at a low noise level ($p = 0.9$). For communication (left), single-qubit versions of these channels are studied, and the goal is to simulate a qubit identity channel id_2. For noise simulation (right), we consider simulating two-qubit versions of the noisy channels via id_2, where by a two-qubit amplitude damping channel we mean two single-qubit amplitude damping channels acting independently on two qubits. Compared with that of conventional quantum channel simulation (horizontal lines), the minimum error in the shadow case is smaller with the same or even lower cost budget.

capacity (2). The proof of this fact will be provided at the end of the next section.

Shadow simulation via noiseless channels.— The dual task to communication is the simulation of a target noisy channel using a noiseless channel. In this case, the key quantity is the simulation cost, defined as the number of noiseless qubits that must be sent from the sender to a receiver. In the context of zero-error shadow simulation assisted by no-signaling resources, we define the one-shot shadow simulation cost of channel $\mathcal{M}$ as

$$S^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{M}) := \inf_{d,\widetilde{\mathcal{S}}\in\mathrm{NS}} \left\{ \log_2 d \;\middle|\; \widetilde{\mathcal{S}}(\mathrm{id}_d) = \mathcal{M},\ c_{\mathrm{smp}}\left(\widetilde{\mathcal{S}}\right) \leq \gamma \right\},$$

where the dimension d is optimized over positive integers. This quantity generalizes the one-shot zero-error simulation cost studied in the conventional quantum channel simulation scenario [7, 10]. In Appendix D, we provide an SDP for the zero-error shadow simulation cost, and we show that the simulation cost can generally be reduced by increasing the sampling cost.

Besides simulating noisy channels, shadow simulation also allows simulating high-dimensional noiseless channels using low-dimensional ones. This shadow simulation can also be viewed as a form of quantum compression, where the goal is to store the expectation values of all possible observables. Alternatively, one can view this shadow simulation as the simulation of a high-dimensional quantum measurement using a low-dimensional one. Differing from previous works that aimed at the simulation of the full measurement statistics [47], however, shadow simulation focuses on the expectation values.

The minimum sampling cost for simulating a higher-dimensional identity channel is provided by the following theorem:

Theorem 3 *Given identity channels* id_d *and* $\mathrm{id}_{d'}$ *with* $d' \geq d \geq 2$, *the minimum sampling cost of an exact shadow simulation of* $\mathrm{id}_{d'}$ *using* id_d *and no-signaling resources is*

$$\gamma^*_{0,\mathrm{NS}}\left(\mathrm{id}_d, \mathrm{id}_{d'}\right) = 2\left(\frac{d'}{d}\right)^2 - 1. \tag{4}$$

Theorem 3 has two important implications. First, it implies that the shadow simulation cost of every quantum channel can be lowered to 1 by allowing a sufficiently large sampling overhead. Indeed, let $\mathcal{M}$ be a quantum channel with one-shot zero-error quantum simulation cost $S^{(1)}_{\mathrm{NS}}(\mathcal{M}) = \log_2 d'$, meaning that $\mathcal{M}$ can be simulated using $\mathrm{id}_{d'}$ through a quantum no-signaling code. In turn, Eq. (4) implies that $\mathrm{id}_{d'}$ can be shadow-simulated using a qubit identity channel, with a sampling cost $(d'^2-2)/2$. Composing the two simulations, one then gets a shadow simulation of $\mathcal{M}$ from id_2 with sampling cost $(d'^2-2)/2$.

Second, Theorem 3 implies that every channel $\mathcal{N}$ with non-zero shadow capacity $Q^{(1)}_{\gamma,\mathrm{NS}}$ for some γ can shadow-simulate every other channel $\mathcal{M}$. In particular, it can simulate an identity channel on arbitrarily many qubits. This observation generalizes the result of Theorem 2 for single-qubit depolarizing channels.

Achieving lower error without sampling overhead.— In the zero-error scenario, we have seen that the shadow capacity and shadow simulation cost coincide with the conventional capacity and simulation cost for $\gamma = 1$. In stark contrast, we now show that in the approximate scenario, shadow simulation can achieve lower error than conventional channel simulation even if $\gamma = 1$, that is, without incurring a sampling overhead. As examples, we consider three common quantum channels: the single-qubit amplitude damping channel $\mathcal{N}_{\mathrm{AD}}$ with two Kraus operators $|0\rangle\langle 0| + \sqrt{p}|1\rangle\langle 1|$ and $\sqrt{1-p}|0\rangle\langle 1|$, the dephasing channel $\mathcal{N}_{\mathrm{deph}}(\cdot) = p(\cdot) + (1-p)\mathrm{diag}(\cdot)$, and the depolarizing channel $\mathcal{N}_{\mathrm{depo}}(\cdot) = p(\cdot) + (1-p)\mathsf{Tr}[\cdot]\mathbb{1}_d/d$. For each channel, the parameter $p \in [0,1]$ indicates the level of the noise. For the depolarizing channel, the parameter d represents the dimension of the system on which they act, and $\mathbb{1}_d$ is the d-dimensional identity operator.

Figure 2 shows the minimum errors in both shadow communication and noisy channel simulation at different cost budgets ranging from 0.9 to 1.2. Surprisingly, shadow simulation codes achieve a smaller error at the same or even a lower level of cost compared with quantum simulation codes, whose sampling cost is 1. The difference is more evident in the plot of noise simulation, where the minimum error of quantum codes is almost the twice of the shadow simulation codes. This implies that classical post-processing can enhance the transmission of expectation values even if no sampling overhead is involved. The underlying reason can be attributed to the existence of a virtual channel simulable by a unit-cost shadow simulation code that is closer to the target channel than all quantum channels simulable by quantum simulation codes.

Conclusions.— In this paper, we introduced the task of shadow simulation of quantum channels, showing that transmitting and processing expectation values of arbitrary observables is generally a less demanding task than transmitting and processing quantum states. Besides their foundational interest, our results are relevant to practical applications to NISQ quantum technologies, as they provide more efficient schemes for measuring observables at the output of noisy quantum devices. An interesting direction of future research is to explore scenarios where only a given set of physically relevant observables is concerned [12, 19]. Our results also open up a systematic way to study new quantum protocols that sample over different transformations of quantum processes, known as quantum supermaps [33–35].

ACKNOWLEDGMENTS

We thank Yin Mo and Chengkai Zhu for useful comments that helped us improve the manuscript. This work has been supported by the Hong Kong Research Grant Council through grants 17307520 and R7035-21F, and by the John Templeton Foundation through grant 62312, The Quantum Information Structure of Spacetime (qiss.fr). The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. Research at the Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation and Science. Xin Wang was supported by the Start-up Fund from The Hong Kong University of Science and Technology (Guangzhou), the Guangdong Quantum Science and Technology Strategic Fund (Grant No. GDZX2303007), and the Education Bureau of Guangzhou Municipality.

* xqzhao7@connect.hku.hk
† felixxinwang@hkust-gz.edu.cn
‡ giulio@cs.hku.hk

[1] K. Temme, S. Bravyi, and J. M. Gambetta, Physical Review Letters **119**, 180509 (2017).
[2] Y. Li and S. C. Benjamin, Physical Review X **7**, 021050 (2017).
[3] S. Endo, S. C. Benjamin, and Y. Li, Physical Review X **8**, 031027 (2018).
[4] D. Kretschmann and R. F. Werner, New Journal of Physics **6**, 26 (2004).
[5] M. Berta, M. Christandl, and R. Renner, Communications in Mathematical Physics **306**, 579 (2011).
[6] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, IEEE Transactions on Information Theory **60**, 2926 (2014).
[7] R. Duan and A. Winter, IEEE Transactions on Information Theory **62**, 891 (2015).
[8] D. Leung and W. Matthews, IEEE Transactions on Information Theory **61**, 4486 (2015).
[9] X. Wang, W. Xie, and R. Duan, IEEE Transactions on Information Theory **64**, 640 (2018).
[10] K. Fang, X. Wang, M. Tomamichel, and M. Berta, IEEE Transactions on Information Theory **66**, 2129 (2019).
[11] X. Zhao, B. Zhao, Z. Xia, and X. Wang, Quantum **7**, 978 (2023).
[12] S. Aaronson, in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing* (2018) pp. 325–338.
[13] J. Preskill, Quantum **2**, 79 (2018).
[14] S. Bravyi, G. Smith, and J. A. Smolin, Physical Review X **6**, 021043 (2016).
[15] T. Peng, A. W. Harrow, M. Ozols, and X. Wu, Physical Review Letters **125**, 150504 (2020).
[16] K. Mitarai and K. Fujii, Quantum **5**, 388 (2021).
[17] C. Piveteau and D. Sutter, IEEE Transactions on Information Theory (2023), 10.1109/TIT.2023.3310797.
[18] F. Buscemi, M. Dall'Arno, M. Ozawa, and V. Vedral, arXiv:1312.4240 (2013).
[19] H.-Y. Huang, R. Kueng, and J. Preskill, Nature Physics **16**, 1050 (2020).
[20] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, Nature Reviews Physics **5**, 9 (2023).
[21] C. Piveteau, D. Sutter, S. Bravyi, J. M. Gambetta, and K. Temme, Physical Review Letters **127**, 200505 (2021).
[22] M. Lostaglio and A. Ciani, Physical Review Letters **127**, 200506 (2021).
[23] Y. Suzuki, S. Endo, K. Fujii, and Y. Tokunaga, PRX Quantum **3**, 010345 (2022).
[24] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, arXiv:2210.00921 (2022).
[25] J. Jiang, K. Wang, and X. Wang, Quantum **5**, 600 (2021).
[26] B. Regula, R. Takagi, and M. Gu, Quantum **5**, 522 (2021).
[27] X. Zhao, L. Zhang, B. Zhao, and X. Wang, arXiv:2309.09963 (2023).
[28] C. Piveteau, D. Sutter, and S. Woerner, npj Quantum Information **8**, 12 (2022).
[29] X. Yuan, B. Regula, R. Takagi, and M. Gu, Physical Review Letters **132**, 050203 (2024).
[30] A. J. Parzygnat, J. Fullwood, F. Buscemi, and G. Chiribella, arXiv:2310.13049 (2023).

[31] H. Yao, X. Liu, C. Zhu, and X. Wang, arXiv:2310.15156 (2023).

[32] Y.-A. Chen, C. Zhu, K. He, M. Jing, and X. Wang, arXiv:2312.02031 (2023).

[33] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Europhysics Letters **83**, 30004 (2008).

[34] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Physical Review A **80**, 022339 (2009).

[35] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Physical Review A **88**, 022318 (2013).

[36] M. Piani, M. Horodecki, P. Horodecki, and R. Horodecki, Physical Review A **74**, 012305 (2006).

[37] G. Chiribella, Physical Review A **86**, 040301 (2012).

[38] D. Leung and W. Matthews, IEEE Transactions on Information Theory **61**, 4486 (2015).

[39] W. Hoeffding, in *The Collected Works of Wassily Hoeffding* (Springer, 1994) pp. 409–426.

[40] A. Y. Kitaev, Russian Mathematical Surveys **52**, 1191 (1997).

[41] C. Shannon, IRE Transactions on Information Theory **2**, 8 (1956).

[42] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, IEEE Transactions on Information Theory **57**, 5509 (2011).

[43] X. Wang and R. Duan, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, 2016) pp. 2244–2248.

[44] X. Wang and R. Duan, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, 2016) pp. 1690–1694.

[45] R. Takagi, Physical Review Research **3**, 033178 (2021).

[46] M. Horodecki, P. W. Shor, and M. B. Ruskai, Reviews in Mathematical Physics **15**, 629 (2003).

[47] M. Ioannou, P. Sekatski, S. Designolle, B. D. Jones, R. Uola, and N. Brunner, Physical Review Letters **129**, 190401 (2022).

[48] A. Jamiołkowski, Reports on Mathematical Physics **3**, 275 (1972).

[49] M.-D. Choi, Linear Algebra and Its Applications **10**, 285 (1975).

[50] G. Gutoski, Quantum Information & Computation **9**, 739 (2009).

[51] J. Watrous, Theory of Computing **5**, 217 (2009).

[52] S. Khatri and M. M. Wilde, arXiv:2011.04672 (2020).

[53] E. M. Rains, IEEE Transactions on Information Theory **47**, 2921 (2001).

Appendix A: Shadow Simulation Codes

A quantum simulation code $(\mathcal{E}_{A'\to A}, \mathcal{D}_{B\to B'})$ can be written as a quantum supermap [33], which sends a quantum channel $\mathcal{N}_{A\to B}$ to another quantum channel $\mathcal{M}_{A'\to B'}$. Each quantum supermap is associated with a bipartite quantum operation that is no-signaling from Bob to Alice, *i.e.*, no transmission of information from Bob to Alice. In the setting of shadow simulation of quantum channels, simulation codes are not restricted to quantum supermaps. A shadow simulation code allows classical post-processing so that its encoding and decoding parts do not have to be quantum channels. For example, one can consider the encoding operation $\widetilde{\mathcal{E}}_{A'\to A} := \sum_j \lambda_j \mathcal{E}_{j,A'\to A}$ and the decoding operation $\widetilde{\mathcal{D}}_{B\to B'} := \sum_k \mu_k \mathcal{D}_{k,B\to B'}$ with real coefficients λ_j, μ_k and quantum channels $\mathcal{E}_{j,A'\to A}, \mathcal{D}_{k,B\to B'}$. The expectation value with respect to the state transmitted through a quantum channel $\mathcal{N}_{A\to B}$ using this shadow simulation code $\left(\widetilde{\mathcal{E}}_{A'\to A}, \widetilde{\mathcal{D}}_{B\to B'}\right)$ can be decomposed as

$$\mathrm{Tr}\left[\widetilde{\mathcal{D}}_{B\to B'} \circ \mathcal{N}_{A\to B} \circ \widetilde{\mathcal{E}}_{A'\to A}(\rho_{RA'}) O_{RB'}\right] = \sum_{j,k} \lambda_j \mu_k \mathrm{Tr}\left[\mathcal{D}_{k,B\to B'} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}_{j,A'\to A}(\rho_{RA'}) O_{RB'}\right]. \tag{A1}$$

Hence, although we cannot directly implement $\widetilde{\mathcal{E}}_{A'\to A}$ and $\widetilde{\mathcal{D}}_{B\to B'}$, we can simulate their effect by sending copies of the state using quantum simulation codes sampled from $\{(\mathcal{E}_{j,A'\to A}, \mathcal{D}_{k,B\to B'})\}$ for multiple rounds and then post-processing the measurement results from all rounds.

Though the encoding operation $\widetilde{\mathcal{E}}$ and the decoding operation $\widetilde{\mathcal{D}}$ are seemingly independent, it is important to note that both maps are implemented with classical post-processing, which only happens at Bob's side after Bob completes the measurement. Therefore, Bob needs information on Alice's sampled operation in each round to guide the post-processing. Hence, we consider simulation codes where Alice and Bob have pre-shared randomness, and such codes are realized by the following steps:

1. Alice randomly samples one encoding channel $\mathcal{E}_{\alpha,A'\to A}$ from the set of channels $\{\mathcal{E}_{j,A'\to A}\}$ with a probability distribution $\Pr(\mathcal{E}_{j,A'\to A}) = |\lambda_j|/\gamma$, where $\gamma = \sum_j |\lambda_j|$, and applies the sampled channel to state $\rho_{RA'}$.

2. Alice then sends the post-encoding state $\mathcal{E}_{\alpha,A'\to A}(\rho_{RA'})$ into the noisy channel $\mathcal{N}_{A\to B}$.

3. Upon receiving the state $\mathcal{N}_{A\to B} \circ \mathcal{E}_{\alpha,A'\to A}(\rho_{RA'})$ coming out of the noisy channel, Bob applies the decoding channel $\mathcal{D}_{\alpha,B\to B'}$ to the received state, where the value α is known to Bob due to the classical randomness shared between him and Alice.

4. Bob measures the decoded state $\mathcal{D}_{\alpha,B\to B'} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}_{\alpha,A'\to A}(\rho_{RA'})$ with an observable $O_{RB'}$, which gives a measurement outcome o.

5. Repeat the above steps for M times, and denote the index α and the measurement outcome o in the m-th round by α_m and o_m, respectively. Then, compute $\xi := \frac{\gamma}{M}\sum_{m=1}^{M}\operatorname{sgn}(\lambda_{\alpha_m})o_m$ as the communicated expectation value, where sgn is the sign function.

This protocol offers an unbiased estimator ξ for the desired expectation value $\mathsf{Tr}\left[\left(\widetilde{\mathcal{S}}\left(\mathcal{N}\right)\right)(\rho)O\right]$, where $\widetilde{\mathcal{S}}$ is a virtual supermap representing a randomness-assisted shadow simulation code whose action on $\mathcal{N}_{A\to B}$ is

$$\widetilde{\mathcal{S}}(\mathcal{N})_{A'\to B'} = \sum_j \lambda_j \mathcal{D}_{j,B\to B'} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}_{j,A'\to A}. \tag{A2}$$

This can be seen by checking the expectation value of ξ:

$$\begin{aligned}
\mathbb{E}\left[\xi\right] &= \frac{\gamma}{M}\sum_{m=1}^{M}\mathbb{E}\left[\operatorname{sgn}(\lambda_{\alpha_m})o_m\right] && \text{(A3)}\\
&= \frac{\gamma}{M}\sum_{m=1}^{M}\sum_j \frac{|\lambda_j|}{\gamma}\operatorname{sgn}(\lambda_j)\mathsf{Tr}\left[\mathcal{D}_j\circ\mathcal{N}\circ\mathcal{E}_j(\rho)O\right] && \text{(A4)}\\
&= \frac{1}{M}\sum_{m=1}^{M}\sum_j \lambda_j\mathsf{Tr}\left[\mathcal{D}_j\circ\mathcal{N}\circ\mathcal{E}_j(\rho)O\right] && \text{(A5)}\\
&= \mathsf{Tr}\left[\sum_j \lambda_j\mathcal{D}_j\circ\mathcal{N}\circ\mathcal{E}_j(\rho)O\right] && \text{(A6)}\\
&= \mathsf{Tr}\left[\left(\widetilde{\mathcal{S}}(\mathcal{N})\right)(\rho)O\right]. && \text{(A7)}
\end{aligned}$$

Each supermap is associated with a bipartite map, and for a randomness-assisted shadow simulation code in Eq. (A2), its corresponding bipartite map is

$$\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_j \lambda_j \mathcal{E}_{j,A'\to A}\otimes\mathcal{D}_{j,B\to B'}. \tag{A8}$$

It is clear that every randomness-assisted shadow simulation code is associated with a Hermitian-preserving bipartite map. This is because the Choi operator of the associated bipartite map is Hermitian, and a map is Hermitian-preserving if and only if its Choi operator is Hermitian. In the following, we show that bipartite maps associated with randomness-assisted shadow simulation codes, besides being Hermitian-preserving, are also no-signaling. For a bipartite map $\widehat{\mathcal{S}}_{A'B\to AB'}$, being no-signaling from Bob to Alice means that the output state at A is independent of the input state at B, *i.e.*, $\mathsf{Tr}_{B'}\circ\widehat{\mathcal{S}}_{A'B\to AB'} = \widehat{\mathcal{S}}_{A'\to A}\circ\mathsf{Tr}_B$, where $\widehat{\mathcal{S}}_{A'\to A}$ is the local effective operation of the map $\widehat{\mathcal{S}}_{A'B\to AB'}$ from A to A'. By the Choi-Jamiołkowski isomorphism [48, 49], we can uniquely represent $\widehat{\mathcal{S}}_{A'B\to AB'}$ using its Choi operator $J^{\widehat{\mathcal{S}}}_{A'BAB'} := \mathrm{id}_{A'B}\otimes\widehat{\mathcal{S}}_{\bar{A}'\bar{B}\to AB'}(|\Gamma\rangle\langle\Gamma|_{A'B\bar{A}'\bar{B}})$, where $|\Gamma\rangle_{A'B\bar{A}'\bar{B}} := \sum_{j=0}^{d_{A'B}-1}|j\rangle_{A'B}|j\rangle_{\bar{A}'\bar{B}}$ is the unnormalized maximally entangled state, $d_{A'B}$ is the dimension of the system $A'B$, and the Hilbert space associated with the system $\bar{A}'\bar{B}$ is isomorphic to that of $A'B$. In terms of the map's Choi operator, no-signaling from Bob to Alice means $\mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = J^{\widehat{\mathcal{S}}}_{A'A}\otimes\mathbb{1}_B$, where $J^{\widehat{\mathcal{S}}}_{A'A} := \mathsf{Tr}_{BB'}[J^{\widehat{\mathcal{S}}}_{A'BAB'}]/d_B$.

Theorem 1 shows that randomness-assisted shadow simulation codes are equivalent to Hermitian-preserving no-signaling bipartite maps, which is both no-signaling from Bob to Alice and no-signaling from Alice to Bob.

Theorem 1 *A virtual supermap $\widetilde{\mathcal{S}}$ is a randomness-assisted shadow simulation code if and only if the corresponding virtual process $\widehat{\mathcal{S}}$ is no-signaling.*

Proof For the "only if" part, let $\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_j \lambda_j\mathcal{M}^{(j)}_{A'\to A}\otimes\mathcal{N}^{(j)}_{B\to B'}$ denote a bipartite map associated with an arbitrary randomness-assisted code, where $\mathcal{M}^{(j)}_{A'\to A}$ and $\mathcal{N}^{(j)}_{B\to B'}$ are quantum channels. It is clear that the Choi operator $J^{\widehat{\mathcal{S}}}_{A'BAB'} = \sum_j \lambda_j J^{\mathcal{M}^{(j)}}_{A'A}\otimes J^{\mathcal{N}^{(j)}}_{BB'}$ is Hermitian, indicating that $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving. Furthermore, as $\mathcal{M}^{(j)}_{A'\to A}$ and $\mathcal{N}^{(j)}_{B\to B'}$ are trace-preserving, *i.e.*, $\mathsf{Tr}_A\left[J^{\mathcal{M}^{(j)}}_{A'A}\right] = \mathbb{1}_{A'}$ and $\mathsf{Tr}_{B'}\left[J^{\mathcal{N}^{(j)}}_{BB'}\right] = \mathbb{1}_B$, we have

$$\mathsf{Tr}_A\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = \sum_j \lambda_j\mathsf{Tr}_A\left[J^{\mathcal{M}^{(j)}}_{A'A}\right]\otimes J^{\mathcal{N}^{(j)}}_{BB'} = \mathbb{1}_{A'}\otimes\sum_j \lambda_j J^{\mathcal{N}^{(j)}}_{BB'} \tag{A9}$$

and

$$\mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right]=\sum_j \lambda_j J^{\mathcal{M}^{(j)}}_{A'A}\otimes \mathsf{Tr}_{B'}\left[J^{\mathcal{N}^{(j)}}_{BB'}\right]=\sum_j \lambda_j J^{\mathcal{M}^{(j)}}_{A'A}\otimes \mathbb{1}_B, \tag{A10}$$

which imply that $\widehat{\mathcal{S}}_{A'B\to AB'}$ is no-signaling.

For the “if” part, we first assume that $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving and no-signaling. By Theorem 14 in Ref. [50], its Choi operator can be decomposed as

$$J^{\widehat{\mathcal{S}}}_{A'BAB'}=\sum_j \lambda_j M^{(j)}_{A'A}\otimes N^{(j)}_{BB'}, \tag{A11}$$

where, for each j, λ_j is a real number, and $M^{(j)}_{A'A}$ and $N^{(j)}_{BB'}$ are Hermitian operators such that $\mathsf{Tr}_A\left[M^{(j)}_{A'A}\right]$ and $\mathsf{Tr}_{B'}\left[N^{(j)}_{BB'}\right]$ are proportional to the identity operators $\mathbb{1}_{A'}$ and $\mathbb{1}_B$, respectively. In other words, we can treat $M^{(j)}_{A'A}$ and $N^{(j)}_{BB'}$ as Choi operators for some Hermitian-preserving and trace-scaling (HPTS) maps $\widetilde{\mathcal{M}}^{(j)}_{A'\to A}$ and $\widetilde{\mathcal{N}}^{(j)}_{B\to B'}$, respectively. Here, trace-scaling means that the map scales the trace of the input operator with a constant factor.

According to Lemma 6 in Ref. [11], every HPTS map can be written as a linear combination of two quantum channels. Thus, we can write $\widehat{\mathcal{S}}_{A'B\to AB'}$ as

$$\begin{aligned}\widehat{\mathcal{S}}_{A'B\to AB'}&=\sum_j \lambda_j\widetilde{\mathcal{M}}^{(j)}_{A'\to A}\otimes\widetilde{\mathcal{N}}^{(j)}_{B\to B'} &\text{(A12)}\\ &=\sum_j \lambda_j\left(m_1\mathcal{M}^{(j,1)}_{A'\to A}+m_2\mathcal{M}^{(j,2)}_{A'\to A}\right)\otimes\left(n_1\mathcal{N}^{(j,1)}_{B\to B'}+n_2\mathcal{N}^{(j,2)}_{B\to B'}\right) &\text{(A13)}\\ &=\sum_j\sum_{k=1}^{2}\sum_{l=1}^{2}\lambda_j m_k n_l\mathcal{M}^{(j,k)}_{A'\to A}\otimes\mathcal{N}^{(j,l)}_{B\to B'}, &\text{(A14)}\end{aligned}$$

which represents a randomness-assisted shadow simulation code. ■

Alternative to pre-shared classical randomness, forward classical communication from Alice to Bob also allows Bob to acquire information on Alice’s local operation in each round. A shadow simulation protocol with the assistance of forward classical communication is represented by a bipartite linear map

$$\widehat{\mathcal{S}}_{A'B\to AB'}=\sum_j \lambda_j\mathcal{M}^{(j)}_{A'\to A}\otimes\mathcal{N}^{(j)}_{B\to B'}, \tag{A15}$$

where $\left\{\mathcal{M}^{(j)}_{A'\to A}\right\}_j$ is a quantum instrument, $\left\{\mathcal{N}^{(j)}_{B\to B'}\right\}_j$ is a collection of quantum channels, and each λ_j is a real coefficient. In the following proposition, we show that not only $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving and one-way no-signaling, but any one-way no-signaling Hermitian-preserving bipartite map represents a forward-classical-assisted shadow simulation code. For completeness, we also consider shadow simulation codes assisted by two-way classical communication, where both $\left\{\mathcal{M}^{(j)}_{A'\to A}\right\}_j$ and $\left\{\mathcal{N}^{(j)}_{B\to B'}\right\}_j$ are quantum instruments. Such codes are equivalent to the set of all bipartite Hermitian-preserving maps.

Theorem 4 *Consider a bipartite linear map $\widehat{\mathcal{S}}_{A'B\to AB'}$. It is Hermitian-preserving if and only if it corresponds to a shadow simulation code assisted by two-way classical communication. It is Hermitian-preserving and B-to-A no-signaling if and only if it corresponds to a forward-classical-assisted shadow simulation code.*

This theorem tells us that shadow simulation codes with one-way classical communication are powerful enough to simulate arbitrary quantum channels and even beyond. An intuitive explanation is that Alice can measure the initial state ρ with an informationally complete POVM and communicate the measurement outcomes to Bob so that Bob is able to reconstruct the expectation value of every observable on ρ transformed by any channel. Now, we prove this theorem by proving the following two lemmas.

Lemma 5 *A bipartite linear map $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving and B-to-A no-signaling if and only if it corresponds to a forward-classical-assisted shadow simulation code.*

Proof The "if" direction is straightforward. Let $\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_j \lambda_j \mathcal{M}^{(j)}_{A'\to A} \otimes \mathcal{N}^{(j)}_{B\to B'}$ represent a forward-classical-assisted shadow simulation code, where each $\left\{\mathcal{M}^{(j)}_{A'\to A}\right\}_j$ is a quantum instrument, and each $\mathcal{N}^{(j)}_{B\to B'}$ is a quantum channel. Then, the Choi operator of $\widehat{\mathcal{S}}_{A'B\to AB'}$ is

$$J^{\widehat{\mathcal{S}}}_{A'BAB'} = \sum_j \lambda_j J^{\mathcal{M}^{(j)}}_{A'A} \otimes J^{\mathcal{N}^{(j)}}_{BB'} . \tag{A16}$$

Clearly, $J^{\widehat{\mathcal{S}}}_{A'BAB'}$ is a Hermitian operator, indicating that $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving. In addition, $\widehat{\mathcal{S}}_{A'B\to AB'}$ is no-signaling from Bob to Alice as

$$\mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = \sum_j \lambda_j J^{\mathcal{M}^{(j)}}_{A'A} \otimes \mathsf{Tr}_{B'}\left[J^{\mathcal{N}^{(j)}}_{BB'}\right] = \sum_j \lambda_j J^{\mathcal{M}^{(j)}}_{A'A} \otimes \mathbb{1}_B \tag{A17}$$

due to $\mathcal{N}$ being trace-preserving.

For the "only if" direction, part of the proof is adapted from the proof of Theorem 14 in Ref. [50]. Let $\widehat{\mathcal{S}}_{A'B\to AB'}$ be a Hermitian-preserving supermap and $\left\{M^{(1)}_{A'A}, \ldots, M^{(D)}_{A'A}\right\}$ be a basis for the Hermitian operator space Herm$\,(A'A)$ on the system $A'A$, where D is the dimension of this space. Then, there exists a unique set of Hermitian operators $\left\{N^{(1)}_{BB'}, \ldots, N^{(D)}_{BB'}\right\} \subseteq$ Herm$\,(BB')$ such that $J^{\widehat{\mathcal{S}}}_{A'BAB'} = \sum_{j=1}^D M^{(j)}_{A'A} \otimes N^{(j)}_{BB'}$. For each j, let $H^{(j)}_{A'A}$ be a Hermitian operator such that $\mathsf{Tr}\left[H^{(j)}_{A'A} M^{(k)}_{A'A}\right] \neq 0$ if and only if $j = k$. Denoting the mapping $M_{A'A} \mapsto \mathsf{Tr}\left[H^{(j)}_{A'A} M^{(k)}_{A'A}\right]$ by $h^{(j)}(M_{A'A})$, we have

$$\left(h^{(j)} \otimes \mathrm{id}_{BB'}\right)\left(J^{\widehat{\mathcal{S}}}_{A'BAB'}\right) = \sum_{k=1}^D h^{(j)}\left(M^{(k)}_{A'A}\right) \otimes N^{(k)}_{BB'} = h^{(j)}\left(M^{(j)}_{A'A}\right) N^{(j)}_{BB'} . \tag{A18}$$

Because $\widehat{\mathcal{S}}_{A'B\to AB'}$ is no-signaling from Bob to Alice, we have $\mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = J^{\widehat{\mathcal{S}}}_{A'A} \otimes \mathbb{1}_B$. Then,

$$\left(h^{(j)} \otimes \mathrm{id}_{BB'}\right) \mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = h^{(j)}\left(J^{\widehat{\mathcal{S}}}_{A'A}\right) \otimes \mathbb{1}_B = h^{(j)}\left(M^{(j)}_{A'A}\right) \mathsf{Tr}_{B'}\left[N^{(j)}_{BB'}\right] , \tag{A19}$$

where the second equality holds because the order of applying $\left(h^{(j)} \otimes \mathrm{id}_{BB'}\right)$ and $\mathsf{Tr}_{B'}$ does not affect the result as they act on different subspaces.

It follows from Eq. (A19) that, for each j, $\mathsf{Tr}_{B'}\left[N^{(j)}_{BB'}\right]$ is proportional to the identity operator $\mathbb{1}_B$, and thus it serves as a Choi operator of an HPTS map, which we denote by $\widetilde{\mathcal{N}}^{(j)}_{B\to B'}$. According to Lemma 6 in Ref. [11], each $\widetilde{\mathcal{N}}^{(j)}_{B\to B'}$ can be written as a linear combination of two quantum channels, *i.e.*,

$$\widetilde{\mathcal{N}}^{(j)}_{B\to B'} = n_{j,1} \mathcal{N}^{(j,1)}_{B\to B'} + n_{j,2} \mathcal{N}^{(j,2)}_{B\to B'} , \tag{A20}$$

where $n_{j,1}$ and $n_{j,2}$ are real numbers and $\mathcal{N}^{(j,1)}_{B\to B'}$ and $\mathcal{N}^{(j,2)}_{B\to B'}$ are quantum channels.

For each Hermitian operator $M^{(j)}_{A'A}$, we can write it as the difference of two positive semidefinite operators, say, $m_{j,1} M^{(j,1)}_{A'A} - m_{j,2} M^{(j,2)}_{A'A}$, where $m_{j,1} M^{(j,1)}_{A'A}$ and $m_{j,2} M^{(j,2)}_{A'A}$ are positive semidefinite and $m_{j,1}$ and $m_{j,2}$ are positive real numbers so that $\mathsf{Tr}_A\left[M^{(j,1)}_{A'A}\right] \leq \mathbb{1}_{A'}$ and $\mathsf{Tr}_A\left[M^{(j,2)}_{A'A}\right] \leq \mathbb{1}_{A'}$. In other words, both $M^{(j,1)}_{A'A}$ and $M^{(j,2)}_{A'A}$ are Choi operators of some completely positive and trace-non-increasing (CPTN) maps, say $\mathcal{M}^{(j,1)}_{A'\to A}$ and $\mathcal{M}^{(j,2)}_{A'\to A}$, respectively. Moreover, the scalars $m_{j,1}$ and $m_{j,2}$ should be chosen so that $\sum_{j=1}^D \sum_{k=1}^2 \mathsf{Tr}_A\left[M^{(j,k)}_{A'A}\right] \leq \mathbb{1}_{A'}/2$. We will see the reason of this requirement later.

Combining the decomposition of every $M^{(j)}_{A'A}$ and every $N^{(j)}_{BB'}$, we have

$$\mathcal{S}_{A'B\to AB'} = \sum_{j=1}^{D} \left(m_{j,1}\mathcal{M}^{(j,1)}_{A'\to A} - m_{j,2}\mathcal{M}^{(j,2)}_{A'\to A} \right) \otimes \left(n_{j,1}\mathcal{N}^{(j,1)}_{B\to B'} + n_{j,2}\mathcal{N}^{(j,2)}_{B\to B'} \right) \tag{A21}$$

$$= \sum_{j=1}^{D} \Big(m_{j,1}n_{j,1}\mathcal{M}^{(j,1)}_{A'\to A} \otimes \mathcal{N}^{(j,1)}_{B\to B'} + m_{j,1}n_{j,2}\mathcal{M}^{(j,1)}_{A'\to A} \otimes \mathcal{N}^{(j,2)}_{B\to B'}$$

$$- m_{j,2}n_{j,1}\mathcal{M}^{(j,2)}_{A'\to A} \otimes \mathcal{N}^{(j,1)}_{B\to B'} - m_{j,2}n_{j,2}\mathcal{M}^{(j,2)}_{A'\to A} \otimes \mathcal{N}^{(j,2)}_{B\to B'} \Big) \tag{A22}$$

$$= \sum_{j=1}^{4D} \lambda_j \mathcal{M}^{(j)}_{A'\to A} \otimes \mathcal{N}^{(j)}_{B\to B'} \tag{A23}$$

with appropriate relabeling, where each $\lambda_j \in \{m_{j,1}n_{j,1}, m_{j,1}n_{j,2}, -m_{j,2}n_{j,1}, -m_{j,2}n_{j,2}\}_j$ is a real number, each $\mathcal{M}^{(j)}_{A'\to A} \in \left\{\mathcal{M}^{(j,1)}_{A'\to A}, \mathcal{M}^{(j,2)}_{A'\to A}\right\}_j$ is a CPTN map, and each $\mathcal{N}^{(j)}_{B\to B'} \in \left\{\mathcal{N}^{(j,1)}_{B\to B'}, \mathcal{N}^{(j,2)}_{B\to B'}\right\}_j$ is a quantum channel. Note that

$$\sum_{j=1}^{4D} \mathsf{Tr}_A \left[J^{\mathcal{M}^{(j)}}_{A'A} \right] = 2 \sum_{j=1}^{D} \sum_{k=1}^{2} \mathsf{Tr}_A \left[J^{\mathcal{M}^{(j,k)}}_{A'A} \right] \le \mathbb{1}_{A'} \tag{A24}$$

due to our choice of scalars $\{m_{j,1}, m_{j,2}\}_j$. Let $\mathcal{M}'_{A'\to A}$ be a CPTN map such that $\sum_{j=1}^{4D} \mathsf{Tr}_A \left[J^{\mathcal{M}^{(j)}}_{A'A}\right] + 2\mathsf{Tr}_A \left[J^{\mathcal{M}'}_{A'A}\right] = \mathbb{1}_{A'}$. Then, $\left\{\mathcal{M}^{(1)}, \ldots, \mathcal{M}^{(4D)}, \mathcal{M}', \mathcal{M}'\right\}$ is a quantum instrument and

$$\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_{j=1}^{4D} \lambda_j \mathcal{M}^{(j)}_{A'\to A} \otimes \mathcal{N}^{(j)}_{B\to B'} + \mathcal{M}'_{A'\to A} \otimes \mathcal{N}'_{B\to B'} - \mathcal{M}'_{A'\to A} \otimes \mathcal{N}'_{B\to B'} \tag{A25}$$

for any quantum channel $\mathcal{N}'_{B\to B'}$. Therefore, any bipartite linear map $\mathcal{S}_{A'B\to AB'}$ that is Hermitian-preserving and B-to-A no-signaling represents a forward-classical-assisted shadow simulation code. ■

Lemma 6 *A bipartite linear map $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving if and only if it corresponds to a shadow simulation code assisted by two-way classical communication.*

Proof The "if" part can be directly verified by checking that the Choi operator of a bipartite map $\sum_j \lambda_j \mathcal{M}^{(j)}_{A'\to A} \otimes \mathcal{N}^{(j)}_{B\to B'}$ is Hermitian, where both $\left\{\mathcal{M}^{(j)}_{A'\to A}\right\}_j$ and $\left\{\mathcal{N}^{(j)}_{B\to B'}\right\}_j$ are quantum instruments.

For the "only if" part, we follow the proof of Lemma 5 to write the Choi operator of a bipartite Hermitian-preserving map $\widehat{\mathcal{S}}_{A'B\to AB'}$ as $J^{\widehat{\mathcal{S}}}_{A'BAB'} = \sum_{j=1}^{D} M^{(j)}_{A'A} \otimes N^{(j)}_{BB'}$, where $M^{(j)}_{A'A}$ and $N^{(j)}_{BB'}$ are Hermitian operators. Each $M^{(j)}_{A'A}$ or $N^{(j)}_{BB'}$ can be written as the difference of two positive semidefinite operators. We write each $M^{(j)}_{A'A}$ as $m_{j,+}M^{(j,+)}_{A'A} - m_{j,-}M^{(j,-)}_{A'A}$ and each $N^{(j)}_{BB'}$ as $n_{j,+}N^{(j,+)}_{BB'} - n_{j,-}N^{(j,-)}_{BB'}$, where $m_{j,\pm}M^{(j,1)}_{A'A}, n_{j,2}N^{(j,\pm)}_{BB'}$ are positive semidefinite and $m_{j,\pm}, n_{j,\pm}$ are positive real numbers that will be fixed later. The Choi operator $J^{\widehat{\mathcal{S}}}_{A'BAB'}$ now can be written as

$$J^{\widehat{\mathcal{S}}}_{A'BAB'} = \sum_{j=1}^{D} \left(m_{j,+}M^{(j,+)}_{A'A} - m_{j,-}M^{(j,-)}_{A'A} \right) \otimes \left(n_{j,+}N^{(j,+)}_{BB'} - n_{j,-}N^{(j,-)}_{BB'} \right) \tag{A26}$$

$$= \sum_{j=1}^{D} \sum_{k\in\{+,-\}} \sum_{l\in\{+,-\}} (-1)^{1-\delta_{k,l}} m_{j,k}n_{j,l} M^{(j,k)}_{A'A} \otimes N^{(j,l)}_{BB'}, \tag{A27}$$

where $\delta_{k,l} = 1$ if $k = l$ and $\delta_{k,l} = 0$ otherwise. Because $M^{(j,\pm)}_{A'A}$ and $N^{(j,\pm)}_{BB'}$ are positive semidefinite operators, they can be treated as Choi operators of completely positive maps, say, $\mathcal{M}^{(j,\pm)}_{A'\to A}$ and $\mathcal{N}^{(j,\pm)}_{B\to B'}$. Then, we can write $\widehat{\mathcal{S}}_{A'B\to AB'}$

as

$$\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_{j=1}^{D}\sum_{k\in\{+,-\}}\sum_{l\in\{+,-\}} (-1)^{1-\delta_{k,l}} m_{j,k}n_{j,l}\mathcal{M}^{(j,k)}_{A'\to A}\otimes\mathcal{N}^{(j,l)}_{B\to B'} \tag{A28}$$

$$= \sum_{j=1}^{4D}\lambda_j \mathcal{M}^{(j)}_{A'\to A}\otimes \mathcal{N}^{(j)}_{B\to B'} \tag{A29}$$

with appropriate relabeling, where each $\lambda_j \in \left\{(-1)^{1-\delta_{k,l}} m_{j,k}n_{j,l}\right\}_{j,k,l}$ is a real number, each $\mathcal{M}^{(j)}_{A'\to A} \in \left\{\mathcal{M}^{(j,\pm)}_{A'\to A}\right\}_j$ or $\mathcal{N}^{(j)}_{B\to B'} \in \left\{\mathcal{N}^{(j,\pm)}_{B\to B'}\right\}_j$ is a CPTN map. We can fix the values of the coefficients $m_{j,\pm}$ and $n_{j,\pm}$ to be large enough so that both $\sum_{j=1}^{4D}\mathcal{M}^{(j)}_{A'\to A}$ and $\sum_{j=1}^{4D}\mathcal{N}^{(j)}_{B\to B'}$ are trace-non-increasing. Let $\mathcal{M}'_{A'\to A}$ and $\mathcal{N}'_{B\to B'}$ be CPTN maps such that $\sum_{j=1}^{4D}\mathcal{M}^{(j)}_{A'\to A} + 2\mathcal{M}'_{A'\to A}$ and $\sum_{j=1}^{4D}\mathcal{N}^{(j)}_{B\to B'} + 2\mathcal{N}'_{B\to B'}$ are CPTP. That is, $\left\{\mathcal{M}^{(1)},\dots,\mathcal{M}^{(4D)},\mathcal{M}',\mathcal{M}'\right\}$ and $\left\{\mathcal{N}^{(1)},\dots,\mathcal{N}^{(4D)},\mathcal{N}',\mathcal{N}'\right\}$ are quantum instruments. Because we can write

$$\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_{j=1}^{4D}\lambda_j \mathcal{M}^{(j)}_{A'\to A}\otimes \mathcal{N}^{(j)}_{B\to B'} + \mathcal{M}'_{A'\to A}\otimes\mathcal{N}'_{B\to B'} - \mathcal{M}'_{A'\to A}\otimes\mathcal{N}'_{B\to B'}, \tag{A30}$$

it follows that $\widehat{\mathcal{S}}_{A'B\to AB'}$ corresponds to a shadow simulation code assisted by two-way classical communication. Hence the proof. ■

From now on, we focus on no-signaling shadow simulation codes. We consider implementing such codes by sampling quantum no-signaling codes. This is possible due to the following proposition.

Proposition 7 *A bipartite linear map is Hermitian-preserving and no-signaling if and only if it is a linear combination of bipartite linear maps that correspond to quantum no-signaling codes.*

Proof For the “if” direction, let $\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_j \mathcal{S}^{(j)}_{A'B\to AB'}$ be a linear combination of bipartite linear maps that correspond to quantum no-signaling codes. The map $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving because $J^{\widehat{\mathcal{S}}}_{A'BAB'}$, the Choi operator of $\widehat{\mathcal{S}}_{A'B\to AB'}$, is Hermitian. Also, $\widehat{\mathcal{S}}_{A'B\to AB'}$ is no-signaling from B to A, because

$$\mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = \sum_j \lambda_j \mathsf{Tr}_{B'}\left[J^{\mathcal{S}^{(j)}}_{A'BAB'}\right] = \sum_j \lambda_j J^{\mathcal{S}^{(j)}}_{A'A}\otimes \mathbb{1}_B = J^{\widehat{\mathcal{S}}}_{A'A}\otimes \mathbb{1}_B, \tag{A31}$$

where the second inequality follows from each $\mathcal{S}^{(j)}_{A'B\to AB'}$ being no-signaling. Similarly, $\widehat{\mathcal{S}}_{A'B\to AB'}$ is no-signaling from A to B as

$$\mathsf{Tr}_{A}\left[J^{\widehat{\mathcal{S}}}_{A'BAB'}\right] = \sum_j \lambda_j \mathsf{Tr}_{A}\left[J^{\mathcal{S}^{(j)}}_{A'BAB'}\right] = \sum_j \lambda_j J^{\mathcal{S}^{(j)}}_{BB'}\otimes \mathbb{1}_{A'} = J^{\widehat{\mathcal{S}}}_{BB'}\otimes \mathbb{1}_{A'}. \tag{A32}$$

Therefore, the map $\widehat{\mathcal{S}}_{A'B\to AB'}$ is Hermitian-preserving and no-signaling.

For the “only if” part, let $\widetilde{\mathcal{S}}_{A'B\to AB'}$ be a Hermitian-preserving and no-signaling bipartite linear map. According to Theorem 1, $\widehat{\mathcal{S}}_{A'B\to AB'}$ can be decomposed as $\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_j \lambda_j \mathcal{M}^{(j)}_{A'\to A}\otimes\mathcal{N}^{(j)}_{B\to B'}$ for some quantum channels $\mathcal{M}^{(j)}_{A'\to A}$ and $\mathcal{N}^{(j)}_{B\to B'}$. Note that each $\mathcal{S}^{(j)}_{A'B\to AB'} \coloneqq \mathcal{M}^{(j)}_{A'\to A}\otimes\mathcal{N}^{(j)}_{B\to B'}$ is a bipartite linear map corresponding to a quantum no-signaling code. Therefore, $\widehat{\mathcal{S}}_{A'B\to AB'} = \sum_j \lambda_j \mathcal{S}^{(j)}_{A'B\to AB'}$ is indeed a linear combination of bipartite linear maps corresponding to quantum no-signaling codes. ■

By decomposing it into a few quantum no-signaling codes, we can implement any no-signaling shadow simulation code by sampling quantum no-signaling codes in a way similar to the protocol given earlier in this section for realizing randomness-assisted shadow simulation codes. The implementation of a no-signaling shadow simulation code incurs a cost quantifying how many sampling rounds are required. Such a cost can be derived from Hoeffding's inequality. Let $\widetilde{\mathcal{S}} = \sum_j \lambda_j \mathcal{S}_j$ be a no-signaling shadow simulation code decomposed into a linear combination of quantum no-signaling codes $\{\mathcal{S}_j\}$ so that

$$\mathsf{Tr}\left[\left(\widetilde{\mathcal{S}}\left(\mathcal{N}\right)\right)(\rho)O\right] = \sum_j \lambda_j \mathsf{Tr}\left[\left(\mathcal{S}_j\left(\mathcal{N}\right)\right)(\rho)O\right] \tag{A33}$$

for any quantum state ρ and any observable O. We assume that the observable is bounded as $\|O\|_\infty \leq 1$ so that each measurement outcome belongs to the interval $[-1,1]$. For post-processing, we multiply each measurement outcome by a factor of magnitude $\gamma := \sum_j |\lambda_j|$, and the average of all the post-processed outcomes serves as an unbiased estimator ξ for $\mathsf{Tr}\left[\left(\widetilde{\mathcal{S}}\left(\mathcal{N}\right)\right)(\rho)O\right]$. According to Hoeffding's inequality [39], the probability that the estimator has an error larger than or equal to ϵ is bounded as

$$\Pr\left(\left|\xi - \mathbb{E}\left[\xi\right]\right| \geq \epsilon\right) \leq 2\exp\left(-\frac{M\epsilon^2}{2\gamma^2}\right), \tag{A34}$$

where M is the number of sampling rounds. Hence, we can conclude that

$$M \geq \frac{2\gamma^2 \log\frac{2}{\delta}}{\epsilon^2} \tag{A35}$$

rounds are enough for the final estimation to have an error smaller than ϵ with a probability no less than $1-\delta$.

The number of rounds M is proportional to γ^2, where γ is the sum of the absolute values of the coefficients in the decomposition of $\widetilde{\mathcal{S}}$. Considering that a no-signaling shadow simulation code $\widetilde{\mathcal{S}}$ can have many different decompositions, we define its sampling cost as the smallest possible γ achieved by any feasible decomposition:

$$c_{\text{smp}}\left(\widetilde{\mathcal{S}}\right) := \inf\left\{\sum_j |\lambda_j| \;\middle|\; \widehat{\mathcal{S}} = \sum_j \lambda_j \widehat{\mathcal{S}}_j,\ \lambda_j \in \mathbb{R},\ \widehat{\mathcal{S}}_j \in \text{CPTP} \cap \text{NS}\right\}. \tag{A36}$$

Note that all the quantum no-signaling channels in the decomposition whose corresponding coefficients have the same sign can be grouped into one single quantum no-signaling channel without changing the cost. Hence, it is sufficient to consider all combinations in the form of $\widehat{\mathcal{S}} = p_+\widehat{\mathcal{S}}^+ - p_-\widehat{\mathcal{S}}^-$, where $p_\pm$ are non-negative coefficients and $\widehat{\mathcal{S}}^\pm$ are quantum no-signaling channels:

$$c_{\text{smp}}\left(\widetilde{\mathcal{S}}\right) = \inf\left\{p_+ + p_- \;\middle|\; \widehat{\mathcal{S}} = p_+\widehat{\mathcal{S}}^+ - p_-\widehat{\mathcal{S}}^-,\ p_\pm \in \mathbb{R}^+, \widehat{\mathcal{S}}_j \in \text{CPTP} \cap \text{NS}\right\}. \tag{A37}$$

Note that every conventional channel simulation protocol has a sampling cost of 1, while a shadow simulation protocol can have a sampling cost either larger or smaller than 1, in addition to being equal to 1.

Besides sampling cost, simulation error is an important indicator on the performance of a simulation code. In the main text, we use diamond distance between the simulated map $\widetilde{\mathcal{M}} := \widetilde{\mathcal{S}}(\mathcal{N})$ and the target channel $\mathcal{M}$ to measure this error. Here, we justify our choice.

As the target of our task is to estimate the expectation value, the most direct measure of the error is

$$\left|\mathsf{Tr}\left[O_{RB'}\widetilde{\mathcal{M}}_{A'\to B'}(\rho_{RA'})\right] - \mathsf{Tr}\left[O_{RB'}\mathcal{M}_{A'\to B'}(\rho_{RA'})\right]\right| \tag{A38}$$

for some given observable $O_{RB'}$ and quantum state $\rho_{RA'}$, where R is some reference system inaccessible to Alice. Because one simulation code should work for every quantum state and every observable, we consider the worst case error, which maximizes the error over all quantum states and observables. Without loss of generality, we consider only observables with $\|O\|_\infty \leq 1$ since every other observable is such an observable multiplied by a scalar:

$$\sup_{\rho_{RA'},\ O_{RB'}:\|O\|_\infty \leq 1} \left|\mathsf{Tr}[O\widetilde{\mathcal{M}}(\rho)] - \mathsf{Tr}[O\mathcal{M}(\rho)]\right|. \tag{A39}$$

Observe that the worst case error is upper-bounded by diamond norm because for any observable O and state ρ, we have

$$\begin{aligned}
\left|\mathsf{Tr}[O\widetilde{\mathcal{M}}(\rho)] - \mathsf{Tr}[O\mathcal{M}(\rho)]\right| &\leq \left|\mathsf{Tr}[O^+(\widetilde{\mathcal{M}}(\rho) - \mathcal{M}(\rho))]\right| + \left|\mathsf{Tr}[O^-(\widetilde{\mathcal{M}}(\rho) - \mathcal{M}(\rho))]\right| && \text{(A40)}\\
&\leq \frac{1}{2}\left\|\widetilde{\mathcal{M}}(\rho) - \mathcal{M}(\rho)\right\|_1 + \frac{1}{2}\left\|\widetilde{\mathcal{M}}(\rho) - \mathcal{M}(\rho)\right\|_1 && \text{(A41)}\\
&= \left\|\widetilde{\mathcal{M}}(\rho) - \mathcal{M}(\rho)\right\|_1 && \text{(A42)}\\
&\leq \left\|\widetilde{\mathcal{M}} - \mathcal{M}\right\|_\diamond, && \text{(A43)}
\end{aligned}$$

where O^+ and O^- are positive semidefinite operators representing the positive and negative parts of O, respectively. Furthermore, this upper bound is tight in the sense that there always exists an observable O and a quantum state ρ that saturate this bound. Specifically, let ρ^* be a quantum state such that $\left\|\widetilde{\mathcal{M}}(\rho^*) - \mathcal{M}(\rho^*)\right\|_1 = \left\|\widetilde{\mathcal{M}} - \mathcal{M}\right\|_\diamond$ and $O^* \geq 0$ be an observable such that $\left|\mathsf{Tr}\left[O\left(\widetilde{\mathcal{M}}(\rho^*) - \mathcal{M}(\rho^*)\right)\right]\right| = \frac{1}{2}\left\|\widetilde{\mathcal{M}}(\rho^*) - \mathcal{M}(\rho^*)\right\|$. Such state ρ^* and observable O^* always exist, and they saturate the upper bound, that is

$$\sup_{\rho,\ O:\|O\|_\infty\leq 1}\left|\mathsf{Tr}\left[O\widetilde{\mathcal{M}}(\rho)\right] - \mathsf{Tr}\left[O\mathcal{M}(\rho)\right]\right| = \left|\mathsf{Tr}\left[O^*\widetilde{\mathcal{M}}(\rho^*)\right] - \mathsf{Tr}\left[O^*\mathcal{M}(\rho^*)\right]\right| \tag{A44}$$

$$= \left\|\widetilde{\mathcal{M}} - \mathcal{M}\right\|_\diamond. \tag{A45}$$

Therefore, diamond distance is indeed the worst case error of estimating expectation values.

Appendix B: General SDPs for Minimum Error and Minimum Sampling Cost

We show that the minimum sampling cost and the minimum error of shadow simulation assisted by no-signaling codes can be formulated as SDPs. The minimum sampling cost can be formulated as

$$\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathcal{M}) = \inf p_+ + p_- \tag{B1a}$$

$$\text{s.t. } \widehat{\mathcal{S}} = p_+\widehat{\mathcal{S}}^+ - p_-\widehat{\mathcal{S}}^-, \tag{B1b}$$

$$\frac{1}{2}\left\|\mathcal{M}_{A'\to B'} - \widetilde{\mathcal{S}}\left(\mathcal{N}_{A\to B}\right)\right\|_\diamond \leq \varepsilon, \tag{B1c}$$

$$\widehat{\mathcal{S}}^\pm \in \mathrm{CPTP}\cap\mathrm{NS}. \tag{B1d}$$

This optimization problem can be modified to one for $\varepsilon^*_{\gamma,\mathrm{NS}}\left(\mathcal{N},\mathcal{M}\right)$ by changing the optimization objective to ε and adding the constraint $p_+ + p_- \leq \gamma$. For a pair of quantum channels, *i.e.*, CPTP maps, the diamond distance between them can be efficiently computed via a simple SDP [51]. For shadow simulation, however, the map $\widetilde{\mathcal{S}}\left(\mathcal{N}\right)$ is HPTS, which is more general than CPTP. Here, we show how to adapt the SDP for the diamond distance between two quantum channels to compute the diamond distance between any two HPTS maps.

Let $\widetilde{\mathcal{N}}_{A\to B} = p_+\mathcal{N}^+_{A\to B} - p_-\mathcal{N}^-_{A\to B}$ and $\widetilde{\mathcal{M}}_{A\to B} = q_+\mathcal{M}^+_{A\to B} - q_-\mathcal{M}^-_{A\to B}$ be two HPTS maps, where $p_\pm$ and $q_\pm$ are non-negative real numbers, and $\mathcal{N}^\pm_{A\to B}$ and $\mathcal{M}^\pm_{A\to B}$ are quantum channels. By the definition of the diamond norm, the diamond distance between these two maps is

$$\frac{1}{2}\left\|\widetilde{\mathcal{N}}_{A\to B} - \widetilde{\mathcal{M}}_{A\to B}\right\|_\diamond = \sup_{\psi_{RA}}\frac{1}{2}\left\|\widetilde{\mathcal{N}}_{A\to B}(\psi_{RA}) - \widetilde{\mathcal{M}}_{A\to B}(\psi_{RA})\right\|_1 \tag{B2}$$

$$= \sup_{\psi_{RA}}\left\{\sup_{M:0\leq M\leq \mathbb{1}}\mathsf{Tr}\left[M\left(\widetilde{\mathcal{N}}_{A\to B}(\psi_{RA}) - \widetilde{\mathcal{M}}_{A\to B}(\psi_{RA})\right)\right]\right.$$

$$\left. - \frac{1}{2}\mathsf{Tr}\left[\widetilde{\mathcal{N}}_{A\to B}(\psi_{RA}) - \widetilde{\mathcal{M}}_{A\to B}(\psi_{RA})\right]\right\}, \tag{B3}$$

where ψ_{RA} is a pure state with $d_R = d_A$, and the second equality follows from the Helstrom-Holevo theorem (see, for example, Theorem 3.13 in Ref. [52]). Defining $p \coloneqq p_+ - p_-$ and $q \coloneqq q_+ - q_-$, we have

$$\frac{1}{2}\left\|\widetilde{\mathcal{N}}_{A\to B} - \widetilde{\mathcal{M}}_{A\to B}\right\|_\diamond = \sup_{\substack{\psi_{RA}\\ M:0\leq M\leq\mathbb{1}}}\mathsf{Tr}\left[M\left(\widetilde{\mathcal{N}}_{A\to B}(\psi_{RA}) - \widetilde{\mathcal{M}}_{A\to B}(\psi_{RA})\right)\right] - \frac{p-q}{2}. \tag{B4}$$

Following the proof from Sec. 3.C.2 in Ref. [52], it is easy to show that the first term on the right hand side of the above equation can be computed using the standard SDP for the diamond distance between two quantum channels. Hence, the diamond distance between two HPTS maps can be calculated as the result obtained from the SDP for two quantum channels minus the normalized difference between the trace scalars of the two maps, *i.e.*,

$$\frac{1}{2}\left\|\widetilde{\mathcal{N}}_{A\to B} - \widetilde{\mathcal{M}}_{A\to B}\right\|_\diamond = \inf_{Z_{AB}\geq 0}\left\{\mu - \frac{p-q}{2}\ \middle|\ Z_{AB} \geq J^{\widetilde{\mathcal{N}}}_{AB} - J^{\widetilde{\mathcal{M}}}_{AB},\ \mathsf{Tr}_B[Z_{AB}] \leq \mu\mathbb{1}_A\right\}, \tag{B5}$$

where $J^{\widetilde{\mathcal{N}}}_{AB}$ and $J^{\widetilde{\mathcal{M}}}_{AB}$ are the Choi operators of $\widetilde{\mathcal{N}}_{A\to B}$ and $\widetilde{\mathcal{M}}_{A\to B}$, respectively. Then, the minimum error $\varepsilon^*_{\gamma,\mathrm{NS}}\left(\mathcal{N},\mathcal{M}\right)$ and minimum sampling cost $\gamma^*_{\varepsilon,\mathrm{NS}}$ can be written as SDPs in terms of the relevant maps' Choi operators.

Proposition 8 *Consider two quantum channels $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A'\to B'}$ whose Choi operators are $J^{\mathcal{N}}_{AB}$ and $J^{\mathcal{M}}_{A'B'}$, respectively. The minimum error of shadow simulation from $\mathcal{N}$ to $\mathcal{M}$ under no-signaling codes with a cost budget γ is given by the following SDP:*

$$\varepsilon^*_{\gamma,\mathrm{NS}}(\mathcal{N},\mathcal{M}) = \inf \varepsilon \tag{B6a}$$

$$\text{s.t. } J^{\widetilde{\mathcal{M}}}_{A'B'} = \operatorname{Tr}_{AB}\Big[\Big(\big(J^{\mathcal{N}}_{AB}\big)^T \otimes \mathbb{1}_{A'B'}\Big)\Big(J^{\widehat{\mathcal{S}}^+}_{A'BAB'} - J^{\widehat{\mathcal{S}}^-}_{A'BAB'}\Big)\Big], \tag{B6b}$$

$$Z_{A'B'} \geq 0,\ Z_{A'B'} \geq J^{\mathcal{M}}_{A'B'} - J^{\widetilde{\mathcal{M}}}_{A'B'},\ \operatorname{Tr}_{B'}[Z_{A'B'}] \leq \frac{2\varepsilon + 1 - p_+ + p_-}{2}\mathbb{1}_{A'}, \tag{B6c}$$

$$J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'} \geq 0,\ \operatorname{Tr}_{AB'}\left[J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}\right] = p_\pm \mathbb{1}_{A'B},\ p_+ + p_- \leq \gamma, \tag{B6d}$$

$$\operatorname{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}\right] = \frac{1}{d_B}\operatorname{Tr}_{BB'}\left[J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}\right] \otimes \mathbb{1}_B, \tag{B6e}$$

$$\operatorname{Tr}_{A}\left[J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}\right] = \frac{1}{d_{A'}}\operatorname{Tr}_{A'A}\left[J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}\right] \otimes \mathbb{1}_{A'}. \tag{B6f}$$

Similarly, the minimum sampling cost $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathcal{M})$ under an error tolerance ε is given by changing the optimization objective of the above SDP to $p_+ + p_-$ and removing the condition $p_+ + p_- \leq \gamma$.

Appendix C: Shadow Communication

In this section, we derive the SDP for $Q^{(1)}_{\gamma,\mathrm{NS}}$, the one-shot zero-error γ-cost shadow capacity assisted by no-signaling codes, given in Theorem 11. To achieve this, we first need to derive SDPs for some other quantities, which are of interest on their own.

First, we tailor the general SDPs of minimum error and minimum sampling cost for the shadow communication task. The original SDPs are given in Proposition 8. The target channel $\mathcal{M}_{A'\to B'}$ becomes id_d, where $d = d_{A'} = d_{B'}$ is the dimension of the target noiseless channel.

Lemma 9 *Given a fixed dimension $d = d_{A'} = d_{B'}$ and an error tolerance ε, the minimum error of shadow simulation from $\mathcal{N}_{A\to B}$ to id_d under no-signaling codes with a cost budget γ is given by the following SDP:*

$$\varepsilon^*_{\gamma,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d) = \inf \varepsilon \tag{C1a}$$

$$\text{s.t. } J^{\widetilde{\mathcal{M}}}_{A'B'} = \operatorname{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T\left(T^+_{AB} - T^-_{AB}\right)\right]\frac{d^2\Phi_{A'B'} - \mathbb{1}_{A'B'}}{d\,(d^2-1)} + \operatorname{Tr}\left[V^+_A - V^-_A\right]\frac{\mathbb{1}_{A'B'} - \Phi_{A'B'}}{d\,(d^2-1)}, \tag{C1b}$$

$$Z_{A'B'} \geq 0,\ Z_{A'B'} \geq J^{\mathrm{id}_d}_{A'B'} - J^{\widetilde{\mathcal{M}}}_{A'B'},\ \operatorname{Tr}_{B'}[Z_{A'B'}] \leq \frac{1}{2}\left(2\varepsilon + 1 - \frac{\operatorname{Tr}\left[V^+_A - V^-_A\right]}{d^2}\right)\mathbb{1}_{A'}, \tag{C1c}$$

$$0 \leq T^\pm_{AB} \leq V^\pm_A \otimes \mathbb{1}_B,\ \operatorname{Tr}_A\left[T^\pm_{AB}\right] = \frac{\operatorname{Tr}\left[V^\pm_A\right]}{d^2}\mathbb{1}_B,\ \frac{\operatorname{Tr}\left[V^+_A + V^-_A\right]}{d^2} \leq \gamma. \tag{C1d}$$

Similarly, the minimum sampling cost $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)$ with an error tolerance ε is given by changing the optimization objective of the above SDP to $\operatorname{Tr}\left[V^+_A + V^-_A\right]/d^2$ and removing the condition $\operatorname{Tr}\left[V^+_A + V^-_A\right]/d^2 \leq \gamma$.

Proof When the target identity channel has dimension d, and we denote it by id_d, the minimum error and the minimum sampling cost of shadow communication over the channel $\mathcal{N}$ are $\varepsilon^*_{\gamma,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)$ and $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)$, respectively, where ε and γ are the error tolerance and cost budget. Below, we exploit the symmetry of optimal solutions under twirling to obtain simplified SDPs for both quantities.

Consider the SDP for minimum error in Proposition 8 with the target channel being id_d first. Note that if $J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}$ are optimal, then for any d-dimensional unitary U, the Choi operators

$$\bar{J}^{\widehat{\mathcal{S}}^\pm}_{A'BAB'} \coloneqq (U_{A'} \otimes \overline{U}_{B'})J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}(U_{A'} \otimes \overline{U}_{B'})^\dagger \tag{C2}$$

are also optimal, where $\overline{U}$ denotes the complex conjugate of U. The optimality of $\bar{J}^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}$ can be checked by verifying that they satisfy all the conditions in the original SDP while keeping the value of ε unchanged. Due to the linearity of the constraints, any convex combination of optimal Choi operators is still optimal. Hence, we now redefine

$$\bar{J}^{\widehat{\mathcal{S}}^\pm}_{A'BAB'} \coloneqq \int dU (U_{A'} \otimes \overline{U}_{B'})J^{\widehat{\mathcal{S}}^\pm}_{A'BAB'}(U_{A'} \otimes \overline{U}_{B'})^\dagger, \tag{C3}$$

where the integral is taken over the Haar measure on the unitary group. This new pair of Choi operators are also optimal. It was shown in Ref. [53] that the twirling operation $\mathcal{T}_{A'B'} : X_{A'B'} \mapsto \int dU (U_{A'} \otimes \overline{U}_{B'}) X_{A'B'} (U_{A'} \otimes \overline{U}_{B'})^\dagger$ has the following action:

$$\mathcal{T}_{A'B'}(X_{A'B'}) = \mathsf{Tr}[X_{A'B'}\Phi_{A'B'}]\Phi_{A'B'} + \frac{\mathsf{Tr}[X_{A'B'}(\mathbb{1}_{A'B'} - \Phi_{A'B'})]}{d^2-1}(\mathbb{1}_{A'B'} - \Phi_{A'B'}), \tag{C4}$$

where $\Phi_{A'B'} = |\Phi\rangle\langle\Phi|_{A'B'}$ is the maximally entangled state with $|\Phi\rangle_{A'B'} \coloneqq \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_{A'}|j\rangle_{B'}$. Thus,

$$\bar{J}^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'} = \Phi_{A'B'} \otimes \mathsf{Tr}_{A'B'}\left[J^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'}\Phi_{A'B'}\right] + (\mathbb{1}_{A'B'} - \Phi_{A'B'}) \otimes \frac{\mathsf{Tr}_{A'B'}\left[J^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'}(\mathbb{1}_{A'B'} - \Phi_{A'B'})\right]}{d^2-1}. \tag{C5}$$

Without any constraints, $\mathsf{Tr}_{A'B'}\left[J^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'}\Phi_{A'B'}\right]$ and $\mathsf{Tr}_{A'B'}\left[J^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'}(\mathbb{1}_{A'B'} - \Phi_{A'B'})\right] / \left(d^2-1\right)$ can be any linear operators. We denote them by $T^{\pm}_{AB}$ and $W^{\pm}_{AB}$, respectively, so that

$$\bar{J}^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'} = \Phi_{A'B'} \otimes T^{\pm}_{AB} + (\mathbb{1}_{A'B'} - \Phi_{A'B'}) \otimes W^{\pm}_{AB}. \tag{C6}$$

We now express SDP (B6) in terms of $T^{\pm}_{AB}$ and $W^{\pm}_{AB}$. The Choi operator of the simulated map $\widetilde{\mathcal{M}}$ in Eq. (B6b) can be written as

$$J^{\widetilde{\mathcal{M}}}_{A'B'} = \mathsf{Tr}\left[(J^{\mathcal{N}}_{AB})^T(T^{+}_{AB} - T^{-}_{AB})\right]\Phi_{A'B'} + \mathsf{Tr}\left[(J^{\mathcal{N}}_{AB})^T(W^{+}_{AB} - W^{-}_{AB})\right](\mathbb{1}_{A'B'} - \Phi_{A'B'}). \tag{C7}$$

The first inequality in condition (B6d) becomes $T^{\pm}_{AB} \geq 0$ and $W^{\pm}_{AB} \geq 0$, and the equality in condition (B6d) can be written as

$$\frac{\mathbb{1}_{A'}}{d} \otimes \mathsf{Tr}_A\left[T^{\pm}_{AB} + (d^2-1)W^{\pm}_{AB}\right] = p_{\pm}\mathbb{1}_{A'B}, \tag{C8}$$

which is equivalent to the requirement that

$$\mathsf{Tr}_A\left[T^{\pm}_{AB} + (d^2-1)W^{\pm}_{AB}\right] = dp_{\pm}\mathbb{1}_{B}. \tag{C9}$$

For the B-to-A no-signaling condition (B6e), its left-hand side can be written as

$$\mathsf{Tr}_{B'}\left[J^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'}\right] = \frac{\mathbb{1}_{A'}}{d} \otimes \left(T^{\pm}_{AB} + \left(d^2-1\right)W^{\pm}_{AB}\right), \tag{C10}$$

and its right-hand side can be written as

$$\frac{1}{d_B}\mathsf{Tr}_{BB'}\left[J^{\widehat{\mathcal{S}}^{\pm}}_{A'BAB'}\right] \otimes \mathbb{1}_B = \frac{\mathbb{1}_{A'}}{d} \otimes \mathsf{Tr}_B\left[T^{\pm}_{AB} + \left(d^2-1\right)W^{\pm}_{AB}\right] \otimes \frac{\mathbb{1}_B}{d_B}. \tag{C11}$$

Hence, the condition (B6e) is equivalent to

$$T^{\pm}_{AB} + \left(d^2-1\right)W^{\pm}_{AB} = \mathsf{Tr}_B\left[T^{\pm}_{AB} + \left(d^2-1\right)W^{\pm}_{AB}\right] \otimes \frac{\mathbb{1}_B}{d_B}. \tag{C12}$$

Similarly, the right-hand side of the A-to-B no-signaling condition (B6f) can be simplified as

$$\frac{\mathbb{1}_{A'B'}}{d^2} \otimes \mathsf{Tr}_A\left[T^{\pm}_{AB} + \left(d^2-1\right)W^{\pm}_{AB}\right] = \frac{p_{\pm}\mathbb{1}_{A'BB'}}{d} \tag{C13}$$

due to Eq. (C9). Hence, the condition (B6f) is equivalent to

$$\Phi_{A'B'} \otimes \mathsf{Tr}_A\left[T^{\pm}_{AB}\right] + (\mathbb{1}_{A'B'} - \Phi_{A'B'}) \otimes \mathsf{Tr}_A\left[W^{\pm}_{AB}\right] = \frac{p_{\pm}\mathbb{1}_{A'BB'}}{d}. \tag{C14}$$

Note that the equation above holds if and only if $\mathsf{Tr}_A\left[T^{\pm}_{AB}\right] = \mathsf{Tr}_A\left[W^{\pm}_{AB}\right] = \frac{p_{\pm}\mathbb{1}_B}{d}$, which implies Eq. (C9).

Now the original SDP has been simplified to

$$\varepsilon^*_{\gamma,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d) = \inf \varepsilon \tag{C15a}$$

$$\text{s.t. } J^{\widetilde{\mathcal{M}}}_{A'B'} = \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T\left(T^+_{AB}-T^-_{AB}\right)\right]\Phi_{A'B'} + \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T\left(W^+_{AB}-W^-_{AB}\right)\right]\left(\mathbb{1}_{A'B'}-\Phi_{A'B'}\right), \tag{C15b}$$

$$Z_{A'B'} \geq 0,\ Z_{A'B'} \geq J^{\mathrm{id}_d}_{A'B'} - J^{\widetilde{\mathcal{M}}}_{A'B'},\ \mathrm{Tr}_{B'}[Z_{A'B'}] \leq \frac{2\varepsilon+1-p_++p_-}{2}\mathbb{1}_{A'}, \tag{C15c}$$

$$T^\pm_{AB} \geq 0,\ W^\pm_{AB} \geq 0,\ \mathrm{Tr}_A\left[T^\pm_{AB}\right] = \mathrm{Tr}_A\left[W^\pm_{AB}\right] = \frac{p_\pm \mathbb{1}_B}{d},\ p_+ + p_- \leq \gamma, \tag{C15d}$$

$$T^\pm_{AB} + \left(d^2-1\right)W^\pm_{AB} = \mathrm{Tr}_B\left[T^\pm_{AB} + \left(d^2-1\right)W^\pm_{AB}\right] \otimes \frac{\mathbb{1}_B}{d_B}. \tag{C15e}$$

Denoting $V^\pm_A \coloneqq d\mathrm{Tr}_B\left[T^\pm_{AB} + \left(d^2-1\right)W^\pm_{AB}\right]/d_B$, by condition (C15e), we can write the variables $W^\pm_{AB}$ in terms of $V^\pm_A$ and $T^\pm_{AB}$ as

$$\left(d^2-1\right)dW^\pm_{AB} = V^\pm_A \otimes \mathbb{1}_B - dT^\pm_{AB}. \tag{C16}$$

Then, other conditions involving $W^\pm_{AB}$ can also be written as conditions on $V^\pm_A$ and $T^\pm_{AB}$. The condition $W^\pm_{AB} \geq 0$ becomes $V^\pm_A \otimes \mathbb{1}_B \geq dT^\pm_{AB}$. The condition $\mathrm{Tr}_A\left[W^\pm_{AB}\right] = \frac{p_\pm \mathbb{1}_B}{d}$ becomes

$$d\mathrm{Tr}_A\left[W^\pm_{AB}\right] = \frac{\mathrm{Tr}\left[V^\pm_A\right]\mathbb{1}_B - p_\pm \mathbb{1}_B}{d^2-1} = p_\pm \mathbb{1}_B, \tag{C17}$$

which is equivalent to requiring $\mathrm{Tr}\left[V^\pm_A\right] = d^2 p_\pm$. Finally, the Choi operator of the simulated map $\widetilde{\mathcal{M}}$ can be written as

$$J^{\widetilde{\mathcal{M}}}_{A'B'} = \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T \Delta T_{AB}\right]\Phi_{A'B'} + \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T\left(\frac{\Delta V_A \otimes \mathbb{1}_B - d\Delta T_{AB}}{d\left(d^2-1\right)}\right)\right]\left(\mathbb{1}_{A'B'}-\Phi_{A'B'}\right) \tag{C18}$$

$$= \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T \Delta T_{AB}\right]\frac{d^2\Phi_{A'B'} - \mathbb{1}_{A'B'}}{d^2-1} + \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{A}\right)^T \Delta V_A\right]\frac{\mathbb{1}_{A'B'} - \Phi_{A'B'}}{d\left(d^2-1\right)}, \tag{C19}$$

where we denote $\Delta T_{AB} \coloneqq T^+_{AB} - T^-_{AB}$, $\Delta V_A \coloneqq V^+_A - V^-_A$, and $J^{\mathcal{N}}_A \coloneqq \mathrm{Tr}_B\left[J^{\mathcal{N}}_{AB}\right]$. Because $\mathcal{N}_{A\to B}$ is a quantum channel, the partial trace of its Choi operator over the output system B equals $\mathbb{1}_A$. Hence,

$$J^{\widetilde{\mathcal{M}}}_{A'B'} = \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T \Delta T_{AB}\right]\frac{d^2\Phi_{A'B'} - \mathbb{1}_{A'B'}}{d^2-1} + \mathrm{Tr}\left[\Delta V_A\right]\frac{\mathbb{1}_{A'B'} - \Phi_{A'B'}}{d\left(d^2-1\right)}. \tag{C20}$$

By further relabeling $dT^\pm_{AB}$ as $T^\pm_{AB}$ and replacing $p_\pm$ with $\mathrm{Tr}\left[V^\pm_A\right]/d^2$ lead to SDP (C1).

Because $p_+ + p_- = \mathrm{Tr}\left[V^+_A + V^-_A\right]/d^2$, by Proposition 8, we know changing the optimization objective of SDP (C1) to $\mathrm{Tr}\left[V^+_A + V^-_A\right]/d^2$ and removing the condition $\mathrm{Tr}\left[V^+_A + V^-_A\right]/d^2 \leq \gamma$ gives us an SDP for $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)$. ■

Now, we turn to zero-error shadow communication. In this case, the preset error tolerance ε is 0. We can greatly simplify the SDP for $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)$ using the fact $\varepsilon = 0$.

Lemma 10 *The zero-error minimum sampling cost of shadow communication with* NS *codes is given by the following SDP:*

$$\gamma^*_{0,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d) = \inf \frac{\mathrm{Tr}\left[V^+_A + V^-_A\right]}{d^2} \tag{C21a}$$

$$\text{s.t. } \mathrm{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T\left(T^+_{AB} - T^-_{AB}\right)\right] = \mathrm{Tr}\left[V^+_A - V^-_A\right] = d^2, \tag{C21b}$$

$$0 \leq T^\pm_{AB} \leq V^\pm_A \otimes \mathbb{1}_B,\ \mathrm{Tr}_A\left[T^\pm_{AB}\right] = \frac{\mathrm{Tr}\left[V^\pm_A\right]}{d^2}\mathbb{1}_B. \tag{C21c}$$

Proof Consider the SDP for $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)$ given in Lemma 9. For $\varepsilon = 0$, we have

$$\mathrm{Tr}_{B'}[Z_{A'B'}] \leq \frac{1}{2}\left(1 - \frac{\mathrm{Tr}\left[\Delta V_A\right]}{d^2}\right)\mathbb{1}_{A'}, \tag{C22}$$

where $\Delta V_A \coloneqq V_A^+ - V_A^-$. On the other hand, taking the partial trace of $J_{A'B'}^{\widetilde{\mathcal{M}}}$ over system B', we get

$$\mathsf{Tr}_{B'}\left[J_{A'B'}^{\widetilde{\mathcal{M}}}\right] = \mathsf{Tr}\left[\left(J_{AB}^{\mathcal{N}}\right)^T \Delta T_{AB}\right] \frac{d\mathbb{1}_{A'} - d\mathbb{1}_{A'}}{d\left(d^2-1\right)} + \mathsf{Tr}\left[\Delta V_A\right] \frac{d\mathbb{1}_{A'} - \mathbb{1}_{A'}/d}{d\left(d^2-1\right)} = \mathsf{Tr}\left[\Delta V_A\right] \frac{\mathbb{1}_{A'}}{d^2}. \tag{C23}$$

Then, it follows that

$$\frac{1}{2}\left(1 - \frac{\mathsf{Tr}\left[\Delta V_A\right]}{d^2}\right)\mathbb{1}_{A'} \geq \mathsf{Tr}_{B'}\left[Z_{A'B'}\right] \geq \mathsf{Tr}_{B'}\left[J_{A'B'}^{\mathrm{id}_d} - J_{A'B'}^{\widetilde{\mathcal{M}}}\right] = \left(1 - \frac{\mathsf{Tr}\left[\Delta V_A\right]}{d^2}\right)\mathbb{1}_{A'}. \tag{C24}$$

For $Z_{A'B'} \geq 0$, we conclude that $Z_{A'B'} = 0$ and $\mathsf{Tr}\left[\Delta V_A\right] = d^2$, implying $J_{A'B'}^{\widetilde{\mathcal{M}}} = J_{A'B'}^{\mathrm{id}}$.

Note that we can also write $J_{A'B'}^{\widetilde{\mathcal{M}}}$ as

$$J_{A'B'}^{\widetilde{\mathcal{M}}} = \mathsf{Tr}\left[\left(J_{AB}^{\mathcal{N}}\right)^T \frac{\Delta T_{AB}}{d}\right]\Phi_{A'B'} + \mathsf{Tr}\left[\left(J_{AB}^{\mathcal{N}}\right)^T\left(\frac{\Delta V_A \otimes \mathbb{1}_B - \Delta T_{AB}}{d\left(d^2-1\right)}\right)\right]\left(\mathbb{1}_{A'B'} - \Phi_{A'B'}\right) \tag{C25}$$

by reorganizing Eq. (C1b) with $\Delta T_{AB} \coloneqq T_{AB}^+ - T_{AB}^-$. Because $J_{A'B'}^{\widetilde{\mathcal{M}}} = J_{A'B'}^{\mathrm{id}} = d\Phi_{A'B'}$, it must be true that

$$\mathsf{Tr}\left[\left(J_{AB}^{\mathcal{N}}\right)^T \Delta T_{AB}\right] = \mathsf{Tr}\left[\Delta V_A\right] = d^2. \tag{C26}$$

Hence the proof. ■

From this lemma, we can derive an SDP for the one-shot zero-error γ-cost shadow capacity as follows.

Theorem 11 *The one-shot zero-error γ-cost shadow capacity assisted by no-signaling codes of a quantum channel $\mathcal{N}_{A\to B}$ is given by the following SDP:*

$$Q_{\gamma,\mathrm{NS}}^{(1)}(\mathcal{N}) = \sup\ \log_2\ \left\lfloor\sqrt{\mathsf{Tr}\left[V_A\right]}\right\rfloor \tag{C27a}$$

$$\text{s.t. } \mathsf{Tr}\left[\left(J_{AB}^{\mathcal{N}}\right)^T T_{AB}\right] = \mathsf{Tr}\left[V_A\right],\ \mathsf{Tr}_A\left[T_{AB}\right] = \mathbb{1}_B,\ 0 \leq T_{AB} + R_{AB} \leq \left(V_A + W_A\right)\otimes\mathbb{1}_B, \tag{C27b}$$

$$0 \leq R_{AB} \leq W_A \otimes \mathbb{1}_B,\ \mathsf{Tr}_A\left[R_{AB}\right] = \frac{\gamma-1}{2}\mathbb{1}_B,\ \mathsf{Tr}\left[W_A\right] = \frac{\gamma-1}{2}\mathsf{Tr}\left[V_A\right]. \tag{C27c}$$

Proof The SDP given in Lemma 10 allows us to formulate $Q_{\gamma,\mathrm{NS}}^{(1)}(\mathcal{N})$ as an optimization problem by replacing d^2 with $\mathsf{Tr}\left[V_A^+ - V_A^-\right]$, and the objective of the optimization is to maximize $\log_2\ \left\lfloor\sqrt{\mathsf{Tr}\left[V_A^+ - V_A^-\right]}\right\rfloor$ according to the definition of $Q_{\gamma,\mathrm{NS}}^{(1)}$:

$$Q_{\gamma,\mathrm{NS}}^{(1)}(\mathcal{N}) = \sup\ \log_2\ \left\lfloor\sqrt{\mathsf{Tr}\left[V_A^+ - V_A^-\right]}\right\rfloor \tag{C28a}$$

$$\text{s.t. } \mathsf{Tr}\left[\left(J_{AB}^{\mathcal{N}}\right)^T\left(T_{AB}^+ - T_{AB}^-\right)\right] = \mathsf{Tr}\left[V_A^+ - V_A^-\right],\ \frac{\mathsf{Tr}\left[V_A^+ + V_A^-\right]}{\mathsf{Tr}\left[V_A^+ - V_A^-\right]} \leq \gamma, \tag{C28b}$$

$$0 \leq T_{AB}^{\pm} \leq V_A^{\pm} \otimes \mathbb{1}_B,\ \mathsf{Tr}_A\left[T_{AB}^{\pm}\right] = \frac{\mathsf{Tr}\left[V_A^{\pm}\right]\mathbb{1}_B}{\mathsf{Tr}\left[V_A^+ - V_A^-\right]}, \tag{C28c}$$

where the inequality in condition (C28b) corresponds to the limited cost budget. This is not an SDP, but observe that the equality in condition (C28c) is equivalent to the following two equations:

$$\mathsf{Tr}_A\left[T_{AB}^+ - T_{AB}^-\right] = \mathbb{1}_B \quad \text{and} \quad \mathsf{Tr}_A\left[T_{AB}^+ + T_{AB}^-\right] = \frac{\mathsf{Tr}\left[V_A^+ + V_A^-\right]}{\mathsf{Tr}\left[V_A^+ - V_A^-\right]}\mathbb{1}_B. \tag{C29}$$

In addition, the inequality in condition (C28b) can be restricted to equality without affecting the optimization result because if $\bar{T}_{AB}^{\pm}$ and $\bar{V}_A^{\pm}$ form a set of optimal solution such that $\mathsf{Tr}\left[\bar{V}_A^+ + \bar{V}_A^-\right]/\mathsf{Tr}\left[\bar{V}_A^+ - \bar{V}_A^-\right] = \bar{\gamma} < \gamma$, then $\bar{T}_{AB}^{\prime\pm} \coloneqq \bar{T}_{AB}^{\pm} + (\gamma - \bar{\gamma})\mathbb{1}_{AB}/2d_A$ and $\bar{V}_A^{\prime\pm} \coloneqq \bar{V}_A^{\pm} + (\gamma - \bar{\gamma})\,\mathsf{Tr}\left[\bar{V}_A^+ - \bar{V}_A^-\right]\mathbb{1}_A/2d_A$ also form a set of optimal solution with $\mathsf{Tr}\left[\bar{V}_A^{\prime +} + \bar{V}_A^{\prime -}\right]/\mathsf{Tr}\left[\bar{V}_A^{\prime +} - \bar{V}_A^{\prime -}\right] = \gamma$. Note that for $\bar{T}_{AB}^{\prime\pm}$ and $\bar{V}_A^{\prime\pm}$ to be valid solution, it must be true that $\mathsf{Tr}\left[\bar{V}_A^+ - \bar{V}_A^-\right] \geq 1$ so that $\bar{V}_A^{\prime\pm} \otimes \mathbb{1}_B \geq \bar{T}_{AB}^{\prime\pm}$. This is indeed the case because from the constraint $T_{A'B'}^{\pm} \leq V_A^{\pm} \otimes \mathbb{1}_B$ we have $\mathsf{Tr}_A\left[\bar{T}^+_{AB}+\bar{T}^-_{AB}\right]\leq \mathsf{Tr}\left[\bar{V}^+_A+\bar{V}^-_A\right]\mathbb{1}_B$. For the equality $\mathsf{Tr}_A\left[\bar{T}^+_{AB}+\bar{T}^-_{AB}\right]= \mathsf{Tr}\left[\bar{V}^+_A+\bar{V}^-_A\right]\mathbb{1}_B/\mathsf{Tr}\left[\bar{V}^+_A-\bar{V}^-_A\right]$ to hold, $\mathsf{Tr}\left[\bar{V}^+_A-\bar{V}^-_A\right]$ has to be larger than or equal to 1.

Now we can safely require $\mathsf{Tr}\left[V^+_A+V^-_A\right]=\gamma\mathsf{Tr}\left[V^+_A-V^-_A\right]$ and thus $\mathsf{Tr}_A\left[T^+_{AB}+T^-_{AB}\right]=\gamma\mathbb{1}_B$. Changing the variables to $T_{AB}\coloneqq T^+_{AB}-T^-_{AB}$, $R_{AB}\coloneqq T^-_{AB}$, $V_A\coloneqq V^+_A-V^-_A$, and $W_A\coloneqq V^-_A$ results in the claimed SDP. ■

In the main text, we claimed that $Q^{(1)}_{\gamma,\mathrm{NS}}$ generalizes the no-signaling-assisted one-shot zero-error quantum capacity $Q^{(1)}_{\mathrm{NS}}$ in the sense that $Q^{(1)}_{1,\mathrm{NS}}(\mathcal{N})=Q^{(1)}_{\mathrm{NS}}(\mathcal{N})$ for any quantum channel $\mathcal{N}$. To see this, note that when $\gamma=1$, variables R_{AB} and W_A from SDP (C27) satisfy $\mathsf{Tr}_A\left[R_{AB}\right]=0$ and $\mathsf{Tr}\left[W_A\right]=0$. Because both R_{AB} and W_A are positive semidefinite operators, they can only be 0. Therefore, the original SDP (C27) reduces to

$$\sup\ \log_2\ \left\lfloor\sqrt{\mathsf{Tr}\left[V_A\right]}\right\rfloor \tag{C30a}$$

$$\text{s.t. } \mathsf{Tr}\left[\left(J^{\mathcal{N}}_{AB}\right)^T T_{AB}\right]=\mathsf{Tr}\left[V_A\right],\ \mathsf{Tr}_A\left[T_{AB}\right]=\mathbb{1}_B,\ 0\leq T_{AB}\leq V_A\otimes\mathbb{1}_B, \tag{C30b}$$

which is an SDP for $Q^{(1)}_{\mathrm{NS}}(\mathcal{N})$ [7, 44].

Below, we provide an exact characterization of $Q^{(1)}_{\gamma,\mathrm{NS}}$ for single-qubit depolarizing channels.

Theorem 2 *Let $\mathcal{N}_{\mathrm{depo},p}(\rho)=p\rho+(1-p)\mathbb{1}_2/2$ be a single-qubit depolarizing channel, where $p\in[0,1]$ is a probability and $\mathbb{1}_2$ is the identity operator on $\mathbb{C}^2$. For $\gamma\geq 1$, the one-shot zero-error shadow capacity assisted by no-signaling resources is*

$$Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p})=\log_2\left\lfloor\sqrt{2p\gamma+p+1}\right\rfloor. \tag{C31}$$

Proof The Choi operator of the depolarizing channel $\mathcal{N}_{\mathrm{depo},p}$ from qubit system A to qubit system B is

$$J^{\mathcal{N}_{\mathrm{depo},p}}_{AB}=p\Gamma_{AB}+\frac{1-p}{2}\mathbb{1}_{AB}, \tag{C32}$$

where $\Gamma_{AB}\coloneqq|\Gamma\rangle\langle\Gamma|_{AB}$ is the unnormalized maximally entangled state with $|\Gamma\rangle_{AB}\coloneqq\sum_{j=0}^{1}|j\rangle_A|j\rangle_B$. We first consider the case where $p\in(0,1]$. It is straightforward to verify that

$$\bar{T}^+_{AB}\coloneqq\frac{d^2-1+p}{4p}\Gamma_{AB},\quad \bar{T}^-_{AB}\coloneqq\frac{d^2-1-3p}{6p}\mathbb{1}_{AB}-\frac{d^2-1-3p}{12p}\Gamma_{AB}, \tag{C33}$$

$$\bar{V}^+_A\coloneqq\frac{d^2(d^2-1+p)}{8p}\mathbb{1}_A,\quad \bar{V}^-_A\coloneqq\frac{d^2(d^2-1-3p)}{8p}\mathbb{1}_A \tag{C34}$$

form a feasible solution to the SDP for $\gamma^*_{0,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p},\mathrm{id}_d)$ as presented in Lemma 10, implying

$$\gamma^*_{0,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p},\mathrm{id}_d)\leq\frac{\mathsf{Tr}\left[\bar{V}^+_A+\bar{V}^-_A\right]}{d^2}=\frac{d^2-1-p}{2p}. \tag{C35}$$

Using the Lagrange dual function, we can derive that the following problem is the dual problem associated with SDP (C21):

$$\gamma^*_{0,\mathrm{NS}}(\mathcal{N},\mathrm{id}_d)\geq\sup\ \lambda-\mu \tag{C36}$$

$$\text{s.t. } M^\pm_{AB}\geq 0,\ M^\pm_{AB}+d^2\mathbb{1}_A\otimes N^\pm_B\geq\pm\lambda\left(J^{\mathcal{N}}_{AB}\right)^T, \tag{C37}$$

$$\mathsf{Tr}_B\left[M^\pm_{AB}\right]=\left(1-\mathsf{Tr}\left[N^\pm_B\right]\pm\mu\right)\mathbb{1}_A. \tag{C38}$$

Again, it is straightforward to verify that, given $J^{\mathcal{N}}_{AB}=J^{\mathcal{N}_{\mathrm{depo},p}}_{AB}$,

$$\bar{\lambda}\coloneqq\frac{d^2}{2p},\quad \bar{\mu}\coloneqq\frac{1+p}{2p},\quad \bar{N}^+_B\coloneqq\frac{1+3p}{4p}\mathbb{1}_B,\quad \bar{N}^-_B\coloneqq\frac{p-1}{4p}\mathbb{1}_B,\quad M^\pm_{AB}=0 \tag{C39}$$

form a feasible solution to the dual problem, implying

$$\gamma^*_{0,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p},\mathrm{id}_d)\geq\bar{\lambda}-\bar{\mu}=\frac{d^2-1-p}{2p}. \tag{C40}$$

Combining Eqs. (C35) and (C40), we conclude that

$$\gamma^*_{0,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p}, \mathrm{id}_d) = \frac{d^2 - 1 - p}{2p}, \tag{C41}$$

which is the minimum sampling cost required to simulate the d-dimensional identity channel id_d from $\mathcal{N}_{\mathrm{depo},p}$. In other words, for any γ such that

$$\frac{d^2 - 1 - p}{2p} \leq \gamma < \frac{(d+1)^2 - 1 - p}{2p}, \tag{C42}$$

we have $Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p}) = \log_2 d$. Solving for the value of d in terms of γ, we obtain $d = \left\lfloor \sqrt{2p\gamma + p + 1} \right\rfloor$, and hence

$$Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p}) = \log_2 \left\lfloor \sqrt{2p\gamma + p + 1} \right\rfloor. \tag{C43}$$

When $p = 0$, the Choi operator of the depolarizing channel is simply $\mathbb{1}_{AB}/2$. Taking this into SDP (C27), we see that $\mathsf{Tr}[V_A]$ can only takes a fixed value of 1. Hence, $Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p}) = 0$ for $p = 0$ and arbitrary γ, which coincides with the value that $\log_2 \left\lfloor \sqrt{2p\gamma + p + 1} \right\rfloor$ evaluates to. Therefore, $Q^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{N}_{\mathrm{depo},p}) = \log_2 \left\lfloor \sqrt{2p\gamma + p + 1} \right\rfloor$ for any $p \in [0, 1]$. ■

To further showcase the difference between shadow simulation and conventional quantum channel simulation, we in addition consider two other common quantum channels: the single-qubit amplitude damping channel $\mathcal{N}_{\mathrm{AD}}$ with two Kraus operators $|0\rangle\langle 0| + \sqrt{p}|1\rangle\langle 1|$ and $\sqrt{1-p}|0\rangle\langle 1|$ and the single-qubit dephasing channel $\mathcal{N}_{\mathrm{deph}}(\cdot) = p(\cdot) + (1-p)\mathrm{diag}(\cdot)$. For each channel, the parameter $p \in [0, 1]$ indicates the level of noise.

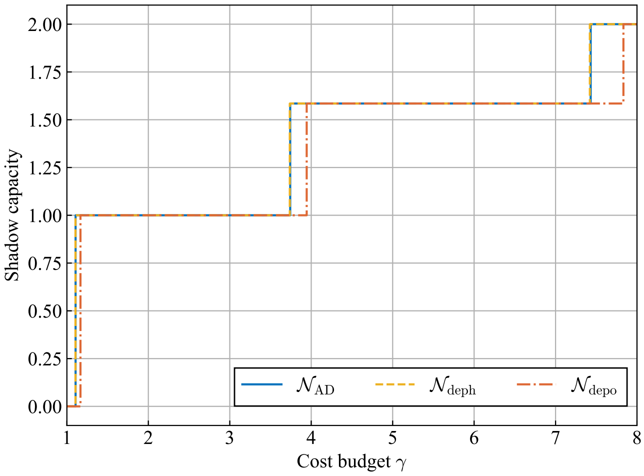


FIG. 3. Comparison between the conventional no-signaling-assisted quantum communication and no-signaling-assisted shadow communication under different cost budgets. Compared with the quantum case, where the one-shot zero-error quantum capacities are 0 for all channels, higher one-shot zero-error shadow capacity is achieved for every channel with increased cost budget.

In Figure 3, we present some numerical results on these channels at a low noise level ($p = 0.9$). For conventional quantum communication with no-signaling codes, all these channels' one-shot zero-error capacities are zero. For shadow communication, on the other hand, the one-shot zero-error capacities of these three channels steadily go up as the budget for sampling cost increases. The stepwise changes in the zero-error capacity show that we can trade in computational resources for better performance in shadow communication, attaining computational power beyond purely quantum protocols.

Appendix D: Shadow Simulation via Noiseless Channels

In this section, we derive the SDP for $S^{(1)}_{\gamma,\mathrm{NS}}$, the one-shot zero-error γ-cost shadow simulation cost assisted by no-signaling codes. Along the way, we derive SDPs for some related quantities, which are of interest on their own.

To begin with, the minimum error and minimum sampling cost of shadow simulation with a noiseless channel can be solved by SDPs in Lemma 12. We omit the proof here as it is very similar to the proof of Lemma 9.

Lemma 12 *For an identity channel* id_d *with dimension* d *and a target quantum channel* $\mathcal{M}_{A'\to B'}$*, the minimum error of the simulation from* id_d *to* $\mathcal{M}_{A'\to B'}$ *assisted by* NS *codes with a cost budget* γ *is given by the following SDP:*

$$\varepsilon^*_{\gamma,\mathrm{NS}}(\mathrm{id}_d,\mathcal{N}) = \inf\ \varepsilon \tag{D1a}$$

$$\text{s.t. } Z_{A'B'} \geq 0,\ Z_{A'B'} \geq J^{\mathcal{M}}_{A'B'} - Y^{+}_{A'B'} + Y^{-}_{A'B'}, \tag{D1b}$$

$$\mathsf{Tr}_{B'}[Z_{A'B'}] \leq \frac{1}{2}\left(2\varepsilon + 1 - \frac{\mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right]}{d^2}\right)\mathbb{1}_{A'}, \tag{D1c}$$

$$0 \leq Y^{\pm}_{A'B'} \leq \mathbb{1}_{A'} \otimes V^{\pm}_{B'},\ \mathsf{Tr}_{B'}\left[Y^{\pm}_{A'B'}\right] = \frac{\mathsf{Tr}\left[V^{\pm}_{B'}\right]}{d^2}\mathbb{1}_{A'},\ \frac{\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]}{d^2} \leq \gamma. \tag{D1d}$$

Similarly, the minimum sampling cost $\gamma^*_{\varepsilon,\mathrm{NS}}(\mathrm{id}_d,\mathcal{M}_{A'\to B'})$ *with an error tolerance* ε *is given by changing the optimization objective of the above SDP to* $\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]/d^2$ *and removing the condition* $\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]/d^2 \leq \gamma$*.*

Provided with Lemma 12, we now give an SDP for the zero-error minimum sampling cost of the shadow simulation of a noisy channel via a noiseless one.

Lemma 13 *The zero-error minimum sampling cost of the shadow simulation of a channel* $\mathcal{M}_{A'\to B'}$ *via a* d*-dimensional identity channel* id_d *assisted by* NS *codes is given by the following SDP:*

$$\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d,\mathcal{M}_{A'\to B'}) = \inf\ \frac{\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]}{d^2} \tag{D2a}$$

$$\text{s.t. } \mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right] = d^2,\ \mathsf{Tr}_{B'}\left[R_{A'B'}\right] = \frac{\mathsf{Tr}\left[V^{-}_{B'}\right]}{d^2}\mathbb{1}_{A'}, \tag{D2b}$$

$$J^{\mathcal{M}}_{A'B'} + R_{A'B'} \leq \mathbb{1}_{A'} \otimes V^{+}_{B'},\ 0 \leq R_{A'B'} \leq \mathbb{1}_{A'} \otimes V^{-}_{B'} \tag{D2c}$$

Proof As in the shadow communication setting, the zero-error simulation of the channel $\mathcal{M}$ requires $J^{\mathcal{N}}_{A'B'} = Y^{+}_{A'B'} - Y^{-}_{A'B'}$ and $\mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right] = d^2$ (see the proof of Lemma 10). The equalities $\mathsf{Tr}_{B'}\left[Y^{\pm}_{A'B'}\right] = \frac{\mathsf{Tr}[V^{\pm}_{B'}]}{d^2}\mathbb{1}_{A'}$ in condition (D1d) can be equivalently written as

$$\mathsf{Tr}_{B'}\left[Y^{+}_{A'B'} + Y^{-}_{A'B'}\right] = \frac{\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]}{d^2}\mathbb{1}_{A'} \quad \text{and} \quad \mathsf{Tr}_{B'}\left[Y^{+}_{A'B'} - Y^{-}_{A'B'}\right] = \frac{\mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right]}{d^2}\mathbb{1}_{A'}. \tag{D3}$$

Note that the latter equality $\mathsf{Tr}_{B'}\left[Y^{+}_{A'B'} - Y^{-}_{A'B'}\right] = \mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right]\mathbb{1}_{A'}/d^2$ can be removed because it is already implied by $J^{\mathcal{N}}_{A'B'} = Y^{+}_{A'B'} - Y^{-}_{A'B'}$ and $\mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right] = d^2$ with the observation that $\mathsf{Tr}_{B'}\left[J^{\mathcal{N}}_{A'B'}\right] = \mathbb{1}_{A'}$ for $\mathcal{N}$ being a quantum channel. Hence, we arrive at the following SDP:

$$\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d,\mathcal{M}_{A'\to B'}) = \inf\ \frac{\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]}{d^2} \tag{D4a}$$

$$\text{s.t. } J^{\mathcal{M}}_{A'B'} = Y^{+}_{A'B'} - Y^{-}_{A'B'},\ \mathsf{Tr}\left[V^{+}_{B'} - V^{-}_{B'}\right] = d^2, \tag{D4b}$$

$$0 \leq Y^{\pm}_{A'B'} \leq \mathbb{1}_{A'} \otimes V^{\pm}_{B'},\ \mathsf{Tr}_{B'}\left[Y^{+}_{A'B'} + Y^{-}_{A'B'}\right] = \frac{\mathsf{Tr}\left[V^{+}_{B'} + V^{-}_{B'}\right]}{d^2}\mathbb{1}_{A'}. \tag{D4c}$$

Denoting $R_{A'B'} := Y^{-}_{A'B'}$, writing $Y^{+}_{A'B'}$ as $J^{\mathcal{M}}_{A'B'} + R_{A'B'}$, and exploiting $\mathsf{Tr}_{B'}\left[J^{\mathcal{M}}_{A'B'}\right] = \mathbb{1}_{A'}$, one can obtain the claimed SDP. ■

From this lemma, we can arrive at the following SDP for the one-shot zero-error γ-cost shadow simulation cost.

Theorem 14 *The one-shot zero-error* γ*-cost simulation cost of a quantum channel* $\mathcal{M}_{A'\to B'}$ *assisted by no-signaling codes is given by the following SDP:*

$$S^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{M}) = \inf\ \log_2\left\lceil\sqrt{\mathsf{Tr}\left[V_{B'}\right]}\right\rceil \tag{D5a}$$

$$\text{s.t. } J^{\mathcal{M}}_{A'B'} + R_{A'B'} \leq \mathbb{1}_{A'} \otimes \frac{\gamma+1}{2}V_{B'},\ 0 \leq R_{A'B'} \leq \mathbb{1}_{A'} \otimes W_{B'}, \tag{D5b}$$

$$\mathsf{Tr}_{B'}\left[R_{A'B'}\right] = \frac{\gamma-1}{2}\mathbb{1}_{A'},\ \mathsf{Tr}\left[W_{B'}\right] = \frac{\gamma-1}{2}\mathsf{Tr}\left[V_{B'}\right]. \tag{D5c}$$

Proof According to the SDP given in Lemma 13, we can write the one-shot simulation cost $S^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{M})$ as an optimization problem by substituting d^2 with $\mathsf{Tr}\left[V^+_{B'} - V^-_{B'}\right]$:

$$S^{(1)}_{\gamma,\mathrm{NS}}(\mathcal{M}) = \inf\ \log_2\ \left\lceil \sqrt{\mathsf{Tr}\left[V^+_{B'} - V^-_{B'}\right]}\right\rceil \tag{D6a}$$

$$\text{s.t. } \mathsf{Tr}_{B'}\left[R_{A'B'}\right] = \frac{\mathsf{Tr}\left[V^-_{B'}\right]}{\mathsf{Tr}\left[V^+_{B'} - V^-_{B'}\right]}\mathbb{1}_{A'},\ \frac{\mathsf{Tr}\left[V^+_{B'} + V^-_{B'}\right]}{\mathsf{Tr}\left[V^+_{B'} - V^-_{B'}\right]} \leq \gamma, \tag{D6b}$$

$$J^{\mathcal{M}}_{A'B'} + R_{A'B'} \leq \mathbb{1}_{A'} \otimes V^+_{B'},\ 0 \leq R_{A'B'} \leq \mathbb{1}_{A'} \otimes V^-_{B'}. \tag{D6c}$$

Note that the inequality in condition (D6b) can be restricted to equality while keeping the optimized value unchanged. This is true because if $R_{A'B'}$ and $\bar{V}^{\pm}_{B'}$ is a set of optimal solution with $\mathsf{Tr}\left[V^+_{B'} + V^-_{B'}\right]/\mathsf{Tr}\left[\bar{V}^+_{B'} - \bar{V}^-_{B'}\right] = \bar{\gamma} < \gamma$, then $R'_{A'B'} := R_{A'B'} + (\gamma - \bar{\gamma})\mathbb{1}_{A'B'}/2d_{B'}$ and $\bar{V}'^{\pm}_{B'} := \bar{V}^{\pm}_{B'} + (\gamma - \bar{\gamma})\mathsf{Tr}\left[\bar{V}^+_{B'} - \bar{V}^-_{B'}\right]\mathbb{1}_{B'}/2d_{B'}$ also form a set of optimal solution such that $\mathsf{Tr}\left[\bar{V}'^+_{B'} + \bar{V}'^-_{B'}\right]/\mathsf{Tr}\left[\bar{V}'^+_{B'} - \bar{V}'^-_{B'}\right] = \gamma$. Note that for $\bar{R}'^{\pm}_{A'B'}$ and $\bar{V}'^{\pm}_{B'}$ to be valid solution, it must be true that $\mathsf{Tr}\left[\bar{V}^+_{B'} - \bar{V}^-_{B'}\right] \geq 1$ so that $\mathbb{1}_{A'} \otimes \bar{V}'^-_{B'} \geq \bar{R}'_{A'B'}$. This is indeed the case because from the constraint $R_{A'B'} \leq \mathbb{1}_{A'} \otimes V^-_{B'}$ we have $\mathsf{Tr}_{B'}\left[\bar{R}_{A'B'}\right] \leq \mathsf{Tr}\left[\bar{V}^-_{B'}\right]\mathbb{1}_{A'}$. For the equality $\mathsf{Tr}_{B'}\left[\bar{R}_{A'B'}\right] = \mathsf{Tr}\left[\bar{V}^-_{B'}\right]\mathbb{1}_{A'}/\mathsf{Tr}\left[\bar{V}^+_{B'} - \bar{V}^-_{B'}\right]$ to hold, $\mathsf{Tr}\left[\bar{V}^+_{B'} - \bar{V}^-_{B'}\right]$ has to be larger than or equal to 1.

By changing the inequality in condition (D6b) to $\mathsf{Tr}\left[V^+_{B'} + V^-_{B'}\right]/\mathsf{Tr}\left[V^+_{B'} - V^-_{B'}\right] = \gamma$, it follows that $\mathsf{Tr}[V^-_{B'}] = (\gamma - 1)\mathsf{Tr}[V^+_{B'}]/(\gamma + 1)$ and thus $\mathsf{Tr}_{B'}\left[R_{A'B'}\right] = (\gamma - 1)\mathbb{1}_{A'}/2$. Changing the variables to $V_{B'} := 2V^+_{B'}/(\gamma + 1)$ and $W_{B'} := V^-_{B'}$ gives the claimed SDP. ■

Similar to the one-shot zero-error shadow capacity, the SDP above implies that $S(1)_{\gamma,\mathrm{NS}}$ is a generalization of the no-signaling-assisted one-shot zero-error quantum simulation cost $S(1)_{\mathrm{NS}}$ as it reduces to the SDP for the latter [7, 10] when $\gamma = 1$. To showcase the difference between $S(1)_{\gamma,\mathrm{NS}}$ and $S(1)_{\mathrm{NS}}$, we consider the two-qubit amplitude damping channel $\mathcal{N}_{\mathrm{AD}}$, the two-qubit dephasing channel $\mathcal{N}_{\mathrm{deph}}$, and the two-qubit depolarizing channel $\mathcal{N}_{\mathrm{depo}}(\cdot) = p(\rho) + (1 - p)\mathbb{1}_4/4$, where $\mathbb{1}_4$ denotes the four-dimensional identity operator, the parameter $p \in [0, 1]$ indicates the level of noise, and by a two-qubit amplitude damping channel we mean two single-qubit amplitude damping channels with the same noise parameter acting independently on two qubits.

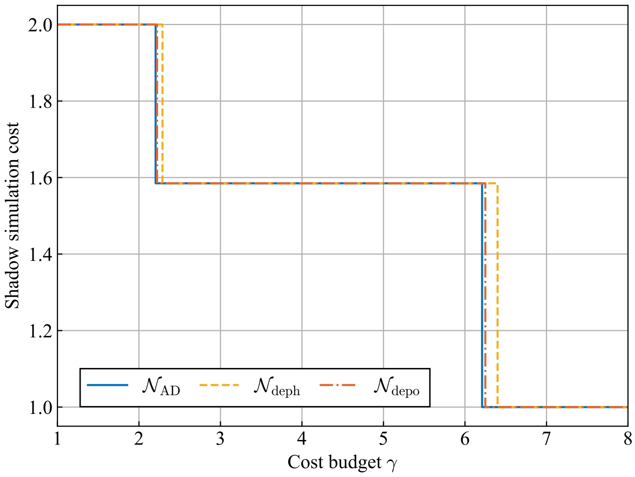


FIG. 4. Comparison between the conventional no-signaling-assisted one-shot zero-error quantum simulation cost $S^{(1)}_{\mathrm{NS}}$ and no-signaling-assisted one-shot zero-error shadow simulation cost $S^{(1)}_{\gamma,\mathrm{NS}}$ under different cost budgets γ. Compared with the quantum case, where the simulation cost is 2 for all channels, lower simulation cost is achieved for each channel with increased cost budget.

As in the task of shadow communication, we present numerical results on these channels at a low noise level ($p = 0.9$) in Figure 4. The zero-error simulation costs of these channels decrease from 2 (quantum simulation cost) to 1 with increased cost budget. Again, the stepwise changes in the zero-error simulation cost show that we can attain computational power beyond purely quantum protocols by trading in more computational resources.

In the main text, we presented the minimum sampling cost of simulating a high-dimensional identity channel with a low-dimensional one. Now, we prove this result.

Theorem 3 *Given identity channels* id_d *and* $\mathrm{id}_{d'}$ *with* $d' \geq d \geq 2$, *the minimum sampling cost of an exact shadow simulation of* $\mathrm{id}_{d'}$ *using* id_d *and no-signaling resources is*

$$\gamma^*_{0,\mathrm{NS}}\left(\mathrm{id}_d, \mathrm{id}_{d'}\right) = 2\left(\frac{d'}{d}\right)^2 - 1. \tag{D7}$$

Proof The Choi operators of the noiseless channel id_d from system A to system B and the noiseless channel $\mathrm{id}_{d'}$ from system A' to system B' are $J^{\mathrm{id}_d}_{AB} = \Gamma_{AB}$ and $J^{\mathrm{id}_{d'}}_{A'B'} = \Gamma_{A'B'}$, respectively. It is straightforward to verify that

$$\bar{V}^+_{B'} = d'\mathbb{1}_{B'}, \quad \bar{V}^-_{B'} = \frac{d'^2 - d^2}{d'}\mathbb{1}_{B'}, \quad \bar{R}_{A'B'} = \frac{d'(d'^2 - d^2)}{(d'^2-1)d^2}\mathbb{1}_{A'B'} - \frac{d'^2 - d^2}{(d'^2-1)d^2}\Gamma_{A'B'} \tag{D8}$$

form a feasible solution to the SDP for $\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d, \mathrm{id}'_d)$ as given in Lemma 13, implying

$$\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d, \mathrm{id}'_d) \leq \frac{1}{d^2}\mathsf{Tr}\left[\bar{V}^+_{B'} + \bar{V}^-_{B'}\right] = \frac{2d'^2}{d^2} - 1. \tag{D9}$$

Using the Lagrange dual function, we can derive that the following problem is the dual problem associated with SDP (D2):

$$\begin{aligned}\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d, \mathcal{M}_{A'\to B'}) \geq \sup\ & \mathsf{Tr}\left[M_{A'B'}J^{\mathcal{M}}_{A'B'}\right] - \lambda & \text{(D10a)}\\ \text{s.t. } & M_{A'B'} \geq 0,\ N_{A'B'} \geq 0,\ M_{A'B'} + N_{A'B'} + K_{A'} \otimes \mathbb{1}_{B'} \geq 0, & \text{(D10b)}\\ & d^2\mathsf{Tr}_{A'}\left[M_{A'B'}\right] = (1+\lambda)\mathbb{1}_{B'},\ d^2\mathsf{Tr}_{A'}\left[N_{A'B'}\right] = (1 - \lambda - \mathsf{Tr}\left[K_{A'}\right])\mathbb{1}_{B'}. & \text{(D10c)}\end{aligned}$$

It is straightforward to verify that

$$\bar{\lambda} = 1, \quad \bar{M}_{A'B'} = \frac{2}{d^2}\Gamma_{A'B'}, \quad \bar{N}_{A'B'} = 0, \quad \bar{K}_{A'} = 0. \tag{D11}$$

form a feasible solution to the dual problem for $\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d, \mathrm{id}_{d'})$, implying

$$\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d, \mathrm{id}_{d'}) \geq \mathsf{Tr}\left[\bar{M}_{A'B'}J^{\mathrm{id}_{d'}}_{A'B'}\right] - \bar{\lambda} = \frac{2d'^2}{d^2} - 1. \tag{D12}$$

Combining Eqs. (D9) and (D12), we conclude that

$$\gamma^*_{0,\mathrm{NS}}(\mathrm{id}_d, \mathrm{id}'_d) = \frac{2d'^2}{d^2} - 1, \tag{D13}$$

which completes the proof. ■

Device-independent quantum key distribution with arbitrarily small nonlocality (extended abstract)

Lewis Wooltorton *[1] [2] Peter Brown †[3] Roger Colbeck ‡[1]

[1] *Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom*
[2] *Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical & Electronic Engineering, University of Bristol, Bristol BS8 1FD, United Kingdom*
[3] *Télécom Paris - LTCI, Inria, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France*

Abstract. [Phys. Rev. Lett. **127**, 050503 (2021)] showed some correlations cannot be used for standard device-independent quantum key distribution (DIQKD), despite being nonlocal. This leads to the question of whether there is a fundamental minimum amount of nonlocality needed for DIQKD. Here we show no such bound exists: arbitrarily good key can be certified using correlations with arbitrarily small nonlocality. Somewhat surprisingly we also show that it is possible to simultaneously certify both perfect key and maximal randomness with a single set of correlations; the inequalities studied provide a direction for improving experimental robustness for DIQKD and DI randomness expansion.

Keywords: DIQKD, self-testing, nonlocality

1 Motivation

Distributing a secret key between two separated parties enables private communication over long distances. Given access to classical resources, security can only be established by making computational assumptions on an adversary, which are difficult to ensure given the advent of quantum computing. In contrast, sharing quantum resources, such as entanglement, enables secure key distribution against an arbitrarily powerful quantum adversary [1, 2, 3].

Despite the theoretical promises of quantum key distribution (QKD), its implementation security is typically dependent on well characterized devices. Any mismatch between the physical device and this characterization can open security loopholes (see e.g., [4]). Device-independent (DI) QKD aims to circumvent this problem, deriving security from the input-output behaviour of devices and without relying on their internal workings [2, 5, 6, 7, 8, 9, 10]. Any observation of nonlocality, that is, input-output statistics incompatible with any classical physical model, is a certificate of quantum behaviour within the device, and can be used to derive security. In a sense, DI protocols certify the underlying quantum mechanism used by the device (or enough about it to conclude that the device can carry out the task).

A natural question to ask is, how nonlocal does a device behaviour need to be to permit DIQKD? Nonlocality is clearly necessary, but when is it sufficient, if at all? Recently, the work of Farkas *et al.* [11] showed that not all nonlocal behaviours can be used for DIQKD under a standard class of protocols. Nevertheless, this left open whether a fundamental bound on the minimum amount of nonlocality needed to perform DIQKD exists.

In the related task of randomness expansion [12, 13, 14, 15, 16, 17], we recently showed that no such bound exists [18] — in fact, perfect randomness expansion is possible with arbitrarily small nonlocality. The main contribution of our submission is to prove an analogous result for DIQKD. In the 2-input 2-output scenario, we show that for an arbitrarily small violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality, there exist extremal quantum behaviours achieving that violation, which generate arbitrarily close to 1 secure key bit per entangled state. Moreover, for any CHSH value between the local bound of 2 and 5/2, there also exist quantum behaviours optimal for key generation. We also generalize the constructions from [18] which achieve the maximum of 2 random bits per entangled state. Finally, we introduce quantum behaviours that generate arbitrarily good key from one pair of measurement settings, and maximum global randomness from another, whilst exhibiting CHSH values between 2 and $1+\sqrt{2}$. To our knowledge, this is the first example of a quantum behaviour with this property in the literature.

2 Methods and results

We consider a spot checking DIQKD protocol with two inputs and two outputs per party, labeled X, Y, A, B (all binary), and an adversary E. The figure of merit is the asymptotic key-rate given by the Devetak-Winter formula [19], $H(A|X=0,E) - H(A|B,X=Y=0)$, minimized over all quantum states and measurements compatible with some observed statistics, where H is the conditional von Neumann entropy. Key-rates of non-asymptotic protocols can also be obtained via techniques like the entropy accumulation theorem [20, 10]. To derive our result, we design Bell expressions whose maximum violation is uniquely achieved by a strategy tailored to key generation. More precisely, the maximum value of our Bell-expressions allow us to self-test [21, 22, 23, 24, 25] the optimal state and measurements, which in turn imply that $H(A|X=0,E)=1$. Furthermore, our Bell expressions also self-test a key generation measurement

*lewis.wooltorton@york.ac.uk
†peter.brown@telecom-paris.fr
‡roger.colbeck@york.ac.uk

for Bob, from which we obtain a minimal error correction cost, i.e., $H(A|B, X = Y = 0) \approx 0$. Note that we do not require a third measurement for Bob, as is the case for many DIQKD protocols (see [26, Section 4.4] for an example using the CHSH inequality). In this Bell scenario, the nonlocality of a behaviour is quantified by its CHSH violation, I_{CHSH}, and we obtain our main result by self-testing behaviours that simultaneously lie close to the local boundary, and generate near perfect key.

The family of Bell expressions we study first appeared in [27, 28], and we provide an alternative self-testing proof using Jordan's lemma [29]. Our proof structure is modular, self-contained, and applicable generally to the 2-input 2-output scenario. The Bell expressions take the form:

$$\begin{aligned}\langle B_{\theta,\phi,\omega}\rangle = &\cos(\theta+\phi)\cos(\theta+\omega)\,\big\langle A_0\big(\cos\omega\, B_0 - \cos\phi\, B_1\big)\big\rangle\\ &+\cos\phi\cos\omega\,\big\langle A_1\big(-\cos(\theta+\omega)\, B_0 + \cos(\theta+\phi)\, B_1\big)\big\rangle,\end{aligned} \tag{1}$$

for any angles (θ, ϕ, ω) satisfying

$$\cos(\theta+\phi)\cos(\phi)\cos(\theta+\omega)\cos(\omega) < 0. \tag{2}$$

For such angles, the quantum bound is given by $\sin(\theta)\sin(\omega-\phi)\sin(\theta+\omega+\phi)$ and is uniquely achieved up to local isometries by the two-qubit strategy:

$$\begin{aligned}|\Phi_0\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\\ A_0 &= \sigma_Z,\ A_1 = \cos(\theta)\,\sigma_Z + \sin(\theta)\,\sigma_X\\ B_0 &= \sin(\phi)\,\sigma_Z + \cos(\phi),\\ B_1 &= \sin(\omega)\,\sigma_Z + \cos(\omega)\,\sigma_X,\end{aligned} \tag{3}$$

where σ_Z and σ_X are the Pauli operators.

By carefully choosing one or more of the parameters (θ, ϕ, ω) such that Eq. (2) holds, we can tune the self-tested measurements of both devices to perform well at a given task. More precisely, we obtain three sub-families of Eq. (1) tailored for randomness generation, key generation, and both, which are saturated by behaviours exhibiting an arbitrarily small CHSH violation. These are summarized below:

(i) A two-parameter family of Bell expressions that certifies 2 bits of global DI randomness, conditioned on the input choice $X = 0, Y = 1$, that is $\inf H(AB|X = 0, Y = 1, E) = 2$. The range of achievable CHSH violations are displayed in Fig. 1, and cover the interval $(2, 3\sqrt{3}/2]$, recovering the result of [18] as a special case.

(ii) A two-parameter family of Bell expressions tailored for maximal key generation, conditioned on the input choice $X = Y = 0$, that is $\inf H(A|X = 0, E) - H(A|B, X = Y = 0) = 1 - \epsilon$ for any $\epsilon > 0$. CHSH violations in the interval $(2, 5/2]$ are achieved, which is our main result: near perfect DIQKD is compatible with arbitrarily small nonlocality. The full range of achievable CHSH values are displayed in Fig. 2.

(iii) A one-parameter family of Bell expressions that certify near optimal key from one pair of measurement settings, and maximum global randomness from another; that is, $\inf H(A|X = 0, E) - H(A|B, X = Y = 0) = 1 - \epsilon$, $\epsilon > 0$, and $\inf H(AB|X = 0, Y = 1, E) = 2$. The interval of CHSH values $(2, 1 + \sqrt{2}]$ is achieved, and can be seen by the dashed black lines in Fig. 2; we see both near perfect key and perfect randomness can be certified from a single quantum behaviour lying arbitrarily close to the local boundary.

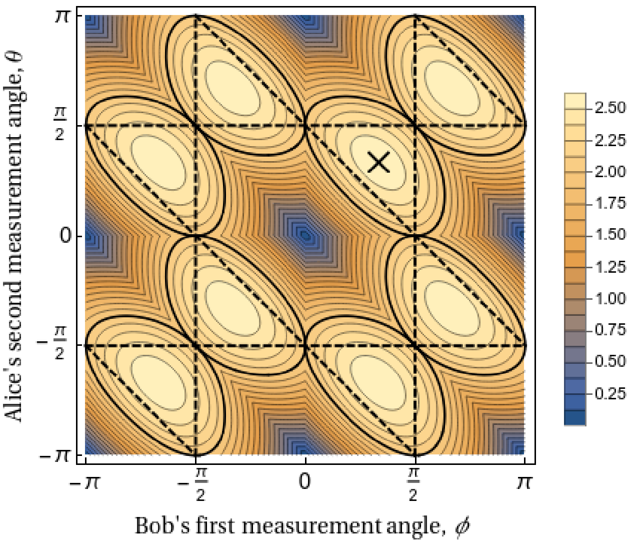


Figure 1: Contour plot of nonlocality, measured using the maximum of the 8 CHSH-type inequalities, for the strategies in Eq. (3) with $\omega = \pi$. The points inside the dashed triangles, excluding the boundary, can be used for perfect DIRE with a single linear Bell inequality: they satisfy Eq. (2) and have a value in $(2, 3\sqrt{3}/2]$ for one of the CHSH-type inequalities, with the maximum of I_{CHSH} indicated with the black cross at $\theta = \phi = \pi/3$. Approaching $\phi = -\pi/2$ or $\phi = \pi/2$ inside the corresponding region also allows arbitrarily good DIQKD. The black contours indicate $I_{\text{CHSH}} = 2$ for at least one CHSH-type inequality.

3 Impact

Our results prove that there is no fundamental bound on the minimum nonlocality needed to enable DIQKD. The underlying reason for this is that there exist extremal quantum behaviours that lie near the boundary of the local set which can be self-tested with a single Bell expression, and consist of a measurement pair with near perfectly correlated outcomes. In addition, such behaviours can have another measurement combination with perfectly un-correlated outcomes, giving rise to a stronger statement concerning maximal key and randomness with arbitrarily small nonlocality. This progresses our understanding of fundamental limits in DI cryptography, and answers a question left open by Farkas *et al.* [11] who, in contrast, showed there exist behaviours in the interior

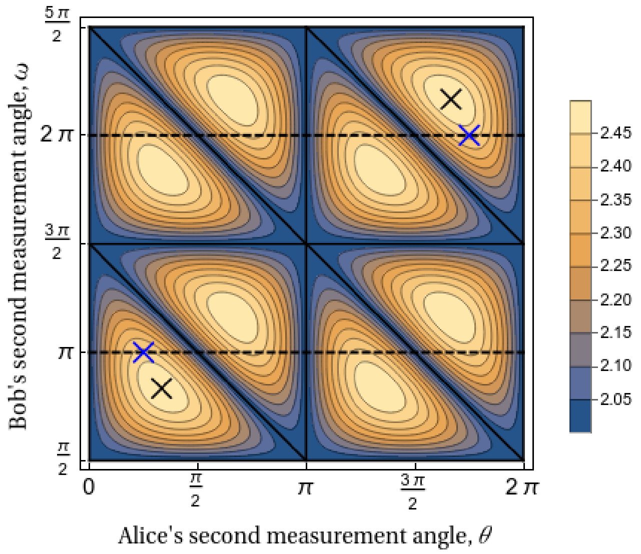


Figure 2: Contour plot of nonlocality, measured using the maximum of the 8 CHSH-type inequalities of the strategies in Eq. (3), at the limit $\phi = \pi/2$. The contours with CHSH values equal to 2 are the black triangular lines, and are the limit points of correlations that achieve arbitrarily perfect DIQKD with a single linear Bell inequality. The black dashed lines show where perfect DIRE can also be achieved, with the blue crosses denoting the maximum value of $I_{\text{CHSH}} = 1 + \sqrt{2}$ at $\theta = \pi/4, \omega = \pi$ and $\theta = 7\pi/4, \omega = 2\pi$. The black crosses denote the global maximum of $I_{\text{CHSH}} = 5/2$ at $\theta = \pi/3, \omega = 5\pi/6$ and $\theta = 5\pi/3, \omega = 13\pi/6$.

of the quantum set, which are nonlocal, yet cannot be used for DIQKD under standard protocols. As we have now shown, this fact does not imply the existence of a fundamental bound.

In addition, we highlighted the versatility of the Bell expressions used, and given the additional degrees of freedom, it would be interesting to understand their practical benefit. For example, an experimentalist could optimize the Bell expression for their setup, possibly yielding larger rates in a DI task such as randomness expansion or key distribution. We also introduced a spot-checking DIQKD protocol which remains in the two-input two-output scenario, rather than adding a third measurement for Bob as is typically done when using the CHSH inequality. This simpler setup removes the need for additional alignment tests, which might make the protocol more efficient with finite numbers of rounds.

Finally, to the best of our knowledge, we have given the first example of behaviours which exhibit near-perfect key and perfect randomness from different measurement combinations. It would be interesting if this could find an application in a novel DI protocol. For example, perfect global randomness implies a single bit of blind randomness per party, per round. One might hope to distill this randomness alongside a DIQKD protocol, replenishing the randomness consumed during key exchange.

For the full technical manuscript, please see arXiv:2309.09650. During the writing up of this work we became aware of a related work [30] that also shows the possibility of key distribution with arbitrarily small nonlocality using an alternative approach.

References

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE, New York, 1984.

[2] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, Sep 2009.

[4] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2:349, 2011.

[5] John Barrett, Lucien Hardy, and Adrian Kent. No signalling and quantum key distribution. *Physical Review Letters*, 95:010503, 2005.

[6] Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007.

[7] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[8] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Physical Review A*, 86:062326, 2012.

[9] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113:140501, Sep 2014.

[10] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications*, 9(1):459, 2018.

[11] Máté Farkas, Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński, and Antonio Acín.

Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. *Physical Review Letters*, 127:050503, Jul 2021.

[12] Roger Colbeck. *Quantum and Relativistic Protocols For Secure Multi-Party Computation.* PhD thesis, University of Cambridge, 2007. Also available as arXiv:0911.3814.

[13] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010.

[14] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A*, 44(9):095305, 2011.

[15] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 417–426, New York, NY, USA, 2014. ACM.

[16] Carl A. Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol. *SIAM Journal of Computing*, 46:1304–1335, 2017.

[17] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8:450–454, 2012.

[18] Lewis Wooltorton, Peter Brown, and Roger Colbeck. Tight analytic bound on the trade-off between device-independent randomness and nonlocality. *Physical Review Letters*, 129:150403, Oct 2022.

[19] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[20] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *Communication in Mathematical Physics*, 379:867–913, 2020.

[21] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information and Computation*, 4:273–286, 2004.

[22] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, Oct 2012.

[23] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87:050102, May 2013.

[24] Jędrzej Kaniewski. Self-testing of binary observables based on commutation. *Physical Review A*, 95:062323, Jun 2017.

[25] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, Sep 2020.

[26] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020.

[27] Thinh P. Le, Chiara Meroni, Bernd Sturmfels, Reinhard F. Werner, and Timo Ziegler. Quantum correlations in the minimal scenario. *Quantum*, 7:947, March 2023.

[28] Victor Barizien, Pavel Sekatski, and Jean-Daniel Bancal. Custom Bell inequalities from formal sums of squares. e-print arXiv:2308.08601, 2023.

[29] C. Jordan. Essai sur la géométrie à n dimensions. *Bulletin de la S. M. F.*, 3:103–174, 1875.

[30] Máté Farkas. Unbounded device-independent quantum key rates from arbitrarily small non-locality. e-print arXiv:2310.08635, 2023.

Finite-key security of differential-phase-shift QKD

Akihiro Mizutani[1] Yuki Takeuchi[2 3] Kiyoshi Tamaki[1]

[1]*Faculty of Engineering, University of Toyama, Japan*
[2]*NTT Communication Science Laboratories, NTT Corporation, Japan*
[3] *NTT Research Center for Theoretical Quantum Information, NTT Corporation, Japan*

Abstract. Differential-phase-shift (DPS) quantum key distribution (QKD) is one of the major QKD protocols, and it is implementable with a simple experimental setup using a train of coherent pulses and a passive measurement unit composed of a basic optical interferometer. Thanks to this simplicity, its field demonstration was conducted in the Tokyo QKD network, and there are high expectations for future practical use. However, the experimental simplicity would imply that the number of available experimental parameters is small, and thus its information-theoretic security proof becomes challenging. In fact, all previous security proofs needed assumptions on eavesdropper's attacks or assumptions that compromise the simplicity of the DPS protocol. In this work, we provide an information-theoretic security proof of the DPS protocol in the finite-key regime while maintaining the inherent experimental simplicity of this protocol. As a result of our security proof, we reveal that a 3 Mbit unconditionally secure key can be distributed over 77 km in 8.3 hours, assuming typical experimental setups. This result demonstrates the feasibility of the DPS protocol for generating secret keys over long distances in realistic experimental setups and contributes to realizing truly secure communication. The full details of this work can be found in [1].

Keywords: quantum cryptography, finite-key security proof, concentration inequality

1 Introduction

Quantum key distribution (QKD) realizes information-theoretically secure communication between two distant parties (Alice and Bob) against any eavesdropper (Eve) [2, 3]. Among QKD protocols, the differential-phase-shift (DPS) protocol [4] is a promising one, which can be implemented with an experimentally simple setup using a train of coherent pulses and a passive measurement unit composed of a Mach-Zehnder interferometer (see Fig. 1). Due to its simplicity, experimental demonstrations were conducted in [5, 6, 7], and also its field demonstration was executed in the Tokyo QKD network [8]. Although the DPS protocol has an advantage of simple implementation, establishing its security proof is a challenging problem. This is because, in general, the security proof of QKD becomes more complex as the experimental setup is simplified. To make the security proof of the DPS protocol easier, previous works restricted Eve's attacks on the quantum channel [9, 10, 11] or made assumptions that compromise the simplicity of the experiment, such as employing a single-photon source [12] or a phase randomized coherent source [13, 14].

In our previous work [15], we established the information-theoretic security proof of the DPS protocol while maintaining the inherent simplicity of this protocol. Unfortunately, this security proof is only valid in the asymptotic regime, where the length of the sifted key is assumed to be infinite. To implement the DPS protocol in the real world, it is indispensable to reveal its key-generation efficiency with a finite key length.

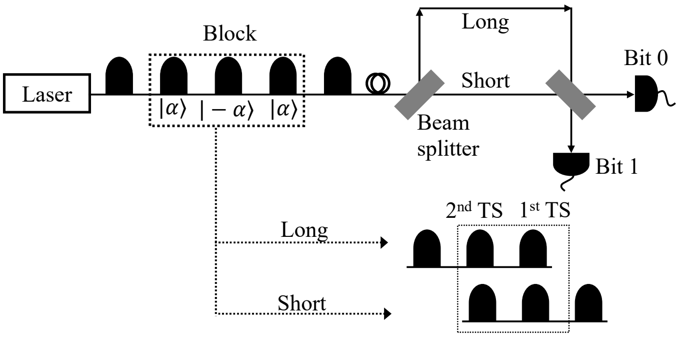


Figure 1: Schematics of our DPS protocol. Alice sends blocks of three pulses to Bob, and he receives them with the one-bit delay Mach-Zehnder interferometer and detectors. A detection event occurs if Bob obtains one photon in total among the 1st and 2nd time slots (TSs).

Here, we solve this problem by providing the finite-key security proof of the DPS protocol [1]. In the finite-key analysis, it is crucial to evaluate statistical deviation terms of concentration inequalities in deriving an upper bound on the amount of privacy amplification N_{PA}. In so doing, it is important to employ a concentration inequality that results in a small deviation with a smaller number of trials; otherwise the speed of convergence to the asymptotic key rate becomes slow, leading to a poor performance. For this, Azuma's inequality [16] is a well-known concentration inequality used in various security proofs [17]-[21]. However, we reveal that the analysis with Azuma's inequality results in a substantially low key rate under a realistic experimental setup. To overcome this problem, we exploit Kato's inequality [22, 23] and show that the key rate is drastically improved. Specifically, our numerical simulation shows that its achievable distance becomes more than four times longer than the one based on the analysis using Azuma's inequality with typical experimental setups. Also, assuming the number of emitted pulses that can be realized within practical experimental times, we find that the rate does not significantly degrade from the asymptotic limit (see Fig. 2).

2 Main result

We first describe our DPS protocol followed by stating our main result, Theorem 1. In the following protocol description (see Fig. 1), we assume that Alice emits weak coherent states $|\alpha\rangle$ of intensity $\mu := \alpha^2 \ll 1$ with modulating the phase either 0 or π perfectly. However, this demanding assumption is not mandatory; as long as Alice emits independent and identically distributed states, she can securely employ them in the DPS protocol, even without knowledge of the emitted states [24, 1]. This is another advantage of the DPS protocol, which is important for the implementation security of QKD [3].

(P1) Alice and Bob respectively repeat the following procedures for N rounds.

  (a) Alice generates uniformly random three bits $b_1b_2b_3 \in \{0,1\}^3$ and sends three coherent states (we call three coherent states *block*)

$$\bigotimes_{i=1}^{3} |(-1)^{b_i}\alpha\rangle_{B_i} \qquad (1)$$

  to Bob via a quantum channel.

  (b) Bob forwards the incoming three pulses into the Mach-Zehnder interferometer followed by photon detection by single-photon detectors. We call the round *detected* if Bob detects one photon in total among the 1st and 2nd time slots. The detection event at the jth time slot determines the raw key bit $d \in \{0,1\}$ depending on which of the two detectors clicks.

(P2) Bob takes note of a set of detected rounds $\mathcal{D} \subseteq \{1,...,N\}$ with length $N_{\mathrm{det}} := |\mathcal{D}|$, a set of time slots $\boldsymbol{j} := (j_i)_{i\in\mathcal{D}}$, and a raw key $\boldsymbol{d} := (d_i)_{i\in\mathcal{D}}$. Here, j_i and d_i are j and d of the ith detected round, respectively. Bob associates each detected round with a code or sample round with probability t or $1-t$, respectively ($0 < t < 1$). He defines the code set $\mathcal{D}_{\mathrm{code}}$ with length $N_{\mathrm{code}} := |\mathcal{D}_{\mathrm{code}}|$, the sample one $\mathcal{D}_{\mathrm{sample}} := \mathcal{D} \setminus \mathcal{D}_{\mathrm{code}}$ with length $N_{\mathrm{sample}} := |\mathcal{D}_{\mathrm{sample}}|$, his sifted key $\kappa_B := (d_i)_{i\in\mathcal{D}_{\mathrm{code}}}$ and the sample bit sequence $\kappa_B^{\mathrm{sample}} := (d_i)_{i\in\mathcal{D}_{\mathrm{sample}}}$.

(P3) Bob announces $\mathcal{D}_{\mathrm{code}}$, $\mathcal{D}_{\mathrm{sample}}$, $\boldsymbol{j}$ and $\kappa_B^{\mathrm{sample}}$ to Alice through an authenticated public channel.

(P4) Alice calculates her sifted key $\kappa_A := (b_{j_i} \oplus b_{j_i+1})_{i\in\mathcal{D}_{\mathrm{code}}}$ and sample bit sequence $\kappa_A^{\mathrm{sample}} := (b_{j_i} \oplus b_{j_i+1})_{i\in\mathcal{D}_{\mathrm{sample}}}$.

(P5) (Bit error correction) Using a pre-shared secret key of length N_{EC}, Bob corrects the bit errors in his sifted key κ_B and obtains the reconciled key κ_B^{rec}. By consuming a pre-shared secret key of length ζ', Alice and Bob verify the correctness of their reconciled keys by comparing the output (ζ'-bit) of a randomly chosen universal$_2$ hash function H_{EC}.

(P6) (Privacy amplification) Alice and Bob conduct privacy amplification by shortening their reconciled keys by N_{PA} bits and respectively share the final keys k_A and k_B of length $N_{\mathrm{fin}} = N_{\mathrm{code}} - N_{\mathrm{PA}}$.

We define the bit error rate in the sample rounds by

$$e_{\mathrm{bit}} := \mathrm{wt}(\kappa_A^{\mathrm{sample}} \oplus \kappa_B^{\mathrm{sample}})/N_{\mathrm{sample}}.$$

Here, wt$(\cdot)$ denotes the Hamming weight. The net length of the final key, namely, the increased length of the secret key is $\ell = N_{\mathrm{code}} - N_{\mathrm{PA}} - N_{\mathrm{EC}} - \zeta'$.

Below, we state the result of our security proof revealing the amount of privacy amplification $N_{\mathrm{PA}} = N_{\mathrm{code}} h\left(\frac{M_{\mathrm{ph}}^{\mathrm{U}}}{N_{\mathrm{code}}}\right)$ against any Eve's attack, based on the phase-error correction approach [28] (see details in Sec. 3). Importantly, the upper bound on the number of phase errors $M_{\mathrm{ph}}^{\mathrm{U}}$ in Eq. (3) is expressed as a function of the experimental parameters obtained in the above protocol; once the protocol is completed, this amount can be determined. We adopt the standard composable security framework [25, 26], where the imperfection of the final keys k_A and k_B is measured by the trace distance between the actual and ideal states of Alice, Bob and Eve, which is upper-bounded by the security parameter ϵ_{sec}.

Theorem 1 *For any ζ, $\zeta' > 0$ and $0 < \epsilon_1, \epsilon_2 < 1$, the above DPS protocol generates the secret key of length*

$$\ell = N_{\mathrm{code}} - N_{\mathrm{code}} h\left(M_{\mathrm{ph}}^{\mathrm{U}}/N_{\mathrm{code}}\right) - N_{\mathrm{EC}} - \zeta', \qquad (2)$$

$$M_{\mathrm{ph}}^{\mathrm{U}} := \frac{(3+\sqrt{5})te_{\mathrm{bit}}N_{\mathrm{sample}}}{1-t} + tq_2N + \Gamma_2 + (3+\sqrt{5})\times \prod_{n=1,3} \sqrt{tq_nN + \Gamma_n + \Delta_n(n,\epsilon_1)} + t\Delta_1(D^2,\epsilon_1) \qquad (3)$$

with $\epsilon_{\mathrm{sec}} = 2^{-\zeta'} + \sqrt{2}\sqrt{3(\epsilon_1+\epsilon_2) + 2^{-\zeta}}$. *Here,* $\Delta_1(x,y) := \sqrt{-2xN_{\mathrm{det}}\ln y}$,

$$D := \max\left\{(4+\sqrt{5}-t)/(1-t), 1/t + 4 + \sqrt{5}\right\},$$

$$\Gamma_n := \left[\sqrt{(\ln\epsilon_2)^2 - 8tq_nN\ln\epsilon_2} - \ln\epsilon_2\right]/2,$$

$h(x)$ is the binary entropy function, $\Delta_3(n,\epsilon)$ is the deviation term of Kato's inequality [22] (see Eq. (42) [1]), and q_n denotes the probability of emitting n or more photons in each emitted block, namely, $q_n = \sum_{\nu=n}^{\infty} e^{-3\mu}(3\mu)^\nu/\nu!$ for $n = 1, 2, 3$.

As a result of the security proof, in Fig. 2, we present our simulation results of the key rate $R = \ell/3N$ with ℓ given in Eq. (2) as a function of the channel transmission η including the detection efficiency. We optimize R over the mean photon number μ of the emitted pulse and the probability t of choosing the code round in step (P2) for each value of η. We assume the number of detected rounds as $N_{\mathrm{det}} = 2N\eta\mu e^{-2\eta\mu}$, $N_{\mathrm{code}} = tN_{\mathrm{det}}$, $N_{\mathrm{sample}} = (1-t)N_{\mathrm{det}}$, and the practical cost of error correction being $N_{\mathrm{EC}} = 1.16N_{\mathrm{code}}h(e_{\mathrm{bit}})$ with 1.16 [27] is an error

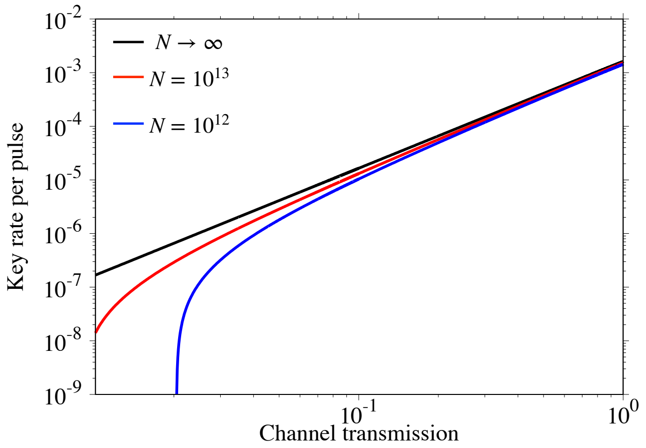


Figure 2: Secret key rate $R = \ell/3N$ of our DPS protocol per an emitted pulse as a function of the overall channel transmission η. From top to bottom, we plot the key rates for $N = \infty, 10^{13}, 10^{12}$ under the 1% bit error rate and a typical security parameter $\epsilon_{\rm sec} \fallingdotseq 10^{-8.1}$.

correction inefficiency. Also, we set $\zeta' = 28$, $\zeta = 58$, and $\epsilon_1 = \epsilon_2 = 2^{-58}/6$, which results in $\epsilon_{\rm sec} \fallingdotseq 10^{-8.1}$. From the result with $N = 10^{13}$ in Fig. 2, if we assume the overall channel transmission as $\eta = 0.5 \times 10^{-\frac{0.2l}{10}}$ with l denoting the distance between Alice and Bob and laser diodes operating at 1 GHz repetition rate, by running our protocol for 8.3 hours, we can generate a 3 Mbit secret key for a channel length of 77 km under 1% bit error rate. The results suggest the feasibility of long-distance QKD with realistic time and experimental setups.

3 Proof idea of Theorem 1

In the proof of Theorem 1, we consider the entanglement-based scenario, which gives the same statistics of the final keys k_A and k_B as in the actual protocol. In this scenario, instead of Alice preparing the state in Eq. (1), she prepares the following entangled state

$$\bigotimes_{i=1}^{3} \left(|0\rangle_{A_i}|\alpha\rangle_{B_i} + |1\rangle_{A_i}|-\alpha\rangle_{B_i}\right)/\sqrt{2}$$

and sends only systems $B_1B_2B_3$ to Bob. Bob's setup is the same as in Fig. 1. When the detection event occurs at the 1st time slot, Alice obtains her shifted key by applying the CNOT gate to qubits A_1 and A_2 and measuring the target qubit A_2 in the Z-basis $\{|0\rangle, |1\rangle\}$. Our proof adopts the complementarity proof technique [28], and its goal is to determine the number of phase errors $M_{\rm ph}$. A phase error is an event where Alice fails to predict the measurement outcome $x_{A_2} \in \{0,1\}$ if qubit A_2 were measured in the complementary X-basis instead of the Z-basis. This prediction is a task of guessing which of the first or second emitted pulse contained a photon. Since the result of this X-measurement cannot be obtained directly from the actual protocol, we need to estimate the number of failures in predicting this outcome from the actually observed quantities. For this prediction, measurements that do not disturb x_{A_2} can be performed. Hence, to enhance the accuracy of her prediction, Alice measures qubit A_1 in the X-basis and obtains the parity information $x_{A_1} \oplus x_{A_2}$. Furthermore, Bob performs a measurement to know which pulse contains a photon by removing the second beam splitter and informs Alice of this information $t_{\rm Bob}$ (see Fig. 3). Using the information $x_{A_1} \oplus x_{A_2}$ and $t_{\rm Bob}$, Alice predicts x_{A_2}. Let Y_i be the binary random variable representing the presence of a phase error in the ith detection event and $M_{\rm ph} = \sum_{i=1}^{N_{\rm det}} Y_i$ be the number of phase errors. Here, due to Eve's attack on the quantum channel, these random variables Y_i are correlated with each other, and therefore, to relate $M_{\rm ph}$ to the actually observed quantities in the protocol, it is necessary to use a concentration inequality applicable to correlated stochastic processes.

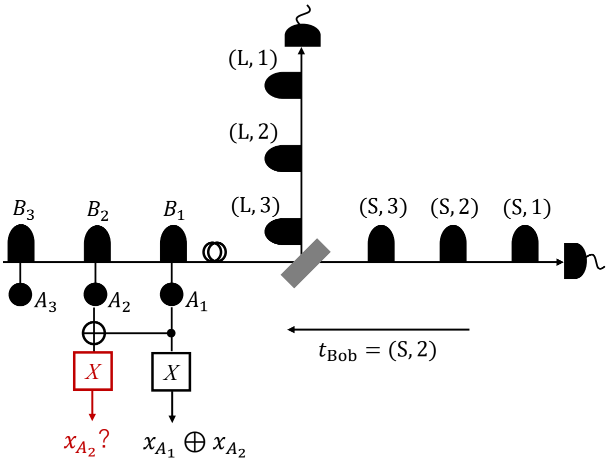


Figure 3: Alice's complementary task of predicting the outcome $x_{A_2} \in \{0,1\}$ if qubit A_2 were measured in the X-basis. A phase error occurs if she fails in the prediction.

In the case of correlated stochastic processes, Azuma's inequality is a well-known concentration inequality to relate a random variable and its expectation [17]-[21]. In Eq. (3), $tq_3N + \Gamma_3 + \Delta_3(3, \epsilon_1)$ is the upper bound on the random variable X_3 representing the number of times Alice emits three photons in a block and Bob obtains a detection event. In the proof of Theorem 1, X_3 appears as the result of evaluation of its expectation $E[X_3]$. We reveal that applying Azuma's inequality to this evaluation results in a significant decrease in the key rate due to the large deviation term $|X_3 - E[X_3]|$ compared to X_3 (see Fig. 5 in [1]). This is because the event of emitting three photons, whose probability is $q_3 \sim \mu^3$, hardly occurs in the protocol using weak coherent states with intensity $\mu \ll 1$. On the other hand, Kato's inequality can incorporate the knowledge of the rarity of the events into the concentration inequality (more precisely, our estimation of X_3 can be reflected in the inequality), thereby reducing the deviation term. This is the reason why we apply Kato's inequality to upper-bound $E[X_3]$ with X_3.

References

[1] **A. Mizutani, Y. Takeuchi, and K. Tamaki, Physical Review Research 5, 023132 (2023).**

[2] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595-604 (2014).

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Reviews of Modern Physics **92**, 025002 (2020).

[4] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[5] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, New. J. Phys. **7**, 232 (2005).

[6] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Optics Express **14**, 13073 (2006).

[7] H. Takesue, S.-W. Nam, Q. Zhang, R.-H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nature Photonics **1**, 343 (2007).

[8] M. Sasaki, M. Fujiwara, H. Ishizuka, et al, Optics Express **19**, 11 (2011).

[9] E. Waks, H. Takesue, and Y Yamamoto, Phys. Rev. A **73**, 012344 (2006).

[10] H. Endo, T. Sasaki, M. Takeoka, M. Fujiwara, M. Koashi, and M. Sasaki, New J. Phys. **24**, 025008 (2022).

[11] M. Sandfuchs, M. Haberland, V. Vilasini, and R. Wolf, arXiv:2301.11340 (2023).

[12] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).

[13] K. Tamaki, G. Kato, and M. Koashi, arXiv:1208.1995v1 (2012).

[14] A. Mizutani, T. Sasaki, G. Kato, Y. Takeuchi, and K. Tamaki, Quantum Science and Technology **3**, 014003 (2017).

[15] A. Mizutani, T. Sasaki, Y. Takeuchi, K. Tamaki, and M. Koashi, npj Quantum Information **5**, 87 (2019).

[16] K. Azuma, Tohoku Math. J. **19**, 357–367 (1967).

[17] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).

[18] S. Pironio, Ll. Masanes, A. Leverrier, and Acín, Phys. Rev. X **3**, 031007 (2013).

[19] U. Vazirani, and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[20] A. Mizutani, M. Curty, C. C. W Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).

[21] K. Tamaki, H.-K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty, Quantum Science and Technology **3**, 014002 (2017).

[22] G. Kato, arXiv:2002.04357v2 (2020).

[23] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, npj Quantum Information **7**, 22 (2021).

[24] A. Mizutani, Phys. Rev. A **102**, 022613 (2020).

[25] R. Renner, and R. Koenig, Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings, Vol. 3378 of Lecture Notes in Computer Science (Springer, ADDRESS, 2005), pp. 407-425.

[26] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings, Vol. 3378 of Lecture Notes in Computer Science (Springer, ADDRESS, 2005), pp. 386-406.

[27] G. Brassard and L. Salvail, Advances in Cryptology EUROCRYPT'93, May 1993.

[28] M. Koashi, New Journal of Physics **11**, 045018 (2009).

Pilot-reference-free continuous-variable quantum key distribution with efficient decoy-state analysis

Anran Jin[1] Xingjian Zhang[2] Liang Jiang[3] Richard V. Penty[1] Pei Zeng[3] *

[1] *University of Cambridge, CAPE Building 9 JJ Thomson Avenue, CB3 0FA Cambridge, UK*
[2] *Tsinghua University, Beijing, 100084 China*
[3] *University of Chicago, Illinois 60637, USA*

Abstract. We propose a continuous-variable quantum key distribution (CV QKD) protocol with time-bin encoding and present a complete security analysis using discrete-variable (DV) methods. The new protocol is secure under the most general attacks and does not require any pilot reference, a costly requirement for common CV QKD. We unify the security analysis of CV QKD under standard DV approaches through the discrete photon-number tagging of the continuous optical fields. Moreover, by applying the DV technique of decoy states to the parameter estimation, our CV QKD protocol yields short-distance key-rate performance comparable to the state-of-the-art Bennett-Brassard-1984 implementation.

Keywords: quantum communication, quantum key distribution, coherent detection, quantum optics

1 Introduction

Continuous-variable quantum key distribution (CV QKD) [1–3] using optical coherent detectors is practically favorable due to its low implementation cost, flexibility of wavelength division multiplexing [4–6], and compatibility with standard coherent communication technologies [7]. However, the security analysis and parameter estimation of CV QKD are complicated due to the infinite-dimensional latent Hilbert space [8]. Also, the transmission of strong reference pulses undermines the security and complicates the experiments [9–14].

In this work, we tackle these two problems by presenting a time-bin-encoding CV protocol with a simple phase-error-based security analysis valid against general coherent attacks [15–17]. With the key encoded into the relative intensity between two optical modes, the need for global references is removed. Furthermore, phase randomization can be introduced to decouple the security analysis of different photon-number components. We can hence tag the photon number for each round, effectively estimate the associated privacy using a carefully designed coherent-detection method, and independently extract encryption keys from each component [18, 19]. Simulations manifest that the protocol using multi-photon components increases the key rate by two orders of magnitude compared to the one using only the single-photon component. Meanwhile, the protocol with four-intensity decoy analysis [20, 21] is sufficient to yield tight parameter estimation with a short-distance key rate comparable to the best Bennett-Brassard-1984 (BB84) implementation.

2 Protocol and security analysis outline

The protocol implementation is given in Fig. 1. Raw keys are obtained when both Alice and Bob choose the Z-basis, Alice chooses light intensity $\mu_a = \mu$, and Bob obtains a non-abort key bit $k_b \neq \emptyset$. The Z-bases are mainly used for key encoding and decoding, and the X-bases are used for parameter estimation. Here, we briefly explain the ideas behind the protocol design.

2.1 Time-bin BB84-like key encoding/decoding (Z-bases)

1. Source states:

(1) Alice's raw key k_a is encoded in the relative intensity between two time-bin modes (0 versus μ_a in two modes);
(2) Joint phase randomization block-diagonalizes the two-mode state on the total photon-number basis (random phase parameter φ_a over two modes).

2. Detection:

(1) Bob's raw key k_b is decoded from light intensity measurement (difference between quadrature absolute values $|q_1|$ and $|q_2|$);
(2) A threshold value τ in quadrature measurement is set to tackle shot noise in homodyne detection (an abort result $k_b = \emptyset$ is allowed);
(3) LO phase randomization block-diagonalizes the POVM elements on the total photon-number basis (random phase parameter φ_b over two LOs).

The key encoding and decoding resembles the time-bin-encoding BB84 protocol with coherent states [22], with the difference that single-photon detectors are replaced with homodyne detectors. As the key is encoded in the relative intensity, the protocol avoids the necessity of a pilot reference pulse.

For security analysis, we set up an equivalent virtual protocol (Fig. 2). On the source side, we set up an equivalent entanglement-based key encoding. On the detection side, we set up an equivalent squashing channel that generates the raw key with the same acceptance ($k_b \neq \emptyset$) probability. Alice's and Bob's raw keys k_a and k_b can be seen as Z-basis measurement results on qubit systems A' and B', respectively. This allows a discrete-variable-type complementarity-based security analysis [17]: Should Alice and Bob instead measure the qubit systems on the complementary X-basis, the probability they obtain different results, or the phase-error rate, e^X, could be used to upper-bound the privacy amplification cost.

*peizeng@uchicago.edu

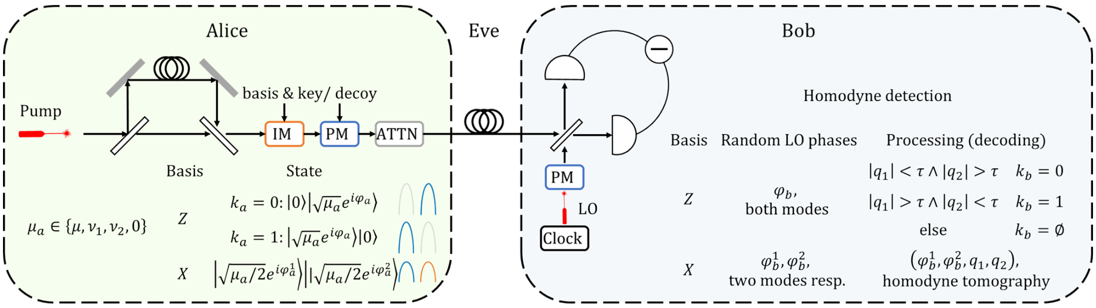

Alice
Eve
Bob
Pump
basis & key/ decoy
IM
PM
ATTN
Basis
State
$\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$
Z
$k_a = 0\colon |0\rangle\left|\sqrt{\mu_a}e^{i\varphi_a}\right\rangle$
$k_a = 1\colon \left|\sqrt{\mu_a}e^{i\varphi_a}\right\rangle|0\rangle$
X
$\left|\sqrt{\mu_a/2}e^{i\varphi_a^1}\right\rangle\left|\sqrt{\mu_a/2}e^{i\varphi_a^2}\right\rangle$
PM
LO
Clock
Homodyne detection
Basis
Random LO phases
Processing (decoding)
Z
φ_b, both modes
$|q_1| < \tau \wedge |q_2| > \tau$ $k_b = 0$
$|q_1| > \tau \wedge |q_2| < \tau$ $k_b = 1$
else $k_b = \emptyset$
X
φ_b^1, φ_b^2, two modes resp.
$(\varphi_b^1, \varphi_b^2, q_1, q_2)$, homodyne tomography

Figure 1: Experimental setup. Alice's state preparation and Bob's detection and processing are listed in the tables. IM: intensity modulation; PM: phase modulation; ATTN: attenuation; LO: local oscillator.

After phase randomization (blue boxes), photon-number measurements M_{n_a} and M_{n_b} can be inserted without changing the key statistics. We can hence tag the emitted and received pulses according to the photon-number space, allowing the Gottesman-Lütkenhaus-Lo-Preskill (GLLP) framework [18] for analyzing the key privacy contained in each photon-number subspace.

2.2 Reverse reconciliation

Alice reconciles her raw keys with respect to Bob's. Therefore, the rounds Bob receives a vacuum state become secure. This is a common practice in usual CV QKD and in accordance with the observation in Ref. [23]. Based on the above design, we have the following result.

Theorem 1 (Asymptotic limit) *For the time-bin CV QKD protocol in Fig. 1 with reverse reconciliation, the distillable secure key rate r is lower bounded by r_{rev},*

$$r \geq r_{\text{rev}} = Q_{*,0} + \sum_{m=1}^{\infty} Q_{m,m}[1 - h(e^X_{m,m})] - fQ^Z h(e^Z), \tag{1}$$

$Q_{m,n}$ (gain): probability of sending an m-photon state and accepting an n-photon state; $e^X_{m,m}$: phase-error rate in the rounds where m photons are sent and m photons are accepted; $Q_{*,0}$: gain of the rounds where Bob accepts a vacuum state; Q^Z: Z-basis gain; e^Z: bit-error rate; f: efficiency of information reconciliation.

We discard the rounds where the total photon number decreases after state transmission, as Eve can apply a photon-number-splitting attack. In addition, we do not account for the terms where the total photon number increases, considering the practical lossy channels.

2.3 Parameter estimation (X-bases)

The phase-error probabilities and gains are defined by particular Fock-basis states. For instance, the single-photon phase-error rate is defined via the probability that Alice transmits $\left|\Psi_1^{\pm}\right\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ while Bob measures $\left|\Psi_1^{\mp}\right\rangle$, and the two-photon phase-error rate is defined via the probability that Alice transmits $\left|\Psi_2^{\pm}\right\rangle = (|02\rangle \pm |20\rangle)/\sqrt{2}$ while Bob measures $\left|\Psi_2^{\mp}\right\rangle$ or $|11\rangle$. To estimate these values, we construct unbiased estimators with the available coherent states and homodyne detection settings.

1. **Source:** To construct the state for desired statistics, we utilize coherent states from both bases,

$$\begin{aligned}&\Pr_\mu(m)\left|\Psi_m^{\pm}\right\rangle\left\langle\Psi_m^{\pm}\right| \\ =&\hat{P}_m\left(\hat{\rho}_\mu^Z \pm \frac{2^{m-2}}{m}\sum_{k=0}^{m-1}\hat{\rho}_\mu^{\frac{2\pi k}{m}} \mp \frac{2^{m-2}}{m}\sum_{k=0}^{m-1}\hat{\rho}_\mu^{\frac{2\pi k}{m}+\delta}\right)\hat{P}_m,\end{aligned} \tag{2}$$

where $\Pr_\mu(m)$ gives the Poisson distribution, $\hat{P}_m$ is the m-photon projector, $\hat{\rho}_\mu^Z$ is the Z-basis state, $\hat{\rho}_\mu^{\varphi_a}$ are the X-basis states with relative phase $\varphi_a^1 - \varphi_a^2 = \varphi_a$, and $\delta = \pi$ for odd m and $\pi/2$ for even m. The yields for each term can be estimated via the decoy-state method [20, 21].

2. **Detection:** We apply homodyne tomography to evaluate the photon-number operators [24–29]. Unbiased estimators can be obtained via weighted integrals over observed statistics, $p(q_1, q_2|\varphi_b^1, \varphi_b^2)$, the joint probability of quadrature measurement results on the two modes conditioned on LO phases φ_b^1 and φ_b^2.

2.4 Finite-size analysis against coherent attacks

The discrete-variable-type analysis allows the use of mature techniques like martingale theory [30–32] for finite-size parameter estimation under coherent attacks. Details can be found in the attached technical version.

3 Performance

We simulate the asymptotic key rate of our protocol with a thermal noise channel and a unit-efficiency homodyne detector. Note an inefficient detector with thermal electronic noise can be equated to a fiber section with transmittance equal to the detector efficiency, and the electronic noise absorbed into the channel excess noise. The fiber attenuation is 0.2 dB/km.

3.1 Utility of multi-photon components

The rounds where Alice sends m photons and Bob receives m photons can assure secure keys. Fig. 3a plots the asymptotic key rate of the i-photon protocol [utilizing at most $m = i$ photon components in Eq. (1)] with optimized setting parameters. Fig. 3b plots the key-rate contribution of each photon component at different distances. The m-photon contribution of the i-photon protocol is defined as $Q_{m,m}/(Q_{*,0} + \sum_{m=1}^{i} Q_{m,m})$ and the vacuum contribution is $Q_{*,0}/(Q_{*,0} + \sum_{m=1}^{i} Q_{m,m})$.

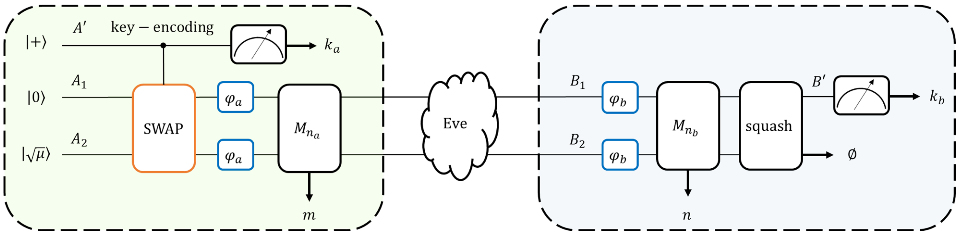
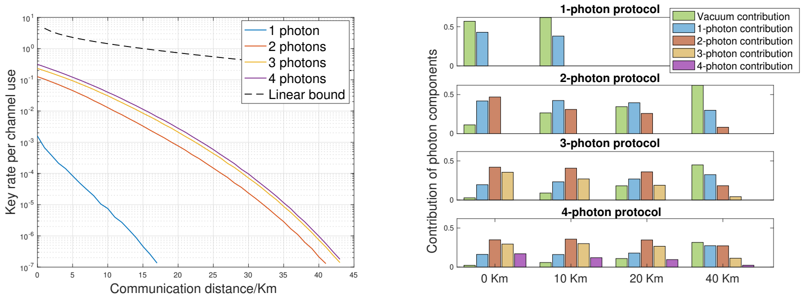


Figure 2: An equivalent protocol of key generation for security analysis.



km		1-photon	2-	3-	4-
0	μ	0.356	1.487	2.395	2.395
	τ	1.437	1.641	1.845	1.845
	e_Z	30.95%	10.52%	5.31%	5.31%
10	μ	0.137	0.924	1.887	2.395
	τ	3.476	2.253	2.457	2.457
	e_Z	29.80%	14.84%	5.66%	4.17%
20	μ	-	0.728	1.487	1.887
	τ	-	3.068	3.068	3.272
	e_Z	-	15.48%	6.91%	3.85%
40	μ	-	0.356	0.728	1.172
	τ	-	4.495	4.495	4.699
	e_Z	-	28.52%	17.07%	8.81%

(a) (b) (c)

Figure 3: **(a)** Solid lines: asymptotic key rates of protocols using up to 1, 2, 3, and 4 photons. Dotted line: linear key rate bound [33, 34]. **(b)** Contributions of $Q_{m,m}$ and $Q_{*,0}$. **(c)** Optimized parameters and bit error rates.

Table 1: Comparison between this work and relevant protocol designs and analyses.

protocol	modulation	detection	pilot	analysis	attack against	finite size	distance
BB84	DV	single-photon	×	analytical	coherent	✓	long
ideal GG02	CV	homo-/hyterodyne	✓	analytical	coherent	✓	mid
realistic GG02				numerical	?	?	
Ref. [3]	DV	homo- & hyterodyne	✓	analytical	coherent	✓	mid
Ref. [23]	DV	hyterodyne	×	analytical	indivial	×	short
Ref. [35]	DV	homodyne	×	numerical	collective*	×	metropolitan
This work	**DV**	**homodyne**	×	**analytical**	**coherent**	✓	**metropolitan**

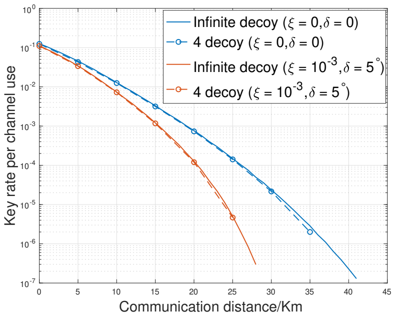


Figure 4: Two-photon protocol performances.

3.2 DV-comparable short-distance key rate

The key rate improves as we make use of the multi-photon components, most remarkable between the one and two-photon protocols. If we consider the protocol with infinite photon-number components, the 0-km key rate is around 0.31 bit/channel, and the BB84 protocol with currently the best single-photon detector of 80% efficiency [36, 37] has 0-km key rate 0.29 bit/channel, based on the model from Ref. [38]. Our key rate matches the best BB84 key rate with practically favorable devices.

3.3 Robustness

Fig. 4 illustrates the practical performances of the two-photon time-bin CV QKD protocol. We consider the issues of (1) the excess noise in transmission and detection, (2) the mode reference misalignment, where the two optical modes generating the time-bin qubit differ by δ in the reference phases intrinsically, and (3) a finite decoy level. Compared to the noiseless case (blue curves), the key rate decays mildly in the practical setup (red curves), considering reasonable parameters of excess noise $\xi = 10^{-3}$ and misalignment $\delta = 5°$. Moreover, an optimized 4-level decoy estimation is almost exact for both the noiseless and the practical setups (optimization using linear programming with a cutoff photon number 10 [39, 40]).

4 Comparison with relevant protocols

To sum up, we compare our protocol and analysis with relevant ones (Table 1). Our protocol has the advantage of removing the need of a reference pilot pulse, robust implementation with practically favorable devices, and reasonable performance in metropolitan distances. Moreover, we provide a complete analytical security analysis valid against coherent attacks in the finite-size regime.

References

[1] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88** (2002), URL `https://doi.org/10.1103/physrevlett.88.057902`.

[2] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **9** (2019), URL `https://doi.org/10.1103/physrevx.9.041064`.

[3] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, Nat. Commun. **12** (2021), URL `https://doi.org/10.1038/s41467-020-19916-1`.

[4] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, New J. Phys. **12**, 103042 (2010), URL `https://doi.org/10.1088/1367-2630/12/10/103042`.

[5] R. Kumar, H. Qin, and R. Alléaume, New J. Phys. **17**, 043027 (2015), URL `https://doi.org/10.1088/1367-2630/17/4/043027`.

[6] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, et al., Commun. Phys. **2** (2019), URL `https://doi.org/10.1038/s42005-018-0105-5`.

[7] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, et al., Nat. Photonics **13**, 839 (2019), URL `https://doi.org/10.1038/s41566-019-0504-5`.

[8] A. Leverrier, Phys. Rev. Lett. **118** (2017), URL `https://doi.org/10.1103/physrevlett.118.200501`.

[9] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **88** (2013), URL `https://doi.org/10.1103/physreva.88.022339`.

[10] L. Fan, Y. Bian, M. Wu, Y. Zhang, and S. Yu, Phys. Rev. Applied **20** (2023), URL `https://doi.org/10.1103/physrevapplied.20.024073`.

[11] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87** (2013), URL `https://doi.org/10.1103/physreva.87.062313`.

[12] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87** (2013), URL `https://doi.org/10.1103/physreva.87.062329`.

[13] D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5** (2015), URL `https://doi.org/10.1103/physrevx.5.041010`.

[14] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Physical Review X **5** (2015), ISSN 2160-3308, URL `http://dx.doi.org/10.1103/PhysRevX.5.041009`.

[15] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999), URL `http://science.sciencemag.org/content/283/5410/2050`.

[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), URL `https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.441`.

[17] M. Koashi, New J. Phys. **11**, 045018 (2009).

[18] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Info. Comput. **4**, 325–360 (2004), ISSN 1533-7146.

[19] X. Ma, Ph.D. thesis, University of Toronto (2008), also available in arXiv:0808.1385, URL `https://arxiv.org/abs/0808.1385`.

[20] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005), URL `http://link.aps.org/doi/10.1103/PhysRevLett.94.230504`.

[21] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005), URL `https://link.aps.org/doi/10.1103/PhysRevLett.94.230503`.

[22] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179, URL `https://doi.org/10.1016/j.tcs.2014.05.025`.

[23] B. Qi, Phys. Rev. A **103** (2021), URL `https://doi.org/10.1103/physreva.103.012606`.

[24] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989), URL `https://link.aps.org/doi/10.1103/PhysRevA.40.2847`.

[25] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993), URL `https://link.aps.org/doi/10.1103/PhysRevLett.70.1244`.

[26] G. M. D'Ariano, C. Macchiavello, and M. G. A. Paris, Phys. Rev. A **50**, 4298 (1994), URL `https://link.aps.org/doi/10.1103/PhysRevA.50.4298`.

[27] G. M. D'Ariano, U. Leonhardt, and H. Paul, Phys. Rev. A **52**, R1801 (1995), URL `https://link.aps.org/doi/10.1103/PhysRevA.52.R1801`.

[28] U. Leonhardt and H. Paul, Prog. Quantum Electron. **19**, 89 (1995), URL `https://www.sciencedirect.com/science/article/pii/007967279400007L`.

[29] G. D'Ariano, J. Eur. Opt. Soc. B **7**, 693 (1995), URL `https://dx.doi.org/10.1088/1355-5111/7/4/022`.

[30] K. Azuma, Tohoku Math. J. Second Ser. **19**, 357 (1967).

[31] G. Kato, arXiv:2002.04357 (2020).

[32] X. Zhang, P. Zeng, T. Ye, H.-K. Lo, and X. Ma, Phys. Rev. Lett. **131**, 140801 (2023), URL `https://link.aps.org/doi/10.1103/PhysRevLett.131.140801`.

[33] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5** (2014), URL `https://doi.org/10.1038/ncomms6235`.

[34] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8** (2017), URL `https://doi.org/10.1038/ncomms15043`.

[35] I. W. Primaatmaja, C. C. Liang, G. Zhang, J. Y. Haw, C. Wang, and C. C.-W. Lim, Quantum **6**, 613 (2022), URL `https://doi.org/10.22331/q-2022-01-03-613`.

[36] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Appl. Phys. Lett. **117**, 144003 (2020), URL `https://doi.org/10.1063/5.0021468`.

[37] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, et al., Nat. Photonics **17**, 416 (2023), URL `https://doi.org/10.1038/s41566-023-01166-4`.

[38] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005), URL `http://link.aps.org/doi/10.1103/PhysRevA.72.012326`.

[39] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86** (2012), URL `https://doi.org/10.1103/physreva.86.052305`.

[40] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A **89** (2014), URL `https://doi.org/10.1103/physreva.89.052333`.

Pilot-reference-free continuous-variable quantum key distribution with efficient decoy-state analysis

Anran Jin,[1] Xingjian Zhang,[2,3,4] Liang Jiang,[5] Richard V. Penty,[1] and Pei Zeng[5,*]

[1]*Electrical Engineering Division, Department of Engineering, University of Cambridge, CAPE Building 9 JJ Thomson Avenue, CB3 0FA Cambridge, UK*

[2]*Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*

[3]*Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[4]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[5]*Pritzker School of Molecular Engineering, The University of Chicago, Illinois 60637, USA*

Continuous-variable quantum key distribution (CV QKD) using optical coherent detectors is practically favorable due to its low implementation cost, flexibility of wavelength division multiplexing, and compatibility with standard coherent communication technologies. However, the security analysis and parameter estimation of CV QKD are complicated due to the infinite-dimensional latent Hilbert space. Also, the transmission of strong reference pulses undermines the security and complicates the experiments. In this work, we tackle these two problems by presenting a time-bin-encoding CV protocol with a simple phase-error-based security analysis valid under general coherent attacks. With the key encoded into the relative intensity between two optical modes, the need for global references is removed. Furthermore, phase randomization can be introduced to decouple the security analysis of different photon-number components. We can hence tag the photon number for each round, effectively estimate the associated privacy using a carefully designed coherent-detection method, and independently extract encryption keys from each component. Simulations manifest that the protocol using multi-photon components increases the key rate by two orders of magnitude compared to the one using only the single-photon component. Meanwhile, the protocol with four-intensity decoy analysis is sufficient to yield tight parameter estimation with a short-distance key-rate performance comparable to the best Bennett-Brassard-1984 implementation.

I. INTRODUCTION

Quantum key distribution (QKD) allows the generation of random secure keys between distant communication parties, of which the security is guaranteed by quantum physical laws. Apart from its theoretical advances, QKD is also one of the few quantum information processing technologies that can be robustly deployed in the fields, where photonic systems are considered the most suitable carriers of QKD operation. In general, two types of QKD protocols exist based on the detection methods: discrete-variable (DV) QKD [1, 2] uses the single-photon detector or photon-number-resolving detector to generate discrete detection information, while continuous-variable (CV) QKD [3–5] applies optical homodyne or heterodyne detection to generate continuous measurement information.

CV QKD has its advantages over DV QKD in short distances, mainly attributing to the distinct features of the coherent detectors used. The homodyne and heterodyne detectors are compatible with the standard classical communication and can be operated at much milder conditions than single-photon detectors. The spatial-temporal filtering of the local oscillators (LO) allows dense wavelength-division multiplexing with intense classical channels [6–8], and the high quantum efficiency and operation rate give CV QKD high key rates in metropolitan distances [9–11]. Moreover, the feasibility of on-chip implementations of the coherent detectors [12] promises large-scale integrated quantum networks. CV QKD is therefore considered highly practical and promising.

However, there exist two major limitations to the reliability of CV QKD. First, the transmission of the strong local oscillators is usually necessary to set up the phase reference between the communication parties, yet this complicates the implementation in the multiplexing separation and the relative phase shift calibration with the signals [13]. The LO transmission also opens up security loopholes where the eavesdropper Eve can affect the estimation of the signal variance by manipulating the LO intensity [14, 15], input time [16] and wavelength [17]. The “local” local oscillator scheme [13, 18] is a valid solution, yet it still requires the transmission of pilot pulses and compensation in the classical post-processing layer, which increase the experimental complexity. Second, the security of CV QKD in the finite-data regime under coherent attacks is still incomplete. In fact, for the traditional entanglement-distillation approach [19], the finite-size coherent attack security is only tackled for Gaussian-modulated CV QKD [20], which is, however, impractical since continuous modulation is never possible in reality.

Recently, several remarkable works on CV QKD have

[*] peizeng@uchicago.edu

been proposed, aiming at closing its security loopholes. In Ref. [5, 21], Matsuura et al. proposed a DV-like security analysis for the binary phase shift keying CV QKD. Their analysis covers finite size and coherent attack intrinsically since it follows the phase-error complementarity approach [22], yet their protocol still assumes the transmission of local oscillators. Qi [23] and Primaatmaja et al. [24] respectively proposed CV QKD protocols with two-mode encoding, generating dual-rail qubits that do not require global references. Their security analyses, however, do not cover the finite-data regime and coherent attacks. In fact, Qi's analysis requires repeated measurements and is only valid for individual attacks, and Primaatmaja et al.'s analysis is based on Devetak-Winter formula [19] and is only valid for collective attacks. Hence, the gap in CV QKD between theory and practice is still a challenging problem to be tackled.

In this work, we close this gap by proposing a new time-bin-encoding CV QKD protocol that enjoys both simple security proof and practical implementation. We remove the necessity of LO transmission by the two-mode encoding, hence closing the security loophole while simplifying the experimental setups. We follow the phase-error complementarity approach [22, 25, 26] so that the security naturally covers the general coherent-attack case. What is more, the intensity-based encoding allows phase randomization to be applied, where we can group the received signals based on the transmitted photon numbers and restore the tagging-based security analysis [27, 28] and the decoy-state method [29, 30]. Instead of generating secure key bits from all raw key bits, we can thus take advantage of the photon-number tags and distill key bits from the rounds with low phase-error rate. Our tagging-based security analysis builds a direct connection between CV QKD and the normal Bennett-Brassard-1984 (BB84) protocol: we clearly show how the multi-photon components in the CV QKD protocol contribute to a higher key rate in short distances. Compared with a similar protocol in Ref. [24] with numerical optimization under collective attacks, our protocol generates higher key rates with simpler parameter estimation using four decoy levels under coherent attacks.

We will start with the protocol description of the time-bin-encoding CV QKD in Sec. II. We present its security analysis based on phase error correction [22, 25, 26] in Sec. III, identifying an equivalent protocol squashing the optical modes into qubits with identical key mapping statistics [5, 27, 31] in Sec. III A. We exploit the block-diagonal structures of both the source and the receiver in Sec. III B, thus invoking the photon-number tagging technique [27, 28] standard in DV QKD in this CV protocol. In Sec. III C, we calculate the parameters in the key-rate formula with quantities on optical modes. The estimation of these quantities will be explained in Sec. IV with homodyne tomography [32] and decoy method [29, 30]. We finally simulate the performances of the time-bin CV QKD under realistic fiber-channel setups in Sec. V.

II. PROTOCOL DESCRIPTION

We present the proposed time-bin-encoding CV QKD protocol in Table I and depict its schematic diagram in Fig. 1. The two communication parties, Alice and Bob, employ the time-bin degree of freedom to encode keys. They use Z-basis for key generation and X-basis for parameter estimation. At the moment, we do not present the details of the X-basis parameter settings. We will specify the choices of the random phase factors, $\varphi_a^1, \varphi_a^2, \varphi_b^1$ and φ_b^2, and the light intensity, $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$, in Sec. IV.

Here, we briefly explain the idea behind the protocol design. The source states of our scheme resemble the ones in the time-bin-encoding BB84 protocol with coherent states [1], where the light intensities of the consecutive pulses naturally encode the key-bit information. As the key information is encoded in the relative intensity between the two modes, Alice does not need to send a pilot phase reference as in common CV QKD.

In our scheme, Bob decodes the key bit information, namely the Z-basis information, by measuring the light intensity of the pulses using the homodyne detectors. For instance, when Bob observes q_1 to be close to 0 and q_2 to be far away from 0, he may naturally guess that the original state sent by Alice corresponds to $k_a = 0$. However, unlike the key decoding with photon-number detectors, the result of measuring a coherent state's quadrature is subjected to a Gaussian distribution rather than a fixed value. The inherent shot noise of the homodyne detection introduces an intrinsic error in distinguishing a vacuum state from a pulse with a non-zero intensity [33]. To suppress the bit error, we introduce a threshold value, τ, in key decoding. The pulse intensity will be considered non-zero only when the quadrature magnitude is larger than τ. So a bit 0 will be decoded if $|q_1| < \tau$ and $|q_2| > \tau$ and bit 1 if $|q_1| > \tau$ and $|q_2| < \tau$. The choice of τ should be optimized with respect to the channel transmittance and pulse intensity. As we will show in Sec. VI, although this key mapping scheme can be further optimized, the performance of the simple key mapping scheme is already near-optimal.

The X-basis is designed to estimate the information leakage of different photon-number components of the Z-basis. Thanks to the phase randomization for both the sources and the detectors, the Z-basis states are block-diagonal on the total photon-number basis on the two optical modes after emitted from the source and before being measured by the homodyne detectors. As we will clarify in Sec. III, we can equivalently introduce total photon-number measurements at these two locations. As a result, Eve's eavesdropping strategy is effectively "twirled" to a photonic channel that only acts on the states incoherently with respect to the total photon numbers. One can thus virtually tag the emitted and received pulses according to the photon-number space, allowing the Gottesman-Lütkenhaus-Lo-Preskill (GLLP) framework [27] for analyzing the key privacy contained

TABLE I: Phase-randomized time-bin-encoding CV QKD

1. On Alice's side (source):
   - *Z-basis*:
     (a) Randomly select a key bit $k_a \in \{0, 1\}$, a phase factor $\varphi_a \in [0, 2\pi)$, and a light intensity $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) Prepare a coherent state of $|0\rangle_{A1} |\sqrt{\mu_a} e^{i\varphi_a}\rangle_{A2}$ for $k_a = 0$ or $|\sqrt{\mu_a} e^{i\varphi_a}\rangle_{A1} |0\rangle_{A2}$ for $k_a = 1$.
   - *X-basis*:
     (a) Randomly select two phase factors φ_a^1 and φ_a^2 and a light intensity $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) Prepare a coherent state of $|\sqrt{\mu_a/2} e^{i\varphi_a^1}\rangle |\sqrt{\mu_a/2} e^{i\varphi_a^2}\rangle$.
2. Alice sends the state through an authenticated channel to Bob.
3. On Bob's side (detection):
   - *Z-basis*:
     (a) Randomly select a phase factor $\varphi_b \in [0, 2\pi)$.
     (b) Use homodyne detectors both with LO phases φ_b to measure the modes and obtain quadratures q_1 and q_2.
     (c) Decode the key bit as 0 if $|q_1| < \tau \wedge |q_2| > \tau$, 1 if $|q_1| > \tau \wedge |q_2| < \tau$, and $\emptyset$ otherwise.
   - *X-basis*:
     (a) Randomly select two phases φ_b^1 and φ_b^2 independently.
     (b) Use homodyne detectors with LO phases φ_b^1 and φ_b^2 to measure the modes and obtain quadratures q_1 and q_2.
     (c) Use φ_1, φ_2 and q_1, q_2 for phase-error estimation (see Sec. IV).
4. Alice and Bob perform basis sifting, where they obtain raw keys in the rounds they both choose Z-basis with light intensity $\mu_a = \mu$ and $k_b \neq \emptyset$.
5. Based on parameter estimation, Alice and Bob perform information reconciliation and privacy amplification to obtain final keys.

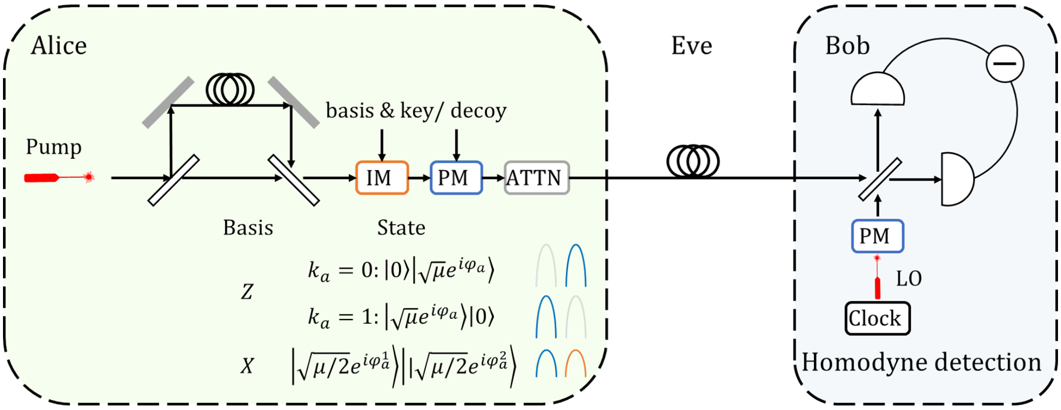

Alice
Pump
basis & key/ decoy
IM
PM
ATTN
Basis
State
Z
$k_a = 0$: $|0\rangle|\sqrt{\mu}e^{i\varphi_a}\rangle$
$k_a = 1$: $|\sqrt{\mu}e^{i\varphi_a}\rangle|0\rangle$
X
$|\sqrt{\mu/2}e^{i\varphi_a^1}\rangle|\sqrt{\mu/2}e^{i\varphi_a^2}\rangle$
Eve
Bob
PM
LO
Clock
Homodyne detection

FIG. 1: Schematic diagram of the experimental setup. The setups of Alice and Bob are shaded in green and blue, respectively. Alice prepares two-mode phase-randomized states according to the basis choice and raw key value in key generation rounds, as shown in the table. In this work, we consider a time-bin encoding, where one obtains two modes via time delay. The state modulation consists of intensity modulation (IM), phase modulation (PM), and necessary attenuation (ATTN). Upon receiving the state, Bob measures each mode with homodyne detectors. He uses a synchronized clock to distinguish adjacent modes and applies phase modulation (PM) to the local oscillator (LO).

in each photon-number subspace. In particular, dealing with photon-number spaces effectively brings our security analysis to the DV regime. In Sec. III, we shall construct observables to estimate the m-photon component phase-error rates $e^X_{m,m}$ for privacy estimation. Intuitively, the phase-error rates $e^X_{m,m}$ provide upper bounds on the key information leakage to the eavesdropper, Eve.

To estimate the m-photon component phase-error rates, $e^X_{m,m}$, ideally, we need a source emitting the photon-number cat states, $(|0\rangle|m\rangle \pm |m\rangle|0\rangle)/\sqrt{2}$, and photon-number-resolving measurements that distinguish the cat states. While this is not directly implementable, we can use only coherent states and homodyne measurements to establish unbiased estimators of $e^X_{m,m}$, as shown in Table II. On the source side, we employ a generalized decoy-state method to estimate the behaviors of photon-number-cat states using coherent states with various intensities [29, 30], which shall be discussed in Sec. IV B. On the detection side, ideally, we also want to measure the photon-number-cat states to obtain unbiased estimation of the phase-error rates, $e^X_{m,m}$. While this is not directly measurable in practice, we employ the homodyne tomography technique and estimate the photon-number-cat state measurement via quadrature measurement results [34–39], which shall be discussed in Sec. IV A.

We briefly remark on the performance of homodyne detection. In key decoding, one may consider the homodyne detection as ill-performed single-photon detectors that introduce an inevitable bit-error rate. On the other hand, homodyne detection allows for more efficient parameter estimation than single-photon detection. As we shall discuss later, the set of all quadrature operators spans the underlying mode, thus allowing one to express any linear operator in terms of the quadrature operators. Therefore, with proper transformation of the quadrature measurement results, homodyne detection allows one to obtain an unbiased estimation of linear operator expectations. This is the reason for accurately estimating phase-error rates with repeated homodyne measurements, including those of the multi-photon components. In comparison, as the single-photon detection is not information-complete, estimation of multi-photon observables requires more complex setups such as sequential beam splitting [40], and one can only obtain upper and lower bounds rather than an unbiased estimation.

III. SECURITY ANALYSIS

We analyze the security of our phase-randomized time-bin-encoding CV QKD protocol along the complementarity approach [22, 26, 27]. As outlined in Fig. 2, we shall set up a series of equivalent protocols of the realistic implementation that do not change the statistics of any observer, with which we define the phase-error observable and estimate the key privacy. In Sec. III A, we shall prove that raw key generation can be effectively regarded as qubit measurements on a pair of entangled qubits, which allows us to borrow the mature complementarity-based security analysis in the DV regime. In brief, on the source side, we transform the preparation of key states to an entanglement-based protocol [25, 26], where a qubit measurement controls the key-encoding process, as shown in Fig. 2(b). On the detection side, we prove that the homodyne measurement can be squashed into an effective qubit measurement, as shown in Fig. 2(c). Moreover, in Sec. III B, we shall rigorously prove that phase randomization twirls the photonic modes into diagonal states on the Fock basis and explain how to apply the tagging idea of the GLLP framework [27, 28]. We also show how to estimate the phase-error rates for different photon-number components from Fock-basis observables in Sec. III C. Later in Sec. IV, we show that the estimation can be realized in the realistic implementation with coherent states and homodyne detection.

To focus on the essence of security analysis, we present the result in a single-round analysis in this section, where one can interpret it as the quantum Shannon limit under collective attacks. Nevertheless, the complementarity-based security analysis is inherently adapted to the most general case, namely the coherent attack, where the statistics over the rounds may not be independent and identically distributed (i.i.d.) [41]. We will discuss the parameter estimation with non-i.i.d. finite statistics in Sec. IV C.

A. Entanglement-based squashing protocol

Here, we show the equivalence of the time-bin CV QKD protocol to a qubit-based entanglement distribution protocol, where the protocols generate the same transmitted quantum states and measurement statistics. The latter protocol enables us to simplify the security analysis and estimate the information leakage from phase-error rates.

We first focus on the key-generation rounds in the protocol where both users choose the Z-basis, of which the whole procedure is depicted in Fig. 2(a). In the realistic implementation, Alice prepares phase-randomized coherent states,

$$\int_0^{2\pi} \frac{d\varphi_a}{2\pi} \left|\Psi(k_a)_{\varphi_a}\right\rangle_{A_1A_2} \left\langle\Psi(k_a)_{\varphi_a}\right|, \tag{1}$$

where

$$\left|\Psi(k_a)_{\varphi_a}\right\rangle_{A_1A_2} = \begin{cases} |0\rangle_{A_1}\left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_2}, & \text{if } k_a = 0, \\ \left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_1}|0\rangle_{A_2}, & \text{if } k_a = 1. \end{cases} \tag{2}$$

We denote the optical modes sent to Bob as A_1 and A_2, which are CV systems. Throughout this paper, we treat the phase of optical modes, φ_a, as fully randomized over $[0, 2\pi)$. Finite phase randomization, $\varphi_a \in \{2j\pi/D\}_{j\in[D]}$, suffices for a practical implementation, where its difference from the full phase randomization is negligible when D is sufficiently large [42]. This is also the case in later

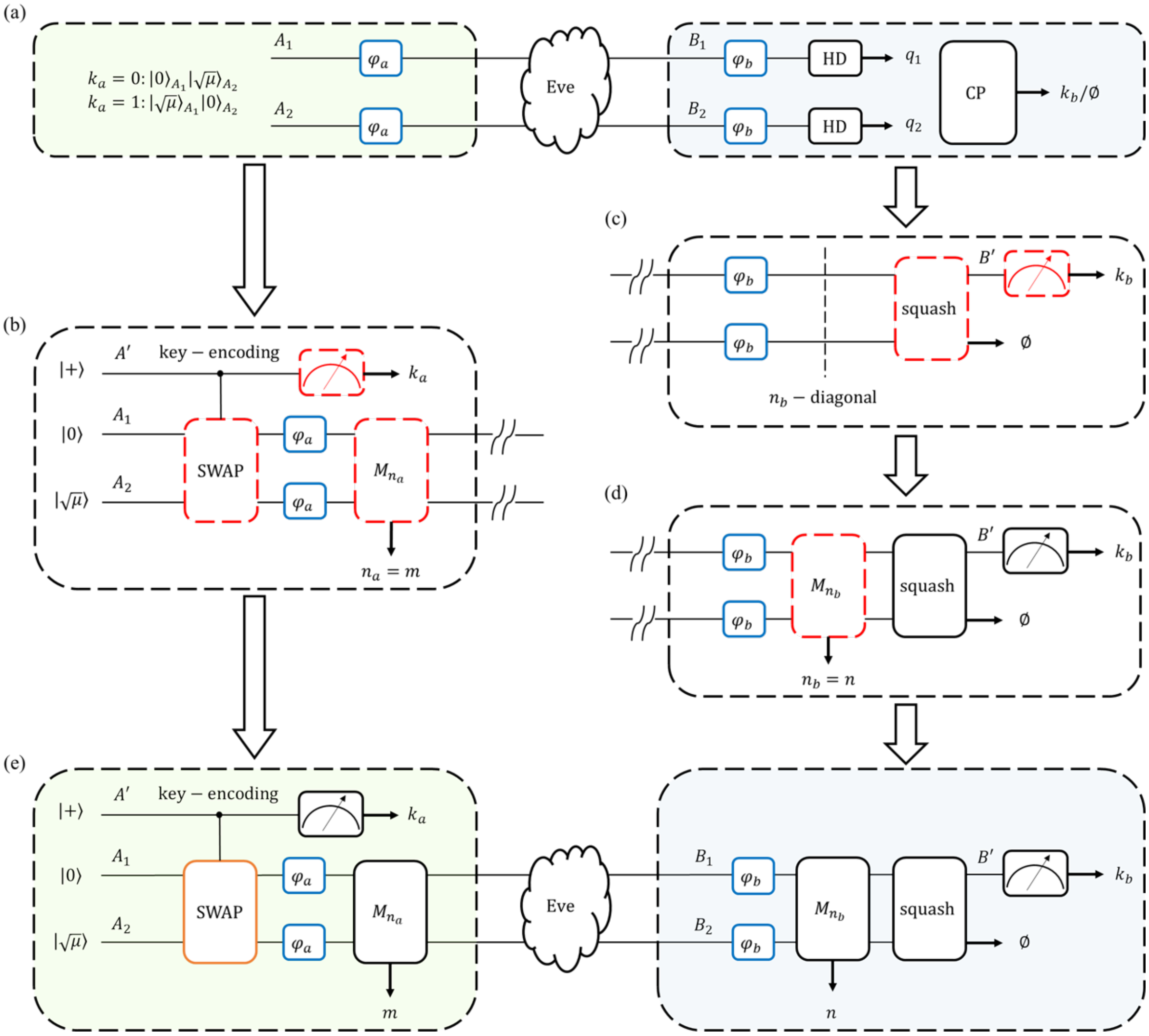


FIG. 2: Equivalent quantum circuits in key generation rounds. Reductions in each step are plotted with red dashed boxes. (a) The realistic implementation. The operations on Alice's and Bob's sides are shaded in green and blue, respectively. Alice prepares weak coherent states on two modes, which depend on the basis choice and the raw key value. On Bob's side, Bob measures the two modes with homodyne detectors (HD) and obtains quadratures q_1 and q_2. Afterward, Bob performs classical post-processing (CP) on the data and obtains a raw key k_b probabilistically, where the key decoding may fail due to the key mapping threshold, denoted as $\emptyset$. The blue rounded boxes represent phase randomization processes in state preparation or for the LOs in homodyne detection. (b) Equivalent entanglement-based state preparation. Key encoding can be interpreted as a qubit control operation on two modes where the control qubit measurement gives Alice's raw key k_a. The joint state on the two modes is diagonal on the Fock basis after phase randomization. One can insert a photon-number measurement, $\hat{M}_{n_a}$, and read out the total photon number, m, without changing the state. (c) Equivalent key-decoding measurement. The joint state of the two modes becomes diagonal on the Fock basis due to detector phase randomization. In key decoding, the modes are first squashed into a qubit probabilistically, where the failure gives the abort signal $\emptyset$. Upon successful squashing into a qubit, the computational-basis measurement gives the raw key bit. (d) Due to detector phase randomization, one can insert a photon-number measurement, $\hat{M}_{n_b}$, and read out the total photon number, n, without changing the state. (e) Equivalent circuit for security analysis. After the above reductions, the key generation measurements can be equivalently defined on a pair of (sub-normalized) qubit states.

TABLE II: State preparation and detection settings in the ideal implementation and the realistic implementation. For brevity, we omit the subscripts of modes and express the detection with the measurement operators. In key generation rounds, Bob applies phase-randomized homodyne detection for key-decoding. The expression of measurement operator $\hat{\Pi}(q_1, q_2)$ is given in Eq. (9), where q_1 and q_2 represent the quadratures of the two modes. The operator is block-diagonal on the total photon-number basis. For parameter estimation, ideally, Alice sends photon-number-cat states, and Bob performs a corresponding projective measurement. In the realistic setting, Alice can only prepare phase-randomized weak coherent states, and Bob can only perform phase-randomized homodyne measurements. The homodyne measurement operator, $\hat{Q}_{\varphi_1} \otimes \hat{Q}_{\varphi_2}$, is given in Eq. (6). Afterward, Bob estimates the photon-number-cat state measurement expectations via homodyne tomography methods, as shown in Eq. (28).

basis	source		detection	
	ideal	real	ideal	real
Z	$\|0\rangle \|m\rangle$ $\|m\rangle \|0\rangle$	$\|0\rangle \|\sqrt{\mu}e^{i\varphi_a}\rangle$ $\|\sqrt{\mu}e^{i\varphi_a}\rangle \|0\rangle$	$\hat{\Pi}(q_1, q_2)$, Eq. (9)	$\hat{\Pi}(q_1, q_2)$
X	$\frac{1}{\sqrt{2}}(\|0\rangle \|m\rangle \pm \|m\rangle \|0\rangle)$	$\|\sqrt{\frac{\mu}{2}}e^{i\varphi_a^1}\rangle \|\sqrt{\frac{\mu}{2}}e^{i\varphi_a^2}\rangle$	$\frac{1}{2}(\|0\rangle \|m\rangle \pm \|m\rangle \|0\rangle)(\langle 0\| \langle m\| \pm \langle m\| \langle 0\|)$	$\hat{Q}_{\varphi_1} \otimes \hat{Q}_{\varphi_2}$, Eq. (6), estimation via Eq. (28)

discussions on the detector phase randomization. Alice's key-state preparation can be effectively seen as an entanglement-based protocol [25, 26]. Given the phase value, φ_a, Alice first prepares the following entangled state,

$$\begin{aligned} |\Psi_{\varphi_a}\rangle_{A'A_1A_2} =& \frac{1}{\sqrt{2}}\big(|0\rangle_{A'} |\Psi(k_a = 0)_{\varphi_a}\rangle_{A_1A_2} \\ &+ |1\rangle_{A'} |\Psi(k_a = 1)_{\varphi_a}\rangle_{A_1A_2} \big), \end{aligned} \tag{3}$$

where system A' is a qubit system that superposes the two possible key states. The entangled state can be prepared by the quantum circuit in Fig. 2(b). Up to phase randomization, systems A' and A_1A_2 are initialized in $|+\rangle$ and $|0\rangle|\sqrt{\mu}\rangle$, and a control-swap operation is then applied from the qubit system to the optical modes. Alice obtains raw key bit k_a by measuring system A' on the computational basis, and the optical modes are prepared into the corresponding key state, $|\Psi(k_a)_{\varphi_a}\rangle$. The complementary observable of Alice's key-generation measurement can thus be defined over qubit system A', which measures the complementary basis of $\{|+\rangle, |-\rangle\} := \{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$.

At the detection side in Fig. 2(a), Bob receives two optical modes B_1 and B_2, takes homodyne measurements, and maps the quadratures to a raw key or an abort signal. This process can be described by a trace-non-preserving completely positive map,

$$\begin{aligned} \mathcal{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2}) = \int_0^{2\pi} \frac{d\varphi_b}{2\pi} \int_{\mathbf{R_0}} dq_1 dq_2 \\ \hat{K}^{(q_1,q_2,\varphi_b)} \hat{\rho}_{B_1B_2} \hat{K}^{(q_1,q_2,\varphi_b)\dagger}, \end{aligned} \tag{4}$$

where

$$\begin{aligned} \hat{K}^{(q_1,q_2,\varphi_b)} :=& |0\rangle_{B'} \langle q_1(\varphi_b), q_2(\varphi_b)|_{B_1,B_2} \\ &+ |1\rangle_{B'} \langle q_2(\varphi_b), q_1(\varphi_b)|_{B_1,B_2}, \end{aligned} \tag{5}$$

$|q(\varphi)\rangle$ is the rotated position eigenstate of quadrature observable

$$\hat{Q}_{\varphi} = \hat{a}e^{-i\varphi} + \hat{a}^{\dagger}e^{i\varphi}, \tag{6}$$

with $\hat{a}$ and $\hat{a}^{\dagger}$ denoting the annihilation and creation operators, respectively, and $\mathbf{R_0} \in \mathbb{R}^2$ records the region that decodes the real-valued tuple, (q_1, q_2), as $k_b = 0$. Note that in our protocol, $\mathbf{R_0} = \{|q_1| < \tau\} \times \{|q_2| > \tau\}$, and the region decodes the quadratures to $k_b = 1$ under the mapping $(q_1, q_2) \mapsto (q_2, q_1)$, which we denote as $\mathbf{R_1} = \{|q_1| > \tau\} \times \{|q_2| < \tau\}$. The LOs of homodyne measurements are synchronically randomized, as denoted by φ_b in Eq. (4). As the key-decoding region does not cover the entire parameter space, $\mathcal{F}_{\text{rand}}^{B_1B_2\to B'}$ is hence not trace-preserving, where $\text{Tr}[\mathcal{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2})]$ gives the probability of obtaining raw key bit $k_b \in \{0, 1\}$. Bob's raw key can be equivalently seen as obtained by measuring the squashed sub-normalized qubit on the computational basis, and the probabilities are given by

$$\begin{aligned} &\Pr(k_b = 0) = \langle 0| \mathcal{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2}) |0\rangle \\ =& \int_0^{2\pi} \frac{d\varphi_b}{2\pi} \int_{\mathbf{R_0}} dq_1 dq_2 \langle q_1(\varphi_b), q_2(\varphi_b)| \hat{\rho}_{B_1B_2} |q_1(\varphi_b), q_2(\varphi_b)\rangle, \\ &\Pr(k_b = 1) = \langle 1| \mathcal{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2}) |1\rangle \\ =& \int_0^{2\pi} \frac{d\varphi_b}{2\pi} \int_{\mathbf{R_1}} dq_1 dq_2 \langle q_1(\varphi_b), q_2(\varphi_b)| \hat{\rho}_{B_1B_2} |q_1(\varphi_b), q_2(\varphi_b)\rangle. \end{aligned} \tag{7}$$

Similar to the treatment to A', we can define the complementary observable of Bob's key generation measurement on qubit system B'.

B. Photon-number tagging of the source and receiver

In the last section, we have shown that raw keys can be equivalently seen as generated from qubit measurements on A' and B'. Should Alice and Bob instead measure the qubit system on the complementary bases, the probability they obtain different results, or the phase-error rate, e^X, could be used to upper-bound the average privacy amplification cost per round as $h(e^X)$, where $h(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy function. Nevertheless, the actual privacy leakage may be less than the direct calculation. Note that the above privacy leakage estimation is averaged over the overall quantum state transmitted from Alice to Bob. The contribution to the privacy leakage of different components in quantum signals can differ. For instance, Eve can apply the photon-number-splitting (PNS) attack in the rounds in which Alice transmits two photons and Bob receives only a single photon [43, 44]; hence no privacy should be expected, rendering the phase-error probability to be 1/2 in these rounds. If Alice and Bob can distinguish such rounds from the others, they can simply discard them in privacy amplification. The GLLP framework makes the above statement rigorous [27, 28]. Suppose Alice and Bob can categorize the transmitted quantum signals into different groups, or tags, and evaluate phase-error probabilities separately. The privacy amplification cost can be evaluated by $\sum_i Q_i h(e_i^X)$, where Q_i is the probability that a signal in the i'th group is transmitted and detected, namely the gain, and e_i^X is the phase-error probability of the group. Due to the concavity of the entropy function, this estimation is no larger than $h(\sum_i Q_i e_i^X)$.

In DV QKD, the tagging idea has been well practiced. In the coherent-state-based BB84 protocol, phase randomization on the source side diagonalizes the quantum signals on the Fock basis [29, 30], and an ideal single-photon detector naturally distinguishes the single photon components from other detected Fock components, allowing Alice and Bob to tag the quantum states with respect to the photon number [45]. Similarly, we now prove that the photon-number tag can also be applied to the phase-randomized CV QKD protocol in Table I. On the source side, the phase randomization diagonalizes the state on the joint Fock basis,

$$\begin{aligned}\hat{\rho}^Z &= \int_0^{2\pi} \frac{d\varphi_a}{2\pi} \quad \frac{1}{2} \left|0\right\rangle_{A_1} \left\langle 0\right| \otimes \left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_2} \left\langle \sqrt{\mu}e^{i\varphi_a}\right| \\ &\quad + \frac{1}{2} \left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_1} \left\langle \sqrt{\mu}e^{i\varphi_a}\right| \otimes \left|0\right\rangle_{A_2} \left\langle 0\right| \\ &= \sum_{m=0}^{\infty} \Pr(m) \frac{1}{2} \left(\left|0m\right\rangle_{A_1A_2} \left\langle 0m\right| + \left|m0\right\rangle_{A_1A_2} \left\langle m0\right|\right),\end{aligned} \tag{8}$$

where $\Pr(m) = e^{-\mu}\mu^m/m!$ is the Poisson distribution. Consequently, one can virtually insert a photon-number measurement after phase randomization to measure the total photon number on the two modes without changing the state, as shown in Fig. 2(b). On the detection side, when Bob takes the Z-basis measurement, the phase-randomized homodyne detector POVM elements can be expanded on the Fock basis [24],

$$\begin{aligned}&\hat{\Pi}(q_1, q_2) \\ &= \int_0^{2\pi} \frac{d\varphi_b}{2\pi} \left|q_1(\varphi_b)\right\rangle_{B_1} \left\langle q_1(\varphi_b)\right| \otimes \left|q_2(\varphi_b)\right\rangle_{B_2} \left\langle q_2(\varphi_b)\right| \\ &= \sum_{n=0}^{\infty} \sum_{k_0=0}^{n} \sum_{l_0=0}^{n} \psi_{k_0}(q_1)\psi_{l_0}(q_1)\psi_{n-k_0}(q_2)\psi_{n-l_0}(q_2) \\ &\qquad \left|k_0, n-k_0\right\rangle_{B_1B_2} \left\langle l_0, n-l_0\right|,\end{aligned} \tag{9}$$

where

$$\psi_n(q_j) = \frac{1}{\sqrt{2^n n! \sqrt{2\pi}}} H_n(q_j/\sqrt{2}) e^{-q_j^2/4} \tag{10}$$

is the coordinate representation of Fock state $|n\rangle$, with H_n being the n-th Hermite polynomial. Therefore, one can virtually insert another photon-number measurement after phase randomization before the squashing channel Eq. (4) on the detection side to measure the total photon number of the received state, as shown in Fig. 2(d).

Based on the above results, we depict a virtual quantum circuit of the protocol when both Alice and Bob chooses the Z-basis in Fig. 2(e). We denote the photon-number measurement results on the source side and the detection side as m and n, respectively. Alice and Bob can thus distill secrete keys separately based on the photon-number tag of (m, n). A lower bound on the key rate can then be given by [27, 28]

$$r \geq \sum_{m=0}^{\infty} Q_{m,m}[1 - h(e_{m,m}^X)] - fQ^Z h(e^Z), \tag{11}$$

where $Q_{m,m}$ and $e_{m,m}^X$ denote the gain and the phase-error rate in the rounds where m photons are sent and m photons are accepted, Q^Z is the Z-basis gain, e^Z is the bit-error rate, and f is the efficiency of information reconciliation. Note not to confuse the gains with quadrature observables. In addition, since Bob's key decoding succeeds probabilistically where he only accepts quadratures above the threshold, we use the term "accepting" to represent receiving a certain state and passing the post-selection. All the gains and error rates in the key-rate formula are restricted to the rounds with light intensity $\mu_a = \mu$. We discard the rounds where the total photon number decreases after state transmission, as the photons that are lost may come from Eve's interception, with which Eve can apply a PNS attack. The corresponding phase-error probability is 1/2; hence these rounds do not contribute to key generation. In addition, as the transmission channel is naturally lossy in a usual setting, we do not account for the terms where the total photon number increases.

Note that the key-rate formula in Eq. (11) assumes forward reconciliation, where Bob reconciles his raw keys to Alice's, k_a, and then the users perform privacy amplification. The rounds where Alice sends a non-vacuum state while Bob receives a vacuum state are hence insecure, since the information carriers are lost through the channel. Instead, if reverse reconciliation is used, where Alice reconciles her raw keys to Bob's, the rounds where Bob receives a vacuum state become secure. One can interpret Bob's raw keys in these rounds as generated from local random numbers, and no information is known *a priori* in transmission. This is a common practice in usual CV QKD and in accordance with the observation in Ref. [23]. The fact that the vacuum component can also contribute to key rate formula is first observed in Ref. [46]. We present as Theorem 1 the key-rate lower bound with reverse reconciliation as the main key-rate formula to be used throughout this paper.

Theorem 1. *For the time-bin CV QKD protocol in Table I with reverse reconciliation, in the asymptotic limit of an infinite data size, the distillable secure key rate r is lower bounded by r_{rev},*

$$r \geq r_{\text{rev}} = Q_{*,0} + \sum_{m=1}^{\infty} Q_{m,m}[1 - h(e^X_{m,m})] - fQ^Z h(e^Z), \tag{12}$$

where $Q_{m,m}$ and $e^X_{m,m}$ denote the gain and the phase-error rate in the rounds where m photons are sent and m photons are accepted, Q^Z is the Z-basis gain, e^Z is the bit-error rate, and f is the efficiency of information reconciliation. $Q_{*,0}$ represents the gain of the rounds where Bob accepts a vacuum state for whatever state sent by Alice.

C. Phase-error probability calculation

We now evaluate the key-rate formula in Eq. (12) with Fock-basis observables [5]. The bit-error rate e^Z can be directly measured, as the Z-measurement statistics in the entanglement-based squashing model are the same as the realistic statistics. To evaluate the gains and phase-error probabilities, we first determine the state before the phase-error measurement under each photon-number tag. Define $\hat{P}_m$ as the projector onto the m-photon state on modes A_1 and A_2. When sending m photons, the source in Fig. 2(b) collapses to

$$\hat{P}_m^{A_1A_2} \hat{\rho}_{A'A_1A_2} \hat{P}_m^{A_1A_2} = \Pr(m) \left|\Psi_m\right\rangle_{A'A_1A_2} \left\langle\Psi_m\right|, \tag{13}$$

where

$$\begin{aligned} \left|\Psi_m\right\rangle_{A'A_1A_2} &= \frac{1}{\sqrt{2}}(\left|0\right\rangle_{A'} \left|0m\right\rangle_{A_1A_2} + \left|1\right\rangle_{A'} \left|m0\right\rangle_{A_1A_2}), \\ \Pr(m) &= \frac{e^{-\mu}\mu^m}{m!}. \end{aligned} \tag{14}$$

Upon transmitting the m-photon state, $\left|\Psi_m\right\rangle_{A'A_1A_2}$, the n-photon state is selected on the detection side after the squashing channel,

$$\mathcal{F}_{\text{rand}}^{B_1B_2\to B'} \left\{ \hat{P}_n^{B_1B_2} \mathcal{N}_E^{A_1A_2\to B_1B_2} \left[\Pr(m) \left|\Psi_m\right\rangle_{A'A_1A_2} \left\langle\Psi_m\right| \right] \hat{P}_n^{B_1B_2} \right\} = Q_{m,n} \hat{\rho}^{(m,n)}_{A'B'}, \tag{15}$$

where $\mathcal{N}_E^{A_1A_2\to B_1B_2}$ represents Eve's channel, and $Q_{m,n}$ denotes the probability of sending an m-photon state and accepting an n-photon state, namely the gain for the states tagged by the photon-number tuple, (m,n). Note the probability that Bob aborts the signal is reflected in $Q_{m,n}$. The normalized state, $\hat{\rho}^{(m,n)}_{A'B'}$, is a bipartite qubit, with which we evaluate the phase-error probability,

$$e^X_{m,n} = \mathrm{Tr}\left[\hat{\rho}^{(m,n)}_{A'B'} \left(\left|+-\right\rangle_{A'B'} \left\langle+-\right| + \left|-+\right\rangle_{A'B'} \left\langle-+\right| \right) \right]. \tag{16}$$

With respect to the complementary-basis measurement result on the qubit A', $+$ or $-$, the state on modes A_1 and A_2 collapses to

$$\left|\Psi_m^{\pm}\right\rangle_{A_1A_2} = \frac{1}{\sqrt{2}}(\left|0m\right\rangle \pm \left|m0\right\rangle)_{A_1A_2} \tag{17}$$

with equal probabilities. For the state on Bob's systems B_1 and B_2 under tag (m,n), $\hat{\rho}^{(m,n)}_{B_1B_2}$, the statistics of the complementary measurement are given by

$$\begin{aligned} {}_{B'}\left\langle\pm\right| \mathcal{F}_{\text{rand}}^{B_1B_2\to B'}[\hat{\rho}^{(m,n)}_{B_1B_2}] \left|\pm\right\rangle_{B'} &= \mathrm{Tr}\left[\hat{\rho}^{(m,n)}_{B_1B_2} \hat{M}_{\pm} \right] \\ &= \mathrm{Tr}\left[\hat{\rho}^{(m,n)}_{B_1B_2} \hat{P}_n \hat{M}_{\pm} \hat{P}_n \right], \end{aligned} \tag{18}$$

where

$$\begin{aligned} \hat{M}_{\pm} = \frac{1}{2} \int_{\mathbf{R_0}} dq_1 dq_2 \int_0^{2\pi} \frac{d\varphi_b}{2\pi} \big[&\left|q_1(\varphi_b), q_2(\varphi_b)\right\rangle \pm \\ &\left|q_2(\varphi_b), q_1(\varphi_b)\right\rangle \big] \left[\left\langle q_1(\varphi_b), q_2(\varphi_b)\right| \pm \left\langle q_2(\varphi_b), q_1(\varphi_b)\right| \right]. \end{aligned} \tag{19}$$

In the last equation in Eq. (18), we utilize the fact that $\hat{\rho}^{(m,n)}_{B_1B_2}$ acts on the n-photon space of system B_1B_2. Combining the above results, we can express the phase-error rate for each tag with observables on optical modes:

Proposition 1. *The phase-error rate $e^X_{m,n}$ of the rounds where m photons are sent and n photons are accepted can be calculated by:*

$$\frac{Q_{m,n}e^X_{m,n}}{\Pr(m)} = \frac{1}{2}\mathrm{Tr}[\mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_m^+\rangle_{A_1A_2}\langle\Psi_m^+|)\hat{P}_n\hat{M}_-\hat{P}_n + \mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_m^-\rangle_{A_1A_2}\langle\Psi_m^-|)\hat{P}_n\hat{M}_+\hat{P}_n], \tag{20}$$

where $Q_{m,n}$ denotes the probability of sending an m-photon state and accepting an n-photon state, and $\Pr(m)$ is the probability of the source emitting m photons. $\mathcal{N}_E$ denotes Eve's channel on the two optical modes and $\hat{P}_n$ denotes the projector onto the n-photon subspace. $|\Psi_m^\pm\rangle$ and $\hat{M}_\pm$ defined in Eq. (17) and (19) respectively.

We can write $\hat{P}_n\hat{M}_{+(-)}\hat{P}_n$ on the Fock basis using Eq. (9), expressing the phase-error rate as quantities on optical modes. Here, we list the final results for a protocol that utilizes up to the two-photon components. The detailed calculation is placed in Appendix A.

- For the single-photon component,

$$\begin{aligned}\frac{Q_{1,1}e^X_{1,1}}{\Pr(1)} = \frac{c_1}{2}\Big\{&\mathrm{Tr}\left[\mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_1^+\rangle_{A_1A_2}\langle\Psi_1^+|)\frac{1}{2}(|01\rangle_{B_1B_2} - |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} - \langle 10|_{B_1B_2})\right] \\ &+\mathrm{Tr}\left[\mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_1^-\rangle_{A_1A_2}\langle\Psi_1^-|)\frac{1}{2}(|01\rangle_{B_1B_2} + |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} + \langle 10|_{B_1B_2})\right]\Big\},\end{aligned} \tag{21}$$

where

$$c_1 = \int_{\mathbf{R_0}} dq_1dq_2[\psi_0^2(q_1)\psi_1^2(q_2) + \psi_0^2(q_2)\psi_1^2(q_1)], \tag{22}$$

and gain $Q_{1,1}$ is given by

$$\frac{Q_{1,1}}{\Pr(1)} = c_1\mathrm{Tr}\left\{\mathcal{N}_E\left[\mathrm{Tr}_{A'}(|\Psi_1\rangle_{A'A_1A_2}\langle\Psi_1|)\right](|01\rangle_{B_1B_2}\langle 01| + |10\rangle_{B_1B_2}\langle 10|)\right\}. \tag{23}$$

Up to the less-than-unity factor c_1 that arises from the data post-selection in key mapping, the formulae are the same as the complementary-basis result in the coherent-state-based BB84 protocol [47]. It can also be seen that the phase-error rate of the rounds where Alice transmits two photons and Bob accepts one photon involves in the probability where Alice transmits $(|02\rangle \pm |20\rangle)/\sqrt{2}$ and Bob receives $(|01\rangle \mp |10\rangle)/\sqrt{2}$. In a pure-loss channel, the superimposed two-photon state $(|02\rangle \pm |20\rangle)/\sqrt{2}$ would lose coherence if one photon is lost during the channel, thus giving 50% phase-error rate. This observation validates the intuition of the PNS attack.

- For the two-photon subspace, based on Eq. (9) and Eq. (20), we have,

$$\begin{aligned}\frac{Q_{2,2}e^X_{2,2}}{\Pr(2)} =&\frac{1}{2}c_2^-\mathrm{Tr}\left[\mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_2^+\rangle_{A_1A_2}\langle\Psi_2^+|)\frac{1}{2}(|02\rangle_{B_1B_2} - |20\rangle_{B_1B_2})(\langle 02|_{B_1B_2} - \langle 20|_{B_1B_2})\right] \\ &+\frac{1}{2}c_2^+\mathrm{Tr}\left[\mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_2^-\rangle_{A_1A_2}\langle\Psi_2^-|)\frac{1}{2}(|02\rangle_{B_1B_2} + |20\rangle_{B_1B_2})(\langle 02|_{B_1B_2} + \langle 20|_{B_1B_2})\right] \\ &+c_2^{11}\mathrm{Tr}\left[\mathcal{N}_E^{A_1A_2\to B_1B_2}(|\Psi_2^-\rangle_{A_1A_2}\langle\Psi_2^-|)\,|11\rangle_{B_1B_2}\langle 11|\right],\end{aligned} \tag{24}$$

where

$$\begin{aligned}c_2^+ &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_2(q_2) + \psi_2(q_1)\psi_0(q_2)]^2, \\ c_2^- &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_2(q_2) - \psi_2(q_1)\psi_0(q_2)]^2, \\ c_2^{11} &= \int_{\mathbf{R_0}} dq_1dq_2[2\psi_1^2(q_1)\psi_1^2(q_2)],\end{aligned} \tag{25}$$

and the two-photon gain is given by

$$\begin{aligned}\frac{Q_{2,2}}{\Pr(2)} =&c_2^+\mathrm{Tr}\left\{\mathcal{N}_E^{A_1A_2\to B_1B_2}[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\frac{1}{2}(|02\rangle_{B_1B_2} + |20\rangle_{B_1B_2})(\langle 02|_{B_1B_2} + \langle 20|_{B_1B_2})\right\} \\ &+c_2^-\mathrm{Tr}\left\{\mathcal{N}_E^{A_1A_2\to B_1B_2}[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\frac{1}{2}(|02\rangle_{B_1B_2} - |20\rangle_{B_1B_2})(\langle 02|_{B_1B_2} - \langle 20|_{B_1B_2})\right\} \\ &+c_2^{11}\mathrm{Tr}\left\{\mathcal{N}_E^{A_1A_2\to B_1B_2}[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\,|11\rangle_{B_1B_2}\langle 11|\right\}.\end{aligned} \tag{26}$$

- The probability of accepting a vacuum state when employing reverse reconciliation is given by

$$Q_{*,0} = \mathrm{Tr}\left[\hat{P}_0^{B_1B_2}\mathcal{N}_E^{A_1A_2\to B_1B_2}\left(\hat{\rho}^Z\right)\hat{P}_0^{B_1B_2}\right]\int_{\mathbf{R_0}} 2\psi_0^2(q_1)\psi_0^2(q_2)dq_1dq_2, \tag{27}$$

where $\hat{\rho}^Z$ is the Z-basis state sent by the source given in Eq. (8); hence $Q_{*,0}$ is given by the product of the probability of receiving a vacuum-state in the Z-basis rounds and a post-selection-related integration factor. Note that the former value is independent of the post-selection.

IV. PARAMETER ESTIMATION AND PRACTICAL PROTOCOL

We briefly show how to estimate the parameters derived in Sec. III C with a practical setup. In the actual protocol, we do not have photon-number-resolving detectors, with which one can directly measure the above parameters. In addition, the phase-error probabilities and gains are defined by particular Fock-basis states, yet the actual photon source emits coherent states. Nevertheless, we can construct unbiased estimators with the available states and detection settings to evaluate these values. On the detection side, we apply the homodyne tomography technique to evaluate the photon-number observables [34–39]. The homodyne tomography allows unbiased estimation of the expected value of a variety of observables, including the photon-number observables, of measuring an unknown quantum state. On the source side, we extend the decoy-state method [29, 30] to evaluate the statistics defined by the non-classical Fock states with the use of the coherent states at hand. We will give a practical version of the protocol at the end of this section. A fully-detailed discussion is placed in Appendix B on how the specific parameters related to key rate calculation can be practically estimated.

A. Effective photon-number resolving via homodyne tomography

Since the eigenstates of the quadrature observables, $|q(\varphi)\rangle$, form a complete basis on an optical mode, one can reconstruct a general observable on an optical mode with homodyne measurements. In our study, the parameters to be estimated involve photon-number measurements on two modes in the form of $\hat{O}_1\otimes\hat{O}_2 = |n_1\rangle_{B_1}\langle m_1|\otimes|n_2\rangle_{B_2}\langle m_2|$. Their measurements on an arbitrary state, $\hat{\rho}$, can be obtained from two independent homodyne measurements with randomized LO phases,

$$\begin{aligned}\langle\hat{O}_1\otimes\hat{O}_2\rangle &= \mathrm{Tr}[(\hat{O}_1\otimes\hat{O}_2)\hat{\rho}]\\ &:= \int_0^\pi\frac{d\varphi_1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_2}{\pi}\int_{-\infty}^{\infty}dq_2\\ &\quad\mathcal{R}[\hat{O}_1](q_1,\varphi_1)\mathcal{R}[\hat{O}_2](q_2,\varphi_2)p(q_1,q_2|\varphi_1,\varphi_2),\end{aligned} \tag{28}$$

where $p(q_1,q_2|\varphi_1,\varphi_2)$ is the joint probability of the quadrature measurements on the two modes conditioned on phases φ_1 and φ_2. The estimators, $\mathcal{R}[\hat{O}_1](q_1,\varphi_1)$ and $\mathcal{R}[\hat{O}_2](q_2,\varphi_2)$, link the quadrature measurement statistics with $\langle\hat{O}_1\otimes\hat{O}_2\rangle$. For a homodyne detector with efficiency η, the estimator for observable $|n\rangle\langle n+d|$ is given by

$$\begin{aligned}\mathcal{R}_\eta[|n\rangle\langle n+d|](q,\varphi) &= e^{id(\varphi+\frac{\pi}{2})}\sqrt{\frac{n!}{(n+d)!}}\\ &\int_{-\infty}^{\infty}dk|k|\exp\left(\frac{1-2\eta}{2\eta}k^2-ikq\right)k^dL_n^d(k^2),\end{aligned} \tag{29}$$

where L_n^d is the generalized Laguerre polynomial. The estimator is shown to be bounded for detector efficiency $\eta > 1/2$ [37, 39], a mild requirement for current technologies [48, 49]. Consequently, repeated measurements allow the users to obtain an unbiased estimation of the photon-number observables that converges in probability. Note that the detector imperfection does not need to be trusted. The homodyne tomography is valid as long as the detector is well-calibrated so that the quadrature measurement is genuine. In Appendix B 1, we shall provide more details of the homodyne tomography techniques.

B. Generalized decoy-state method

To effectively realize the non-classical states on the source side, we extend the standard decoy-state method [29, 30]. We take advantage of two-mode coherent states with simultaneous phase randomization on the two modes. We denote the state with phase difference φ as

$$\begin{aligned}\hat{\rho}_\mu^\varphi &= \int_0^{2\pi}\frac{d\theta}{2\pi}\left|\sqrt{\frac{\mu}{2}}e^{i\theta}\right\rangle\left\langle\sqrt{\frac{\mu}{2}}e^{i\theta}\right|\otimes\left|\sqrt{\frac{\mu}{2}}e^{i(\theta+\varphi)}\right\rangle\left\langle\sqrt{\frac{\mu}{2}}e^{i(\theta+\varphi)}\right|\\ &= \sum_{m=0}^{\infty}\sum_{k=0,l=0}^{m}\frac{e^{-\mu}\left(\frac{\mu}{2}\right)^N e^{i(l-k)\varphi}}{\sqrt{k!l!(m-k)!(m-l)!}}|k,m-k\rangle\langle l,m-l|,\end{aligned} \tag{30}$$

where we specify the light intensity with the subscript, μ. With proper linear combination of these states, we can effectively construct the photon-number-cat states that we are interested in. It is well-known that $(|01\rangle\pm|10\rangle)/\sqrt{2}$ is the single-photon component of $\hat{\rho}_\mu^{0(\pi)}$,

$$\Pr_\mu(1)\left|\Psi_1^{+(-)}\right\rangle\left\langle\Psi_1^{+(-)}\right| = \hat{P}_1\hat{\rho}_\mu^{0(\pi)}\hat{P}_1, \tag{31}$$

where $\Pr_\mu$ represents the Poisson distribution determined by light intensity μ, as given in Eq. (14). Thus, the estimation problem is transformed into the estimation of the single-photon yields of $\hat{\rho}_\mu^0$ and $\hat{\rho}_\mu^\pi$. For the multi-photon components $(|0m\rangle \pm |m0\rangle)/\sqrt{2}$, a direct calculation shows

$$\Pr_\mu(m) \left|\Psi_m^+\right\rangle \left\langle\Psi_m^+\right| = \hat{P}_m \left(\hat{\rho}_\mu^Z + \frac{2^{m-2}}{m} \sum_{k=0}^{m-1} \hat{\rho}_\mu^{\frac{2\pi k}{m}} - \frac{2^{m-2}}{m} \sum_{k=0}^{m-1} \hat{\rho}_\mu^{\frac{2\pi k}{m}+\delta} \right) \hat{P}_m, \tag{32}$$

$$\Pr_\mu(m) \left|\Psi_m^-\right\rangle \left\langle\Psi_m^-\right| = \hat{P}_m \left(\hat{\rho}_\mu^Z - \frac{2^{m-2}}{m} \sum_{k=0}^{m-1} \hat{\rho}_\mu^{\frac{2\pi k}{m}} + \frac{2^{m-2}}{m} \sum_{k=0}^{m-1} \hat{\rho}_\mu^{\frac{2\pi k}{m}+\delta} \right) \hat{P}_m, \tag{33}$$

where $\delta = \pi$ for odd m and $\pi/2$ for even m, and $\hat{\rho}_\mu^Z$ is the state emitted from the source in a key generation round. Consequently, the terms that define $e_{m,m}^X$ and $Q_{m,m}$ can be constructed from the statistics when emitting the states of $\hat{\rho}_\mu^Z$ and $\hat{\rho}_\mu^\varphi$ with $\varphi \in \{2\pi k/m, 2\pi k/m + \delta\}_{k=0}^{m-1}$. Notably, the extended decoy method allows estimating the gains with the number of parameters increasing only linearly in the photon number. In later discussions, we shall utilize up to the two-photon components. Specifically, for $m = 2$,

$$\begin{aligned} \Pr_\mu(2) \left|\Psi_2^\pm\right\rangle \left\langle\Psi_2^\pm\right| = & \hat{P}_2 \Big[\hat{\rho}_\mu^Z \pm \left(\frac{1}{2}\hat{\rho}_\mu^0 + \frac{1}{2}\hat{\rho}_\mu^\pi \right) \\ & \mp \left(\frac{1}{2}\hat{\rho}_\mu^{\frac{\pi}{2}} + \frac{1}{2}\hat{\rho}_\mu^{\frac{3\pi}{2}} \right) \Big] \hat{P}_2. \end{aligned} \tag{34}$$

One may notice in Eq. (34) there are states outside the encoding subspace $|02\rangle$ and $|20\rangle$ being introduced, which gives Eve possibility to distinguish the X-basis states. In fact, the X basis is comprised of the mixture of $(|02\rangle \pm |20\rangle)/\sqrt{2}$ and $|11\rangle$. As a result, it is not possible for Eve to distinguish between the Z-basis states and the $(|02\rangle \pm |20\rangle)/\sqrt{2}$ states of the X basis. It is possible for Eve to distinguish the $|11\rangle$ state, yet it does not yield knowledge on the encoded key information since it is orthogonal to the $|02\rangle$ and $|20\rangle$ space. Hence, the standard decoy argument still applies even if the parameter-estimation space consists of a direct sum of the key-encoding space and some orthogonal spaces.

C. General parameter estimation under the coherent attack

In this section, we discuss the security analysis and parameter estimation in the most general case. In the most general adversarial scenario, namely the coherent attack, Eve can apply a joint quantum operation over the rounds for eavesdropping, which may correlate or even entangle the states transmitted to Bob. Eve collects all the side information leaked to her in the protocol and then guesses the legitimate users' keys. Under such an attack, the measurement statistics obtained by Bob are generally correlated over the rounds [41].

The complementarity-based security analysis remains valid with finite statistics under a coherent attack [22]. The information leakage is quantified via the number of phase errors, while the occurrence of a phase error in each round may be non-i.i.d. That is, one should interpret the gains and phase-error rates in Eq. (12) as frequencies in non-i.i.d. statistics. For instance, $Q_{1,1}$ should be regarded as the frequency of the events that Alice sends a single-photon state, and Bob accepts a single-photon state among key generation rounds in the virtual experiment. The remaining problem is to estimate these parameters via observed statistics.

To tackle the non-i.i.d. parameter estimation problem, we can apply a martingale-based analysis. We shall present the details in Appendix C. Here, we explain its basic idea. As the starting point, in the i'th round, the users can evaluate the probability of choosing some experimental setting and observing a particular event conditioned on the experimental history, including the events of sending an m-photon state and accepting an n-photon state and the occurrence of a phase error if they choose the key generation setting, and observing a particular homodyne detection result if they choose to perform the parameter estimation operations. The events' correlations with the experimental history are inherently taken into account in the definitions of conditional probabilities. We can set up martingales for a series of events, such as the occurrence of phase errors in each round of the virtual protocol, and link their frequencies with the associated conditional probabilities via concentration results like Azuma's inequality [50]. Note that such concentration results work for general non-i.i.d. correlations. Furthermore, the setting choices randomly chosen by Alice and Bob are independent of the experimental history and unknown to Eve. Therefore, conditioned on the experimental history, the probabilities of different possible events in a round are linked. For instance, the probability that the users take key generation measurements and a phase error occurs in a round is measurable via the probability that they instead take parameter estimation measurements and observe certain statistics. The relation is in the form of Eq. (20), while now the probabilities are interpreted as conditional ones that cover the correlations. The relations between conditional probabilities then link the martingales for the parameter estimation measurement with the ones for the gains and phase-error rates, completing the parameter estimation. In the end, the total number of keys that can be securely distilled from finite statistics under the coherent attack is given by a formula of the following form:

Theorem 2 (Informal)**.** *For the CV QKD protocol with N_μ^{zz} rounds for key generation, given the failure probability in parameter estimation ε_{pe}, suppose the gains have lower bounds $Q_{*,0}^L$ and $Q_{m,m}^L$, and the phase-error rates have upper bounds $e_{m,m}^{X(U)}$. Then, given the failure probability in privacy amplification ε_{pa}, conditioned on the success of information reconciliation, except a total failure probability $\varepsilon = \varepsilon_{\text{pe}} + \varepsilon_{\text{pa}}$, the finite-size key rate r is lower bounded by:*

$$\begin{aligned} r \geq & Q_{*,0}^L + \sum_{m=1}^{\infty} \left(Q_{m,m}^L \left\{ 1 - h[e_{m,m}^{X(U)}] \right\} \right) \\ & - fQ^Z h(e^Z) - \frac{1}{N_\mu^{zz}} \log \frac{1}{\varepsilon_{\text{pa}}}, \end{aligned} \tag{35}$$

where f is the information reconciliation efficiency, Q^Z is the Z-basis gain, and e^Z is the bit error rate.

The term $\log \varepsilon_{\text{pa}}$ in the key-rate formula originates from the failure probability in privacy amplification [22, 51]. The parameter estimation failure probability ε_{pe} comes from the use of martingale-based concentration results. In the asymptotic limit of infinite data size, ε_{pe} converges to zero, and the effect of ε_{pa} on the key rate becomes negligible; hence the key rate formula degenerates to that in Eq. (12). In Appendix C, we provide the details of non-i.i.d. parameter estimation and the formal description of the key-rate formula.

D. Practical protocol

Combining the above ingredients, we provide a practical protocol that utilizes up to the two-photon components in Table III. In parameter estimation, Bob applies homodyne tomography to estimate the statistics of measuring photon-number observables, including $|00\rangle$, $(|01\rangle \pm |10\rangle)/\sqrt{2}$, $(|02\rangle \pm |20\rangle)/\sqrt{2}$, and $|11\rangle$, on various states transmitted from the source, originally $\hat{\rho}_{\mu_a}^Z$ and $\hat{\rho}_\mu^{\varphi_a}$. Afterward, the users can obtain upper and lower bounds on the gains and phase-error rates by applying the extended decoy-state method. We provide the detailed parameter estimation procedures in Appendix B and discuss dealing with general non-i.i.d. statistics under a coherent attack in Appendix C.

In the end, we make some remarks on the protocol. Notice that in contrast to the conventional BB84-type protocols, our protocol also uses for parameter estimation the signals where Alice chooses Z basis and Bob chooses X basis. Alice's announcement of the relative phase does not reveal key information since the key is encoded in the relative intensity between the two modes. We assume Alice and Bob apply continuous phase randomization, although it is only practical to use discrete random phases. The effect of the discretization requires further investigation. In addition, in the X basis, Alice only transmits coherent states with relative phases in $\{0, \pi/2, \pi, 3\pi/2\}$. These relative phases are enough to estimate the phase-error rate of an up-to-two-photon protocol according to Eq. (34).

V. PERFORMANCES AND COMPARISON

We demonstrate in this section the asymptotic key rate-distance performances of the time-bin CV QKD protocol. We consider a thermal noise channel with a unit-efficiency homodyne detector. An inefficient detector with thermal electronic noise can be equated to a fiber section with transmittance equal to the detector efficiency, and the electronic noise absorbed into the channel excess noise (Eq. (D2)). The fiber attenuation is 0.2 dB/km, and the error-correction efficiency f is taken to be 1. The simulation formulae can be found in Appendix D. According to the key rate formula Eq. (12), the rounds where Alice sends m photons and Bob receives m photons can assure to generate secure keys. We plot in Fig. 3a the asymptotic key rate of the i-photon protocol assuming perfect decoy estimation and no excess noise, where in an i-photon protocol we only extract secure keys from a maximal i-photon components. In this ideal case, the phase error rates of all the protocols are zero. The optimized source intensities μ and the post-selection thresholds τ are listed in Table IV, as well as the resulted Z-basis error rate. Notice that the two-photon-protocol key rate derived from our DV method is similar to that from Ref. [24] using CV method, both reversely reconciled. This implies the connection between DV and CV security analysis, as well as the validity of the DV reverse reconciliation idea in Section III B. To facilitate the discussion, we also plot in Fig. 3b the contribution of each photon components to the key rate at different distances. In each group of bars, the relative contribution of the vacuum, one, two, three, four-photon components are plotted respectively, where the m-photon contribution of the i-photon protocol is defined to be $Q_{m,m}/(Q_{*,0} + \sum_{m=1}^{i} Q_{m,m})$ and the vacuum contribution is $Q_{*,0}/(Q_{*,0} + \sum_{m=1}^{i} Q_{m,m})$, i.e., the relative contribution to the raw key rate.

It can be seen that the key rate improves as we make use of the multi-photon components. The improvement is most remarkable between the one and two-photon protocols. This is reasonable since in the one-photon protocol, the multi-photon components are considered insecure, thus limiting the source intensity. The low source

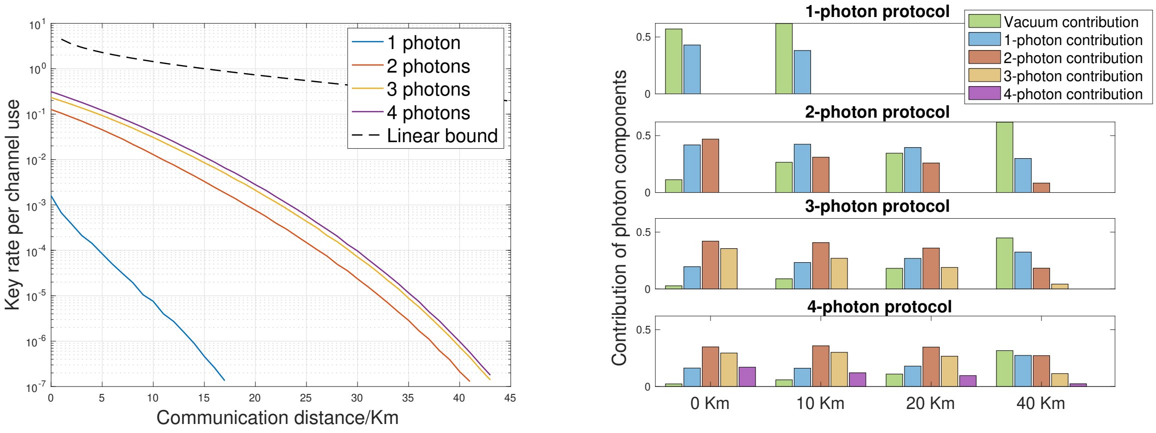
TABLE III: Practical time-bin CV QKD with decoy states using up to two photons

1. On Alice's side (source):
   - *Z-basis*:
     (a) Randomly select a key bit $k_a \in \{0, 1\}$, a phase factor $\varphi_a \in [0, 2\pi)$, and a light intensity $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) Prepare a coherent state of $|0\rangle_{A1} |\sqrt{\mu_a} e^{i\varphi_a}\rangle_{A2}$ for $k_a = 0$ or $|\sqrt{\mu_a} e^{i\varphi_a}\rangle_{A1} |0\rangle_{A2}$ for $k_a = 1$.
   - *X-basis*:
     (a) Randomly select a phase factor $\varphi_a^1 \in [0, 2\pi)$ and another phase factor with relative phase φ_a randomly in $\varphi_a^2 - \varphi_a^1 \in \{0, \pi/2, \pi, 3\pi/2\}$. Randomly select a light intensity $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) Prepare a coherent state of $|\sqrt{\mu_a/2} e^{i\varphi_a^1}\rangle |\sqrt{\mu_a/2} e^{i\varphi_a^2}\rangle$.
2. Alice sends the state through an authenticated channel to Bob.
3. On Bob's side (detection):
   - *Z-basis*:
     (a) Randomly select a phase factor $\varphi_b \in [0, 2\pi)$.
     (b) Use homodyne detectors with LO phases φ_b to measure the modes and obtain quadratures q_1 and q_2.
     (c) Decode the key bit as 0 if $|q_1| < \tau \wedge |q_2| > \tau$, 1 if $|q_1| > \tau \wedge |q_2| < \tau$, and $\emptyset$ otherwise.
   - *X-basis*:
     (a) Randomly select two phases $\varphi_b^1, \varphi_b^2 \in [0, \pi)$.
     (b) Use homodyne detectors with LO phases φ_b^1 and φ_b^2 to measure the modes and obtain quadratures q_1 and q_2.
4. Alice announces the light intensity in each round and relative phase between the two modes in X-basis states $\varphi_a = \varphi_a^2 - \varphi_a^1$.
5. Alice and Bob perform basis sifting, where they obtain raw keys in the rounds they both choose Z-basis with light intensity $\mu_a = \mu$ and $k_b \neq \emptyset$.
6. Bob estimates the gains and phase-error rates from the statistics in the rounds where Alice sends the Z-basis states $\hat{\rho}_{\mu_a}^Z$ or X-basis states $\hat{\rho}_{\mu_a}^{\varphi_a}$ with $\varphi_a \in \{0, \pi/2, \pi, 3\pi/2\}$.
7. Alice and Bob perform reverse information reconciliation and privacy amplification to obtain final keys.

intensity would result in severe bit error rate and higher post-selection thresholds, which in turn suppress the key rate. Whilst in the two-photon protocol where the two-photon components are considered secure, the limit on the source intensity can be lifted, and the bit error rate would drop, resulting in higher key rates. This is manifested in Fig. 3b, where the single-photon protocol sees significant vacuum contribution, whilst the two-photon protocol, at short distances, does not. Since the vacuum component would yield 50% bit error rate, we see the lower bit error rate of the two-photon protocol than the single-photon protocol as in Table IV.

When we further make use of the three-photon components, the key rate as well as the source intensity still increase, yet less obviously. This is mainly because the fraction of the rounds where three photons are sent and three photons are received, decaying cubically with the channel transmittance, are not dominating, especially at longer distances. For example, we see in Fig. 3b that at 20 km, the contribution of the three-photon component is less than that of the single and two-photon components, and at 40 km the three-photon component rarely has contribution to the key rate. This trend is justified further in the four-photon protocol, where in Fig. 3b we see the four-photon-component contribution is quite small for longer distances, and in turn the key rate of the four-photon protocol only improves marginally than that of the three-photon protocol. Simulation shows that resorting to higher-than-four photon-number components has negligible increase to the key rate. Hence, If we consider the protocol with infinite photon-number components, the 0-km key rate is around 0.31 bit/channel, and the BB84 protocol with currently the best single-photon detector of 80% efficiency [54, 55] has 0-km key rate 0.29 bit/channel, based on the model from Ref. [45]. Our key rate thus matches the best BB84 key rate with practically favorable devices.

The practical performances of the two-photon time-bin CV QKD protocol are illustrated in Fig. 4. For a reasonable range of excess noise ξ from 10^{-3} to 10^{-2} with respect to channel output, the key rate decays mildly as shown in Fig. 4a. Notice that the key rate is almost unaffected at 0 km since no noise photon is introduced to give phase error, and the bit error is almost unchanged



(a)

(b)

FIG. 3: **(a)** The solid lines illustrate the asymptotic key rates of protocols using maximal one, two, three and four photons to generate keys. The dotted line is the linear key rate bound [52, 53]. We plot the PLOB bound here. The channel and devices are assumed to be ideal with no excess noise and inefficiency. **(b)** The relative contribution of $Q_{m,m}$, i.e. the gain of the rounds where m photons are sent and m photons are received. The m-photon contribution of the i-photon protocol is relative to the raw key rate. Each group of bars illustrate the contribution of vacuum, one, two, three and four-photon components of the protocol at a certain distance.

TABLE IV: The optimized intensities and post-selection thresholds of protocols using one to four photons respectively at different distances. μ_i, τ_i and e_Z^i denote the optimized intensity, post-selection threshold and the Z-basis error rate of the i-photon protocol. These parameters generate the four key rate plots in Fig. 3a, assuming infinite decoy levels.

	μ_1	μ_2	μ_3	μ_4	τ_1	τ_2	τ_3	τ_4	e_Z^1	e_Z^2	e_Z^3	e_Z^4
0 km	0.356	1.487	2.395	2.395	1.437	1.641	1.845	1.845	30.95%	10.52%	5.31%	5.31%
10 km	0.137	0.924	1.887	2.395	3.476	2.253	2.457	2.457	29.80%	14.84%	5.66%	4.17%
20 km	—	0.728	1.487	1.887	—	3.068	3.068	3.272	—	15.48%	6.91%	3.85%
40 km	—	0.356	0.728	1.172	—	4.495	4.495	4.699	—	28.52%	17.07%	8.81%

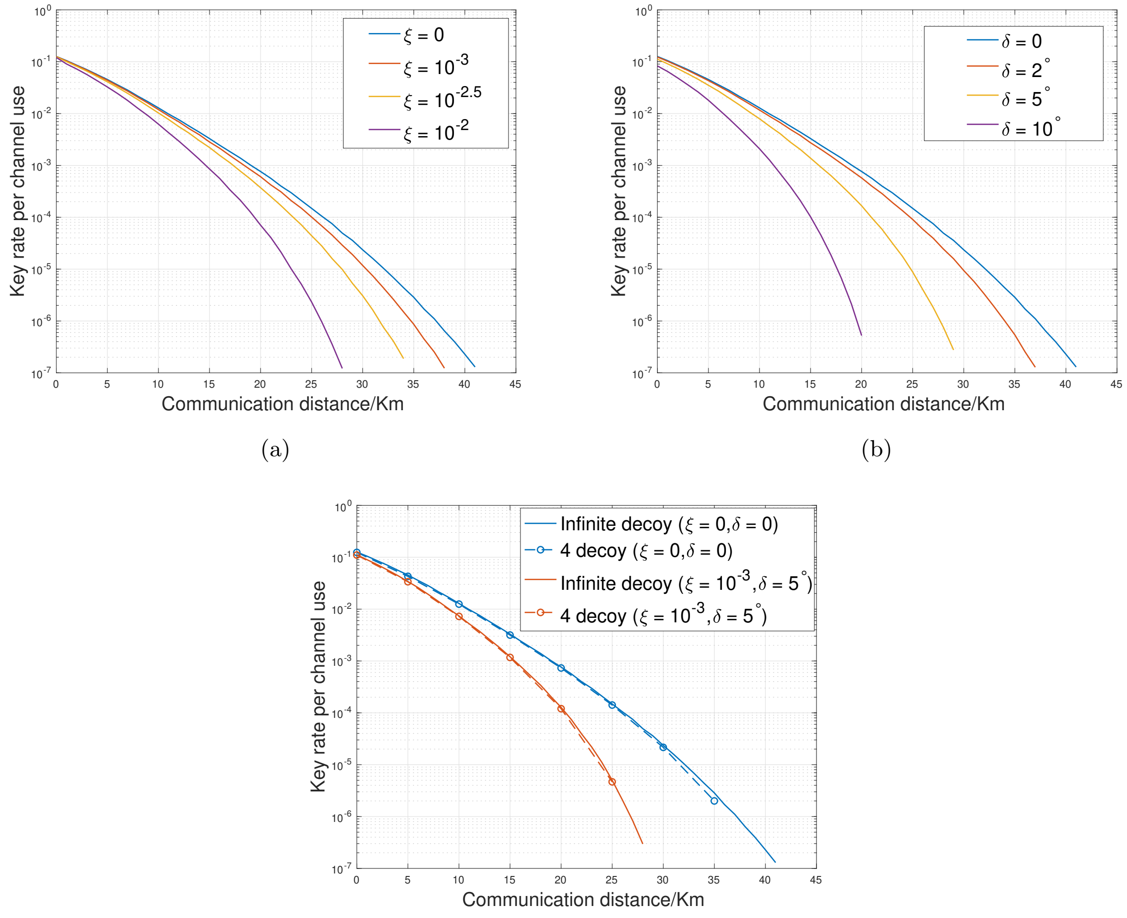
for a negligible increase in the shot-noise variance. This demonstrates the robustness of the phase-error analysis to the excess noise.

Fig. 4b illustrates the key rate against the mode reference misalignment, where the two optical modes generating the time-bin qubit differ by δ in the reference phases intrinsically. The misalignment in relative phases does not affect the Z basis as we encode the key bits into the relative intensities, and it only affects the X basis where the phase error is defined as the flips in relative phases. Our protocol thus has robustness against misalignment.

Fig. 4c illustrates the key rates of the decoy-state protocol in Sec. IV B. We set one decoy level at vacuum, and heuristically optimize the two decoy intensities ν_1 and ν_2 and the signal intensity μ. The decoy estimations are done by linear programming with a cutoff photon number 10 [56, 57]. A detailed treatment of the decoy estimation of the two-photon protocol is placed in Appendix B. We see for both the noiseless setup, with no excess noise and misalignment, and the practical setup, with 10^{-3} excess noise and 5° misalignment, the 4-level decoy estimation is almost exact. This clearly surpassed the practical performance of the protocol in Ref. [24], since our protocol uses simpler estimation of the phase error by identifying the principal components in key generation. The optimized parameters of the practical setup are listed in Table V.

VI. REFINED KEY MAPPING SCHEME

In the time-bin-encoded CV QKD protocol in Table I, we consider a simple key mapping strategy with a threshold value τ illustrated in Fig. 5a. It can be seen that the security analysis in Sec. III does not rely on the specific shapes of the key mapping regions $\mathbf{R_0}$ and $\mathbf{R_1}$, as long as they differ by a swap of the two optical modes. As a result, we can optimize $\mathbf{R_0}$ and $\mathbf{R_1}$ for a higher key-rate



(a)

(b)

(c)

FIG. 4: Practical performances of the two-photon protocol. **(a)** Key rate against excess noise with respect to channel output, assuming infinite decoy levels. **(b)** Key rate against misalignment, i.e. the phase-reference difference between the two optical modes generating the time-bin qubit, assuming infinite decoy levels. **(c)** Key rate derived using decoy methods. The noiseless setup (blue curves) uses fixed decoy levels at 1.2×10^{-4}, 1×10^{-4} and vacuum, and the optimized protocol parameters of the practical setup (red curves) are listed in Table V.

TABLE V: Optimal protocol parameters in generating the key rate plot with 10^{-3} excess noise and 5° misalignment, using 4 decoy levels, as in Fig. 4c. The heuristically optimized signal intensity, post-selection threshold and the decoy intensities are as given. There is one more decoy intensity set to be vacuum. The decoy estimation is done by linear programming with cutoff photon number 10.

Distance (km)	Signal intensity μ	Threshold τ	Decoy intensity ν_1	Decoy intensity ν_2
0	1.487	1.641	1.737×10^{-1}	1.000×10^{-4}
5	1.172	2.049	3.406×10^{-3}	2.740×10^{-4}
10	0.924	2.457	2.993×10^{-2}	1.000×10^{-4}
15	0.924	3.068	1.861×10^{-2}	1.000×10^{-4}
20	0.728	3.476	1.355×10^{-2}	2.441×10^{-4}
25	0.728	4.291	1.355×10^{-2}	1.562×10^{-4}

performance indicated by r in Eq. (12).

To get a higher key rate r, we want to avoid the post-selection of the detected signal region (q_1, q_2) as long as the bit error rate e^Z can be ensured low. To this end, we introduce a maximum-likelihood-based key mapping and analyze its performance. Corresponding to bit 0 or 1, Bob would receive coherent states $|0\rangle\,|\alpha e^{i\varphi_a}\rangle$ or $|\alpha e^{i\varphi_a}\rangle\,|0\rangle$ for some randomized phase φ_a and α after attenuation in a pure-loss channel. Corresponding to bit value 0 and 1, the probability distributions f_0 and f_1 of the homodyne measurement results (q_1, q_2) are given by

$$f_0(q_1,q_2) = \int_0^{2\pi} \frac{d\varphi}{4\pi^2} \exp\frac{\left[-q_1^2 - (q_2 - 2|\alpha|\cos\varphi)^2\right]}{2}, \tag{36}$$

$$f_1(q_1,q_2) = \int_0^{2\pi} \frac{d\varphi}{4\pi^2} \exp\frac{\left[-q_2^2 - (q_1 - 2|\alpha|\cos\varphi)^2\right]}{2}, \tag{37}$$

where φ is the difference between the source and detector phase randomization.

Upon detecting a specific pair of quadratures (q_1, q_2), the maximum-likelihood key mapping scheme requires to decode bit 0 if $f_0(q_1,q_2) > f_1(q_1,q_2)$ and bit 1 if $f_1(q_1,q_2) > f_0(q_1,q_2)$. According to Eq. (36) and (37), the maximum-likelihood key mapping is equivalent to the decoding of bit 0 if $q_1^2 < q_2^2$ and bit 1 if $q_1^2 > q_2^2$. This refined key mapping takes in detection results such as point A in Fig. 5a where q_1^2 is significantly different from q_2^2, thus reducing the post-selection loss of the gain. However, in the region where q_1^2 and q_2^2 are comparable, the key mapping error will be large, making a large contribution to the final bit error rate e^Z. Conditioned on the detection outcome (q_1, q_2), the key mapping error $e_0^Z(q_1,q_2)$ in $\mathbf{R_0}$ is related to the likelihood function by

$$e_0^Z(q_1,q_2) = \Pr((q_1,q_2) \in \mathbf{R_0} | k_a = 1) = \frac{f_1(q_1,q_2)}{Q(q_1,q_2)}, \tag{38}$$

with the key mapping gain $Q(q_1,q_2) = f_0(q_1,q_2) + f_1(q_1,q_2)$. We can similarly define $e_1^Z(q_1,q_2)$ for the $\mathbf{R_1}$ region. The final bit error rate e^Z is

$$\begin{aligned} e^Z = &\frac{1}{2}\int_{\mathbf{R_0}} dq_1 dq_2\, e_0^Z(q_1,q_2)\, Q(q_1,q_2) \\ &+ \frac{1}{2}\int_{\mathbf{R_1}} dq_1 dq_2\, e_1^Z(q_1,q_2)\, Q(q_1,q_2). \end{aligned} \tag{39}$$

For example, at point B in Fig. 5a, the key mapping error is 50%. To discard the erroneous results, we can set a threshold $t > 1$ and require to decode bit 0 if $f_0(q_1,q_2) > tf_1(q_1,q_2)$ and bit 1 if $f_1(q_1,q_2) > tf_0(q_1,q_2)$. The region in between will be discarded. Fig. 5b below illustrates the numerically plotted key mapping regions given the light amplitude $\alpha = 1$ at $t = 10$, where the grey region is discarded. It can be seen that the key mapping regions are nearly isosceles right triangles with non-zero intercepts $\pm\tau$ with the quadrature axes. We thus present the approximately maximum-likelihood key mapping scheme as the following:

$$k_b = \begin{cases} 0 & \text{if } (q_2 - \tau > \pm q_1) \vee (q_2 + \tau < \pm q_1), \\ 1 & \text{if } (q_1 - \tau > \pm q_2) \vee (q_1 + \tau < \pm q_2), \\ \emptyset & \text{otherwise.} \end{cases} \tag{40}$$

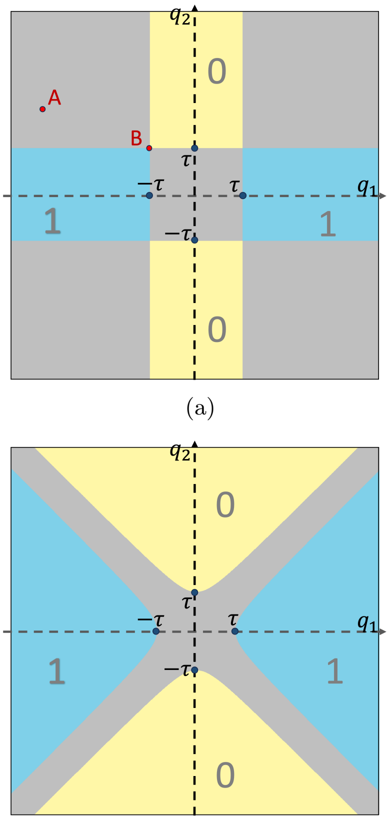
As in Sec. V, we regard the intercept τ as a protocol parameter. We optimize it and the source intensity μ for each distance to yield the optimal key rate. However, numerical optimization shows that this refined key mapping would only improve the key-rate performances marginally. It increases the key rate at 0 km of the ideal 2-photon protocol from 0.1261 bit/channel to 0.1314 bit/channel and that of the ideal 4-photon protocol from 0.3131 bit/channel to 0.3242 bit/channel, with almost no increase to the maximal transmission distance. This is due to the low gain of the newly-accepted region such as point A in Fig. 5a. Considering the experimental cost as well, we thus suggest that using the simple threshold key mapping as in Sec. II is good enough in practice.

VII. CONCLUSION AND OUTLOOK

In summary, we present the time-bin-encoding CV QKD protocol with a phase-error-based security analysis. Similar to the ideas in DV protocols [31] and other CV protocols [5], we introduce a squashing channel to “squash” the original privacy-estimation problem on two optical modes to a single qubit, enabling the definition of phase-error rate. The phase randomization on both the source and detector enables the introduction of the photon-number-tagging method, identifying the central components for key generation. Combined with the decoy-state estimation, the parameter estimation is made simple and efficient. We expect our methods of constructing squashing models and applying phase randomization can be applied to many other CV protocols.

One of our major observations is that coherent detectors can be used to estimate the privacy of multi-photon signals. This is also pointed out in Ref. [24]. Such detectors may also be helpful to the DV protocols. In fact, we may consider a hybrid protocol: single-photon detectors for key generation and homodyne detectors for parameter estimation. The multi-photon components in this protocol can contribute to key generation compared with the single-photon BB84 protocol.

We provide a general framework for the finite-size analysis of this CV protocol based on martingale theory. The photon-number tagging method greatly simplifies the finite-size analysis. A direct follow-up of this work is to complete the finite-size analysis, encompassing the effects on the distillable key rate, the decoy-method accuracy, and the deviation of the homodyne tomography. In the literature, variants of Azuma’s inequality have been applied for faster convergence of parameter estimation in



(a)

(b)

FIG. 5: The simple and the maximum-likelihood-based key mapping. The two axes represent the two homodyne measurement results (q_1, q_2). The yellow region is decoded as 0 and the blue decoded as 1. The grey region is discarded. **(a)** The simple key mapping scheme used throughout this paper, being rectangular. Point A has key mapping error 0.02% and point B 50%, yet point A is discarded whilst B is accepted. **(b)** The maximum-likelihood key mapping scheme, being approximately triangular. The post-selection is done for coherent light amplitude $\alpha = 1$, where only the region with likelihood ratio greater than 10 is kept in this showcase. In this refined key mapping, point A is accepted and point B is discarded.

quantum key distribution [58, 59], such as Kato's inequality [60]. One can bring such techniques to the protocol in this work for better practicality.

It is tempting to further enhance the key rate and the maximal distance of this protocol. We may consider the high-dimensional time-bin encoding, which is relatively easy to implement experimentally [61–63]. The high-dimensional complementarity security analysis [64] can be invoked, and the squashing channel should map the optical modes to a qudit. We can also apply the trusted-noise model to alleviate the effect of the detector noise [65, 66]. The model requires the modification of the detector POVM, which is still block-diagonal on the Fock basis [24]. One may also consider using squeezed states as the light source to reduce the shot noise in one quadrature and use the other only for parameter estimation. This may tackle the large bit error rate due to the shot noise, the issue that renders the 0-km performance of our protocol not as good as the usual CV QKD scheme. We can also examine the variations of our protocol based on the combination with new DV QKD schemes such as the measurement-device-independent-type schemes [67, 68] and their extensions, including the twin-field-type [69–71] and the mode-pairing schemes [72, 73].

ACKNOWLEDGMENTS

We acknowledge insightful discussions with Hoi-Kwong Lo and Xiongfeng Ma. A.J. and R.V.P. acknowledge support from the UK EPSRC Quantum Communications Hub, project EP/T001011/1. A.J. acknowledges funding from Cambridge Trust. X. Z. acknowledges support from the National Natural Science Foundation of China Grant No. 11975222, Grant No. 12174216, and the Innovation Program for Quantum Science and Technology Grant No. 2021ZD0300804. P. Z. and L. J. acknowledge support from the ARO(W911NF-23-1-0077), ARO MURI (W911NF-21-1-0325), AFOSR MURI (FA9550-19-1-0399, FA9550-21-1-0209), NSF (OMA-1936118, ERC-1941583, OMA-2137642), NTT Research, Packard Foundation (2020-71479), and the Marshall and Arlene Bennett Family Research Program.

A. J. and X. Z. contributed equally to this work.

Appendix A: Phase-error calculation details

We give the detailed derivation of the phase-error probability expressions Eq. (21) to (27) for the zero, one and two-photon components. According to Eq. (20), the calculation involves in expanding the X-basis measurement operator $M_\pm$ based on Eq. (9). For the single-photon subspace, we have

$$\begin{aligned}\hat{P}_1\left(\int_0^{2\pi}\frac{d\varphi}{2\pi}\left|q_1(\varphi)\right\rangle\left\langle q_1(\varphi)\right|\otimes\left|q_2(\varphi)\right\rangle\left\langle q_2(\varphi)\right|\right)\hat{P}_1 &= \psi_0^2(q_1)\psi_1^2(q_2)\left|01\right\rangle\left\langle 01\right| + \psi_1^2(q_1)\psi_0^2(q_2)\left|10\right\rangle\left\langle 10\right| + \\ &\psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|01\right\rangle\left\langle 10\right| + \psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|10\right\rangle\left\langle 01\right|\end{aligned} \tag{A1}$$

$$\begin{aligned}\hat{P}_1\left(\int_0^{2\pi}\frac{d\varphi}{2\pi}\left|q_2(\varphi)\right\rangle\left\langle q_2(\varphi)\right|\otimes\left|q_1(\varphi)\right\rangle\left\langle q_1(\varphi)\right|\right)\hat{P}_1 &= \psi_1^2(q_1)\psi_0^2(q_2)\left|01\right\rangle\left\langle 01\right| + \psi_0^2(q_1)\psi_1^2(q_2)\left|10\right\rangle\left\langle 10\right| + \\ &\psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|01\right\rangle\left\langle 10\right| + \psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|10\right\rangle\left\langle 01\right|\end{aligned} \tag{A2}$$

$$\begin{aligned}\hat{P}_1\left(\int_0^{2\pi}\frac{d\varphi}{2\pi}\left|q_1(\varphi)\right\rangle\left\langle q_2(\varphi)\right|\otimes\left|q_2(\varphi)\right\rangle\left\langle q_1(\varphi)\right|\right)\hat{P}_1 &= \psi_0^2(q_1)\psi_1^2(q_2)\left|01\right\rangle\left\langle 10\right| + \psi_1^2(q_1)\psi_0^2(q_2)\left|10\right\rangle\left\langle 01\right| + \\ &\psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|01\right\rangle\left\langle 01\right| + \psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|10\right\rangle\left\langle 10\right|\end{aligned} \tag{A3}$$

$$\begin{aligned}\hat{P}_1\left(\int_0^{2\pi}\frac{d\varphi}{2\pi}\left|q_1(\varphi)\right\rangle\left\langle q_2(\varphi)\right|\otimes\left|q_2(\varphi)\right\rangle\left\langle q_1(\varphi)\right|\right)\hat{P}_1 &= \psi_1^2(q_1)\psi_0^2(q_2)\left|01\right\rangle\left\langle 10\right| + \psi_0^2(q_1)\psi_1^2(q_2)\left|10\right\rangle\left\langle 01\right| + \\ &\psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|01\right\rangle\left\langle 01\right| + \psi_0(q_1)\psi_0(q_2)\psi_1(q_1)\psi_1(q_2)\left|10\right\rangle\left\langle 10\right|\end{aligned} \tag{A4}$$

Hence the single-photon phase-error operator is given by

$$\begin{aligned}\hat{P}_1\hat{M}_\pm\hat{P}_1 &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_1(q_2)\pm\psi_0(q_2)\psi_1(q_1)]^2 \quad \frac{1}{2}(\left|01\right\rangle\pm\left|10\right\rangle)(\left\langle 01\right|\pm\left\langle 10\right|) \\ &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0^2(q_1)\psi_1^2(q_2)+\psi_1^2(q_1)\psi_0^2(q_2)] \quad \frac{1}{2}(\left|01\right\rangle\pm\left|10\right\rangle)(\left\langle 01\right|\pm\left\langle 10\right|),\end{aligned} \tag{A5}$$

Note that the second equality is deduced as the cross terms are odd functions with respect to q_1 and q_2, and the key-mapping region is symmetrical. This gives Eq. (21). The gain $Q_{1,1}$ involves in measuring $\hat{P}_1(\hat{M}_+ + \hat{M}_-)\hat{P}_1$ which is clearly in the form of Eq. (23).

The two-photon case involves in more terms, but we can make use of the symmetry of the key mapping region $\mathbf{R_0}$ to eliminate the odd terms. The calculation goes by:

$$\begin{aligned}\hat{P}_2\left(\int_0^{2\pi}\frac{d\varphi}{2\pi}\left|q_1(\varphi)\right\rangle\left\langle q_1(\varphi)\right|\otimes\left|q_2(\varphi)\right\rangle\left\langle q_2(\varphi)\right|\right)\hat{P}_2 &= \psi_0^2(q_1)\psi_2^2(q_2)\left|02\right\rangle\left\langle 02\right| + \psi_0(q_1)\psi_0(q_2)\psi_2(q_1)\psi_2(q_2)\left|02\right\rangle\left\langle 20\right| \\ + \psi_0(q_1)\psi_0(q_2)\psi_2(q_1)\psi_2(q_2)\left|20\right\rangle\left\langle 02\right| &+ \psi_0^2(q_2)\psi_2^2(q_1)\left|20\right\rangle\left\langle 20\right| + \psi_1^2(q_1)\psi_1^2(q_2)\left|11\right\rangle\left\langle 11\right| + \text{ odd terms}\end{aligned} \tag{A6}$$

The X-basis measurement is thus given by:

$$\begin{aligned}\hat{P}_2\hat{M}_+\hat{P}_2 &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_2(q_2)+\psi_2(q_1)\psi_0(q_2)]^2 \quad \frac{1}{2}(\left|02\right\rangle+\left|20\right\rangle)(\left\langle 02\right|+\left\langle 20\right|) \\ &+ \int_{\mathbf{R_0}} dq_1dq_2 2\psi_1^2(q_1)\psi_1^2(q_2)\left|11\right\rangle\left\langle 11\right|\end{aligned} \tag{A7}$$

$$\hat{P}_2\hat{M}_-\hat{P}_2 = \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_2(q_2)-\psi_2(q_1)\psi_0(q_2)]^2 \quad \frac{1}{2}(\left|02\right\rangle-\left|20\right\rangle)(\left\langle 02\right|-\left\langle 20\right|) \tag{A8}$$

This recovers Eq. (24), and adding the two equations together gives the expression for the gain $Q_{2,2}$ as in Eq. (26). Expanding the vacuum subspace according to Eq. (9) gives the coefficients as in Eq. (27).

Appendix B: Parameter estimation

In this section, we show how to estimate the quantities in the key-rate formula with realistic devices. We first state parameter estimation in terms of probabilities in a single round, and one can interpret the results as obtained from sufficiently many rounds under a collective attack. In the next section, we will generalize the results to the finite-size regime under a coherent attack. For convenience, we first review the terms to be estimated in the virtual protocol that utilizes up to the two-photon component, as given in Sec. III C. As a reminder, note that we distinguish the terms "receiving" and "accepting."

1. $Q_{*,0}$: The probability of accepting a vacuum state, given by Eq. (27).
2. $Q_{1,1}$: The probability of sending $|\Psi_1\rangle_{A'A_1A_2}$ and accepting a single-photon state, given by Eq. (23).
3. $Q_{2,2}$: The probability of sending $|\Psi_2\rangle_{A'A_1A_2}$ and accepting a two-photon state, given by Eq. (26).
4. $e^X_{1,1}$: the phase-error probability when sending a single-photon state and accepting a single-photon state, determined by the probabilities of sending $(|01\rangle \pm |10\rangle)/\sqrt{2}$ and accepting $(|01\rangle \mp |10\rangle)/\sqrt{2}$, given by Eq. (21).
5. $e^X_{2,2}$: the phase-error probability when sending a two-photon state and accepting a two-photon state, determined by the probabilities of sending $(|02\rangle \pm |20\rangle)/\sqrt{2}$ and accepting $(|02\rangle \mp |20\rangle)/\sqrt{2}$ and sending $(|02\rangle - |20\rangle)/\sqrt{2}$ and accepting $|11\rangle$, given by Eq. (24).

1. Homodyne tomography

The first issue we need to tackle is the estimation of photon-number statistics. Due to the lack of photon-number-resolving detectors, these operators are not directly measurable. Nevertheless, we can apply homodyne tomography and obtain unbiased estimation [34–39]. For a systematic review, we recommend the tutorial textbook of Ref. [32].

We start with a single-mode system. Consider the displacement operators given by

$$\begin{aligned}\hat{D}(\alpha) =& \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})\\ =& \exp\left[(-ik)\left(\hat{a}^\dagger e^{i\varphi} + \hat{a}e^{-i\varphi}\right)\right]\\ :=& \exp(-ik\hat{Q}_\varphi),\end{aligned} \tag{B1}$$

where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators of the mode, respectively, α is a complex scalar, and α^* denotes the complex conjugate of α. In the second equation, we use the polar variables to represent α, $\alpha = -ike^{i\varphi}$. We call $\hat{Q}_\varphi$ the quadrature operator. Measuring $\hat{Q}_\varphi$ corresponds to the homodyne measurement, where the phase of the LO is φ. By definition, $\hat{D}(\alpha)$ is a Hermitian operator. The set of all displacement operators forms an orthogonal and complete function basis on a mode; hence any linear operator on a mode, $\hat{O}$, can be expanded with displacement operators,

$$\hat{O} = \int_0^\pi \frac{d\varphi}{\pi}\int_{-\infty}^\infty \frac{dk|k|}{4}\mathrm{Tr}(\hat{O}e^{ik\hat{Q}_\varphi})e^{-ik\hat{Q}_\varphi}. \tag{B2}$$

When measuring $\hat{O}$ on a state, $\hat{\rho}$, the expected value is given by

$$\begin{aligned}\langle\hat{O}\rangle =& \mathrm{Tr}(\hat{O}\hat{\rho})\\ =& \int_0^\pi \frac{d\varphi}{\pi}\int_{-\infty}^\infty \frac{dk|k|}{4}\mathrm{Tr}(\hat{O}e^{ik\hat{Q}_\varphi})\mathrm{Tr}(\hat{O}e^{-ik\hat{Q}_\varphi})\\ :=& \int_0^\pi \frac{d\varphi}{\pi}\int_{-\infty}^\infty dq\mathrm{Tr}[\hat{O}K(\hat{Q}_\varphi - q)]p(q|\varphi)\\ :=& \int_0^\pi \frac{d\varphi}{\pi}\int_{-\infty}^\infty dq\mathcal{R}[\hat{O}](q,\varphi)p(q|\varphi),\end{aligned} \tag{B3}$$

where the value of the term

$$K(q) := \int_{-\infty}^\infty \frac{dk}{4}|k|e^{ikq} \tag{B4}$$

should be determined by the Cauchy principal value, $p(q|\varphi)$ is the conditional probability of obtaining quadrature q when the phase of the homodyne measurement is φ, and $\mathcal{R}[\hat{O}](q,\varphi)$ is the kernel function of $\hat{O}$ with respect to the homodyne measurement. Eq. (B3) gives a sampling procedure to estimate $\langle\hat{O}\rangle$ for a general unknown system using homodyne measurements [36, 37, 39]. Namely,

1. Repeat the following process for N times:
   (a) Choose the LO phase of the homodyne measurement, $\varphi_i \in [0,\pi]$, uniformly at random.
   (b) Measure the system and record the result, q_i.
2. Calculate the average value of the kernel function with respect to the observed statistics, $\sum_{i=1}^{N}\mathcal{R}[\hat{O}](q_i,\varphi_i)/N$.

When the kernel function is bounded, the law of large numbers guarantees the convergence,

$$\langle\hat{O}\rangle = \lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}\mathcal{R}[\hat{O}](q_i,\varphi_i). \tag{B5}$$

Note that, when $\hat{O}$ is an Hermitian operator or we know that $\mathrm{Im}\left(\langle\hat{O}\rangle\right)=0$, we have

$$\begin{aligned}\langle\hat{O}\rangle &= \mathrm{Re}\left(\langle\hat{O}\rangle\right)\\ &= \int_0^{\pi}\frac{d\varphi}{\pi}\int_{-\infty}^{\infty}dq\,\mathrm{Re}\left(\mathcal{R}[\hat{O}](q,\varphi)\right)p(q|\varphi).\end{aligned} \tag{B6}$$

That is, we can redefine the estimator to be the real part of $\mathcal{R}[\hat{O}](q,\varphi)$, which is still unbiased.

In our protocol, we are interested in the photon-number operators, $|n\rangle\langle n+d|$, where $|n\rangle$ is the eigenstate of the n-photon eigenstate. For a single mode, the estimator of this operator is given by

$$\mathcal{R}_\eta[|n\rangle\langle n+d|](q,\varphi) = e^{id(\varphi+\frac{\pi}{2})}\sqrt{\frac{n!}{(n+d)!}}\int_{-\infty}^{\infty}dk|k|\exp\left(\frac{1-2\eta}{2\eta}k^2-ikq\right)k^d L_n^d(k^2), \tag{B7}$$

where η is the detector efficiency, and L_n^d is the generalized Laguerre polynomial [36, 37, 74]. The kernel function is bounded when $\eta > 1/2$, allowing for a converging tomography result by increasing samples [37, 39].homodyne tomography can be generalized to estimate the statistics of a multiple-mode observable. In our case, one needs to estimate separable observables on two modes, $\hat{O}_1\otimes\hat{O}_2$, where we specify the modes with subscripts. One can apply independent homodyne measurements to each mode for the estimation. Notably, as $\hat{D}(\alpha_1)\otimes\hat{D}(\alpha_2)$ forms a complete basis on the joint system, then

$$\hat{O}_1\otimes\hat{O}_2 = \int_0^{\pi}\frac{d\varphi_1}{\pi}\int_{-\infty}^{\infty}\frac{dk_1|k_1|}{4}\mathrm{Tr}(\hat{O}_1e^{ik_1\hat{Q}_{\varphi_1}})\int_0^{\pi}\frac{d\varphi_2}{\pi}\int_{-\infty}^{\infty}\frac{dk_2|k_2|}{4}\mathrm{Tr}(\hat{O}_2e^{ik_2\hat{Q}_{\varphi_2}})(e^{-ik_1\hat{Q}_{\varphi_1}}\otimes e^{-ik_2\hat{Q}_{\varphi_2}}). \tag{B8}$$

Consequently,

$$\begin{aligned}\langle\hat{O}_1\otimes\hat{O}_2\rangle &= \mathrm{Tr}[(\hat{O}_1\otimes\hat{O}_2)\hat{\rho}]\\ &= \int_0^{\pi}\frac{d\varphi_1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^{\pi}\frac{d\varphi_2}{\pi}\int_{-\infty}^{\infty}dq_2\mathcal{R}[\hat{O}_1](q_1,\varphi_1)\mathcal{R}[\hat{O}_2](q_2,\varphi_2)p(q_1,q_2|\varphi_1,\varphi_2).\end{aligned} \tag{B9}$$

As a remark, note that the quantum state of the two modes, $\hat{\rho}$, can generally be entangled. In the experiment, the users simply need two independently phase-randomized homodyne detectors and record the joint conditional probability distribution of quadratures (q_1,q_2) given the LO phases (φ_1,φ_2).

In practical homodyne measurements, due to the usage of analog-to-digital converters (ADC), the measured quadrature value q will be discrete with a finite resolution Δ. In the former CV QKD protocols like Ref. [24], the parameter estimation is done by linear programming [75] instead of optical homodyne tomography; as a result, the finite resolution Δ will not affect the estimation accuracy as long as Δ is small.

To characterize how the finite resolution Δ will disturb the parameter estimation by optical homodyne tomography, we numerically estimate the bias caused by Δ. We estimate the expectation values of the (non-Hermitian) observables $\hat{O}_{01} := |0\rangle\langle 1|$ and $\hat{O}_{02} := |0\rangle\langle 2|$ with a coherent state $|\sqrt{\mu}\rangle$ input ($\mu = 0.5$). We choose $\hat{O}_{01}$ and $\hat{O}_{02}$ since they are directly related to the phase error operator in Proposition 1.

When the homodyne detection results is quantized with the bin width Δ, if we use the observable estimator $\mathcal{R}_\eta[|n\rangle\langle n+d|](q,\phi)$ given by Eq. (B7), the expectation value becomes

$$\mathbb{E}\left(\mathcal{R}[\hat{O}](q,\phi)\right) = \int_0^\pi \frac{d\phi}{\pi} \sum_{t=-\infty}^{\infty} \Pr(q = t\Delta|\phi)\, \mathcal{R}[\hat{O}](q = t\Delta, \phi), \tag{B10}$$

where

$$\Pr(q = t\Delta|\phi) = \int_{t\Delta}^{(t+1)\Delta} p(q|\phi), \tag{B11}$$

is the quantized version of the probabilistic distribution of the homodyne detection result q. The finite-bin effect is then characterized by the estimation bias $\left|\mathbb{E}\left(\mathcal{R}[\hat{O}](q,\phi)\right) - \hat{O}\right|$.

We plot the estimator bias of $\hat{O}_{01}$ and $\hat{O}_{02}$ with respect to the bin width Δ in Fig. 6. We see that the bias is almost proportional to Δ^2, i.e., it decays rapidly if we reduce the bin width Δ. With a width $\Delta = 0.01$ shot noise unit which is easily achievable in the experiment, the bias of $\hat{O}_{01}$ and $\hat{O}_{02}$ are smaller than 10^{-5}. As a result, the estimation bias is negligible with practical homodyne measurement devices.

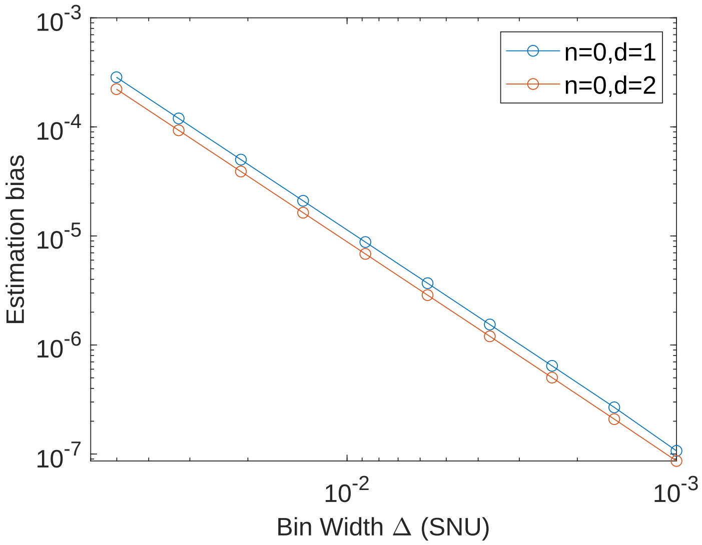


FIG. 6: Estimation bias of the observable $|n\rangle\langle n+d|$ with respect to the homodyne bin width Δ. The input state is a coherent state $|\sqrt{\mu}\rangle$ with $\mu = 0.5$. The detection efficiency $\eta_{det} = 1$.

2. Parameter estimation procedures

Now we present the parameter estimation procedures based on the homodyne tomography and extended decoy methods. In the experiment, given that they choose certain bases and light intensity, the users can collect data and evaluate the conditional probabilities for taking $(\varphi_b^1, \varphi_b^2) = \vec{\varphi}_b$ and observing $(q_1, q_2) = \vec{q}$ in the homodyne measurements, or the yields. For simplicity, we use notations of $Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}$ and $Y^\varphi_{\mu_a,(\vec{\varphi}_b,\vec{q})}$. In the subscript, μ_a denotes the light intensity, and $(\vec{\varphi}_b, \vec{q})$ denotes the homodyne measurement results of Bob. When the superscript writes Z, it denotes that Alice chooses the Z-basis; when the superscript writes φ, it denotes that Alice chooses the X-basis and $\varphi_a^2 - \varphi_a^1 = \varphi$. Via homodyne tomography, these values can be used to estimate $Y^Z_{\mu_a,\hat{O}}$ and $Y^\varphi_{\mu_a,\hat{O}}$, namely, the expected value of measuring observable $\hat{O}$ conditioned on the corresponding input settings. Following Eq. (B3), the yields are given by

$$\begin{aligned} Y^Z_{\mu_a,\hat{O}} &= \int_0^\pi d\varphi_b^1 \int_0^\pi d\varphi_b^2 \int_{-\infty}^{\infty} dq_1 \int_{-\infty}^{\infty} dq_2 \mathcal{R}[\hat{O}](\vec{q}, \vec{\varphi}_b) Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}, \\ Y^\varphi_{\mu_a,\hat{O}} &= \int_0^\pi d\varphi_b^1 \int_0^\pi d\varphi_b^2 \int_{-\infty}^{\infty} dq_1 \int_{-\infty}^{\infty} dq_2 \mathcal{R}[\hat{O}](\vec{q}, \vec{\varphi}_b) Y^\varphi_{\mu_a,(\vec{\varphi}_b,\vec{q})}. \end{aligned} \tag{B12}$$

In the second step, we apply the extended decoy state methods to estimate the gains and phase-error probabilities in Eq. (12), the key-rate formula. With finite decoy states, the users can obtain upper and lower bounds on these quantities [28]. We take the estimation of $e^X_{2,2}$ for example, which is the most complicated task for a two-photon protocol. According to Eq. (24) we have

$$\frac{Q_{2,2}e^X_{2,2}}{\Pr(2)} = \frac{1}{2}c_2^- Y_{|\Psi_2^+\rangle,|\Psi_2^-\rangle} + \frac{1}{2}c_2^+ Y_{|\Psi_2^-\rangle,|\Psi_2^+\rangle} + c_2^{11} Y_{|\Psi_2^-\rangle,|11\rangle}. \tag{B13}$$

We then invoke the extended decoy method. To upper-bound $Y_{|\Psi_2^+\rangle,|\Psi_2^-\rangle}$, i.e. the probability of transmitting $|\Psi_2^+\rangle$ whilst receiving $|\Psi_2^-\rangle$, we have according to Eq. (34)

$$Y_{|\Psi_2^+\rangle,|\Psi_2^-\rangle} \leq Y^{Z,U}_{m=2,|\Psi_2^-\rangle} + \frac{1}{2}Y^{\varphi=0,U}_{m=2,|\Psi_2^-\rangle} + \frac{1}{2}Y^{\varphi=\pi,U}_{m=2,|\Psi_2^-\rangle} - \frac{1}{2}Y^{\varphi=\frac{\pi}{2},L}_{m=2,|\Psi_2^-\rangle} - \frac{1}{2}Y^{\varphi=\frac{3\pi}{2},L}_{m=2,|\Psi_2^-\rangle}, \tag{B14}$$

where $Y^{\varphi,U(L)}_{m=2,|\Psi_2^-\rangle}$ denotes the upper(lower) bound of the two-photon subspace contribution of $Y^{\varphi}_{\mu,|\Psi_2^-\rangle}$, i.e. the probability of transmitting ρ^φ_μ whilst receiving $|\Psi_2^-\rangle$. This is found by the following standard linear programming for decoy analysis:

$$\begin{aligned} &\text{max.(min.) } Y^{\varphi}_{m=2,|\Psi_2^-\rangle} \\ &\text{s.t. } \sum_{m=0}^{N_c} e^{-\mu_a}\frac{\mu_a^m}{m!}Y^{\varphi}_{m,|\Psi_2^-\rangle} = Y^{\varphi}_{\mu_a,|\Psi_2^-\rangle}, \\ &\mu_a \in \{\mu, \nu_1, \nu_2, 0\}. \end{aligned} \tag{B15}$$

Note that N_c is a cut-off photon number chosen to be 10 in this work.

We list the estimation procedures and the involved quantities in Table VI. Note that the original data can be re-used to estimate various quantities in homodyne tomography by varying the kernel function with respect to the observable under consideration.

TABLE VI: Parameter estimation with homodyne tomography and decoy states. In our work, the light intensity is chosen from the set $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$. For simplicity, we denote the photon-number operator, $|n_1 n_2\rangle\langle n_1 n_2|$, as $|n_1 n_2\rangle$ in the subscripts of the yields, and similarly for $|\Psi_n^\pm\rangle$. We denote the lower and upper bounds with additional superscripts of L and U, respectively. Note that one can directly estimate $Q_{*,0}$ in the rounds of $\mu_a = \mu$. The estimation of $e^X_{2,2}$ involves statistics in the rounds that Alice chooses the Z-basis and X-basis with $\varphi = k\pi/2$.

Original data	Estimation via homodyne tomography	Final estimation with decoy states
	$Y^Z_{\mu,\lvert 00\rangle}$	$Q_{*,0}$
$Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}$	$Y^Z_{\mu_a,\lvert 01\rangle}, Y^Z_{\mu_a,\lvert 10\rangle}$	$Q^L_{1,1}, Q^U_{1,1}$
	$Y^Z_{\mu_a,\lvert 02\rangle}, Y^Z_{\mu_a,\lvert 20\rangle}, Y^Z_{\mu_a,\lvert 11\rangle}$	$Q^L_{2,2}, Q^U_{2,2}$
$Y^\varphi_{\mu_a,(\vec{\varphi}_b,\vec{q})}$	$Y^{\varphi=\pi}_{\mu_a,\lvert\Psi_1^+\rangle}, Y^{\varphi=0}_{\mu_a,\lvert\Psi_1^+\rangle}, Y^{\varphi=\pi}_{\mu_a,\lvert\Psi_1^-\rangle}, Y^{\varphi=0}_{\mu_a,\lvert\Psi_1^-\rangle}$	$e^{X,L}_{1,1}, e^{X,U}_{1,1}$
	$Y^{\varphi=k\pi/2}_{\mu_a,\lvert\Psi_2^+\rangle}, Y^{\varphi=k\pi/2}_{\mu_a,\lvert\Psi_2^-\rangle}, Y^{\varphi=k\pi/2}_{\mu_a,\lvert 11\rangle}$	$e^{X,L}_{2,2}, e^{X,U}_{2,2}$
$Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}$	$Y^Z_{\mu_a,\lvert\Psi_2^+\rangle}, Y^Z_{\mu_a,\lvert\Psi_2^-\rangle}, Y^Z_{\mu_a,\lvert 11\rangle}$	

Appendix C: Martingale-based analysis against coherent attacks

To tackle the most general attack, namely, a coherent attack, we apply a martingale-based approach. We first review the basics of martingale theory.

Definition 1 (Martingale)**.** *Consider a probability space, $(\Omega, \mathcal{F}, P)$, where Ω is the sample space, $\mathcal{F}$ is the event space, and P is the probability measure, and a filtration $\mathbb{F} = \{\mathcal{F}_i\}_{i\in\mathbb{N}}, \mathcal{F}_i \subseteq \mathcal{F}_j \subseteq \mathcal{F}, \forall i \leq j$. A sequence of random variables, $X_0, X_1, \cdots$, such that $\forall i, X_i$ is $\mathcal{F}_i$-measurable, is called a martingale with respect to filtration $\mathbb{F}$ if $\forall i$,*

$$\begin{aligned} \mathbb{E}(|X_i|) &< \infty, \\ \mathbb{E}(X_{i+1}|\mathcal{F}_i) &= X_i. \end{aligned} \tag{C1}$$

For a martingale, the summation of its composed random variables converges to the expected value in probability, as shown by Azuma's inequality [50] and its variants.

Theorem 3 (Azuma's inequality [50])**.** *Given a probability space, $(\Omega, \mathcal{F}, P)$, and a filtration, $\mathbb{F} = \{\mathcal{F}_i\}_{i\in\mathbb{N}}$, suppose $\mathbb{X} = \{X_i\}_{i\in\mathbb{N}}$ is a real-valued martingale bounded by two sets of predictable processes with respect to $\mathbb{F}$, $\mathbb{A} = \{A_i\}_{i\in\mathbb{N}}$ and $\mathbb{B} = \{B_i\}_{i\in\mathbb{N}}$, such that*

$$\begin{aligned} A_i \leq X_i - X_{i-1} \leq B_i, \\ B_i - A_i \leq c_i, \end{aligned} \tag{C2}$$

where $c_i \in [0, \infty)$ are constants. Then $\forall \delta > 0$ and $\forall n \in \mathbb{N}^+$,

$$\begin{aligned} \Pr(X_n - X_0 \geq \delta) \leq \exp\left(-\frac{2\delta^2}{\sum_{i=1}^n c_i^2}\right), \\ \Pr(X_n - X_0 \leq -\delta) \leq \exp\left(-\frac{2\delta^2}{\sum_{i=1}^n c_i^2}\right). \end{aligned} \tag{C3}$$

By applying the union bound, we have the inequality

$$\Pr(|X_n - X_0| \geq \delta) \leq 2\exp\left(-\frac{2\delta^2}{\sum_{i=1}^n c_i^2}\right). \tag{C4}$$

In our discussion, we also encounter martingales that may take complex values. We can apply Azuma's inequality for real-valued variables to the real and imaginary parts separately and bound the absolute values of the martingale variables. In this work, we apply a result from Ref. [76].

Theorem 4. *Given a probability space, $(\Omega, \mathcal{F}, P)$, and a filtration, $\mathbb{F} = \{\mathcal{F}_i\}_{i\in\mathbb{N}}$, suppose $\mathbb{X} = \{X_i\}_{i\in\mathbb{N}}$ is a complex-valued martingale with a bounded difference, such that*

$$\begin{aligned} X_0 = 0, \\ |X_i - X_{i-1}| \leq c_i, \end{aligned} \tag{C5}$$

where $c_i \in [0, \infty)$ are constants. Then $\forall \delta > 0$ and $\forall n \in \mathbb{N}^+$,

$$\Pr(|X_n| \geq \delta) \leq 2e^2 \exp\left(-\frac{2\delta^2}{\sum_{i=1}^n c_i^2}\right). \tag{C6}$$

1. Estimation of $Q_{1,1}$

In this section, we present a thorough analysis on the estimation of $Q_{1,1}$, showing how to apply the martingale analysis to obtain a non-i.i.d. estimation result that holds against coherent attacks. Note that in the finite-data-size analysis under a coherent attack, $Q_{1,1}$ should be understood as a frequency, and $N_\mu^{zz} Q_{1,1}$ is the number of key generation rounds in the virtual experiment where Alice sends a single-photon state and Bob accepts a single-photon state. Here, we denote the number of key generation rounds as N_μ^{zz} in accordance with the basis choise and light intensity. In particular, the statistics over the rounds can be correlated. Consider the following random variable in the i'th round,

$$\zeta_{\{\mu,(1,1)\}}^{(i)} = \begin{cases} 1, \text{ if } \mu_a^{(i)} = \mu \wedge ZZ \wedge n^{(i)} = 1 \wedge m^{(i)} = 1 \wedge (q_1^{(i)}, q_2^{(i)}) \in \mathbf{R_0} \cup \mathbf{R_1} , \\ 0, \text{ otherwise.} \end{cases} \tag{C7}$$

where we write ZZ to denote the bases choices, with the former denoting Alice's choice and the latter denoting Bob's, and specify the round number in the superscript, (i). We call $\zeta_{\{\mu,(1,1)\}}^{(i)}$ a counter variable, which adds one in the virtual experiment when the light intensity is μ, both Alice and Bob choose the Z-basis, Alice sends a single-photon state, and Bob receives a single-photon state and accepts the signal in the post-selection. Note that $\zeta_{\{\mu,(1,1)\}}^{(i)}$ embeds randomness from both the experimental setting and measurement outcomes. We have

$$\sum_{i=1}^{N} \zeta_{\{\mu,(1,1)\}}^{(i)} = N_\mu^{zz} Q_{1,1}, \tag{C8}$$

and conditioned on the history before the i'th round, $\mathcal{F}_{i-1}$, the expected value of $\zeta^{(i)}_{\{\mu,(1,1)\}}$ is given by

$$\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right] = p_\mu p_{zz} c_1 \mathrm{Pr}_\mu(1)\mathrm{Tr}\left\{\mathcal{N}_E\left[\mathrm{Tr}_{A'}(|\Psi_1\rangle_{A'A_1A_2}\langle\Psi_1|)\right](|01\rangle_{B_1B_2}\langle 01| + |10\rangle_{B_1B_2}\langle 10|)\right\}, \tag{C9}$$

where p_μ is the probability that the light intensity is μ, p_{zz} is the probability that both users choose the Z-basis, and c_1 relates to the accepting probability, as given in Eq. (22). The quantum channel controlled by Eve, $\mathcal{N}_E$, may introduce correlated statistics among rounds that are not independent and identically distributed. Then, the following random variables form a martingale,

$$\Delta^{(t)}_{\{\mu,(1,1)\}} = \begin{cases} 0, & \text{if } t=0, \\ \sum_{i=1}^{t}\left\{\zeta^{(i)}_{\{\mu,(1,1)\}} - \mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right]\right\}, & \text{if } t=1,\cdots,N, \end{cases} \tag{C10}$$

where N is the total number of rounds in the experiment. In addition, the martingale has a bounded difference,

$$-\mathbb{E}\left[\zeta^{(t)}_{\{\mu,(1,1)\}}|\mathcal{F}_{t-1}\right] \leq \Delta^{(t)}_{\{\mu,(1,1)\}} - \Delta^{(t-1)}_{\{\mu,(1,1)\}} \leq 1 - \mathbb{E}\left[\zeta^{(t)}_{\{\mu,(1,1)\}}|\mathcal{F}_{t-1}\right]. \tag{C11}$$

We denote $c_{\mu,(1,1)} := 1$. In a virtual experiment where Alice and Bob perform the photon-number measurements, the value of $\Delta^{(N)}_{\{\mu,(1,1)\}}$ can be bounded on both sides by applying Azuma's inequality; hence the value of $\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,(1,1)\}}$ can be bounded with respect to the expected values in Eq. (C9). Given the estimation failure probability

$$\varepsilon_{\{\mu,(1,1)\}} = \exp\left[-\frac{2{\delta_{\{\mu,(1,1)\}}}^2}{N{c_{\{\mu,(1,1)\}}}^2}\right] = \exp\left[-\frac{2{\delta_{\{\mu,(1,1)\}}}^2}{N}\right], \tag{C12}$$

we have

$$\begin{aligned} \mathrm{Pr}\left\{\Delta^{(N)}_{\{\mu,(1,1)\}} - \Delta^{(0)}_{\{\mu,(1,1)\}} \geq \delta_{\{\mu,(1,1)\}}\right\} &= \mathrm{Pr}\left\{\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,(1,1)\}} - \sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}] \geq \delta_{\{\mu,(1,1)\}}\right\} \leq \varepsilon_{\{\mu,(1,1)\}}, \\ \mathrm{Pr}\left\{\Delta^{(N)}_{\{\mu,(1,1)\}} - \Delta^{(0)}_{\{\mu,(1,1)\}} \leq -\delta_{\{\mu,(1,1)\}}\right\} &= \mathrm{Pr}\left\{\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,(1,1)\}} - \sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}] \leq -\delta_{\{\mu,(1,1)\}}\right\} \leq \varepsilon_{\{\mu,(1,1)\}}. \end{aligned} \tag{C13}$$

For brevity, we shall use the big-O notation. Then, except a negligible failure probability, we have the upper and lower bounds on $Q_{1,1}$,

$$\frac{1}{N^{zz}_\mu}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}] - O(\sqrt{-N\ln\varepsilon_{\{\mu,(1,1)\}}})\right\} \leq Q_{1,1} \leq \frac{1}{N^{zz}_\mu}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}] + O(\sqrt{-N\ln\varepsilon_{\{\mu,(1,1)\}}})\right\}. \tag{C14}$$

Notwithstanding, the expected value, $\mathbb{E}[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}]$, is not directly accessible. For this purpose, we link it with the parameter estimation measurement results, which involve the decoy state method and homodyne tomography. By applying the decoy state method, we can effectively lower and upper bound the fraction of single-photon component in the key generation rounds,

$$\begin{aligned} \mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right] &\leq p_\mu p_{zz}\mathrm{Pr}_\mu(1)\left(c_1\sum_{\mu_a} d^U_{\{\mu_a,(1,1)\}}\mathrm{Tr}\left\{\mathcal{N}_E\left[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})\right](|01\rangle_{B_1B_2}\langle 01| + |10\rangle_{B_1B_2}\langle 10|)\right\} + c^U_{Q_{1,1}}\right), \\ \mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right] &\geq p_\mu p_{zz}\mathrm{Pr}_\mu(1)\left(c_1\sum_{\mu_a} d^L_{\{\mu_a,(1,1)\}}\mathrm{Tr}\left\{\mathcal{N}_E\left[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})\right](|01\rangle_{B_1B_2}\langle 01| + |10\rangle_{B_1B_2}\langle 10|)\right\} + c^L_{Q_{1,1}}\right), \end{aligned} \tag{C15}$$

where we specify the upper and lower bounds obtained by the decoy-state method with superscripts U and L, respectively. As discussed in Appendix B 2, by applying a linear programming either analytically or numerically [28], we can derive the optimal coefficients in the decoy-state method for each light intensity μ_a, $d^{U(L)}_{\{\mu_a,(1,1)\}}$. Note that there may be an additional constant term returned by the linear programming, which we denote as $c^{U(L)}_{Q_{1,1}}$. Here, we overload the notation, μ_a, with the meaning of a specific light intensity in $\{\mu,\nu_1,\nu_2,0\}$ and distinguish it from Alice's choice in a round, $\mu_a^{(i)}$. Using the homodyne tomography method,

$$\mathrm{Tr}\left\{\mathcal{N}_E\left[\hat{\rho}^Z_{\mu_a}\right]|n_0n_1\rangle_{B_1B_2}\langle n_0n_1|\right\}=\int_0^\pi\frac{d\varphi_b^1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_b^2}{\pi}\int_{-\infty}^{\infty}dq_2\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0n_1|](\vec{q},\vec{\varphi}_b)p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b),\tag{C16}$$

where $(\vec{q},\vec{\varphi}_b)$ represents the homodyne measurement result, with LO phases $\vec{\varphi}_b=(\varphi_1,\varphi_2)$ and quadratures $\vec{q}=(q_1,q_2)$ on the two modes, and the value of $\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0n_1|](\vec{q},\vec{\varphi}_b)$ comes from the kernel function in homodyne tomography by using homodyne detectors with efficiency η. The expressions of the kernel functions can be obtained through Eq. (B7) and (B9). For the estimation of $Q_{1,1}$, we shall use kernel functions with $|n_0n_1\rangle=|01\rangle$ and $|10\rangle$. To explicitly express the quantum state being measured, namely $\mathcal{N}_E\left[\hat{\rho}^Z_{\mu_a}\right]$, we specify it with sub- and superscripts in the probability distribution $p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b)$. The measurement results are collected in the rounds where the light intensity is chosen as μ_a, Alice chooses the Z-basis, and Bob chooses the X-basis. Combining Eq. (C9), (C15) and (C16), we have

$$\begin{aligned}\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right]\leq&p_\mu p_{zz}\mathrm{Pr}_\mu(1)\Bigg(c_1\sum_{\mu_a}d^U_{\{\mu_a,(1,1)\}}\Bigg\{\int_0^\pi\frac{d\varphi_b^1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_b^2}{\pi}\int_{-\infty}^{\infty}dq_2\mathcal{R}_\eta[|01\rangle\langle 01|](\vec{q},\vec{\varphi}_b)p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b)\\&+\int_0^\pi\frac{d\varphi_b^1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_b^2}{\pi}\int_{-\infty}^{\infty}dq_2\mathcal{R}_\eta[|10\rangle\langle 10|](\vec{q},\vec{\varphi}_b)p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b)\Bigg\}+c^U_{Q_{1,1}}\Bigg),\\\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right]\geq&p_\mu p_{zz}\mathrm{Pr}_\mu(1)\Bigg(c_1\sum_{\mu_a}d^L_{\{\mu_a,(1,1)\}}\Bigg\{\int_0^\pi\frac{d\varphi_b^1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_b^2}{\pi}\int_{-\infty}^{\infty}dq_2\mathcal{R}_\eta[|01\rangle\langle 01|](\vec{q},\vec{\varphi}_b)p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b)\\&+\int_0^\pi\frac{d\varphi_b^1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_b^2}{\pi}\int_{-\infty}^{\infty}dq_2\mathcal{R}_\eta[|10\rangle\langle 10|](\vec{q},\vec{\varphi}_b)p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b)\Bigg\}+c^L_{Q_{1,1}}\Bigg).\end{aligned}\tag{C17}$$

Note that we assess the probability distribution $p^Z_{\mu_a}(\vec{q}|\vec{\varphi}_b)$ also via a finite sample of data. For this purpose, we apply the martingale analysis once more. Consider the following random variables for the i'th round in the experiment,

$$\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}=\begin{cases}\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0n_1|](\vec{q},\vec{\varphi}_b),\text{ if }\mu_a^{(i)}=\mu_a\wedge ZX\wedge(q_1^{(i)},q_2^{(i)})=\vec{q},(\varphi_b^{1(i)},\varphi_b^{2(i)})=\vec{\varphi}_b,\\\qquad\qquad 0,\qquad\qquad\text{otherwise,}\end{cases}\tag{C18}$$

which relate to the parameter estimation measurements when the light intensity is μ_a and Alice chooses the Z-basis. We also call $\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}$ counter variables. According to homodyne tomography, we have

$$\mathbb{E}[\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}|\mathcal{F}_{i-1}]=p_{\mu_a}p_{zx}\mathrm{Tr}\left\{\mathcal{N}_E\left[\mathrm{Tr}_{A'}(|\Psi_1\rangle_{A'A_1A_2}\langle\Psi_1|)\right](|n_0n_1\rangle_{B_1B_2}\langle n_0n_1|)\right\},\tag{C19}$$

and

$$\sum_{i=1}^N\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}=\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0n_1|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}),\tag{C20}$$

where the summation of the right-hand side is taken over the rounds with light intensity μ_a and basis choices of Alice choosing the Z-basis and Bob choosing the X-basis, and $\vec{q}^{(i)},\vec{\varphi}_b^{(i)}$ represent the observed quadrature measurement statistics in the i'th round. While the weighted expectation with respect to the kernel function in Eq. (C16) is a real value, in the experiment, the summation in Eq. (C20) may take a complex value due to the kernel function value. One can simply take the real part of the summation as the estimation result. In the following discussion, we omit this specification for brevity.

Similar to Eq. (C10), the following random variables form a martingale,

$$\Delta^{(t)}_{\{\mu_a,Z,|n_0n_1\rangle\}}=\begin{cases}0,&\text{if }t=0,\\\sum_{i=1}^t\left\{\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}-\mathbb{E}\left[\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}|\mathcal{F}_{i-1}\right]\right\},&\text{if }t=1,\cdots,N.\end{cases}\tag{C21}$$

For $\eta > 1/2$, the above martingale has a bounded difference. One can numerically evaluate the maximum absolute value of $\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0n_1|](\vec{q},\vec{\varphi}_b)$, which we denote as $r_{\{\eta,|n_0n_1\rangle\}}$. Then, the martingale has a bounded difference,

$$|\Delta^{(t)}_{\{\mu_a,Z,|n_0n_1\rangle\}} - \Delta^{(t-1)}_{\{\mu_a,Z,|n_0n_1\rangle\}}| < 2r_{\{\eta,|n_0n_1\rangle\}}. \tag{C22}$$

We denote $c_{\{\mu_a,Z,|n_0n_1\rangle\}} := 2r_{\{\eta,|n_0n_1\rangle\}}$. By applying Azuma's inequality, we can link the observed statistics, $\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}$, with their expected values. Given the estimation failure probability

$$\varepsilon_{\{\mu_a,Z,|n_0n_1\rangle\}} = 2e^2\exp\left[-\frac{2\delta_{\{\mu_a,Z,|n_0n_1\rangle\}}{}^2}{Nc_{\{\mu_a,Z,|n_0n_1\rangle\}}{}^2}\right], \tag{C23}$$

we have

$$\begin{aligned}&\Pr\left\{\left|\Delta^{(N)}_{\{\mu_a,Z,|n_0n_1\rangle\}} - \Delta^{(0)}_{\{\mu_a,Z,|n_0n_1\rangle\}}\right| \geq \delta_{\{\mu_a,Z,|n_0n_1\rangle\}}\right\}\\ =&\Pr\left\{\left|\sum_{i=1}^N \zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}} - \sum_{i=1}^N \mathbb{E}[\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}|\mathcal{F}_{i-1}]\right| \geq \delta_{\{\mu_a,Z,|n_0n_1\rangle\}}\right\}\\ \leq&\varepsilon_{\{\mu_a,Z,|n_0n_1\rangle\}},\end{aligned} \tag{C24}$$

Combining all these results, we arrive at the final result: except for a given failure probability

$$\varepsilon_{Q_{1,1}} = \varepsilon_{\{\mu,(1,1)\}} + \sum_{\mu_a}\left(\varepsilon_{\{\mu_a,Z,|01\rangle\}} + \varepsilon_{\{\mu_a,Z,|10\rangle\}}\right), \tag{C25}$$

$$\begin{aligned}Q_{1,1} \leq& Q^U_{1,1}\\ :=&\frac{p_\mu p_{zz}\mathrm{Pr}_\mu(1)}{N^{zz}_\mu}\Bigg[c_1\sum_{\mu_a}\frac{d^U_{\{\mu_a,(1,1)\}}}{p_{\mu_a}p_{zx}}\Bigg\{\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|01\rangle\langle 01|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|01\rangle\}}}\right)\\ &+\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|10\rangle\langle 10|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|10\rangle\}}}\right)\Bigg\} + Nc^U_{Q_{1,1}} + O\left(\sqrt{-N\ln\varepsilon_{\{\mu,(1,1)\}}}\right)\Bigg],\end{aligned} \tag{C26}$$

$$\begin{aligned}Q_{1,1} \geq& Q^L_{1,1}\\ :=&\frac{p_\mu p_{zz}\mathrm{Pr}_\mu(1)}{N^{zz}_\mu}\Bigg[c_1\sum_{\mu_a}\frac{d^L_{\{\mu_a,(1,1)\}}}{p_{\mu_a}p_{zx}}\Bigg\{\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|01\rangle\langle 01|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|01\rangle\}}}\right)\\ &+\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|10\rangle\langle 10|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|10\rangle\}}}\right)\Bigg\} + Nc^L_{Q_{1,1}} - O\left(\sqrt{-N\ln\varepsilon_{\{\mu,(1,1)\}}}\right)\Bigg].\end{aligned} \tag{C27}$$

To sum up, we depict the flowchart of estimating $Q_{1,1}$ from the observed statistics in Fig. 7.

2. Estimation of $Q_{2,2}$

In this section, we discuss the estimation of $Q_{2,2}$. While conceptually the same as the estimation of $Q_{1,1}$, the two-photon component makes the estimation procedure complex. First, construct the counter variable in the i'th round,

$$\zeta^{(i)}_{\{\mu,(2,2)\}} = \begin{cases}1, \text{ if } \mu_a^{(i)} = \mu \wedge ZZ \wedge n^{(i)} = 2 \wedge m^{(i)} = 2 \wedge (q_1^{(i)}, q_2^{(i)}) \in \mathbf{R_0}\cup\mathbf{R_1}, \\ 0, \text{ otherwise.}\end{cases} \tag{C28}$$

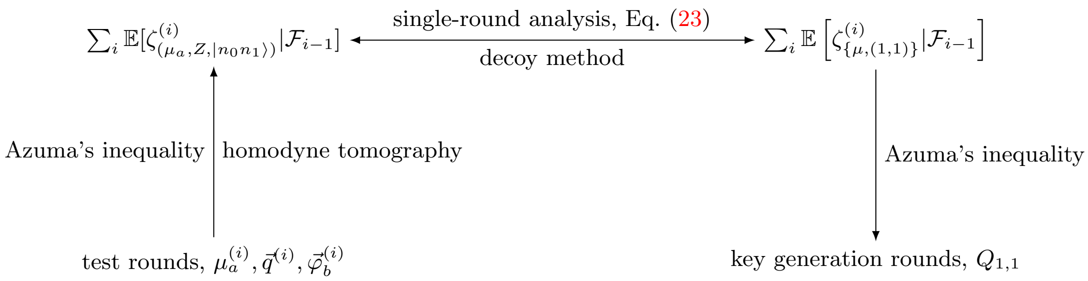

$\sum_i \mathbb{E}[\zeta^{(i)}_{(\mu_a,Z,|n_0 n_1\rangle)}|\mathcal{F}_{i-1}]$
single-round analysis, Eq. (23)
decoy method
$\sum_i \mathbb{E}\left[\zeta^{(i)}_{\{\mu,(1,1)\}}|\mathcal{F}_{i-1}\right]$
Azuma's inequality
homodyne tomography
Azuma's inequality
test rounds, $\mu_a^{(i)}, \vec{q}^{(i)}, \vec{\varphi}_b^{(i)}$
key generation rounds, $Q_{1,1}$

FIG. 7: Flowchart of martingale-based parameter estimation procedures. Here, we take the estimation of $Q_{1,1}$ as an example. The users start with the observed statistics in the test rounds and aim to estimate $Q_{1,1}$. Azuma's inequality is applied twice in the estimation. The single-round analysis in terms of conditional probabilities links the two martingales and hence relates the observed statistics in the test rounds with the target value in the key generation rounds.

which adds one in the virtual experiment when the light intensity is μ, both Alice and Bob choose the Z-basis, Alice sends a two-photon state, and Bob receives a two-photon state and accepts the signal in the post-selection. We have

$$\sum_{i=1}^{N} \zeta^{(i)}_{\{\mu,(2,2)\}} = N_\mu^{zz} Q_{2,2}, \tag{C29}$$

and conditioned on the history before the i'th round, $\mathcal{F}_{i-1}$, the expected value of $\zeta^{(i)}_{\{\mu,(2,2)\}}$ is given by

$$\begin{aligned}\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}\right] = p_\mu p_{zz}\mathrm{Pr}(2)\Bigg(&\frac{1}{2}(c_2^+ + c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\,|02\rangle_{B_1B_2}\langle 02|\right\}\\ &+\frac{1}{2}(c_2^+ - c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\,|02\rangle_{B_1B_2}\langle 20|\right\}\\ &+\frac{1}{2}(c_2^+ - c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\,|20\rangle_{B_1B_2}\langle 02|\right\}\\ &+\frac{1}{2}(c_2^+ + c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\,|20\rangle_{B_1B_2}\langle 20|\right\}\\ &+c_2^{11}\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\,|11\rangle_{B_1B_2}\langle 11|\right\}\Bigg).\end{aligned} \tag{C30}$$

where p_μ is the probability that the light intensity is μ, p_{zz} is the probability that both users choose the Z-basis, and c_2^+, c_2^-, c_2^{11} relate to the accepting probability, as given in Eq. (26). Going through a similar analysis as for $Q_{1,1}$, where we construct a martingale sequence based on the variables $\zeta^{(i)}_{\{\mu,(2,2)\}}$ and apply Azuma's inequality, we arrive at the estimation result that given the failure probability

$$\varepsilon_{\{\mu,(2,2)\}} = \exp\left[-\frac{2\delta_{\{\mu,(2,2)\}}{}^2}{N}\right], \tag{C31}$$

we have

$$\begin{aligned}\mathrm{Pr}\left\{\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,(2,2)\}} - \sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}] \geq \delta_{\{\mu,(2,2)\}}\right\} \leq \varepsilon_{\{\mu,(2,2)\}},\\ \mathrm{Pr}\left\{\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,(2,2)\}} - \sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}] \leq -\delta_{\{\mu,(2,2)\}}\right\} \leq \varepsilon_{\{\mu,(2,2)\}}.\end{aligned} \tag{C32}$$

Then, except for a negligible failure probability, we have the upper and lower bounds on $Q_{2,2}$,

$$\frac{1}{N_\mu^{zz}}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}] - O(\sqrt{-N\ln\varepsilon_{\{\mu,(2,2)\}}})\right\} \leq Q_{2,2} \leq \frac{1}{N_\mu^{zz}}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}] + O(\sqrt{-N\ln\varepsilon_{\{\mu,(2,2)\}}})\right\}. \tag{C33}$$

To estimate the sum of expected values $\sum_{i=1}^{N} \mathbb{E}[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}]$, on the source side, we apply the decoy state method. This part is similar to the single-photon case, where we simply need to use the data where Alice chooses the Z-basis. By running the linear programming, we shall have a result in the form of

$$\begin{aligned}\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}\right] \leq p_\mu p_{zz}\mathrm{Pr}_\mu(2)\Bigg(\sum_{\mu_a} d^U_{\{\mu_a,(2,2)\}}\Bigg\{&\frac{1}{2}(c_2^+ + c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|02\right\rangle_{B_1B_2}\left\langle 02\right|\right\} \\ &+\frac{1}{2}(c_2^+ - c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|02\right\rangle_{B_1B_2}\left\langle 20\right|\right\} \\ &+\frac{1}{2}(c_2^+ - c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|20\right\rangle_{B_1B_2}\left\langle 02\right|\right\} \\ &+\frac{1}{2}(c_2^+ + c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|20\right\rangle_{B_1B_2}\left\langle 20\right|\right\} \\ &+c_2^{11}\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|11\right\rangle_{B_1B_2}\left\langle 11\right|\right\}\Bigg\} + c^U_{Q_{2,2}}\Bigg),\end{aligned} \tag{C34}$$

$$\begin{aligned}\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(2,2)\}}|\mathcal{F}_{i-1}\right] \geq p_\mu p_{zz}\mathrm{Pr}_\mu(2)\Bigg(\sum_{\mu_a} d^L_{\{\mu_a,(2,2)\}}\Bigg\{&\frac{1}{2}(c_2^+ + c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|02\right\rangle_{B_1B_2}\left\langle 02\right|\right\} \\ &+\frac{1}{2}(c_2^+ - c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|02\right\rangle_{B_1B_2}\left\langle 20\right|\right\} \\ &+\frac{1}{2}(c_2^+ - c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|20\right\rangle_{B_1B_2}\left\langle 02\right|\right\} \\ &+\frac{1}{2}(c_2^+ + c_2^-)\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|20\right\rangle_{B_1B_2}\left\langle 20\right|\right\} \\ &+c_2^{11}\mathrm{Tr}\left\{\mathcal{N}_E[\mathrm{Tr}_{A'}(\hat{\rho}^Z_{\mu_a})]\left|11\right\rangle_{B_1B_2}\left\langle 11\right|\right\}\Bigg\} + c^L_{Q_{2,2}}\Bigg).\end{aligned} \tag{C35}$$

On the detection side, nonetheless, more terms are involved. With respect to Eq. (C30), besides the Hermitian operators $\left|n_0n_1\right\rangle_{B_1B_2}\left\langle n_0n_1\right|$ with $\left|n_0n_1\right\rangle = \left|02\right\rangle, \left|20\right\rangle, \left|11\right\rangle$, we also need to use homodyne tomography to estimate the terms with $\left|n_0n_1\right\rangle_{B_1B_2}\left\langle n_0'n_1'\right|$, namely the terms involving $\left|20\right\rangle\left\langle 02\right|$ and $\left|02\right\rangle\left\langle 20\right|$. Note that though these operators are not directly measurable, homodyne tomography allows us to link the physically measured statistics, $\vec{q}$ and $\vec{\varphi}_b$, with them through the kernel function. The expressions of the kernel functions can be obtained through Eq. (B7) and (B9). Consider the following random variables for the i'th round in the experiment,

$$\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}} = \begin{cases}\mathcal{R}_\eta[\left|n_0n_1\right\rangle\left\langle n_0'n_1'\right|](\vec{q},\vec{\varphi}_b), & \text{if } \mu_a^{(i)} = \mu_a \wedge ZX \wedge (q_1^{(i)},q_2^{(i)}) = \vec{q}, (\varphi_b^{1(i)},\varphi_b^{2(i)}) = \vec{\varphi}_b, \\ 0, & \text{otherwise},\end{cases} \tag{C36}$$

which relate to the parameter estimation measurements when the light intensity is μ_a and Alice chooses the Z-basis. For simplicity, we write $\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\}}$ when $n_0 = n_0', n_1 = n_1'$, as in the case of the single-photon term estimation. According to homodyne tomography, we have

$$\mathbb{E}[\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}|\mathcal{F}_{i-1}] = p_{\mu_a}p_{zx}\mathrm{Tr}\left\{\mathcal{N}_E\left[\mathrm{Tr}_{A'}(\left|\Psi_1\right\rangle_{A'A_1A_2}\left\langle\Psi_1\right|)\right](\left|n_0n_1\right\rangle_{B_1B_2}\left\langle n_0'n_1'\right|)\right\}, \tag{C37}$$

and

$$\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}} = \sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[\left|n_0n_1\right\rangle\left\langle n_0'n_1'\right|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}), \tag{C38}$$

where the summation of the right-hand side is taken over the rounds with light intensity μ_a and basis choices of Alice choosing the Z-basis and Bob choosing the X-basis, and $\vec{q}^{(i)},\vec{\varphi}_b^{(i)}$ represent the observed quadrature measurement statistics in the i'th round. By constructing relative martingale sequences and applying Azuma's inequality, we can link the observed statistics, $\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}$, with their expected values. Given the estimation failure probability

$$\varepsilon_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}} = 2e^2\exp\left[-\frac{2\delta_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}{}^2}{Nc_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}{}^2}\right], \tag{C39}$$

where $c_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}} := 2\max|\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0'n_1'|](\vec{q},\vec{\varphi}_b)|$ is a bounded value for $\eta > 1/2$, we have

$$\Pr\left\{\left|\sum_{i=1}^N \zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}} - \sum_{i=1}^N \mathbb{E}[\zeta^{(i)}_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}|\mathcal{F}_{i-1}]\right| \geq \delta_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}\right\} \leq \varepsilon_{\{\mu_a,Z,|n_0n_1\rangle\langle n_0'n_1'|\}}. \tag{C40}$$

Combining all these results, we arrive at the final result: except for a given failure probability

$$\varepsilon_{Q_{2,2}} = \varepsilon_{\{\mu,(2,2)\}} + \sum_{\mu_a}\left(\varepsilon_{\{\mu_a,Z,|02\rangle\}} + \varepsilon_{\{\mu_a,Z,|02\rangle\langle 20|\}} + \varepsilon_{\{\mu_a,Z,|20\rangle\langle 02|\}} + \varepsilon_{\{\mu_a,Z,|20\rangle\}} + \varepsilon_{\{\mu_a,Z,|11\rangle\}}\right), \tag{C41}$$

$$\begin{aligned}
Q_{2,2} \leq & Q_{2,2}^U \\
= & \frac{p_\mu p_{zz}\Pr_\mu(2)}{N_\mu^{zz}}\left[\sum_{\mu_a}\frac{d^U_{\{\mu_a,(2,2)\}}}{p_{\mu_a}p_{zx}}\left\{\frac{1}{2}(c_2^+ + c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|02\rangle\}}}\right)\right.\right. \\
& + \frac{1}{2}(c_2^+ - c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|02\rangle\langle 20|\}}}\right) \\
& + \frac{1}{2}(c_2^+ - c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|20\rangle\langle 02|\}}}\right) \\
& + \frac{1}{2}(c_2^+ + c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|20\rangle\}}}\right) \\
& \left.\left. + c_2^{11}\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|11\rangle\}}}\right)\right\} + Nc^U_{Q_{2,2}} + O\left(\sqrt{-N\ln\varepsilon_{\{\mu,(2,2)\}}}\right)\right],
\end{aligned} \tag{C42}$$

$$\begin{aligned}
Q_{2,2} \geq & Q_{2,2}^L \\
= & \frac{p_\mu p_{zz}\Pr_\mu(2)}{N_\mu^{zz}}\left[\sum_{\mu_a}\frac{d^L_{\{\mu_a,(2,2)\}}}{p_{\mu_a}p_{zx}}\left\{\frac{1}{2}(c_2^+ + c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|02\rangle\}}}\right)\right.\right. \\
& + \frac{1}{2}(c_2^+ - c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|02\rangle\langle 20|\}}}\right) \\
& + \frac{1}{2}(c_2^+ - c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|20\rangle\langle 02|\}}}\right) \\
& + \frac{1}{2}(c_2^+ + c_2^-)\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|20\rangle\}}}\right) \\
& \left.\left. + c_2^{11}\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|11\rangle\}}}\right)\right\} + Nc^L_{Q_{2,2}} - O\left(\sqrt{-N\ln\varepsilon_{\{\mu,(2,2)\}}}\right)\right].
\end{aligned} \tag{C43}$$

3. Estimation of $Q_{*,0}$

In comparison with other terms, the estimation of $Q_{*,0}$ is simple, as we do not need to apply the decoy state method. Corresponding to Eq. (27), construct the counter variable in the i'th round,

$$\zeta^{(i)}_{\{\mu,(*,0)\}} = \begin{cases} 1, \text{ if } \mu_a^{(i)} = \mu \wedge ZZ \wedge m^{(i)} = 0 \wedge (q_1^{(i)}, q_2^{(i)}) \in \mathbf{R_0} \cup \mathbf{R_1}, \\ 0, \text{ otherwise.} \end{cases} \tag{C44}$$

which adds one in the virtual experiment when the light intensity is μ, both Alice and Bob choose the Z-basis, and Bob receives a vacuum state and accepts the signal in the post-selection. We have

$$\sum_{i=1}^{N} \zeta^{(i)}_{\{\mu,(*,0)\}} = N^{zz}_{\mu} Q_{*,0}, \tag{C45}$$

and conditioned on the history before the i'th round, $\mathcal{F}_{i-1}$, the expected value of $\zeta^{(i)}_{\{\mu,(*,0)\}}$ is given by

$$\mathbb{E}\left[\zeta^{(i)}_{\{\mu,(*,0)\}}|\mathcal{F}_{i-1}\right] = p_{\mu} p_{zz} \int_{\mathbf{R_0}} 2\psi_0^2(q_1)\psi_0^2(q_2) dq_1 dq_2 \mathrm{Tr}\left[\hat{P}_0 \mathcal{N}_E\left(\hat{\rho}^Z\right)\hat{P}_0\right], \tag{C46}$$

where p_μ is the probability that the light intensity is μ, and p_{zz} is the probability that both users choose the Z-basis. By constructing a martingale sequence based on the variables $\zeta^{(i)}_{\{\mu,(*,0)\}}$ and applying Azuma's inequality, we arrive at the estimation result that given the failure probability

$$\varepsilon_{\{\mu,(*,0)\}} = \exp\left[-\frac{2\delta_{\{\mu,(*,0)\}}{}^2}{N}\right], \tag{C47}$$

we have

$$\Pr\left\{\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,(*,0)\}} - \sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(*,0)\}}|\mathcal{F}_{i-1}] \leq -\delta_{\{\mu,(*,0)\}}\right\} \leq \varepsilon_{\{\mu,(*,0)\}}. \tag{C48}$$

Then, except for a negligible failure probability, we have the lower bound on $Q_{*,0}$,

$$Q_{*,0} \geq Q^L_{*,0} := \frac{1}{N^{zz}_{\mu}}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,(*,0)\}}|\mathcal{F}_{i-1}] - O(\sqrt{-N\ln\varepsilon_{\{\mu,(*,0)\}}})\right\}. \tag{C49}$$

On the detection side, consider the following random variables for the i'th round in the experiment,

$$\zeta^{(i)}_{\{\mu,Z,|00\rangle\}} = \begin{cases} \mathcal{R}_\eta[|00\rangle\langle 00|](\vec{q},\vec{\varphi}_b), \text{ if } \mu_a^{(i)} = \mu \wedge ZX \wedge (q_1^{(i)}, q_2^{(i)}) = \vec{q}, (\varphi_b^{1(i)}, \varphi_b^{2(i)}) = \vec{\varphi}_b, \\ 0, \qquad\qquad \text{otherwise}, \end{cases} \tag{C50}$$

which relate to the parameter estimation measurements when the light intensity is μ and Alice chooses the Z-basis. By constructing martingale sequences and applying Azuma's inequality, we can link the observed statistics, $\zeta^{(i)}_{\{\mu,Z,|00\rangle\}}$, with their expected values. Given the estimation failure probability

$$\varepsilon_{\{\mu,Z,|00\rangle\}} = 2e^2\exp\left[-\frac{2\delta_{\{\mu,Z,|00\rangle\}}{}^2}{Nc_{\{\mu,Z,|00\rangle\}}{}^2}\right], \tag{C51}$$

where $c_{\{\mu,Z,|00\rangle\}} := 2\max|\mathcal{R}_\eta[|00\rangle\langle 00|](\vec{q},\vec{\varphi}_b)|$ is a bounded value for $\eta > 1/2$, we have

$$\Pr\left\{\left|\sum_{i=1}^{N}\zeta^{(i)}_{\{\mu,Z,|00\rangle\}} - \sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{\mu,Z,|00\rangle\}}|\mathcal{F}_{i-1}]\right| \geq \delta_{\{\mu,Z,|00\rangle\}}\right\} \leq \varepsilon_{\{\mu,Z,|00\rangle\}}. \tag{C52}$$

Combining all these results, we arrive at the final result: except for a given failure probability

$$\varepsilon_{Q_{*,0}} = \varepsilon_{\{\mu,(*,0)\}} + \varepsilon_{\{\mu,Z,|00\rangle\}}, \tag{C53}$$

$$\begin{aligned} Q_{*,0} \geq & Q^L_{*,0} \\ := & \frac{p_{zz}}{p_{zx}N^{zz}_{\mu}}\int_{\mathbf{R_0}} 2\psi_0^2(q_1)\psi_0^2(q_2)dq_1dq_2\left[\sum_{i:\mu_a^{(i)}=\mu_a,ZX}\mathcal{R}_\eta[|00\rangle\langle 00|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\right. \\ & \left. - O\left(\sqrt{-N\ln\varepsilon_{\{\mu_a,Z,|00\rangle\}}}\right) - O\left(\sqrt{-N\ln\varepsilon_{\{\mu,(*,0)\}}}\right)\right]. \end{aligned} \tag{C54}$$

4. Estimation of $e^X_{1,1}$

In this section, we discuss the estimation of $e^X_{1,1}$ based on the single-round result in Eq. (21). While conceptually similar to the estimation of the gains, there are two additional issues that make its estimation more involved:

1. We shall first estimate lower and upper bounds on the value $N^{zz}_\mu Q_{1,1} e^X_{1,1}$, the total number of phase errors in the virtual protocol. Afterward, combined with the estimation of $Q_{1,1}$ in Appendix C 1, we obtain estimations of $e^X_{1,1}$, the phase error rate in key generation rounds where the signal is accepted by Bob.

2. On the source side, to evaluate the terms $|\Psi_1^\pm\rangle$, we need to apply the extended decoy method given in Eq. (31). This involves the rounds where Alice chooses the X-basis.

For simplicity, we shall simply list the counter variables and their estimation results. The relevant martingale variables are constructed similarly to the above sections, which are also conditioned on the filtration $\{\mathcal{F}_i\}_i$. First, construct the counter variable in the i'th round for the phase error variable,

$$\zeta^{(i)}_{\{e^X_{1,1}\}} = \begin{cases} 1, \text{ if } \mu_a^{(i)} = \mu \wedge ZZ \wedge n^{(i)} = 2 \wedge m^{(i)} = 2 \wedge (q_1^{(i)}, q_2^{(i)}) \in \mathbf{R_0} \cup \mathbf{R_1} \wedge \text{ a phase error occurs },\\ 0, \text{ otherwise.} \end{cases} \tag{C55}$$

which adds one in the virtual experiment when the light intensity is μ, both Alice and Bob choose the Z-basis, Alice sends a single-photon state, Bob receives a single-photon state and accepts the signal in the post-selection, and a phase error occurs. We have

$$\sum_{i=1}^{N} \zeta^{(i)}_{\{e^X_{1,1}\}} = N^{zz}_\mu Q_{1,1} e^X_{1,1}, \tag{C56}$$

and conditioned on the history before the i'th round, $\mathcal{F}_{i-1}$, the expected value of $\zeta^{(i)}_{\{e^X_{1,1}\}}$ is given by

$$\begin{aligned}\mathbb{E}\left[\zeta^{(i)}_{\{e^X_{1,1}\}}|\mathcal{F}_{i-1}\right] = \frac{1}{2}p_\mu p_{zz} c_1 \mathrm{Pr}(1)\Big\{&\mathrm{Tr}\left[\mathcal{N}_E(|\Psi_1^+\rangle_{A_1A_2}\langle\Psi_1^+|)\frac{1}{2}(|01\rangle_{B_1B_2} - |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} - \langle 10|_{B_1B_2})\right]\\ &+\mathrm{Tr}\left[\mathcal{N}_E(|\Psi_1^-\rangle_{A_1A_2}\langle\Psi_1^-|)\frac{1}{2}(|01\rangle_{B_1B_2} + |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} + \langle 10|_{B_1B_2})\right]\Big\}.\end{aligned} \tag{C57}$$

Except a given failure probability $\varepsilon_{\{e^X_{1,1}\}}$, we have upper and lower bounds on $Q_{1,1}e^X_{1,1}$,

$$\frac{1}{N^{zz}_\mu}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{e^X_{1,1}\}}|\mathcal{F}_{i-1}] - O(\sqrt{-N\ln\varepsilon_{\{e^X_{1,1}\}}})\right\} \le Q_{1,1}e^X_{1,1} \le \frac{1}{N^{zz}_\mu}\left\{\sum_{i=1}^{N}\mathbb{E}[\zeta^{(i)}_{\{e^X_{1,1}\}}|\mathcal{F}_{i-1}] + O(\sqrt{-N\ln\varepsilon_{\{e^X_{1,1}\}}})\right\}. \tag{C58}$$

On the source side, we apply the decoy state method given in Eq. (31), where we need to use the data where Alice chooses the X-basis with relative phase 0 and π between the two modes,

$$\begin{aligned}\mathbb{E}\left[\zeta^{(i)}_{\{e^X_{1,1}\}}|\mathcal{F}_{i-1}\right] =&\frac{1}{2}p_\mu p_{zz} c_1 \mathrm{Pr}(1)\Big\{\mathrm{Tr}\left[\mathcal{N}_E(|\Psi_1^+\rangle_{A_1A_2}\langle\Psi_1^+|)\frac{1}{2}(|01\rangle_{B_1B_2} - |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} - \langle 10|_{B_1B_2})\right]\\ &+\mathrm{Tr}\left[\mathcal{N}_E(|\Psi_1^-\rangle_{A_1A_2}\langle\Psi_1^-|)\frac{1}{2}(|01\rangle_{B_1B_2} + |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} + \langle 10|_{B_1B_2})\right]\Big\}\\ =&\frac{1}{2}p_\mu p_{zz} c_1\Big\{\mathrm{Tr}\left[\mathcal{N}_E[\hat{P}_1\hat{\rho}^0_\mu\hat{P}_1]\frac{1}{2}(|01\rangle_{B_1B_2} - |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} - \langle 10|_{B_1B_2})\right]\\ &+\mathrm{Tr}\left[\mathcal{N}_E[\hat{P}_1\hat{\rho}^\pi_\mu\hat{P}_1]\frac{1}{2}(|01\rangle_{B_1B_2} + |10\rangle_{B_1B_2})(\langle 01|_{B_1B_2} + \langle 10|_{B_1B_2})\right]\Big\},\end{aligned} \tag{C59}$$

which has the upper and lower bounds of

$$
\begin{aligned}
\mathbb{E}\left[\zeta^{(i)}_{\{e^X_{1,1}\}}|\mathcal{F}_{i-1}\right] \leq & \frac{1}{2}p_\mu p_{zz}\mathrm{Pr}(1)\Bigg(c_1\sum_{\mu_a}\Bigg\{d^{\varphi=0,U}_{\{\mu_a,(1,1)\}}\mathrm{Tr}\left[\mathcal{N}_E(\hat{\rho}^0_{\mu_a})\frac{1}{2}(|01\rangle_{B_1B_2}-|10\rangle_{B_1B_2})(\langle 01|_{B_1B_2}-\langle 10|_{B_1B_2})\right] \\
& + d^{\varphi=\pi,U}_{\{\mu_a,(1,1)\}}\mathrm{Tr}\left[\mathcal{N}_E(\hat{\rho}^\pi_{\mu_a})\frac{1}{2}(|01\rangle_{B_1B_2}+|10\rangle_{B_1B_2})(\langle 01|_{B_1B_2}+\langle 10|_{B_1B_2})\right]\Bigg\} + c^{\varphi=0,U}_{(1,1)} + c^{\varphi=\pi,U}_{(1,1)}\Bigg), \\
\mathbb{E}\left[\zeta^{(i)}_{\{e^X_{1,1}\}}|\mathcal{F}_{i-1}\right] \geq & \frac{1}{2}p_\mu p_{zz}\mathrm{Pr}(1)\Bigg(c_1\sum_{\mu_a}\Bigg\{d^{\varphi=0,L}_{\{\mu_a,(1,1)\}}\mathrm{Tr}\left[\mathcal{N}_E(\hat{\rho}^0_{\mu_a})\frac{1}{2}(|01\rangle_{B_1B_2}-|10\rangle_{B_1B_2})(\langle 01|_{B_1B_2}-\langle 10|_{B_1B_2})\right] \\
& + d^{\varphi=\pi,L}_{\{\mu_a,(1,1)\}}\mathrm{Tr}\left[\mathcal{N}_E(\hat{\rho}^\pi_{\mu_a})\frac{1}{2}(|01\rangle_{B_1B_2}+|10\rangle_{B_1B_2})(\langle 01|_{B_1B_2}+\langle 10|_{B_1B_2})\right]\Bigg\} + c^{\varphi=0,L}_{(1,1)} + c^{\varphi=\pi,L}_{(1,1)}\Bigg).
\end{aligned}
\tag{C60}
$$

To deal with the Fock-basis terms, we utilize the homodyne tomography results, where we construct martingales based on the counter variables

$$
\zeta^{(i)}_{\{\mu_a,\varphi,|n_0n_1\rangle\langle n_0'n_1'|\}} = \begin{cases} \mathcal{R}_\eta[|n_0n_1\rangle\langle n_0'n_1'|](\vec{q},\vec{\varphi}_b), \text{ if } \mu_a^{(i)} = \mu_a \wedge XX \wedge \varphi_a = \varphi \wedge (q_1^{(i)},q_2^{(i)}) = \vec{q}, (\varphi_b^{1(i)},\varphi_b^{2(i)}) = \vec{\varphi}_b, \\ \quad\quad 0, \quad\quad\quad \text{otherwise,} \end{cases}
\tag{C61}
$$

which relate to the parameter estimation measurements when the light intensity is μ_a and Alice chooses the X-basis. According to homodyne tomography, we have

$$
\mathbb{E}[\zeta^{(i)}_{\{\mu_a,\varphi,|n_0n_1\rangle\langle n_0'n_1'|\}}|\mathcal{F}_{i-1}] = p_{\mu_a}p_{xx}\mathrm{Tr}\left\{\mathcal{N}_E\left[\hat{\rho}^\varphi_{\mu_a}\right](|n_0n_1\rangle_{B_1B_2}\langle n_0'n_1'|)\right\},
\tag{C62}
$$

and

$$
\sum_{i=1}^N \zeta^{(i)}_{\{\mu_a,\varphi,|n_0n_1\rangle\langle n_0'n_1'|\}} = \sum_{i:\mu_a^{(i)}=\mu_a,XX,\varphi_a=\varphi}\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0'n_1'|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}),
\tag{C63}
$$

where the summation of the right-hand side is taken over the rounds with light intensity μ_a, Alice choosing the X-basis with relative phase $\varphi_a = \varphi$, and Bob choosing the X-basis, and $\vec{q}^{(i)}, \vec{\varphi}_b^{(i)}$ represent the observed quadrature measurement statistics in the i'th round. When homodyne detectors have an efficiency $\eta > 1/2$, except a given estimation failure probability $\varepsilon := \varepsilon_{\{\mu_a,\varphi,|n_0n_1\rangle\langle n_0'n_1'|\}}$, we have

$$
\left|\sum_{i:\mu_a^{(i)}=\mu_a,XX,\varphi_a=\varphi}\mathcal{R}_\eta[|n_0n_1\rangle\langle n_0'n_1'|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{i=1}^N\mathbb{E}[\zeta^{(i)}_{\{\mu_a,\varphi,|n_0n_1\rangle\langle n_0'n_1'|\}}|\mathcal{F}_{i-1}]\right| \leq O(\sqrt{-N\ln\varepsilon}).
\tag{C64}
$$

Combining all the above results, except for a given failure probability, we have the upper bound on the phase error rate,

$$\begin{aligned}
Q_{1,1}e^X_{1,1} \leq & E^X_{1,1} \\
:= & \frac{p_\mu p_{zz}\mathrm{Pr}(1)}{N^{zz}_\mu}\left(\frac{1}{4}c_1\left\{\sum_{\mu_a}\frac{1}{p_{\mu_a}p_{xx}}\right.\right. \\
& \times\left[d^{\varphi=0,U}_{\{\mu_a,(1,1)\}}\left(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|01\rangle\langle 01|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|01\rangle\langle 10|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\right.\right. \\
& \quad - \left.\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|10\rangle\langle 01|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|10\rangle\langle 10|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O(\sqrt{N})\right) \\
& \quad + d^{\varphi=\pi,U}_{\{\mu_a,(1,1)\}}\left(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|01\rangle\langle 01|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|01\rangle\langle 10|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\right. \\
& \quad \left.\left.\left. + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|10\rangle\langle 01|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|10\rangle\langle 10|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + O(\sqrt{N})\right)\right]\right\} \\
& \left. + Nc^{\varphi=0,U}_{(1,1)} + Nc^{\varphi=\pi,U}_{(1,1)} + O(\sqrt{N})\right).
\end{aligned} \tag{C65}$$

For simplicity and better readability, we omit the failure probabilities in the expressions. Note that each big-O term corresponds to uses of Azuma's inequality. Finally, $e^X_{1,1}$ can be upper bounded by

$$e^X_{1,1} \leq e^{X,U}_{1,1} := \frac{E^X_{1,1}}{Q^L_{1,1}}, \tag{C66}$$

where $Q^L_{1,1}$ is given by Eq. (C27).

5. Estimation of $e^X_{2,2}$

The estimation of $e^X_{2,2}$ follows the same procedures as the above quantities. This involves all the cumbersome issues, including both the rounds where Alice chooses the Z-basis and the X-basis, the use of extended decoy state, and the homodyne tomography for non-Hermitian operators. Nevertheless, we have shown how to tackle each issue in the above discussions. Here, we simply present the final result. Except for a given failure probability, we have that

$$Q_{2,2}e^X_{2,2} \leq E^X_{2,2} := \frac{p_\mu p_{zz}\mathrm{Pr}_\mu(2)}{N^{ZZ}_\mu}[N_1 + N_2 + N_3 + O(\sqrt{N})], \tag{C67}$$

where the big-O term here corresponds to a use of Azuma's inequality, N_1, N_2, N_3 refer to the upper bounds on the numbers of three types of errors: $|\Psi_2^+\rangle$ received as $|\Psi_2^-\rangle$, $|\Psi_2^-\rangle$ received as $|\Psi_2^+\rangle$, and $|\Psi_2^-\rangle$ received as $|11\rangle$, with values

$$
\begin{aligned}
N_1 = \frac{c_2^-}{2}\sum_{\mu_a}\frac{1}{p_{\mu_a}}\Bigg\{ \frac{1}{2p_{xx}}\Bigg[& d^{\varphi=0,U}_{\{\mu_a,|\Psi_2^-\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) \\
& - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg) \\
& + d^{\varphi=\pi,U}_{\{\mu_a,|\Psi_2^-\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) \\
& - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg) \\
& - d^{\varphi=\pi/2,L}_{\{\mu_a,|\Psi_2^-\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) \\
& - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg) \\
& - d^{\varphi=3\pi/2,L}_{\{\mu_a,|\Psi_2^-\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) \\
& - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg)\Bigg] \\
& + \frac{1}{p_{zx}} d^{Z,U}_{\{\mu_a,|\Psi_2^-\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) \\
& - \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)}) + \sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg) \\
& + Nc^{\varphi=0,U}_{|\Psi_2^-\rangle} + Nc^{\varphi=\pi,U}_{|\Psi_2^-\rangle} + Nc^{\varphi=\pi/2,U}_{|\Psi_2^-\rangle} + Nc^{\varphi=3\pi/2,U}_{|\Psi_2^-\rangle} + Nc^{Z,U}_{|\Psi_2^-\rangle} + O(\sqrt{N})\Bigg\},
\end{aligned}
\tag{C68}
$$

$$
\begin{aligned}
N_2 = \frac{c_2^+}{2}\sum_{\mu_a}\frac{1}{p_{\mu_a}}\Bigg\{\frac{1}{2p_{xx}}\Bigg[& -d^{\varphi=0,L}_{\{\mu_a,|\Psi_2^+\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\\
& +\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg)\\
& -d^{\varphi=\pi,L}_{\{\mu_a,|\Psi_2^+\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\\
& +\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg)\\
& +d^{\varphi=\pi/2,U}_{\{\mu_a,|\Psi_2^+\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\\
& +\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg)\\
& +d^{\varphi=3\pi/2,U}_{\{\mu_a,|\Psi_2^+\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\\
& +\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg)\Bigg]\\
& +\frac{1}{p_{zx}}d^{Z,U}_{\{\mu_a,|\Psi_2^+\rangle\}}\Bigg(\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|02\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|02\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\\
& +\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|20\rangle\langle 02|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|20\rangle\langle 20|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg)\\
& +Nc^{\varphi=0,U}_{|\Psi_2^+\rangle}+Nc^{\varphi=\pi,U}_{|\Psi_2^+\rangle}+Nc^{\varphi=\pi/2,U}_{|\Psi_2^+\rangle}+Nc^{\varphi=3\pi/2,U}_{|\Psi_2^+\rangle}+Nc^{Z,U}_{|\Psi_2^+\rangle}+O(\sqrt{N})\Bigg\},
\end{aligned}
\tag{C69}
$$

$$
\begin{aligned}
N_3 = & c_2^{11}\sum_{\mu_a}\frac{1}{p_{\mu_a}}\Bigg\{\frac{1}{2p_{xx}}\Bigg[-d^{\varphi=0,L}_{\{\mu_a,|11\rangle\}}\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=0}}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})-d^{\varphi=\pi,L}_{\{\mu_a,|11\rangle\}}\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi}}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\\
& +d^{\varphi=\pi/2,U}_{\{\mu_a,|11\rangle\}}\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=\pi/2}}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+d^{\varphi=3\pi/2,U}_{\{\mu_a,|11\rangle\}}\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ XX,\varphi_a=3\pi/2}}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})\Bigg]\\
& +\frac{1}{p_{zx}}d^{Z,U}_{\{\mu_a,|11\rangle\}}\sum_{\substack{i:\mu_a^{(i)}=\mu_a,\\ ZX}}\mathcal{R}_\eta[|11\rangle\langle 11|](\vec{q}^{(i)},\vec{\varphi}_b^{(i)})+Nc^{\varphi=0,U}_{|11\rangle}+Nc^{\varphi=\pi,U}_{|11\rangle}+Nc^{\varphi=\pi/2,U}_{|11\rangle}+Nc^{\varphi=3\pi/2,U}_{|11\rangle}+Nc^{Z,U}_{|11\rangle}+O(\sqrt{N})\Bigg\}.
\end{aligned}
\tag{C70}
$$

In the above formulae, $d^{\varphi=0,U}_{\mu_a,|\Psi_2^-\rangle}$, for instance, refers to the coefficient of the upper-bound decoy-state terms for the case where the light intensity is μ_a, the relative phase between the modes sent by Alice is $\varphi = 0$, and the phase error belongs to the case that $|\Psi_2^+\rangle$ is measured as $|\Psi_2^-\rangle$. The other terms follow the same terminology rule. The big-O terms come from applications of Azuma's inequality. Finally, $e^X_{2,2}$ can be upper bounded by

$$e^X_{2,2} \leq e^{X,U}_{2,2} := \frac{E^X_{2,2}}{Q^L_{2,2}}, \tag{C71}$$

where $Q^L_{2,2}$ is given by Eq. (C43).

6. Summary of the finite-size analysis

To summarize, we list the counter variables to establish martingales in parameter estimation in Fig. 8. The general approach goes as follows: In the i'th round, for a specific experimental setting and observable $\hat{O}$, consider a counter variable, $\zeta^{(i)}_{\{\text{setting},\hat{O}\}}$, which is in the form of Eq. (C7) and Eq. (C18). In the figure, we list the non-trivial values that the counter variables may take in the (virtual) experiment. Each blue box represents the outcome of a random variable, where randomness originates from either the random choice for the experimental setting or the measurement outcome. The counter variable takes a non-trivial value if the experiment takes the path that leads to its associating event. Otherwise, it takes the value 0. Then, for each setting and observable, the following series of random variables form a martingale,

$$\Delta^{(t)}_{\{\text{setting},\hat{O}\}} = \begin{cases} 0, & \text{if } t = 0, \\ \sum_{i=1}^{t} \left\{ \zeta^{(i)}_{\{\text{setting},\hat{O}\}} - \mathbb{E}\left[\zeta^{(i)}_{\{\text{setting},\hat{O}\}} | \mathcal{F}_{i-1} \right] \right\}, & \text{if } t = 1, \cdots, N. \end{cases} \tag{C72}$$

As we embed all possible randomness origins in the experiment in defining these observables, all the counter variables in the i'th round, $\zeta^{(i)}_{\{\text{setting},\hat{O}\}}$, are defined over the same filtration. Therefore, we can link their expected values via the single-round analysis and hence the parameter estimation measurement statistics with the quantities we are interested in.

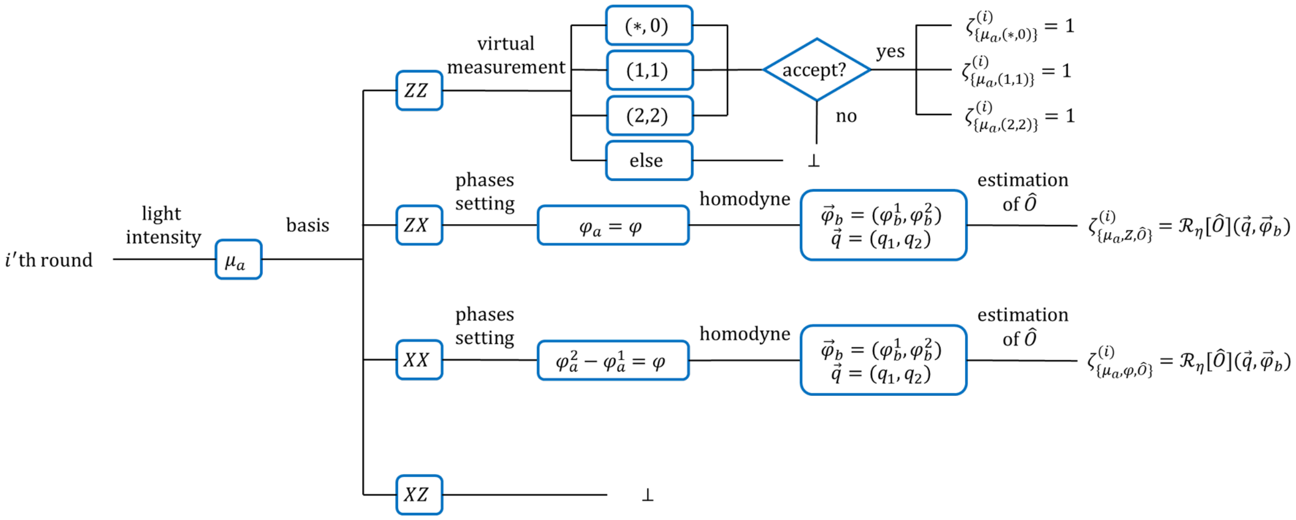

i'th round
light intensity
μ_a
basis
ZZ
virtual measurement
$(*,0)$
$(1,1)$
$(2,2)$
else
accept?
yes
no
$\perp$
$\zeta^{(i)}_{\{\mu_a,(*,0)\}} = 1$
$\zeta^{(i)}_{\{\mu_a,(1,1)\}} = 1$
$\zeta^{(i)}_{\{\mu_a,(2,2)\}} = 1$
ZX
phases setting
$\varphi_a = \varphi$
homodyne
$\vec{\varphi}_b = (\varphi_b^1, \varphi_b^2)$
$\vec{q} = (q_1, q_2)$
estimation of $\hat{O}$
$\zeta^{(i)}_{\{\mu_a,Z,\hat{O}\}} = \mathcal{R}_\eta[\hat{O}](\vec{q},\vec{\varphi}_b)$
XX
phases setting
$\varphi_a^2 - \varphi_a^1 = \varphi$
homodyne
$\vec{\varphi}_b = (\varphi_b^1, \varphi_b^2)$
$\vec{q} = (q_1, q_2)$
estimation of $\hat{O}$
$\zeta^{(i)}_{\{\mu_a,\varphi,\hat{O}\}} = \mathcal{R}_\eta[\hat{O}](\vec{q},\vec{\varphi}_b)$
XZ
$\perp$

FIG. 8: The counter variables to set up martingales in parameter estimation. For each experimental setting and observable that is involved in parameter estimation, we set up a corresponding counter random variable in each round, $\zeta^{(i)}_{\{\text{setting},\hat{O}\}}$. We list the values that should be given to these random variables when an associating path is taken in the experiment. In other circumstances, the counter variables take the value 0.

To end this section, we give a formal theorem of the finite-size key generation result.

Theorem 5. *For the time-bin CV QKD protocol in Table III with reverse reconciliation, suppose the total number of rounds is N and the number of key generation rounds is N_μ^{zz}. Given the failure probability in parameter estimation $\varepsilon_{\mathrm{pe}} \in (0,1)$, which involves the estimation of the gains $Q_{1,1}, Q_{2,2}, Q_{*,0}$ and phase-error rates $e_{1,1}^X, e_{2,2}^X$, and the failure probability in privacy amplification $\varepsilon_{\mathrm{pa}} \in (0,1)$, then conditioned on the success of information reconciliation, except a total failure probability $\varepsilon = \varepsilon_{\mathrm{pe}} + \varepsilon_{\mathrm{pa}}$, the number of secure key bits that can be obtained from the protocol is lower-bounded by*

$$n \geq n_{\mathrm{rev}} = N_\mu^{zz}\left\{Q_{*,0}^L + Q_{1,1}^L\left[1 - h\left(e_{1,1}^{X,U}\right)\right] + Q_{2,2}^L\left[1 - h\left(e_{2,2}^{X,U}\right)\right] - fQ^Z h(e^Z)\right\} - \log\frac{1}{\varepsilon_{\mathrm{pa}}}, \tag{C73}$$

where Q^Z is the Z-basis gain, e^Z is the bit error rate, f is the efficiency of information reconciliation, $Q_{*,0}^L$ is the lower bound on $Q_{*,0}$ given in Eq. (C49), $Q_{1,1}^L$ and $Q_{1,1}^U$ are the lower and upper bounds on $Q_{1,1}$ given in Eq. (C27) and (C26), $Q_{2,2}^L$ and $Q_{2,2}^U$ are the lower and upper bounds on $Q_{2,2}$ given in Eq. (C43) and (C42), $e_{1,1}^{X,U}$ is the upper bound on $e_{1,1}^X$ given in Eq. (C66), and $e_{2,2}^{X,U}$ is the upper bound on $e_{2,2}^X$ given in Eq. (C71).

Appendix D: Simulation formulae under thermal-noise channel

We present the simulation formulae of the asymptotic time-bin CV QKD under a thermal-noise channel with excess noise ξ from the output. We set $\hbar = 2$ so that the vacuum variance is 1. A thermal noise channel is characterized as a Gaussian completely positive map transforming the first and second moment $(\bar{r}, V)$, representing the mean vector and covariance matrix of the quadrature operators, of the input state as [33]:

$$\begin{aligned} &\bar{r} \mapsto \sqrt{\eta}\bar{r}, \\ &V \mapsto \eta V + (1-\eta)\mathbb{I} + \xi\mathbb{I}, \end{aligned} \tag{D1}$$

where η is the channel transmittance. Two thermal channels with transmittance η and η' and excess noise ξ and ξ' concatenate to another thermal channel with transmittance $\eta\eta'$ and excess noise $(\eta'\xi + \xi')$ since

$$\begin{aligned} &\bar{r} \mapsto \sqrt{\eta'\eta}\bar{r}, \\ &V \mapsto \eta'(\eta V + (1-\eta)\mathbb{I} + \xi\mathbb{I}) + (1-\eta')\mathbb{I} + \xi'\mathbb{I} \\ &= \eta'\eta V + (1-\eta'\eta)\mathbb{I} + (\eta'\xi + \xi')\mathbb{I}. \end{aligned} \tag{D2}$$

On the bit-error side, the thermal noise can be seen as adding ξ to the unity variance of the coherent states. Hence, if Alice transmits a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ through a thermal-noise channel with transmittance η and excess noise ξ, and Bob applies homodyne detection with LO phase φ, the detection result q will follow a distribution

$$\Pr(q|\mu, \theta - \varphi) = \frac{1}{\sqrt{2\pi}}\exp\left\{-\frac{[q - 2\sqrt{\eta\mu}\cos(\theta-\varphi)]^2}{2(1+\xi)}\right\}. \tag{D3}$$

Since both the signal states and the receiver LO are uniformly phase randomized, $(\theta - \varphi)$ is also uniformly randomized with $[0, 2\pi)$ in a cyclic manner. The bit error rate e_μ^Z and the Z-basis gain Q_μ^Z can thus be calculated according to the post-selection threshold τ, uniformly randomizing over $[0, 2\pi)$.

The calculation of the vacuum gain $Q_{*,0}$, according to Eq. (27), requires the probability of sending the Z-basis state whilst receiving vacuum. This can be calculated via the Wigner function for Gaussian state, and in specific

$$\mathrm{Tr}\left[\hat{P}_0^{B_1B_2}\mathcal{N}_E^{A_1A_2\to B_1B_2}\left(\hat{\rho}^Z\right)\hat{P}_0^{B_1B_2}\right] = \left(\frac{2}{2+\xi}\right)^2\exp\left(-\frac{2\eta\mu}{2+\xi}\right). \tag{D4}$$

The single- and two-photon gains, $Q_{1,1}$ and $Q_{2,2}$, and phase-error rates, $e_{1,1}^X$ and $e_{2,2}^X$, are more complicated in calculation. In the infinite-decoy setup, we calculate the photon gains directly. We decompose the thermal noise $\hat{\rho}_{\mathrm{th}}$ into Fock states,

$$\hat{\rho}_{\mathrm{th}} = \sum_{k=0}^{\infty}\frac{\bar{k}^k}{(\bar{k}+1)^{k+1}}|k\rangle\langle k|, \tag{D5}$$

where $\bar{k} = \xi/2(1-\eta)$ is the average photon number of the thermal noise. The optical mode from Alice can be seen as mixing with the thermal noise through an η-transmittance beam splitter. We calculate the effect of the thermal noise in an ensemble manner, that is, we calculate the case where the channel injects k and l noise photons to the two consecutive optical modes respectively, and mix the results according to the noise photon-number distribution in Eq. (D5). We set a cutoff photon-number at $N_c = 3$ since the thermal noise is relatively low. Simulation shows that higher cutoffs have negligible effects on the key rate. We also account for the effects of the misalignment angle δ, which introduces a $\sin^2(m\delta/2)$ error to the m-photon phase error rate. We ignore the correlation between the misalignment and thermal noise photon as a second-order small quantity.

The calculations of the quantities of interest are listed below. The notation of (k, l) represents the conditional probability that the thermal sources emit k and l photons respectively to the two optical modes:

1. The probability of sending $(|01\rangle\langle 01| + |01\rangle\langle 01|)/2$ whilst accepting one photon in total (Eq. (23)):

$$Q_{1,1}(k,l) = c_1 \mathrm{Pr}(1)\eta^{k+l-1}\left\{[(k+1)\eta - k]^2 + l(k+1)(1-\eta)^2\right\}, \tag{D6}$$

$$Q_{1,1} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)Q_{1,1}(k,l), \tag{D7}$$

where

$$\mathrm{P_{th}}(k) = \frac{\bar{k}^k}{(\bar{k}+1)^{k+1}} \text{ with } \bar{k} = \frac{\xi}{2(1-\eta)}. \tag{D8}$$

2. The probability of sending $(|01\rangle \pm |10\rangle)/\sqrt{2}$ whilst receiving $(|01\rangle \mp |10\rangle)/\sqrt{2}$ (Eq. (21)):

$$\frac{e^X_{1,1}(k,l)Q_{1,1}}{\mathrm{Pr}(1)} = \frac{c_1}{4}\eta^{k+l-1}(1-\eta)^2(k^2+l^2+k+l) + c_1\sin^2\left(\frac{\delta}{2}\right), \tag{D9}$$

$$e^X_{1,1} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)e^X_{1,1}(k,l). \tag{D10}$$

3. The probability of sending $(|02\rangle\langle 02| + |20\rangle\langle 20|)/2$ whilst accepting within the $(|02\rangle\langle 02| + |20\rangle\langle 20|)$ and $|11\rangle\langle 11|$ subspace (Eq. (26)):

$$Q^{02}_{2,2}(k,l) = \frac{1}{2}c^{02}_2\,\mathrm{Pr}(2)\eta^{k+l-2}\left\{\left[\eta^2 - 2k\eta(1-\eta) + \frac{1}{2}k(k-1)(1-\eta)^2\right]^2 + \frac{1}{4}l^2(l-1)^2(1-\eta)^4\right\} + \{k \leftrightarrow l\}, \tag{D11}$$

$$Q^{11}_{2,2}(k,l) = \frac{1}{2}c^{11}_2\,\mathrm{Pr}(2)\eta^{k+l-2}\left[\sqrt{2(k+1)l}\eta(1-\eta) - \sqrt{\frac{1}{2}kl(k+1)(1-\eta)^2}\right]^2 + \{k \leftrightarrow l\}, \tag{D12}$$

$$Q_{2,2} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)\left[Q^{02}_{2,2}(k,l) + Q^{11}_{2,2}(k,l)\right], \tag{D13}$$

where the expression $\{k \leftrightarrow l\}$ denotes exchanging the k's and l's in the term ahead.

4. The probability of sending $(|02\rangle \pm |20\rangle)/\sqrt{2}$ whilst receiving $(|02\rangle \mp |20\rangle)/\sqrt{2}$ and $|11\rangle$ (Eq. (24)).

$$\frac{e^{02,X}_{2,2}(k,l)Q_{2,2}}{\mathrm{Pr}(2)} = \frac{c^{02}_2}{4}\eta^{k+l-2}\left[2(k-l)(1-\eta)\eta + (k^2-k-l^2-l)(1-\eta)^2\right]^2 + c^{02}_2\sin^2(\delta), \tag{D14}$$

$$\frac{e^{11,X}_{2,2}(k,l)Q_{2,2}}{\mathrm{Pr}(2)} = c^{11}_2\eta^{k+l-2}(1-\eta)^2\left\{l(k+1)\left[\eta - \frac{1}{2}k(1-\eta)\right]^2 + k(l+1)\left[\eta - \frac{1}{2}l(1-\eta)\right]^2\right\}, \tag{D15}$$

$$\frac{e^X_{2,2}Q_{2,2}}{\mathrm{Pr}(2)} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)\left[e^{02,X}_{2,2}(k,l) + e^{11,X}_{2,2}(k,l)\right]. \tag{D16}$$

In the finite-decoy setup, the estimations of photon gains are derived from the statistics of coherent-state gains. We need to calculate the probability of transmitting certain coherent states whilst receiving certain photon states. This can be also be done by the Gaussian-state Wigner function. Let $\kappa = 2/(2+\xi)$. Denote the output of a thermal noise channel when transmitting the coherent state $|\alpha\rangle$ as ρ_α. Its Fock-basis matrix elements are:

$$\langle 0|\,\rho_\alpha\,|0\rangle = \kappa\exp(-\kappa|\alpha|^2), \tag{D17}$$

$$\langle 1|\,\rho_\alpha\,|1\rangle = \kappa(\kappa^2|\alpha|^2 + 1 - \kappa)\exp(-\kappa|\alpha|^2), \tag{D18}$$

$$\langle 0|\,\rho_\alpha\,|1\rangle = -\kappa^2\alpha^*\exp(-\kappa|\alpha|^2), \tag{D19}$$

$$\langle 2|\,\rho_\alpha\,|2\rangle = \kappa(\frac{1}{2}\kappa^4|\alpha|^4 + 2(\kappa^2-\kappa^3)|\alpha|^2 + (1-\kappa^2))\exp(-\kappa|\alpha|^2), \tag{D20}$$

$$\langle 0|\,\rho_\alpha\,|2\rangle = \frac{1}{\sqrt{2}}\kappa^3(\alpha^*)^2\exp(-\kappa|\alpha|^2). \tag{D21}$$

The statistics required by the decoy method are all based on the gains of separable coherent states. For example, the probability of sending $|\alpha\rangle\otimes|\beta\rangle$ whilst receiving $(|02\rangle + |20\rangle)/\sqrt{2}$ can be computed by

$$\begin{aligned}&\frac{1}{2}(\langle 02| + \langle 20|)\rho_\alpha\otimes\rho_\beta(|02\rangle + |20\rangle)\\ =\ &\frac{1}{2}\left(\langle 0|\,\rho_\alpha\,|0\rangle\,\langle 2|\,\rho_\beta\,|2\rangle + \langle 2|\,\rho_\alpha\,|2\rangle\,\langle 0|\,\rho_\beta\,|0\rangle + \langle 0|\,\rho_\alpha\,|2\rangle\,\langle 2|\,\rho_\beta\,|0\rangle + \langle 2|\,\rho_\alpha\,|0\rangle\,\langle 0|\,\rho_\beta\,|2\rangle\right).\end{aligned} \tag{D22}$$

[1] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.

[2] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

[3] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. **88**, 10.1103/physrevlett.88.057902 (2002).

[4] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, Phys. Rev. X **9**, 10.1103/physrevx.9.041064 (2019).

[5] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, Finite-size security of continuous-variable quantum key distribution with digital signal processing, Nat. Commun. **12**, 10.1038/s41467-020-19916-1 (2021).

[6] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, Feasibility of quantum key distribution through a dense wavelength division multiplexing network, New J. Phys. **12**, 103042 (2010).

[7] R. Kumar, H. Qin, and R. Alléaume, Coexistence of continuous variable QKD with intense DWDM classical channels, New J. Phys. **17**, 043027 (2015).

[8] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and M. Sasaki, Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels, Commun. Phys. **2**, 10.1038/s42005-018-0105-5 (2019).

[9] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, High key rate continuous-variable quantum key distribution with a real local oscillator, Opt. Express **26**, 2794 (2018).

[10] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, High-speed gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation, Opt. Express **28**, 32882 (2020).

[11] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, and B. Xu, Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area, Commun. Phys. **5**, 10.1038/s42005-022-00941-z (2022).

[12] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photonics **13**, 839 (2019).

[13] D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, Phys. Rev. X **5**, 10.1103/physrevx.5.041010 (2015).

[14] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems, Phys. Rev. A **88**, 10.1103/physreva.88.022339 (2013).

[15] L. Fan, Y. Bian, M. Wu, Y. Zhang, and S. Yu, Quantum hacking against discrete-modulated continuous-variable quantum key distribution using modified local oscillator intensity attack with random fluctuations, Phys. Rev. Applied **20**, 10.1103/physrevapplied.20.024073 (2023).

[16] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, Phys. Rev. A **87**, 10.1103/physreva.87.062313 (2013).

[17] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, Phys. Rev. A **87**, 10.1103/physreva.87.062329 (2013).

[18] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection, Physical Review X **5**, 10.1103/physrevx.5.041009 (2015).

[19] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A: Math. Phys. Eng. Sci. **461**, 207 (2005).

[20] A. Leverrier, Security of continuous-variable quantum key distribution via a gaussian de finetti reduction, Phys. Rev. Lett. **118**, 10.1103/physrevlett.118.200501 (2017).

[21] T. Matsuura, S. Yamano, Y. Kuramochi, T. Sasaki, and M. Koashi, Refined finite-size analysis of binary-modulation continuous-variable quantum key distribution (2023).

[22] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).

[23] B. Qi, Bennett-brassard 1984 quantum key distribution using conjugate homodyne detection, Phys. Rev. A **103**, 10.1103/physreva.103.012606 (2021).

[24] I. W. Primaatmaja, C. C. Liang, G. Zhang, J. Y. Haw, C. Wang, and C. C.-W. Lim, Discrete-variable quantum key distribution with homodyne detection, Quantum **6**, 613 (2022).

[25] H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[26] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

[27] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Info. Comput. **4**, 325–360 (2004).

[28] X. Ma, *Quantum cryptography: from theory to practice*, Ph.D. thesis, University of Toronto (2008), also available in arXiv:0808.1385.

[29] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[30] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[31] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Squashing models for optical measurements in quantum communication, Phys. Rev. Lett. **101**, 10.1103/physrevlett.101.093601 (2008).

[32] G. M. D'Ariano, L. Maccone, and M. F. Sacchi, Homodyne tomography and the reconstruction of quantum states of light, in *Quantum Information with Continuous Variables of Atoms and Light* (PUBLISHED BY IMPERIAL COLLEGE PRESS AND DISTRIBUTED BY WORLD SCIENTIFIC PUBLISHING CO., 2007) pp. 141–158.

[33] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[34] K. Vogel and H. Risken, Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase, Phys. Rev. A **40**, 2847 (1989).

[35] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Measurement of the wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum, Phys. Rev. Lett. **70**, 1244 (1993).

[36] G. M. D'Ariano, C. Macchiavello, and M. G. A. Paris, Detection of the density matrix through optical homodyne tomography without filtered back projection, Phys. Rev. A **50**, 4298 (1994).

[37] G. M. D'Ariano, U. Leonhardt, and H. Paul, Homodyne detection of the density matrix of the radiation field, Phys. Rev. A **52**, R1801 (1995).

[38] U. Leonhardt and H. Paul, Measuring the quantum state of light, Prog. Quantum Electron. **19**, 89 (1995).

[39] G. D'Ariano, Tomographic measurement of the density matrix of the radiation field, J. Eur. Opt. Soc. B **7**, 693 (1995).

[40] M. Kumazawa, T. Sasaki, and M. Koashi, Rigorous characterization method for photon-number statistics, Opt. Express **27**, 5297 (2019).

[41] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[42] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, New J. Phys. **17**, 053014 (2015).

[43] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[44] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A **61**, 10.1103/physreva.61.052304 (2000).

[45] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[46] H.-K. Lo, Getting something out of nothing (2005), arXiv:quant-ph/0503004 [quant-ph].

[47] C. Marand and P. D. Townsend, Quantum key distribution over distances as long as 30 km, Opt. Lett. **20**, 1695 (1995).

[48] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, Ultrasensitive pulsed, balanced

homodyne detector: application to time-domain quantum measurements, Opt. Lett. **26**, 1714 (2001).

[49] S. Grandi, A. Zavatta, M. Bellini, and M. G. A. Paris, Experimental quantum tomography of a homodyne detector, New J. Phys. **19**, 053015 (2017).

[50] K. Azuma, Weighted sums of certain dependent random variables, Tohoku Math. J. Second Ser. **19**, 357 (1967).

[51] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).

[52] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 10.1038/ncomms6235 (2014).

[53] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 10.1038/ncomms15043 (2017).

[54] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, Appl. Phys. Lett. **117**, 144003 (2020).

[55] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, High-rate quantum key distribution exceeding 110 mb s–1, Nat. Photonics **17**, 416 (2023).

[56] X. Ma, C.-H. F. Fung, and M. Razavi, Statistical fluctuation analysis for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 10.1103/physreva.86.052305 (2012).

[57] F. Xu, H. Xu, and H.-K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 10.1103/physreva.89.052333 (2014).

[58] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Inf. **7**, 22 (2021).

[59] X. Zhang, P. Zeng, T. Ye, H.-K. Lo, and X. Ma, Quantum complementarity approach to device-independent security, Phys. Rev. Lett. **131**, 140801 (2023).

[60] G. Kato, Concentration inequality using unconfirmed knowledge, arXiv:2002.04357 (2020).

[61] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[62] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Sci. Technol. **4**, 035008 (2019).

[63] I. Vagniluca, B. D. Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient time-bin encoding for practical high-dimensional quantum key distribution, Phys. Rev. Appl. **14**, 10.1103/physrevapplied.14.014051 (2020).

[64] A. Jin, P. Zeng, R. V. Penty, and X. Ma, Reference-frame-independent design of phase-matching quantum key distribution, Phys. Rev. Appl. **16**, 10.1103/physrevapplied.16.034017 (2021).

[65] V. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: A threat and a defense, Entropy **18**, 20 (2016).

[66] B. Qi and C. C. W. Lim, Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator, Phys. Rev. Appl. **9**, 10.1103/physrevapplied.9.054008 (2018).

[67] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 10.1103/physrevlett.108.130503 (2012).

[68] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 10.1103/physreva.86.062319 (2012).

[69] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[70] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).

[71] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[72] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 10.1038/s41467-022-31534-7 (2022).

[73] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).

[74] U. Leonhardt, H. Paul, and G. M. D'Ariano, Tomographic reconstruction of the density matrix via pattern functions, Phys. Rev. A **52**, 4899 (1995).

[75] E. Lavie, I. W. Primaatmaja, W. Y. Kon, C. Wang, and C. C. W. Lim, Estimating the photon-number distribution of photonic channels for realistic devices and applications in photonic quantum information processing, Phys. Rev. Appl. **16**, 034020 (2021).

[76] T. P. Hayes, A large-deviation inequality for vector-valued martingales, Combinatorics, Probability and Computing (2005).

Security of hybrid BB84 with heterodyne detection

Jasminder S. Sidhu[1] * Rocco Maggi[2] Saverio Pascazio[2 3] Cosmo Lupo[2 3 †]

[1] *SUPA Department of Physics, The University of Strathclyde, Glasgow, G4 0NG, UK*
[2] *Dipartimento Interateneo di Fisica, Università di Bari, 70126, Bari, Italy*
[3] *INFN, Sezione di Bari, 70126 Bari, Italy*

Abstract. We explore a hybrid QKD protocol that leverages advantages of discrete and continuous-variable protocols to enhance the feasibility for near-term implementation of global quantum communications and compatibility with existing telecommunications architectures. Security proofs for hybrid protocols inherit challenges associated with unbounded dimensions. We address these challenges by exploiting symmetry. Our approach enables truncation of the Hilbert space with precise control of the approximation errors, leading to tight, semi-analytical expressions for the asymptotic key rate under collective attacks. We explore the performance of our protocol under passive attacks, linear loss, and Gaussian noise.

Keywords: Hybrid quantum information theory, quantum key distribution, quantum networking.

Global quantum communications are in the vanguard of early application of quantum technologies [1, 2]. A pressing challenge in transforming quantum cryptographic protocols to implementation is the disparity between theory and experiments. Closing this disparity in *discrete-variable* (DV) and *continuous-variable* (CV) *quantum key distribution* (QKD) has been the subject of significant effort [3, 4]. A hybrid approach has recently emerged as an exciting and promising solution towards practical implementation [5, 6, 7]. The central motivation behind hybrid protocols is to assimilate the best features of both DV and CV protocols to generate mature security proofs, simplify implementation, and improve compatibility with existing telecommunication infrastructures.

An immediate difficulty in the maturity of hybrid protocols is that they inherit an infinite-dimensional Hilbert space from CV protocols, which introduces technical challenges for their security proofs. In this work, we explore the potential of single-photon-based hybrid QKD, where information is encoded in discrete polarisation variables and decoded continuously via heterodyne detection. We provide the first rigorous security proof for hybrid protocols within the collective attack framework to establish a tight lower bound on the asymptotic key rate, allowing for semi-analytical expressions. We conclude by assessing the practical implementation and deployment of our hybrid protocol across large-scale quantum networks. For complete details, see Ref. [8].

One of the central results in this work is our use of state symmetries to establish novel invariant states that are exploited in our security proof. In particular, the symmetry we appeal to is the invariance of two-party composite states under $(U \otimes U^*)$ transformations, where U belongs to the special unitary SU(2) Lie group that physically represents a linear-optics passive unitary acting on two polarisation modes. Crucially, the invariant states we derive have a significantly reduced parameterisation, which provides a quadratic speedup in the numerical calculation of the secret key rate [9, 10, 11] and enables an truncation of the Hilbert space with precise control of the approximation errors. The tightness of our method enables higher key rates and increased robustness to noise over previous security proofs. We quantify this improvement within an experimentally feasible parameter space, providing insights into the current readiness for implementation. Additionally, we compare the performance of hybrid protocols with DV and CV protocols to discuss their current viability for applications in quantum networking, which remains an important open question in the field. As such, this work is first to quantify tradeoffs in the use of hybrid protocols that would be instrumental in guiding future research into their use for quantum networking.

To start, we provide an outline of the hybrid protocol. Two polarisation modes are used by the transmitter (Alice) to encode quantum information. The receiver (Bob) uses an independent detection model to infer the encoded bit value [5]. This detection model uses a heterodyne measurement on the state to compare the output with a given threshold value $\tau > 0$. Threshold measurements are described by the *positive operator-valued measure* (POVM) elements $M_H = R_1^H \otimes R_0^V$ and $M_V = R_0^H \otimes R_1^V$, where

$$\begin{aligned} R_0^u &= \frac{1}{\pi}\int_{|\beta|^2 \le \tau} d^2\beta \, |\beta\rangle_u\langle\beta| = \sum_{n=0}^{\infty}(1-\lambda_n)\,|n\rangle_u\langle n| \,, \\ R_1^u &= \frac{1}{\pi}\int_{|\beta|^2 > \tau} d^2\beta \, |\beta\rangle_u\langle\beta| = \sum_{n=0}^{\infty}\lambda_n\,|n\rangle_u\langle n| \,, \end{aligned} \tag{1}$$

with $u \in \{H, V\}$, $\lambda_n = \Gamma[1+n,\tau]/n!$ and Γ the incomplete gamma function. This inference is a key map that identifies a horizontally (vertically) polarised photon following a successful detection associated to the measurement outcome M_H (M_V). Events corresponding to the null outcome $M_0 = I - M_H - M_V$ are discarded and do not contribute to key generation. Alice and Bob repeat this procedure m times. The raw keys are post-processed for parameter estimation, error correction, and privacy amplification, in a manner equivalent to standard BB84.

We use the *entanglement-based* (EB) representation to assess the security of our protocol, where Alice prepares the entangled polarisation state

$$|\phi\rangle_{AA'} = (|H\rangle_A|H\rangle_{A'} + |V\rangle_A|V\rangle_{A'})/\sqrt{2}\,. \tag{2}$$

[*] jsmdrsidhu@gmail.com
[†] cosmo.lupo@poliba.it

A noisy communication channel $\mathcal{N}_{A'\to B}$ maps this state into $\rho_{AB} = I_A \otimes \mathcal{N}_{A'\to B}(|\phi\rangle_{AA'}\langle\phi|)$ where I_A is the identity channel acting on photon A. In the limit of $m \to \infty$, the asymptotic secret key rate rate for collective attacks is given by [9, 10, 11]

$$r = \max_{\tau>0} \min_{\rho_{AB}\in\mathcal{S}} D\left[\mathcal{G}(\rho_{AB})\|\mathcal{Z}(\mathcal{G}(\rho_{AB}))\right] - Qh_2(E)\,, \quad (3)$$

where $D[\cdot\|\cdot]$ is the quantum relative entropy, $\mathcal{G}$ is a partial isometry key map that gives a coherent representation of the measurement and decoding applied by the receiver

$$\mathcal{G}(\rho_{AB}) = (I \otimes K)\rho_{AB}(I \otimes K^\dagger)\,, \quad (4)$$

with

$$K = |H\rangle_{B_1} \otimes \sqrt{M_H} + |V\rangle_{B_1} \otimes \sqrt{M_V}\,, \quad (5)$$

and where $\mathcal{Z}$ is a pinching map that induces complete dephasing to the auxiliary system B_1. The second term in Eq. (3) accounts for the number of bits per photon leaked during error correction and is determined through the gain Q, which defines the probability that Bob obtains a valid measurement output, and the *qubit error rate* (QBER) E, with $h_2(x)$ the binary Shannon entropy. Since the communication channel $\mathcal{N}_{A'\to B}$ is generally unknown, the asymptotic key rate is determined from Eq. (3). The minimisation is constrained over the set $\mathcal{S}$ of feasible states that are compatible with an experimental implementation. These constraints ensure: **(I)** the reduced state of Alice photon remains maximally mixed, **(II)** the gain Bob estimates from experimental data matches the trace of the state $\mathcal{G}(\rho_{AB})$, such that $Q = \mathrm{Tr}[(M_H + M_V)\rho_B]$, **(III)** the experimentally estimated error, c, matches the expectation value $\mathrm{Tr}[(|H\rangle\langle H| \otimes M_V + |V\rangle\langle V| \otimes M_H)\rho_{AB}]/2$, such that $E = 2c/Q$ [12], and **(IV)** experimental estimates for the photon number distribution, P_j, of the unknown state ρ_{AB} obtained by Bob via heterodyne detection [13] matches $P_j = \sum_{a=0}^{j} \mathrm{Tr}[(|a\rangle_H\langle a| + |j-a\rangle_V\langle j-a|)\rho_B]$ up to a certain photon number k. Constraints **(II)-(IV)** define an experimentally feasible optimisation region. The key rate in Eq. (3) is optimised over the detector threshold.

As a first example, we explore the performance of our hybrid protocol over a pure loss channel. The communication channel $\mathcal{N}_{A'\to B}$ is a wiretap channel that induces polarisation-independent loss with transmissivity factor $\eta \in [0,1]$. Since all qubits reaching Bob are secure, we find $Q = D[\rho_{AB}]$ allowing a simple analytic expression for the asymptotic secret key rate $r = Q(1 - h_2(E))$. From this, we find that our hybrid protocol scales as $\mathcal{O}(\eta^2)$ in the limit of large communication distances ($\eta \ll 1$). Most DV and CV protocols are characterised by a linear scaling $\mathcal{O}(\eta)$. The worse scaling of hybrid protocols than discrete-variable ones is due to decreasing gain with increasing range, and is the penalty to pay for improved compatibility with terrestrial networks. This work is the first to quantify this tradeoff that would be instrumental in guiding future research into the use of hybrid protocols for quantum networking. We find the optimal value for the detector threshold is $\tau \simeq 1.59$ at large distances.

For communication channels beyond pure-loss, the key rate must be evaluated numerically using Eq. (3) since we no longer know ρ_{AB}. The security of our protocol becomes challenging on two accounts. First, since the Hilbert space associated with the receiver is infinite-dimensional, a cutoff into a finite-dimensional subspace is required. Despite this, the joint state ρ_{AB} truncated to k photons on Bob's side, scales quadratically with k, maintaining a significant bottleneck for efficient numerical optimisation. Second, such a truncation introduces a cutoff error, which could impact the security of the keys.

We solve both challenges by exploiting symmetries to make the protocol invariant under local *linear-optics passive* (LOP) transformations of the form $(U \otimes U^*)$, where U belongs to the SU(2) Lie group [14]. In the EB representation, this invariance maps any joint state ρ_{AB} into the invariant state,

$$\rho_{AB}^{(\mathrm{inv})} = \int d\mu_U\ (U \otimes U^*)\rho_{AB}(U \otimes U^*)^\dagger\,, \quad (6)$$

where $d\mu_U$ is the Haar measure on the group. Since LOP unitaries are passive, our invariant states are block-diagonal in the photon number basis. The invariant states we derive have a significantly reduced parameterisation from quadratic to linear in the cutoff photon number k. By symmetrising our hybrid protocol, we greatly simplify the security analysis to provide an exact numerical optimisation with full control of the error due to finite-dimensional cut-off, and semi-analytical expressions for the key rate. Explicit expressions for the invariant states associated with different photon number subspaces are derived in our supporting technical manuscript in Ref. [8].

To take advantage of our invariant states, note that Bob will observe a distribution of photon numbers after a general attack. Since the invariant states are block-diagonal in the number basis, we can write

$$\rho_{AB}^{(\mathrm{inv})} = \sum_{j=0}^{\infty} P_j \rho_{1:j}^{(\mathrm{inv})} \geq P_0\rho_{1:0}^{(\mathrm{inv})} + \sum_{j=1}^{k} P_j \rho_{1:j}^{(\mathrm{inv})}(f_j)\,, \quad (7)$$

where $\rho_{1:j}^{(\mathrm{inv})}$ is an invariant state with one photon on Alice side and j photons on Bob side, P_j is the probability of having j, and k is the photon number cutoff. In our supporting technical paper (Ref. [8]), we demonstrate that for $j = 0$ the invariant state associated with the vacuum subspace is unique and for all $j > 0$ there exists a one-parameter family of invariant states, $\rho_{1:j}^{(\mathrm{inv})}(f_j)$, with $f_j \in [0,1]$, which accounts for the second term within the inequality in Eq. (7). Similarly, by linearity, constraints **(II)-(IV)** generalise to a sum over each photon subspace. Since $\mathcal{G}(\rho_{1:j}^{(\mathrm{inv})})$ and $\mathcal{Z}(\mathcal{G}(\rho_{1:j}^{(\mathrm{inv})}))$ have orthogonal support for all $j \neq j'$, the relative entropy in Eq. (3) is the sum of relative entropies evaluated on each photon subspace. By using invariant states, the optimisation of the asymptotic key rate in Eq. (3) for a cutoff photon number k is suppressed from k^2 parameters to k parameters $f_j \in [0,1]$, for $j = 1, \ldots, k$, demonstrating a quadratic speedup.

Our key rate framework can be immediately used to model any general communication channel $\mathcal{N}$. We first consider passive attacks, which preserve the number of photons in the channel thereby limiting the minimisation of the key rate to the vacuum and single-photon subspace on Bob's side $\rho_{AB}^{(\mathrm{inv})} = (1-\eta)\rho_{1:0}^{(\mathrm{inv})} + \eta\rho_{1:1}^{(\mathrm{inv})}(f_1)$, where η is the channel transmissivity. We show it is possible to

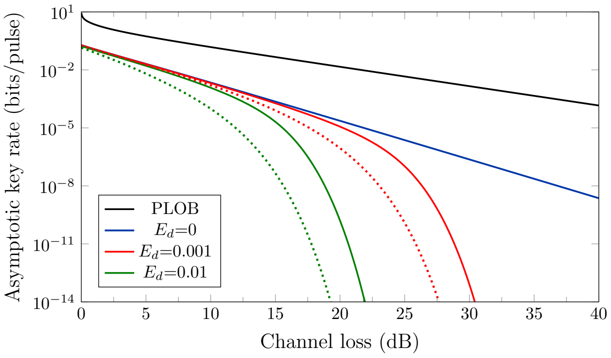


Figure 1: **Protocol comparison**: Asymptotic key rate vs loss (dB) for our symmetrised hybrid protocol (solid lines) and Ref. [5] (dotted lines), for different error probabilities, E_d. Black line illustrates PLOB bound [15].

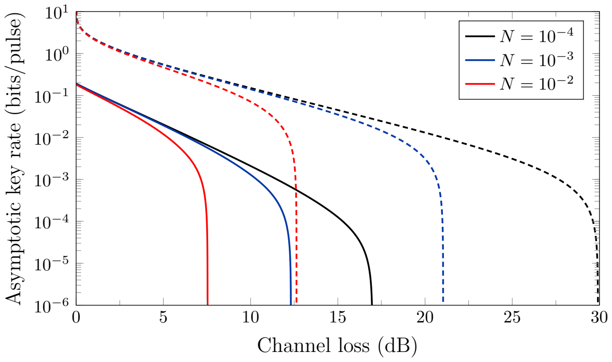


Figure 2: **Comparing with continuous-modulation**: Asymptotic key rates vs loss (dB) for our theory (solid lines) and continuous-modulation CV QKD (dashed lines) for different excess noise, quantified through N.

analytically solve the key rate optimisation in our technical manuscript, where we also derive a solution for f_1 in terms of the two experimentally accessible parameters Q and c. We also use the passive channel to compare the performance of our symmetrised hybrid protocol with the unsymmetrised variant in Ref. [5]. This comparison is illustrated in Fig. 1 as a function of the detector misalignment, quantified by the parameter E_d. The ideal case of $E_d = 0$ reduces the key rate to that of passive attacks and matches the result in Ref. [5]. For practical scenarios with $E_d > 0$, our theory (solid lines) provides higher rates than previous methods (dashed lines) and can also tolerate higher channel losses.

Since electronic noise is a significant challenge for QKD protocols based on coherent detection, we include its effects in a general communication channel to explore the robustness of our hybrid protocol against noisy heterodyne detection. We model electronic noise as a Gaussian noise with zero mean and variance N, which transforms each mode of the field according to map

$$\rho \to \int \frac{d^2\alpha}{\pi N} e^{-|\alpha|^2/N} \mathcal{D}(\alpha)\rho\mathcal{D}(\alpha)^{\dagger}\,, \tag{8}$$

where $\mathcal{D}(\alpha)$ is the displacement operator. Note that this map preserves $(U \otimes U^*)$ symmetry. The communication channel, $\mathcal{N}_{A'\to B}$, we model from Alice to Bob is a Gaussian channel that first applies a pure-loss channel of transmissivity η, followed by mode-wise application of the channel in Eq. (8).

The asymptotic key rate can then be lower bounded with the number of bits per photon leaked for error correction given by $Q_{(3)}h_2[2c_{(3)}/Q_{(3)}]$. The rate must be determined by choosing suitable bounds for both the gain and error parameter, $Q_{(3)}$ and $c_{(3)}$ respectively that do not impact the security. Since the error correction function monotonically increases with both parameters, an upper bound on the number of bits per photon leaked during error correction is obtained from upper bounds on $Q_{(3)}$ and $c_{(3)}$. Suitable upper bounds are derived in our technical paper. Note that in this example, the rate is expected to be tight if the variance N of the Gaussian noise is not too large, a condition that implies a small value for the probability $(1 - \sum_{j=0}^{3} P_j)$.

The key rate is illustrated in Fig. 2. The hybrid protocol is sensitive to excess noise in the detector with $N = 10^{-6}$ closely approximating the ideal scenario of no electronic noise. Suppression of excess noise down to the 10^{-4} regime in CV-QKD is possible through carrier frequency switching [16]. In Fig. 2 we compare the performance of our hybrid protocol with CV QKD. In particular, we used the reverse coherent information from Ref. [17], which gives an upper bound on the key rate achievable in CV QKD with heterodyne detection and reverse reconciliation. For an excess noises of $N = 10^{-4}$, our scheme can tolerate losses up to ∼17 dB, corresponding to an optical fibre transmission of 85 km. The protocol can therefore deliver high-rate QKD in terrestrial or free-space quantum networks over metropolitan scales.

In conclusion, hybrid protocols combine the salient features of DV and CV protocols to adopt mature security proofs and improved compatibility with existing telecommunication infrastructures. Returning to the original motivation of improving the implementation of QKD protocols, our symmetrised hybrid protocol achieves this in a number of ways. First, in contrast to DV QKD, our hybrid protocol allows for the use of faster receivers and does not require sifting since a single decoding measurement applies to both encoding bases. Second, in contrast to CV QKD, our hybrid protocol does not require a shared local oscillator or a pilot tone. This significantly reduces transmitter and receiver complexity and the potential for side-channel attacks [18, 19]. Combined with a key rate optimiser that is closely aligned to an experimental implementation, our work provides a feasible route towards practical implementation of the protocol.

This work introduces several technical results. First, we establish a rigorous security proof under collective attacks to yield a tight lower bound on the asymptotic key rate for single-photon-based hybrid QKD. Second, we introduce a method to derive invariant states by exploiting state symmetries allowing for a quadratic speed-up in the numerical rate optimisation and providing a general utility. We explore the performance of our hybrid protocol within an experimentally feasible parameter space, to show it can deliver high rate metropolitan-scale QKD. We also quantify the tradeoff between hybrid QKD protocols and CV/DV approaches that would be instrumental to guide future research in quantum networking. Collectively, these technical results constitute an advance in understanding the utility of hybrid QKD.

References

[1] S. Pirandola et al. "Advances in quantum cryptography". In: *Adv. Opt. Photon.* 12.4 (Dec. 2020), pp. 1012–1236. URL: http://aop.osa.org/abstract.cfm?URI=aop-12-4-1012.

[2] Jasminder S. Sidhu et al. "Advances in space quantum communications". In: *IET Quantum Communication* 2.4 (2021), pp. 182–217. DOI: https://doi.org/10.1049/qtc2.12015.

[3] Shouvik Ghorai, Eleni Diamanti, and Anthony Leverrier. "Composable security of two-way continuous-variable quantum key distribution without active symmetrization". In: *Phys. Rev. A* 99 (1 Jan. 2019), p. 012311. DOI: 10.1103/PhysRevA.99.012311. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.012311.

[4] Takaya Matsuura et al. "Finite-size security of continuous-variable quantum key distribution with digital signal processing". In: *Nature Communications* 12.1 (2021). DOI: 10.1038/s41467-020-19916-1.

[5] Bing Qi. "Bennett-Brassard 1984 quantum key distribution using conjugate homodyne detection". In: *Phys. Rev. A* 103 (1 Jan. 2021), p. 012606. DOI: 10.1103/PhysRevA.103.012606.

[6] Ignatius William Primaatmaja et al. "Discrete-variable quantum key distribution with homodyne detection". In: *Quantum* 6 (Jan. 2022), p. 613. ISSN: 2521-327X. DOI: 10.22331/q-2022-01-03-613.

[7] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution". In: *Phys. Rev. X* 9 (4 Dec. 2019), p. 041064. DOI: 10.1103/PhysRevX.9.041064.

[8] Jasminder S Sidhu et al. "Security of hybrid BB84 with heterodyne detection". In: *arXiv:2402.16941* (Feb. 2024). DOI: 10.48550/arXiv.2402.16941.

[9] Patrick J. Coles. "Unification of different views of decoherence and discord". In: *Phys. Rev. A* 85 (4 Apr. 2012), p. 042103. DOI: 10.1103/PhysRevA.85.042103. URL: https://link.aps.org/doi/10.1103/PhysRevA.85.042103.

[10] Coles, Patrick J. and Metodiev, Eric M. and Lütkenhaus, Norbert. "Numerical approach for unstructured quantum key distribution". In: *Nature Commun.* 7 (1 May 2016), p. 11712. DOI: 10.1038/ncomms11712.

[11] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. "Reliable numerical key rates for quantum key distribution". In: *Quantum* 2 (July 2018), p. 77. ISSN: 2521-327X. DOI: 10.22331/q-2018-07-26-77.

[12] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* 2nd ed. Vol. 11. Wiley-Interscience, 2006. ISBN: 9780471241959.

[13] Bing Qi, Pavel Lougovski, and Brian P. Williams. "Characterizing photon number statistics using conjugate optical homodyne detection". In: *Opt. Express* 28.2 (Jan. 2020), pp. 2276–2290. DOI: 10.1364/OE.383358. URL: https://opg.optica.org/oe/abstract.cfm?URI=oe-28-2-2276.

[14] P. Aniello, C. Lupo, and M. Napolitano. "Exploring Representation Theory of Unitary Groups via Linear Optical Passive Devices". In: *Open Systems & Information Dynamics* 13 (2006), p. 415. DOI: https://doi.org/10.1007/s11080-006-9023-1.

[15] Stefano Pirandola et al. "Fundamental limits of repeaterless quantum communications". In: *Nature Communications* 8 (1 2017), p. 15043. DOI: 10.1038/ncomms15043. URL: https://doi.org/10.1038/ncomms15043.

[16] Jing Dong et al. "Effective Excess Noise Suppression in Continuous-Variable Quantum Key Distribution through Carrier Frequency Switching". In: *Entropy* 25.9 (2023). ISSN: 1099-4300. DOI: 10.3390/e25091286.

[17] Stefano Pirandola et al. "Direct and Reverse Secret-Key Capacities of a Quantum Channel". In: *Phys. Rev. Lett.* 102 (5 Feb. 2009), p. 050503. DOI: 10.1103/PhysRevLett.102.050503. URL: https://link.aps.org/doi/10.1103/PhysRevLett.102.050503.

[18] Xiang-Chun Ma et al. "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems". In: *Phys. Rev. A* 88 (2 Aug. 2013), p. 022339. DOI: 10.1103/PhysRevA.88.022339.

[19] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution". In: *Phys. Rev. A* 87 (6 June 2013), p. 062313. DOI: 10.1103/PhysRevA.87.062313.

Generation of three-dimensional cluster entangled state

Young-Sik Ra[1] *

[1] *Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, South Korea*

Abstract. Measurement-based quantum computing is a promising paradigm of quantum computation, where universal computing is achieved through a sequence of local measurements. The backbone of this approach is the preparation of multipartite entanglement, known as cluster states. While a cluster state with two-dimensional (2D) connectivity is required for universality, a three-dimensional (3D) cluster state is necessary for additionally achieving fault tolerance.

In this talk, I will present the experimental generation of a 3D cluster state based on the continuous-variable optical platform (arXiv:2309.05437 (2023)). To realize 3D connectivity, we harness a crucial advantage of time-frequency modes of ultrafast quantum light: an arbitrary complex mode basis can be accessed directly, enabling connectivity as desired.

In the second part of my talk, I will discuss another topic: the characterization of multimode quantum channels. Specifically, I will present our recent experiment on the complete characterization of Bosonic Gaussian channels in multiple time-frequency modes.

*youngsikra@gmail.com, qoqi.kaist.ac.kr

Magic-induced computational separation in entanglement theory

Andi Gu,[1, *] Salvatore F.E. Oliviero,[2, †] and Lorenzo Leone[3, ‡]

[1] *Department of Physics, Harvard University, 17 Oxford Street, Cambridge, MA 02138, USA*
[2] *NEST, Scuola Normale Superiore and Istituto Nanoscienze,*
Consiglio Nazionale delle Ricerche, Piazza dei Cavalieri 7, IT-56126 Pisa, Italy
[3] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

This work aims to answer the following question: what is the difference between 'low-magic' entanglement and 'high-magic' entanglement? We take an operational approach to understanding the relationship between magic and entanglement by studying tasks such as entanglement estimation, distillation, and dilution. This approach reveals that magic has notable implications for entanglement. Specifically, we find an operational separation that divides Hilbert space into two distinct regimes: the entanglement-dominated (ED) phase and magic-dominated (MD) phase. Roughly speaking, ED states have entanglement that significantly surpasses their magic, while MD states have magic that dominates their entanglement. The competition between the two resources in these two phases induces a computational phase separation between them: there are sample- and time-efficient quantum algorithms for almost any entanglement task on ED states, while these tasks are provably computationally intractable in the MD phase. Our results find applications in diverse areas such as quantum error correction, many-body physics, and the study of quantum chaos, providing a unifying framework for understanding the behavior of quantum systems.

Keywords: Entanglement theory, Magic-state resource theory, computational phase-transition, computationally bounded observers, entanglement estimation, entanglement cost, entanglement distillation, entanglement reversibility, entanglement witnessing, multipartite entanglement, topological entanglement, entanglement robustness.

This work is based on Refs. [1, 2].

I. Overview

Entanglement serves as a foundational pillar in quantum information theory, delineating the boundary between what is classical and what is quantum [3, 4]. The common assumption is that higher entanglement corresponds to a greater degree of 'quantumness'. However, this folk belief is challenged by the fact that classically simulable operations, such as Clifford circuits, can create highly entangled states [5]. The simulability of these states is suggestive: are there qualitative differences between the 'low-magic' entanglement generated by Clifford circuits, and 'high-magic' entanglement generated by non-Clifford circuits? Perhaps there are finer-grained aspects of entanglement, even in the bipartite case, that cannot be captured by quantifying it along a single axis. For a full understanding of the nature of entanglement in a state, might it be necessary to know something about the state's magic?

Motivated by these questions, this work presents a rigorous investigation on the role of magic in entanglement theory. We take an operational approach to understanding their relationship. While this perspective has long been used to study entanglement [6], the role of magic has never been addressed in such analyses; indeed, there has been no reason to expect that magic has any implications for entanglement tasks. In this work, we show that not only does magic have surprisingly strong implications for entanglement, but we also offer a complete characterization of these implications. We find a sharp operational distinction that splits Hilbert space into two distinct phases: the entanglement-dominated (ED) phase and magic-dominated (MD) phase. Roughly speaking, the ED phase contains states whose entanglement significantly surpasses their magic, while the MD phase corresponds to cases where magic dominates entanglement. These two phases are demarcated by a computational separation induced by the competition between the two resources. That is, there are sample- and time-efficient quantum algorithms that solve a number of entanglement detection and manipulation problems for ED states. Conversely,

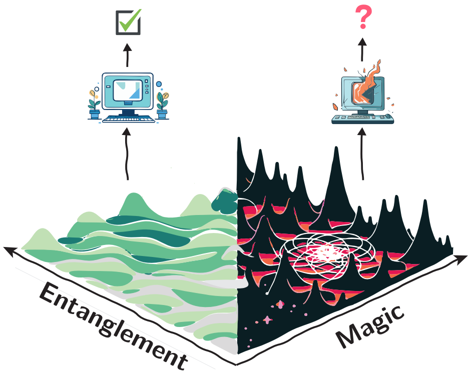


FIG. 1. Entanglement structure of states in the ED and MD phases.

[*] andigu@g.harvard.edu
[†] salvatore.oliviero@sns.it
[‡] lorenzo.leone@fu-berlin.de

we show that entanglement detection and manipulation is provably computationally intractable in the MD phase.

The first problem we study is the ubiquitous task of measuring entanglement entropy. We begin by describing an efficient algorithm to estimate the entanglement entropy of any ED state with vanishing error, even for volume-law states; in contrast, we show that in the MD phase, accurate entanglement estimation is inefficient beyond logarithmic entanglement (below this, the swap test allows for efficient estimation). We then turn to entanglement manipulation — specifically, entanglement distillation and dilution. We show that within the class of ED states, we can always efficiently find a polynomial-depth circuit that distills almost all of the entanglement into Bell pairs. We also prove the converse, which says that, in the MD phase, it is impossible to find such efficient and optimal distillation protocols. This reveals a sharp computational separation in distillable entanglement. Similarly, we demonstrate that we can always identify an efficient dilution protocol that utilizes an optimal number of Bell pairs to prepare any state in the ED phase. Conversely, for MD states, we rule out the existence of an efficient dilution protocol that consumes an optimal number of Bell pairs. These findings reveal a computational separation in entanglement cost between ED and MD states. Combining insights from both entanglement dilution and distillation, we uncover a sharp distinction in the entanglement structure of ED and MD states, illustrated in the ED-MD phase diagram (Fig. 1). Within the ED phase, entanglement is structured in a manner that can always be manipulated efficiently and (almost) reversibly. In contrast, within the MD phase, entanglement manipulation is generally inefficient and irreversible.

As applications of our theory, we present efficient entanglement witnesses for noisy ED states, which in turn reveals that the entanglement of ED states is far more robust than typical states, whose entanglement robustness is limited by the Fannes inequality. We also develop an efficient testing algorithm which can classify states within the ED and MD phases. To conclude, we highlight the relevance of our findings in many-body physics by showcasing a broad class of physically relevant Hamiltonians whose eigenstates are all in the ED phase. As one application of this, we demonstrate the robustness of topological entanglement entropy in 3D topological models such as the X-cube model and Haah's code. We also find connections between stabilizer code Hamiltonians and ED states, which extends the applicability of our results to quantum error correcting codes.

II. Computational ED-MD separation

We first formally define the entanglement- and magic-dominated phases. We note that the majority of states in the Hilbert space are MD. However, it is well-known that most states in Hilbert space also cannot be prepared in polynomial time, hence are irrelevant in practice [7–9]. In contrast, ED states are ubiquitous. For instance, typical Clifford-dominated circuits with $o(n)$ non-Clifford gates (importantly, this far exceeds the classical simulability limit $O(\log n)$) produces ED states almost surely. This is just one example; ED states can be generated by circuits that have up to $o(\exp(n))$ non-Clifford gates. Let us now define ED and MD states, using *stabilizer nullity* ν as a measure of magic [10] and *entanglement entropy* S as an entanglement measure.

Definition 1 (Entanglement and magic-dominated phases)**.** *Let $|\psi\rangle$ be a state with $2^{n-\nu}$ Pauli stabilizers; we say that this state has stabilizer nullity ν. Let $A|B$ a bipartition and let $S(\psi_A)$ be the von Neumann entropy of $\psi_A \equiv \mathrm{Tr}_B |\psi\rangle\langle\psi|$. $|\psi\rangle$ is entanglement-dominated if $S(\psi_A) = \omega(\nu)$, and it is magic-dominated if $S(\psi_A) = O(\nu)$.*

We will study the measurability and manipulability of entanglement in these two classes of states. For entanglement manipulation, there are two tasks: entanglement distillation and dilution. The goal of entanglement distillation is to use LOCC to transform a state ψ into as many Bell pairs M_+ as possible. This number is the *distillable entanglement* of ψ. For the reverse of entanglement distillation, namely entanglement dilution, the aim is to prepare ψ via LOCC using a minimal number of Bell pairs M_-, which is called the *entanglement cost* of ψ.

Theorem 1 (Efficient entanglement measurement and manipulation for ED states)**.** *Let $|\psi\rangle$ be an ED state across the bipartition $A|B$. There exists sample- and time-efficient algorithms for each of the following tasks.*

1. Entanglement estimation: *Estimates $S(\psi_A)$ up to an $o(1)$ relative error.*
2. Entanglement distillation: *Distills M_+ Bell pairs from ψ using LOCC operations, with $M_+/S(\psi_A) = 1 - o(1)$. Unlike more conventional protocols [11], this protocol requires only a single copy of the input state and makes no error: it is a* one-shot, zero error protocol.
3. Entanglement dilution: *Prepares ψ across the bipartition $A|B$ using LOCC, M_- Bell pairs, where $M_-/S(\psi_A) = 1 + o(1)$, and $N_{\mathrm{CC}} = o(S(\psi_A))$ bits of classical communication.*

Theorem 2 (Hardness of entanglement estimation and manipulation for MD states)**.** *There are no sample- and time-efficient quantum algorithms for entanglement characterization and manipulation within the MD phase.*

1. Entanglement estimation*: There is no efficient protocol which can estimate $S(\psi_A)$ to within a constant relative error for arbitrary MD states.*
2. Entanglement distillation*: The (efficient) distillable entanglement for general MD states is $M_+/S(\psi_A) = o(1)$.*
3. Entanglement dilution*: The (efficient) entanglement cost for arbitrary MD states. is $M_-/S(\psi_A) = \omega(1)$.*

Protocol	Entanglement-dominated	Magic-dominated
An efficient state-agnostic protocol which produces an estimate $\tilde{S}(\psi_A)$ of the true entanglement $S(\psi_A)$.	$\frac{\lvert S(\psi_A)-\tilde{S}(\psi_A)\rvert}{S(\psi_A)} = o(1)$	$\frac{\lvert S(\psi_A)-\tilde{S}(\psi_A)\rvert}{S(\psi_A)} = \omega(1)$
An efficient state-agnostic LOCC protocol which distills M_+ Bell pairs from the state ψ.	$M_+/S(\psi_A) = 1 - o(1)$	$M_+/S(\psi_A) = o(1)$
An efficient state-agnostic LOCC protocol which uses M_- Bell pairs to prepare ψ across $A\vert B$.	$M_-/S(\psi_A) = 1 + o(1)$	$M_-/S(\psi_A) = \omega(1)$

TABLE I. Schematic of the ED-MD separation within entanglement theory. Based on Theorem 1 and Theorem 2.

III. Applications of ED-MD separation

Multipartite entanglement distillation. Besides bipartite entanglement distillation, there's also the challenge of multipartite entanglement distillation. In this scenario, if k parties share an entangled state, their goal is to distill some target k-partite entangled state (e.g., a GHZ state) using LOCC operations. Interestingly, it has been established that this task is unachievable for the vast majority of states [12, 13]. However, identifying a generalization of the ED phase in k-partite setting, we show that we can *deterministically* distill many copies of a k-partite GHZ state from ED states using an efficient LOCC protocol.

Entanglement witnessing and robustness. While precisely measuring entanglement can be a challenging and noise-sensitive task, the less ambitious goal of merely witnessing entanglement can be easier and more noise-resilient [14, 15]. The purpose of a witness is to experimentally validate the presence of genuine entanglement in an imperfectly prepared version of the target state. We define an entanglement witness for ED states that can be measured with $O(1)$ sample complexity. We strengthen this result by defining a similar witness for multipartite entanglement. This witness verifies entanglement across k parties — that is, it rules out the possibility of the state being unentangled across any of the k given partitions. As a corollary of this, we find that entanglement for ED states can be far more robust than the entanglement of generic states. The reason for this is as follows. The Fannes inequality roughly says that $|S(\rho_A) - S(\psi_A)| \lesssim n_A T$, where T is the trace distance between ψ and its noisy version ρ. If ψ were a generic state with $S(\psi_A) \sim \sqrt{n_A}$, then we would generally need $T < 1/\sqrt{n_A}$ to guarantee that ρ were not separable across $A|B$. On the other hand, if ψ were in the ED phase, we show that we could tolerate up to $T \lesssim 1 - 2^{-\Omega(\sqrt{n_A})}$, showing that the entanglement within the ED phase is extremely robust.

Phase classification and testing. In light of the clear divide between ED-MD phases, one might ask whether it is possible, given query access to an unknown state $|\psi\rangle$, to determine the phase in which it resides. We formalize this task as a property testing problem and show that the separation between ED-MD phases can indeed be efficiently tested. More precisely, we present a polynomial-time algorithm that can discriminate whether $|\psi\rangle$ is an ED state or it is ϵ-far from any state in the ED phase and, as such, lies in the MD phase.

Applications to physics. We conclude by discussing the implications of our results in the context of many-body physics by first showcasing a broad class of many-body Hamiltonians whose eigenstates are all ED states. We use these Hamiltonians to study the robustness of topological entanglement entropy to perturbations in models such as the X-cube model or Haah's code. Taking advantage of the fact that the topological entanglement entropy in these models scales extensively, we show that this topological entanglement persists under any perturbation to the Hamiltonian that has a subextensive (i.e., $o(n)$) number of terms.

IV. Summary

We believe our findings will captivate the AQIS audience for several reasons. Our work links two ostensibly unrelated quantum resources — entanglement and magic. We rigorously establish the surprising existence of a sharp computational separation, across various entanglement-related tasks, between two classes of states which are characterized by the dominance of either entanglement or magic. We introduce a variety of innovative techniques, including a 'deformed' stabilizer formalism, and a new encoding strategy for pseudorandom quantum states. Moreover, our approach goes beyond the mere information-theoretic framework. The existence of these two phases has strong implications for entanglement detection in noisy experiments. Additionally, our techniques have profound consequences for many seemingly unrelated areas. For instance, we apply our results to many-body physics, showing the robustness of topological entanglement entropy. In summary, this work not only offers a fresh perspective on resource theories but also makes conceptual and theoretical contributions to multiple research areas.

[1] A. Gu, S. F. Oliviero, and L. Leone, Magic-induced computational separation in entanglement theory (2024), arXiv:2403.19610v2, 2403.19610.

[2] A. Gu, S. F. E. Oliviero, and L. Leone, Doped stabilizer states in many-body physics and where to find them (2024), arXiv:2403.14912 [quant-ph].

[3] J. S. Bell, On the Einstein Podolsky Rosen paradox, Physics Physique Fizika **1**, 195 (1964).

[4] J. S. Bell, On the Problem of Hidden Variables in Quantum Mechanics, Reviews of Modern Physics **38**, 447 (1966).

[5] D. Gottesman, The heisenberg representation of quantum computers, talk at, in *International Conference on Group Theoretic Methods in Physics* (1998).

[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Reviews of Modern Physics **81**, 865 (2009).

[7] D. Poulin, A. Qarry, R. Somma, and F. Verstraete, Quantum simulation of time-dependent hamiltonians and the convenient illusion of hilbert space, Physical Review Letters **106**, 10.1103/physrevlett.106.170501 (2011).

[8] E. Knill, Approximation by quantum circuits (1995), arXiv:quant-ph/9508006 [quant-ph].

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[10] M. Beverland, E. Campbell, M. Howard, and V. Kliuchnikov, Lower bounds on the non-Clifford resources for quantum computations, Quantum Science and Technology **5**, 035009 (2020).

[11] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Physical Review A **53**, 2046–2052 (1996).

[12] J. I. de Vicente, C. Spee, and B. Kraus, Maximally entangled set of multipartite quantum states, Physical Review Letters **111**, 10.1103/physrevlett.111.110502 (2013).

[13] D. Sauerwein, N. R. Wallach, G. Gour, and B. Kraus, Transformations among pure multipartite entangled states via local operations are almost never possible, Physical Review X **8**, 10.1103/physrevx.8.031020 (2018).

[14] B. M. Terhal and K. G. H. Vollbrecht, Entanglement of formation for isotropic states, Physical Review Letters **85**, 2625 (2000).

[15] O. Gühne and G. Tóth, Entanglement detection, Physics Reports **474**, 1–75 (2009).

Extended abstract - Pseudomagic quantum states

Andi Gu,[1] Lorenzo Leone,[2] Soumik Ghosh,[3] Jens Eisert,[4] Susanne Yelin,[1] and Yihui Quek[1]

[1] *Department of Physics, Harvard University, Cambridge, MA 02138, USA*
[2] *Department of Physics, University of Massachusetts Boston, Boston, MA 02125, USA*
[3] *Department of Computer Science, University of Chicago, Chicago, Illinois 60637, USA*
[4] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

Notions of nonstabilizerness, or "magic", quantify how non-classical quantum states are in a precise sense: states exhibiting low nonstabilizerness preclude quantum advantage. We introduce 'pseudomagic' ensembles of quantum states that, despite low nonstabilizerness, are computationally indistinguishable from those with high nonstabilizerness. Our work is driven by the observation that only quantities measurable by a *computationally bounded observer* – intrinsically limited by finite-time computational constraints – hold physical significance. Ultimately, our findings suggest that nonstabilizerness is a 'hide-able' characteristic of quantum states: some states are much more magical than is apparent to a computationally bounded observer.

Keywords: Magic-state resource theory, computational indistinguishability, computationally bounded observer, Clifford computation, magic-state distillation, entanglement distillation, stabilizer entropy, quantum chaos, quantum scrambling, quantum cryptography, EFI pairs, property testing

This work is based on Ref. [1].

I. Overview

The delicate and elusive boundary between quantum and classical computation is a central question in current research, with a focus on identifying uniquely quantum resources that contribute to a quantum advantage. One such resource is so-called *magic* ("nonstabilizerness"), which is a measure of the non-Clifford resources needed to prepare a quantum state [2–4]. Among other relations, it has been shown that the amount of magic is directly connected to the hardness of classically simulating a quantum state [5–13], the yield of magic state distillation protocols [2, 14–23], the overhead required for fault-tolerant quantum computation [24–27], and is directly proportional to the degree of chaos in a system [28–31]. Given this multitude of interpretations, one might naturally expect that quantum states with high magic are inherently different, and operationally more non-classical, than states with low magic. This work challenges that intuition. Indeed, we find that the situation can be more intricate than that. We demonstrate the surprising existence of families of states with actually small values of magic while they operationally appear as states with maximum values of magic. We call this phenomenon pseudomagic. In our work, we make a number of contributions that comprehensively elucidate the remarkable implications of this phenomenon, including an *independence theorem* that allows us to tune the magic and entanglement of pseudorandom states independently from one another.

Pseudomagic quantum states are ensembles of states with low magic that are *computationally indistinguishable* in polynomial time from an ensemble of states with maximally high magic. Because they masquerade as maximally-magical ensembles, we say that these ensembles display 'pseudomagic'. Our construction of the low-magic ensembles is simple but powerful: they are simply the *subset phase states* introduced in Ref. [32]. Moreover, their magic can also be finely *tuned*: for any value of magic strictly greater than $\log(n)$ and up to n, we demonstrate the existence of a pseudomagic ensemble with that amount of magic. Our pseudomagic ensembles force us to reconsider quantum chaos, give rise to a fundamental cryptographic primitive and allow us to prove bounds on testing stabilizerness and certain forms of magic-state distillation.

The astute reader may notice that the states that display pseudomagic are the *same* states that display pseudoentanglement [32]. However, this connection is merely a happy coincidence: we show that both the entanglement and magic of these ensembles can be *varied independently* of one another to obtain any legal value of magic and any legal value of entanglement. Here, 'legal' means a value compatible with the defini-

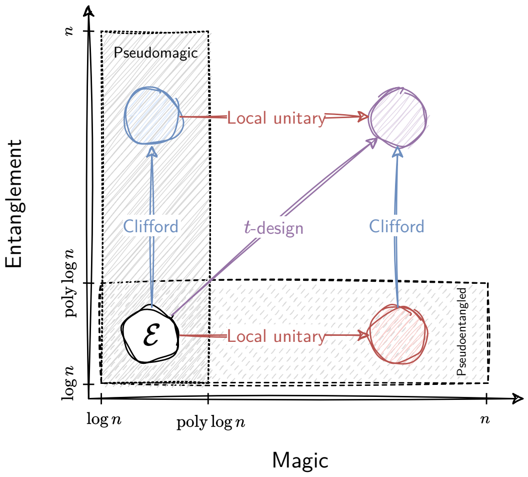


FIG. 1. Efficient conversion of pseudorandom states in all four entanglement/magic quadrants.

tions of pseudomagic or pseudoentanglement. This is not obvious–not even conceptually–as most sufficiently general random states (Haar random states, t-designs, etc) are expected to feature both high entanglement and magic.

Our independence theorem allows us to make a 'lemons-into-lemonade' conceptual shift: the fact that pseudomagic and pseudoentanglement can be tuned independently allows us to strengthen not only our theorems, but also the theorems relating to pseudoentanglement presented in Ref. [32]. Namely, this switch allows us to significantly limit the possibilities for devising efficient algorithms for magic state distillation or nonstabilizerness testing that are tuned to specific levels of entanglement in the input state. Similarly, this imposes limits on entanglement distillation or entanglement testing protocols that are tuned to specific levels of magic in the input states. We expect our independence theorem to be an important tool in the computational study of resource theories in the future.

We end with a meta-perspective. The field of quantum computing is testament to the fact that physics enhances our understanding of what and how we can compute. Our work provides the philosophical counterpart to this statement. It says that computational limits should, conversely, be a sanity check for theoretical physics: if certain physical quantities, say those that purport to assess quantum chaotic behaviour, are in fact not efficiently computationally detectable, in what sense can they be considered real?

II. Pseudomagic quantum states

We start by introducing our central object of study:

Definition 1 (Pseudomagic (informal))**.** *For magic measure $\mathcal{M}$, we say that a pair of n-qubit state ensembles A, B are a pseudomagic pair with gap $(g(n), f(n))$ (where $f(n) > g(n)$) if:*

(a) A is a 'high magic' ensemble $\{|\phi_{k_1}\rangle\}$ such that $\mathcal{M}(\phi_{k_1}) = f(n)$ with high probability over k_1, and

(b) B is a 'low magic' ensemble $\{|\psi_{k_2}\rangle\}$ such that $\mathcal{M}(\phi_{k_1}) = g(n)$ with high probability over k_2;

moreover the two ensembles are indistinguishable by any polynomial time algorithm.

Many distinct magic measures can be used to define pseudomagic. While we elect to primarily use the stabilizer Rényi entropies M_α (for non-negative integer α) in the rest of this work, in the main text, we show that our specific constructions also immediately extend to other measures: robustness of magic [14], stabilizer fidelity [9], stabilizer extent [9] and max relative entropy of magic [33]. We additionally identify conditions that would guarantee that our arguments would go through for a given magic measure.

While we typically use the Haar-random ensemble, which has maximal magic of $\Theta(n)$ with high probability, as the high-magic ensemble, we also construct low-magic ensembles with *tunable* magic – that is, for every value of $g(n)$ not ruled out by computational limitations, we can construct a B displaying that amount of magic. These are known as the *subset phase states*, and are indexed by a binary pseudorandom function f and subset $S \subseteq \{0,1\}^n$ of size 2^k such that $\omega(\log n) < k \leq n$ as $|\psi_{f,S}\rangle = |S|^{-1/2} \sum_{x\in S}(-1)^{f(x)}|x\rangle$. We can control the magic in these states by varying the size of the subset: $M_\alpha(\psi_{f,S}) = O(\log|S|)$. Subset phase states were first introduced in Ref. [32], where it was demonstrated that they also display tunable entanglement depending similarly on the log of the size of the subset. However, we show that for any pseudorandom ensemble, in fact we can tune its entanglement and magic independently, in the following sense:

Theorem 1. *For any value of magic $a \in [poly\log n, n]$, and any value of entanglement $b \in [poly\log n, n]$, there exists an ensemble of states that has magic a and entanglement b with high probability with respect to the states in the ensemble. This ensemble is also indistinguishable from Haar-random states, which have magic $\Theta(n)$ and entanglement $\Theta(n)$.*

The fact that magic and entanglement can be tuned independently of one another is illustrated in Fig. 1. This independence theorem turns out to be a powerful tool that we will exploit to strengthen our applications, which we now describe. Indeed, our general framework allows for a wealth of *further applications.*

III. Applications of pseudomagic

Quantum chaos and scrambling. The resource theory of magic is an essential component of what understanding we have of quantum chaos [34–36]. For a unitary evolution to be deemed as chaotic, meaning it attains the universal (Haar) value of *out-of-time-order correlators* [37, 38], it must necessarily produce maximal $\Theta(n)$ magic [39, 40]. Given that, the mere existence of pseudomagic states suggests the existence of non-chaotic unitaries that nonetheless generate states indistinguishable from those produced by chaotic ones, like Haar random states. We formalize this intuition in the following theorem:

Theorem 2. *Let $\mathcal{E}$ be an ensemble of pseudomagic states that is also pseudorandom. Let $|\psi\rangle \in \mathcal{E}$ and let U such that $|\psi\rangle = U|0\rangle^{\otimes n}$. The $2k$-point OTOCs of U (for $k \geq 4$) are exponentially separated from the Haar value. Therefore, although it generates a state that is on-average computationally indistinguishable from Haar-random, U cannot be considered chaotic.*

In other words, our pseudomagic states are provably not chaotic, even though they are computationally indistinguishable from maximally chaotic Haar random states. This apparently innocuous result carries a profound implication: no physical observer, that is naturally subject to computational limits, can distinguish chaotic from non-chaotic evolution solely based on the observed resultant state.

Implications to resource distillation. We also explore a task of significance for notions of *quantum error correction.* This is the transformation of generic non-stabilizer states into specific, useful non-stabilizer states, such as the canonical magic state vector $|T\rangle$, a task we term as *black-box magic-state distillation.* It is well-known that magic monotones cannot increase under stabilizer operations, imposing a resource-theoretic maximum of the number of distillable magic states from a given starting state. As a preliminary result, we show that this theoretical maximum is a vast overestimate for the output of any *efficient* algorithm.

Theorem 3. *Given a magic monotone $\mathcal{M}$, any efficient stabilizer protocol that synthesizes a state $|B\rangle\langle B|$ from an arbitrary (and potentially also mixed) input state ρ requires $\Omega(\mathcal{M}(|B\rangle\langle B|)/\log^{1+c}\mathcal{M}(\rho))$ copies of ρ, for any constant $c > 0$.*

In short, under this setting, we demonstrate a logarithmic reduction in the 'value' of the magic in the input state. One could contend, however, that our theorem only constrains input state *agnostic* algorithms – whereas many magic state or entanglement distillation protocols are hand-crafted to work on input states with certain assumed structure [2, 41]. Does our lower bound in Theorem 3 still hold up against such tailored algorithms? Could one, as Ref. [42] proposed, distill magic from highly entangled states – if we limit ourselves to computationally efficient distillers? We use our independence theorem 1 to answer in the negative:

Theorem 4. *Consider an entanglement distillation protocol that distills EPR pairs from states drawn from an ensemble $\{\psi_k\}$. For any $f(n) \in [\operatorname{poly}\log n, n]$, even if we are guaranteed that the states ψ_k have magic $\Theta(f(n))$ with overwhelming probability, the protocol can distill at most $O(\log^{1+c} S(\rho))$ Bell pairs with high probability, where $S(\rho)$ is the entanglement entropy of an input state ρ across a bipartition of the system that is linear in n. Similarly, the bound on magic state distillation in Theorem 3 holds even if we are promised that the input state ρ has entanglement $\Theta(g(n))$ across exponentially-many linearly-sized cuts, with any $g(n) \in [\operatorname{poly}\log n, n]$.*

Remarkably, thanks to Theorem 1, it is possible to generalize this theorem to states that display on average *any* amount of magic/entanglement bounded between $\omega(\log n)$ and n.

Other applications A cornerstone of classical cryptography is the *one-way function* (OWF), a function that is easy to compute but challenging to invert. Quantumly, however, OWFs are not essential for certain cryptographic structures to remain secure [43, 44]. Instead, we show that a candidate cryptographic building block known as "EFI pairs" [45] is implied by the bare existence of pseudomagic pairs.

Theorem 5. *Efficiently-generatable pseudo-magic ensembles with stabilizer 1-entropy that can be tuned between $\omega(\log n)$ and n imply EFI pairs.*

Finally, we consider the problem of property testing for non-stabilizerness.

Theorem 6. *Let $0 \leq m < M \leq n$. Any tester for the stabilizer entropy M_α that determines whether for a given state $|\psi\rangle$ $M_\alpha(\psi) \notin [m, M]$ with success proba-*

bility $\geq 2/3$ *requires* $K = \Omega(2^{\frac{m}{4+c}})$ *copies of* $|\psi\rangle$ *for any constant* $c > 0$.

This restriction also extends to a number of other magic monotones, and can be strengthened to hold against non-stabilizerness testers designed for input states with bounded entanglement. We may similarly strengthen the property testing lower bounds in Section 3 of Ref. [32] to hold for input states with bounded magic.

IV. Summary

Pseudomagic highlights the significance of computational limitations in theoretical physics, introducing a unique perspective where the observer plays the main character: from a mere verifier of quantum theories to an integral part of the theory itself. Our insights lay the groundwork for a grand unified theory of 'pseudoresourcefulness' with pseudoentanglement and pseudomagic as special cases. Such a theory would be a modern reinterpretation of the *observer effect* that is at the heart of quantum mechanics: it is not only the information the observer can obtain, but also what she can *process* that matters.

[1] A. Gu, L. Leone, S. Ghosh, J. Eisert, S. Yelin, and Y. Quek, A little magic means a lot (2023), arXiv:2308.16228 [quant-ph].

[2] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[3] M. Howard and E. Campbell, Phys. Rev. Lett. **118**, 090501 (2017).

[4] S. D. Bartlett, Nature **510**, 345 (2014).

[5] D. Gottesman, Stabilizer codes and quantum error correction (1997), quant-ph/9705052.

[6] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).

[7] S. Bravyi and D. Gosset, Phys. Rev. Lett. **116**, 250501 (2016).

[8] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016).

[9] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Quantum **3**, 181 (2019).

[10] J. R. Seddon, B. Regula, H. Pashayan, Y. Ouyang, and E. T. Campbell, PRX Quantum **2**, 010345 (2021).

[11] A. Mari and J. Eisert, Phys. Rev. Lett. **109**, 230503 (2012).

[12] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, New J. Phys. **16**, 013009 (2014).

[13] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New J. Phys. **14**, 113011 (2012).

[14] M. Howard and E. T. Campbell, Phys. Rev. Lett. **118**, 090501 (2017).

[15] J. O'Gorman and E. T. Campbell, Phys. Rev. A **95**, 032338 (2017).

[16] S. Bravyi and J. Haah, Phys. Rev. A **86**, 052329 (2012).

[17] E. T. Campbell and M. Howard, Phys. Rev. A **95**, 022316 (2017).

[18] E. T. Campbell and M. Howard, Phys. Rev. Lett. **118**, 060501 (2017).

[19] E. T. Campbell, Phys. Rev. A **83**, 032317 (2011).

[20] H. Dawkins and M. Howard, Phys. Rev. Lett. **115**, 030501 (2015).

[21] E. T. Campbell and D. E. Browne, Phys. Rev. Lett. **104**, 030503 (2010).

[22] H. Anwar, E. T. Campbell, and D. E. Browne, New J. Phys. **14**, 063006 (2012).

[23] A. Krishna and J.-P. Tillich, Phys. Rev. Lett. **123**, 070507 (2019).

[24] A. Y. Kitaev, Ann. Phys. **303**, 2 (2003).

[25] E. T. Campbell and D. E. Browne, Phys. Rev. Lett. **104**, 030503 (2010).

[26] E. T. Campbell, B. M. Terhal, and C. Vuillot, Nature **549**, 172–179 (2017).

[27] Q. Xu, J. P. B. Ataides, C. A. Pattison, N. Raveendran, D. Bluvstein, J. Wurtz, B. Vasic, M. D. Lukin, L. Jiang, and H. Zhou, Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays (2023), arXiv:2308.08648.

[28] L. Leone, S. F. E. Oliviero, and A. Hamma, Phys. Rev. Lett. **128**, 050402 (2022).

[29] L. Leone, S. F. E. Oliviero, and A. Hamma, Phys. Rev. A **107**, 022429 (2023).

[30] K. Goto, T. Nosaka, and M. Nozaki, Phys. Rev. D **106**, 126009 (2022).

[31] R. J. Garcia, K. Bu, and A. Jaffe, Proc. Natl. Ac. Sc. **120**, e2217031120 (2023).

[32] S. Aaronson, A. Bouland, B. Fefferman, S. Ghosh, U. Vazirani, C. Zhang, and Z. Zhou, Quantum pseudoentanglement (2023), arXiv:2211.00747.

[33] Z.-W. Liu and A. Winter, PRX Quantum **3**, 020333 (2022).

[34] L. Leone, S. F. E. Oliviero, and A. Hamma, Entropy **23**, 1073 (2021).

[35] S. F. E. Oliviero, L. Leone, F. Caravelli, and A. Hamma, SciPost Physics **10**, 76 (2021).

[36] K. Goto, T. Nosaka, and M. Nozaki, Phys. Rev. D **106**, 126009 (2022).

[37] D. A. Roberts and B. Yoshida, JHEP **2017** (4), 121.

[38] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, JHEP **2016** (2), 4.

[39] L. Leone, S. F. E. Oliviero, Y. Zhou, and A. Hamma, Quantum **5**, 453 (2021).

[40] S. F. E. Oliviero, L. Leone, and A. Hamma, Phys. Lett. A **418**, 127721 (2021).

[41] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722–725 (1996).

[42] N. Bao, C. Cao, and V. P. Su, Phys. Rev. A **105**, 10.1103/physreva.105.022602 (2022).

[43] W. Kretschmer (Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021).

[44] T. Morimae and T. Yamakawa, in *Advances in Cryptology – CRYPTO 2022* (Springer Nature Switzerland, 2022) pp. 269–295.

[45] Z. Brakerski, R. Canetti, and L. Qian, On the computational hardness needed for quantum cryptography (2022), arXiv:2209.04101.

Towards practical quantum position verification

George Cowperthwaite[1] Adrian Kent[1 2 *] Damián Pitalúa-García[1 †]

[1] *Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.*

[2] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*

Abstract. We discuss protocols for quantum position verification schemes based on the standard quantum cryptographic assumption that a tagging device can keep classical data secure [1]. Our schemes use a classical key replenished by quantum key distribution. The position verification requires no quantum communication or quantum information processing. The security of classical data makes the schemes secure against non-local spoofing attacks that apply to schemes that do not use secure tags. The schemes are practical with current technology and allow for errors and losses. We describe how a proof-of-principle demonstration might be carried out.

Keywords: quantum position verification, practical quantum cryptography, mistrustful quantum cryptography

Our paper is on the arXiv [2].

Position verification or authentication is a well studied problem in cryptography (e.g., [3]). The task comprises to challenge a tag (or prover) to authenticate its location by sending it communications at light speed, with instructions to process the signals instantaneously and return responses at light speed. If the challenges are sent from several appropriately located test stations (or verifiers), relativistic signalling constraints can ensure that if the tag functions correctly, but at a different location from that expected, this will be detected by the verifiers, because there will necessarily either be time delays or incorrect or missing responses. Realistically, the signals should be sent as close as possible to light speed, the processing should be as fast as possible, and the protocol aims to guarantee location within as small a region as possible.

It has been shown that in a purely classical setting, where the tag only receives and processes classical messages, unconditionally secure position verification cannot be achieved [4]. This is because a set of spoofers surrounding the tag can communicate with the verifiers, faking the intended communication with the tag.

Quantum position verification or authentication (QPV or QPA), also called quantum tagging, was first discussed in a patent [5] published in 2006. In the idealized version, the key idea is that the challenges sent to the tag comprise quantum communications. As spoofers cannot copy quantum information chosen from a non-classical ensemble (for example qubits in BB84 states), quantum tagging schemes are not generally vulnerable to the simple copy-and-redirect spoofing attacks applicable to purely classical schemes [4]. However, they may be vulnerable to other attacks, as we now review.

QPV was first discussed in the academic literature in-Ref. [6], which proposed schemes that were claimed to be unconditionally secure. However, as first pointed out in Ref. [7], although the schemes in Refs. [5, 6] indeed protect against simple attacks that (only) copy and broadcast classical signals and reroute quantum signals, they are vulnerable to teleportation attacks, which effectively simulate the operation of the tag at distant sites. Hence none of them are unconditionally secure.

More generally, Ref. [8] showed that, for any scheme in this general class, the operations carried out by the tag can in principle be simulated (for the verifiers) by spoofers who are located between the tag and verifiers. These spoofing attacks involve non-local quantum computations using pre-distributed quantum entanglement. Since the known attacks require large amounts of pre-distributed entanglement and error-corrected quantum computation, the schemes may guarantee security given presently very credible technological assumptions. Nonetheless, they are not unconditionally secure.

The no-go theorem of Ref. [8] is a theoretically beautiful result, one of several (im)possibility theorems in relativistic quantum information processing that are either based on, or act as counterpoints to, fundamental results in non-relativistic quantum information processing.

However, in many (perhaps most?) plausible scenarios the possibility of quantum teleportation and non-local computation attacks is either unnecessary or insufficient to establish that practical quantum position verification is necessarily insecure. In essence, these non-local attacks establish that spoofers can deceive distant verifiers into believing that a tagging device is present at the expected location, when in fact it is not. But there is an important prior question: do verifiers generally really care about the location of a tagging device *per se*? A quantum tag is essentially a small device that measures and perhaps applies unitaries to incoming quantum states, according to classical instructions, following a fixed public algorithm. As the name suggests, its purported role is to ensure the location of a tagged object or person, and *this* is what the verifiers care about.

This implies that security for any form of quantum tagging or position verification has to be based on some physical assumptions. For example, in principle, the tagging device can be destroyed or removed from the tagged object and replaced by another tagging device that be-

[*] apak@damtp.cam.ac.uk

[†] D.Pitalua-Garcia@damtp.cam.ac.uk

haves identically to the original one. Thus, precluding these attacks must necessarily make some physical assumptions, for example, that such replacement of tagging devices cannot be arbitrarily fast in practice, and that in this way cannot pass unnoticed by the verifiers.

Since we need physical assumption anyway, we consider tagging schemes based on a standard assumption in classical and quantum cryptography, that it is possible to store secret classical data. This assumption seems particularly justifiable in scenarios aiming to verify that the location of the tagged object or person is within a highly secure perimeter, for example, a military base or a bank branch. In these scenarios, it is usually necessary that such perimeters are able to store secret information securely. In particular, this is a standard cryptographic requirement if such locations are able to communicate secretly with other locations (for example, with other bank branches or other military bases).

Ref. [1] introduced tagging schemes that are unconditionally secure, modulo this assumption, in the sense that the tag itself cannot (except with small probability) be spoofed or replaced so long as it remains intact and the data it contains remains secret. In this paper, we explore further versions of this scheme with a security analysis and discuss their practical implementation.

In our paper, we present schemes for position verification in which the position verification queries and responses are purely classical, involving no quantum communication or quantum information processing. These communications are authenticated using a key previously shared between the prover and verifiers. Quantum information transmission and measurement is required only to refresh the key via quantum key distribution. Our schemes are practical to implement with current technology. Their security is based on a standard assumption in quantum cryptography, also made in QKD, that a classical key can be stored securely (by the prover in our schemes), as initially proposed in Ref. [1].

When QPV schemes use position verification queries and/or responses that involve quantum communications, they typically use photons to encode quantum states. This poses challenges, including errors in state preparation, processing and measurement, losses, and security problems due to imperfect single-photon sources and single-photon detectors (e.g., photon-number splitting attacks [9, 10] and multiphoton attacks [11]) and side-channel attacks (e.g., [11]). The problem of losses is particularly challenging in schemes with large distances between the tagging device and the verifiers. An advantage of our schemes is that the queries and responses are purely classical. Quantum communications are needed only to replenish the key via QKD, which is secure against errors and losses. Moreover, the QKD communications, unlike the position verification queries and responses, are not tightly time constrained.

Given our assumptions, our schemes are secure against arbitrarily powerful quantum spoofers, who may share an arbitrary amount of entanglement. This is also an advantage compared to the best known quantum schemes, which have only been proved secure against spoofers that share an amount of entanglement linear in the classical information [12, 13].

References

[1] A. Kent. Quantum tagging for tags containing secret classical data. *Phys. Rev. A*, 84(2):022335, 2011.

[2] G. Cowperthwaite, A. Kent and D. Pitalúa-García. Towards practical quantum position verification. arXiv:2309.10070, 2023.

[3] S. Capkun, M. Cagalj and M. Srivastava. Secure Localization with Hidden and Mobile Base Stations. In *Proc. IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pages 1–10, 2006.

[4] N. Chandran, V. Goyal, R. Moriarty and R. Ostrovsky. Position based cryptography. In *CRYPTO '09, S. Halevi, ed., Lecture Notes in Comput. Sci. 5677*, pages 391–407, 2009.

[5] A. P. Kent, W. J. Munro, T. P. Spiller and R. G. Beausoleil. Tagging systems. US Patent No. US20060022832A1, 2006.

[6] R. A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81(4):042319, 2010.

[7] A. Kent, W. J. Munro and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, 2011.

[8] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky and C. Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM J. on Comp.*, 43(1):150–178, 2014.

[9] B. Huttner, N. Imoto, N. Gisin and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, 1995.

[10] G. Brassard, N .Lütkenhaus, T. Mor and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, 2000.

[11] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent and D. Pitalúa-García. Multiphoton and side-channel attacks in mistrustful quantum cryptography. *PRX Quantum*, 2(3):030338, 2021.

[12] A. Bluhm, M. Christandl and F. Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nat. Phys.*, 18:623–626, 2022.

[13] L. Escolà-Farràs and F. Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Phys. Rev. Lett.*, 131(14):140802, 2023.

Towards practical quantum position verification

George Cowperthwaite,[1] Adrian Kent,[1, 2, *] and Damián Pitalúa-García[1, †]

[1] *Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.*

[2] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada.*

(Dated: November 14, 2023)

We discuss protocols for quantum position verification schemes based on the standard quantum cryptographic assumption that a tagging device can keep classical data secure [1]Our schemes use a classical key replenished by quantum key distribution. The position verification requires no quantum communication or quantum information processing. The security of classical data makes the schemes secure against non-local spoofing attacks that apply to schemes that do not use secure tags. The schemes are practical with current technology and allow for errors and losses. We describe how a proof-of-principle demonstration might be carried out.

I. INTRODUCTION

The task of quantum position verification or authentication (QPV or QPA), also called quantum tagging, was first discussed in a patent [2] published in 2006. In the idealized version, the key idea is to challenge a tag (or prover) to authenticate its location by sending it quantum and classical communications at light speed, with instructions to process the signals instantaneously and return responses at light speed. If the challenges are sent from several appropriately located test stations (or verifiers), relativistic signalling constraints can ensure that if the tag functions correctly, but at a different location from that expected, this will be detected by the verifiers, because there will necessarily either be time delays or incorrect or missing responses. Realistically, the signals should be sent as close as possible to light speed, the processing should be as fast as possible, and the protocol aims to guarantee location within as small a region as possible.

As spoofers cannot copy quantum information chosen from a non-classical ensemble (for example qubits in BB84 states), quantum tagging schemes are not generally vulnerable to the simple copy-and-redirect spoofing attacks applicable to purely classical schemes. However, they may be vulnerable to other attacks, as we now review.

QPV was first discussed in the academic literature in Refs. [3, 4], which proposed schemes that were claimed to be unconditionally secure. However, as first pointed out in Ref. [5], although the schemes in Refs. [2–4] indeed protect against simple attacks that (only) copy and broadcast classical signals and reroute quantum signals, they are vulnerable to teleportation attacks, which effectively simulate the operation of the tag at distant sites. Hence none of them are unconditionally secure.

More generally, Ref. [6] showed that, for any scheme in this general class, the operations carried out by the tag can in principle be simulated (for the verifiers) by spoofers who are located between the tag and verifiers. These spoofing attacks involve non-local quantum computations using pre-distributed quantum entanglement. Since the known attacks require large amounts of pre-distributed entanglement and error-corrected quantum computation, the schemes may guarantee security given presently very credible technological assumptions. Nonetheless, they are not unconditionally secure.

The no-go theorem of Ref. [6] is a theoretically beautiful result, one of several (im)possibility theorems in relativistic quantum information processing (e.g., [7–16]) that are either based on, or act as counterpoints to, fundamental results in non-relativistic quantum information processing (e.g. [17–24]).

However, in many (perhaps most?) plausible scenarios the possibility of quantum teleportation and non-local computation attacks is either unnecessary or insufficient to establish that practical quantum position verification is necessarily insecure. In essence, these non-local attacks establish that spoofers can deceive distant verifiers into believing that a tagging device is present at the expected location, when in fact it is not. But there is an important prior question: do verifiers generally really care about the location of a tagging device *per se*? A quantum tag is essentially a small device that measures and perhaps applies unitaries to incoming quantum states, according to classical instructions, following a fixed public algorithm. As the name suggests, its purported role is to ensure the location of a tagged object or person, and *this* is what the verifiers care about.

In one scenario commonly considered in the literature, a position verification protocol is defined to allow a prover to prove their location (L) to distant verifiers. The protocol is said to be insecure if spoofers at other locations (not including L) can simulate the actions of an honest prover when the prover is in fact absent. This is an important scenario, which captures the type of insecurity established by the results of Refs. [5, 6].

However it is also important to keep in mind that there are other interesting scenarios. For example, the prover might be mislocated but still active, with spoofers using

[*] apak@cam.ac.uk

[†] D.Pitalua-Garcia@damtp.cam.ac.uk

the prover's actions as part of their spoofing strategy in order to persuade the verifiers that the prover remains at L. The prover here might be oblivious to their mislocation (having wandered or been unwittingly deceived about their location), or might be cooperating with the spoofers (if, for example, they are a tagged prisoner attempting to escape confinement with outside help).

It is also crucial to note that the term "prover" is ambiguous and potentially misleading when considering practical applications. As used in theoretical analyses, it generally represents the actions of a proving device (i.e. some form of tag). However, the term suggests a person or agent. If Bob carries a mobile device to respond to challenges from Alice's various verifying stations, but he and the device are separable, then the protocol may verify the device's location but not his.

Moreover, to the extent that QPV protocols in the prover-verifier model are secure (given suitable technological bounds on the spoofers), they only establish the location of *a* suitable tagging device, not necessarily *Bob's* tagging device. Any substitute device with the same functionality can implement the protocol correctly. We emphasize that, in the scenario under discussion, the spoofers know every detail of the tagging device's operations: the teleportation attacks of Ref. [5] and the more general non-local computation attacks of Ref. [6] require this. So, if these attacks apply, constructing an identical tag is indeed an option for the spoofers.

Now, if spoofers want to deceive verifiers that someone or something is somewhere they are not, it is presumably either because the object or person has been destroyed or has been moved, or encouraged or deceived (perhaps by GPS spoofing) into moving, to the wrong location. To achieve this, one option is to detach the tag and leave it in position, while dislocating the taggee. Another is to dislocate or destroy both tag and taggee, leaving an identical replica tag in the required position. Either way, the verifiers are left with the false impression that the tagged object remains in place, while in fact they have been untagged and/or dislocated and/or destroyed.

It is true that, if the spoofers dislocate a tag but leave it operational, it may continue to receive and respond to at least some of the verifiers' signals, and this might alert them to interference. Alternatively, some alarm device on the tagged object might alert the verifiers by signalling to them, or the tagged person might do so (in scenarios where they are cooperating with the verifiers). But note that these are also issues if spoofers apply teleportation or non-local computation attacks. To apply these, the spoofers must intercept (at least) quantum signals from the verifiers and use these to generate their spoofed responses. The prover will thus either not receive the quantum information components of their challenges (in which case they might send an alarm signal) or else spoofed quantum information components generated by the spoofers. These spoofed quantum information components may be drawn from the same distribution as the original challenges but will not be identical to them. So, the prover's responses will not generally be valid for the original challenges. If these responses reach the verifiers, they will, again be alerted.

However, in both cases, the spoofers can in principle prevent any alarm or false responses reaching the verifiers by screening the first tag and object/person, jamming all possible communications between them and the verifiers. We emphasize, though, that they also need to do this if they apply teleportation [5] or non-local computation [6] attacks, if the tag/object/person is dislocated but not destroyed. So the need for jamming does not differentiate between these attacks and pure dislocation attacks.

There are conceivable scenarios that do differentiate between these attacks. For example, the prover could be in a region that the spoofers can surround, and signal into, but not enter. The spoofers may be able to spoof GPS within the region, causing the prover to move to the wrong location. They may also be able to spoof the prover's responses to the verifiers using teleportation or non-local computation attacks, giving the verifiers the impression that the prover is at the correct location. And they may be able to jam any communication from the prover to the verifiers, so that the verifiers receive only the spoofed responses. However, the spoofers may not be able to apply direct attacks involving physical dislocation or detachment. The security assumptions here are somewhat delicate, because the spoofers must be able to send physical signals into the region in order to spoof the prover's GPS, but the power of anything they send into the region must be limited. They might perhaps be assumed to be able to send low-energy microwave and radio signals into the region but not, for instance, robots. This scenario requires quite strong and specific physical limitations on the spoofers, and so evidently does not allow unconditional cryptographic security.

More generally, precluding object dislocation/destruction and tag detachment/substitution attacks inevitably requires physical assumptions. For example, it must be hard to detach, destroy or move the tag quickly enough that the tagging protocol can continue with a substitute tag without an interruption being evident. The light speed signalling bound does give an unconditional constraint on movement. For example, a tag responding every microsecond could be moved no more than $\approx$ 300m between responses. However, the signalling bound gives no effective unconditional constraint on attacks involving destruction and replacement: in principle, a tag could be progressively destroyed on one side and replaced on the other side of a boundary that moves at near light speed, without detection. Defences against such attacks must be based on physical assumptions that cannot be unconditionally guaranteed. Also, in many scenarios, the light speed movement bound may be too weak, and stronger bounds again rely on further physical assumptions (for example, that the tag cannot be moved faster than the speed of sound, or perhaps than the fastest aeroplane developed to date).

In summary, security for any form of quantum tagging or position verification has to be based on some physical assumptions. We emphasize that this is not only because of non-local computation attacks, which can only be precluded by technological assumptions bounding the power of spoofers. Dislocation/destruction and detachment/substitution attacks can also only be precluded by physical assumptions on the properties of the tag (and its attachment).

Given that we need such assumptions anyway, there are strong reasons for exploring tagging schemes based on a physical assumption that is standard in classical and quantum cryptography, namely that a piece of infrastructure (in this case the tag) is able to store secret classical data. Ref. [1] introduced tagging schemes that are unconditionally secure, modulo this assumption, in the sense that the tag itself cannot (except with small probability) be spoofed or replaced so long as it remains intact and the data it contains remains secret. In this paper, we explore further versions of this scheme and discuss their practical implementation.

II. SECURITY SCENARIO

We assume that the verifiers, referred to collectively as Alice and individually as $A_1, \ldots, A_M$, and the prover (Bob), are human or other agents, all of whom trust one another. They have a fixed agreed reference frame F. For simplicity, we assume that Bob is supposed to remain at a constant location during the position verification scheme. We assume that Alice has some prior unreliable knowledge of Bob's location (e.g. a reported GPS reading from Bob, or knowledge of a pre-agreed location which Bob is supposed to reach), and wishes to verify it to within as small an error margin as possible, at some sequence of times T_j, for $j = 1, \ldots, N$. We assume that the A_i can communicate with each other via authenticated channels.

In this simple scenario, the aim of the scheme is that, if Bob does remain at a fixed location L during the scheme, he can allow Alice to verify that he is close to L at the given times. In more general scenarios, Bob may move (perhaps up to some speed bound), and the aim may be to identify his position (up to some uncertainty) at any given time. The protocols we describe can be adapted to these more general scenarios, but for clarity we focus here on the simple scenario.

Position verification is non-trivial because of the potential presence of adversaries, who may interfere with, jam, or substitute signals between Alice and Bob. They may also apply physical attacks – for example physically dislocating Bob.

We assume spacetime is Minkowski, as is approximately the case near the Earth surface. The small general relativistic corrections required can easily be allowed for if needed (i.e. if they are significant enough), but we ignore them here. Our discussions assume an asymmetry between Alice, whose agents A_i each are within and control separate secure laboratories, which we might imagine as well-resourced fixed bases, and Bob, who is a single agent in a single laboratory. To simplify the discussion, we suppose Alice has a master agent, A_0, with whom the A_i communicate: A_0 may be A_i for some i, or at a separate location. We assume the locations of Alice's laboratories are reliably known to A_0 and that all Alice's agents (including A_0) have reliable clocks within their laboratories that are all synchronized. We also assume that Alice's laboratories are robust and secure enough that destruction/dislocation attacks on them are not a concern – or at least, that it is a reasonable working assumption that such attacks will not succeed, perhaps because if they did then the loss would be so devastating that the failure to verify Bob's location securely becomes irrelevant. However, Bob cannot directly verify his position: there is no trusted global GPS and any incoming reference data he might use could be spoofed. His laboratory may also be technologically more limited than Alice's and may be vulnerable to destruction/dislocation attacks.

The A_i are at separate sites that are also separated (and may be quite distant) from the location L, which lies within their convex hull. We can consider 1D or 2D position verification, which assume that Bob and the A_i are constrained to lie on a given line or plane. In the 3D case, there is no such constraint, of course. In d dimensions, we must have $M \geq (d+1)$ to satisfy the convex hull condition. The A_i send classical or quantum signals at appropriate times. They receive classical or quantum signals from Bob and verify that these are the prescribed responses (up to a stipulated error rate) and are received at the correct times (up to stipulated timing errors).

Following Ref. [1], we additionally assume that B and the A_i can keep some classical information secure within their respective laboratories, i.e. that adversaries cannot obtain this information unless and until the relevant agent chooses to transmit it outside their laboratory. We assume this holds true even if adversaries are able to move or destroy Bob's laboratory. While this is a strong assumption, it is a standard one in quantum key distribution (QKD) and other areas of cryptography. It effectively counters replacement attacks, since if a tagging device within Bob's laboratory contains a significant amount of secret information, adversaries have only a small probability of constructing an identical replacement.

More precisely, there is only a small probability that *any given attempted replacement* will be identical. Adversaries could construct a set of replacements R_i, where R_i contains key k_i, so that each possible key is contained within one of the replacements. This guarantees that the tag has been precisely replicated, but does not give the adversary a way of identifying which replacement is the replica, and does not facilitate a useful spoofing attack. Even for a relatively short key of 62 bits (as in the security analysis provided in section V), a successful attack of this form requires $2^{62} \approx 10^{18}$ replacements.

III. SCHEME 1: BOB CAN KEEP A CLASSICAL KEY SECRET BUT HAS NO TRUSTED CLOCK

We work with the following slight variation of the scheme of Ref. [1]. Let Alice have M agents $A_1, \ldots, A_M$ surrounding the expected location L of Bob. We assume this expected location L is initially known to Alice, and may not necessarily be known to Bob. We assume that in the absence of adversarial interference L is fixed throughout the position verification protocol, i.e. that Bob remains stationary.

Alice and Bob agree on a sufficiently large integer n, and on a sufficiently small tolerable error rate $0 \leq \gamma << 1$, which act as security parameters. In this scheme we assume Bob does not possess a trusted clock.

We simplify the description by making the idealized assumption that all communications take place at or near the speed of light through vacuum, which we denote by c. The scheme tolerates small delays, at the cost of reducing the precision to which Alice can verify Bob's precision.

In essence, the scheme requires Alice and Bob to authenticate to each other using previously distributed secret keys. For all $i = 1, 2, \ldots, M$, Alice's agent A_i and B perform the following actions.

1. At some time prior to the position verification protocol, A_i and B share a secret key $k_i = \{k_{i1}, \ldots, k_{iN}\}$, where each substring k_{ij} has n bits, and N is as large as required. They keep this secret from eavesdroppers, although A_i may share it securely with other A_j. The key sharing may be done arbitrarily far in advance. Let $k_{ij} = (q_{ij}, r_{ij})$, where q_{ij} and r_{ij} are sub-strings of k_{ij} comprising the first m bits and the last $(n - m)$ bits of k_{ij}, respectively. Here 'q' and 'r' stand for 'query' and 'reply'. For simplicity, we assume the key-sharing is error-free, i.e. that A_i and B have identical versions of k_i. This can be achieved, with high probability, by standard key reconciliation methods. A small allowed key sharing error rate can also be incorporated in the error-tolerant ($\gamma > 0$) versions of the position verification protocol, as described below.

2. A and B may also, prior to the position verification protocol, share a separate secret key k. This key may be expanded as and when needed by QKD, if A and B have the appropriate resources, and used to extend the secret keys k_i (i.e. to increase the number of substrings N).

   The position verification protocol typically involves many rounds of queries and replies. We describe here round j.

3. Each A_i sends query-message-ij, comprising the plain text 'Query ij' followed by q_{ij} (the query substring of k_{ij}) to B. The messages are sent at light speed, timed so that they should arrive at location L at time T_j. The messages are sent in such a way that, in the absence of interference, they can be distinguished even if they arrive simultaneously. For example, they may be sent using different frequencies, or using a code that allows superimposed classical messages to be distinguished.

4. B processes the messages purportedly received from the various A_i sequentially, using some ordering algorithm for distinguishable messages received simultaneously. We thus, in the next step, describe his response to a single message in the sequence.

5. B receives the message ('Query ij'',$q'_{ij'}$), purportedly from A_i. Because of possible adversarial interference, we do not assume that $j' = j$, even if the message arrives at T_j, nor that A_i has in fact sent query-message-ij, nor that $q'_{ij'} = q_{ij'}$. B keeps a register R_i recording the second index j of the last query-message-ij that he received and validated with first index i. If $R_i = (j'-1)$, then B sets R_i to j'. If not, he aborts the protocol (i.e. does not continue with the steps below) and stops responding to any future queries. (Here and below, we give the simplest response to detection of an apparent spoofing. B stops communicating; the A_i become aware that the protocol has failed; they presumably take appropriate action. Of course, other ways of proceeding are possible and in some circumstances preferable. For example, B may continue to respond to valid queries so long as the proportion of invalid queries is smaller than some pre-agreed threshold. With suitable adjustments of security parameters, this modified protocol can continue to give useful security guarantees.)

6. B checks whether the Hamming distance $d(q'_{ij'}, q_{ij'}) \leq \gamma m$. If so, he accepts the query as authentic. If not, he aborts, as above.

   Timing: If B is indeed at location L, the messages arrive at time T_j, and his authentication takes place within the time interval $[T_j, T_j + \delta_1]$, where δ_1 is the processing time required.

7. If B authenticates the query purporting to come from A_i in the previous step, he sends the plain text 'Reply ij'' followed by $r_{ij'}$ (i.e, the reply sub-string of $k_{ij'}$) to A_i. Otherwise B does not respond, and accepts no subsequent queries from any A_i, even if they are authenticated.

   Depending on which option is more technologically convenient, B either broadcasts his response to all the A_i. or sends it just to the agent A_i identified by the authenticated Query ij'. (Note that it is possible that A_i is not the sender even though Bob has authenticated the query.) We call these respectively the *broadcast* and *narrowcast* versions of the protocol. In the broadcast version, if B broadcasts simultaneous messages to more than one A_i, the messages are sent in such a way that, in the absence of interference, they can be distinguished even if they arrive simultaneously (as above).

Timing: If B is indeed at L, he sends his reply by the time $T_j + \delta_1 + \delta_2$, where δ_2 is the time taken by B to transmit.

8. In the narrowcast version, suppose that A_i receives ('Reply $i'j'$', $r'_{i'j'}$), purportedly from Bob. If $i = i'$, and $j' = j$ (where j is the current round, i.e. A_i has received and authenticated replies from all rounds $k < j$), A_i verifies that the Hamming distance $d(r_{ij}, r'_{ij}) \leq \gamma(n - m)$ and that she has received the reply r'_{ij} not later than the time $T_j + \frac{d_i}{c} + \delta_L$, where δ_L has been agreed in advance by Bob and Alice and must satisfy $\delta_L \geq \delta_1 + \delta_2$. If so, she accepts the reply as authentic and sends the confirmation message '$s_{ij} = 1$' via an authenticated channel to the master agent A_0. Otherwise, she sends the message '$s_{ij} = 0$'.

   In the broadcast version, A_i ignores all messages not of the form ('Reply ij'', $r'_{ij'}$) for some string r' and some j'. That is, A_i considers only replies apparently addressed to her. For those messages, she follows the verification steps for j' and r' above, and sends confirmation messages as above.

   Timing: If B is indeed at L, then A_i authenticates his reply by the time $T_j + \frac{d_i}{c} + \delta_1 + \delta_2 + \delta_3$, where d_i is the distance from L to A_i and δ_3 is the time taken for A_i to authenticate. She sends her confirmation message at time $T_j + \frac{d_i}{c} + \delta_1 + \delta_2 + \delta_3 + \delta_4$, where δ_4 is the time taken by Alice to generate and transmit the confirmation message.

9. If A_0 receives $s_{ij} = 1$ and authenticates it as a message from A_i for all $i = 1, 2, \ldots, M$, then she authenticates that the location of B at time T_j was L, within some position uncertainty given by $c\delta_L$. If she receives $s_{ij} = 0$ for some i then the position verification in round j fails.

   Timing: Suppose that the authenticated channel from A_i to A_0 had length d'_i and that messages travel on it at speed $c'_i \leq c$. A_0 completes the authentication by the time

$$T_A = T_j + \max_i \left\{ \frac{d_i}{c} + \frac{d'_i}{c'_i} \right\} + \delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5 \,,$$

   where δ_5 is the time taken for A_0 to compute whether all confirmation messages satisfy $s_{ij} = 1$.

Comments on Geometry: A successful verification by A_i guarantees that, at time T_j, B was within a ball B_i with A_i at the centre, with radius $d_i + c\delta_L$. Using the information of her agents, A_0 can verify B's location to have been within the intersection of the balls $B_1, \ldots, B_M$. In the ideal case $\delta_L = 0$, this intersection is exactly the location L. Thus, by increasing M, and appropriately locating Alice's agents we can reduce the uncertainty of B's location in the verification scheme.

Note that a proof of principle implementation for 3D position verification could be carried out for $M = 2$, with A_1 and A_2 approximately collinear with L, on opposite sides of L. If the collinearity is a good approximation, this may verify location to good precision. The precision is greater if we may assume A_1, A_2 and B are constrained to lie exactly on a line, so that we effectively carry out position verification in 1D.

An implementation with $M = 1$ can only guarantee that B is within a ball surrounding Alice's sole agent A_1. Nonetheless, implementation of $M = 1$ would allow a proof of principle test of the technology, since we can extrapolate the results to $M > 1$ and estimate the precision that would be obtained for any given configuration of the A_i and B.

Comment on key lengths and error tolerance: It may be useful to vary the key lengths in some scenarios, so that k_{ij} has length n_{ij}. It may also be useful to allow the error thresholds to vary, so that communications in round j from A_i to B have threshold $\gamma_{ij}^{\rightarrow}$, and from B to A_i have threshold $\gamma_{ij}^{\leftarrow}$. For simplicity we consider fixed n and γ in our discussion.

IV. TIME DELAYS OF SCHEME 1

We identify three main types of time delays.

1. $\Delta_L = \delta_1 + \delta_2$ provides the uncertainty in A_i's estimate of $d(A_i, L)$, assuming that she is confident of the value of δ_3, which is determined by her own equipment. (In practice there will presumably be at least slight uncertainties in δ_3. We neglect these for simplicity; they can be included in the calculation of Δ_L if significant.) We would like to make Δ_L as short as possible in order for the location L to be verified as precisely as possible. As mentioned above, we require $\Delta_L \leq \delta_L$.

2. $\Delta_V = \delta_3 + \delta_4 + \delta_5$ comprises the delay that A_0 takes in learning A_i's estimate $d(A_i, B)$, after A_i receives B's response. During the interval $\Delta_L + \Delta_V$, B could be displaced, with A_0 learning this (if at all) only later. So we would also like to make Δ_V as short as possible, all else being equal.

3. Δ_R denotes the time difference between one verification and the following one, where R denotes 'repetition'. All else being equal, we would like to repeat the location verification protocol as frequently as possible and thus minimize Δ_R.

The relative importance of minimizing Δ_L, Δ_V and Δ_R, and the value of tradeoffs among them, depends on the scenario. One factor is whether Bob's potential displacement (either by wandering or by the action of adversaries) is bounded only by c, or whether in practice a significantly lower bound (such as the speed of sound in air, or the speed of the fastest planes currently available) is justified.

V. SOME POSSIBLE ATTACKS ON SCHEME 1

Our security analysis below applies for arbitrarily powerful spoofers, who might have arbitrarily advanced quantum technology and who could share an arbitrarily large amount of entanglement. Our analysis is based on the assumption that Bob can keep classical information secret from spoofers. The assumption that collaborating parties have laboratories in which they can keep data secure is standard (and necessary) for quantum key distribution schemes and many other quantum cryptographic protocols. We believe it is equally reasonable in many scenarios in which position verification is required. Nonetheless, it is ultimately a technological assumption, whose validity should be examined in any given application and scenario.

A. Desynchronizing Alice's clocks

As mentioned above, Alice's agents must keep their laboratories securely synchronized to a common reference frame F during the verification scheme. We assume they trust their locations. This is reasonable in scenarios in which Alice has a secure and stable infrastructure. They also require secure clock synchronization. This is a general issue in relativistic quantum cryptography. In practice, it is often partially addressed by keeping clocks synchronized using GPS devices within the required time uncertainty [25–29]. However, adversaries may spoof the GPS signals [30], desynchronizing Alice's clocks.

To defend against such attacks, the A_i may initially synchronize their clocks in a single secure laboratory (for example A_0's) and then displace these securely to their separate laboratories. To counter clock drift, this process could in principle be repeated at suitably short intervals during the protocol, ensuring that the A_i's clocks are repeatedly re-synchronized with new incoming synchronized clocks. Note that this requires not only a supply of accurate clocks, but also secure distribution channels that ensure the clocks remain very well synchronized as they are distributed.

B. Impersonating Alice and Bob

The spoofer may have multiple agents S_k at separate locations: we refer to them collectively as S. The spoofer S could try to impersonate B in an strategy that combines spoofing A_i to B, with the aim of learning the strings r_{ij}, and spoofing B to A_i. We consider this for a single A_i; the discussion obviously extends to multiple agents.

Suppose that rounds up to $(j-1)$ have been honestly completed by A_i and B. Before B receives A_i's communication for round j, S could send the plain text 'Query ij' to B followed by some string q'_{ij} of m bits. Assuming S has no previous information about q_{ij}, with probability 2^{-m}, $q'_{ij} = q_{ij}$ and B sends r_{ij} to S. S can then send r_{ij} to A_i, impersonating B when A_i later sends the authentic 'Query ij' with string q_{ij}.

With probability $1-2^{-m}$, $q'_{ij} \neq q_{ij}$, in which case B does not transmit r_{ij} in following queries by S or Alice. In this case, S generates a random guess r'_{ij} of r_{ij} and sends it to A_i after the plain text 'Reply ij', assuming she does not have any previous knowledge about r_{ij}. S succeeds in this case with probability $2^{-(n-m)}$.

Thus, if the keys k_{ij} are perfectly random and secret, S's probability to succeed in impersonating B in the previous strategy is

$$P_{\rm S} = \left(\frac{1}{2}\right)^m + \left[1-\left(\frac{1}{2}\right)^m\right]\left(\frac{1}{2}\right)^{n-m}. \qquad (1)$$

We have assumed here that $\gamma = 0$, i.e., neither A nor B accept errors in the received strings. P_S is minimized (for fixed even n) for $m = \frac{n}{2}$, when,

$$P_S = 2\left(\frac{1}{2}\right)^{\frac{n}{2}} - \left(\frac{1}{2}\right)^n \leq 2^{1-\frac{n}{2}}\,. \qquad (2)$$

This gives a strong security bound of $P_S \approx 10^{-9}$ with relatively short keys of $n = 62$ bits.

We now consider the case $\gamma > 0$. We have

$$P_S(\gamma) = \left(\frac{1}{2}\right)^m |Q_m^\gamma| + \left[1-\left(\frac{1}{2}\right)^m |Q_m^\gamma|\right]\left(\frac{1}{2}\right)^{n-m} |Q_{n-m}^\gamma|, \qquad (3)$$

where $Q_N^\gamma = \{x \in \{0,1\}^N | w(x) \leq \gamma N\}$, and where $w(x)$ denotes the Hamming weight of the bit string x.

We assume that n is even and that $m = \frac{n}{2}$. We obtain from (3) that

$$\begin{aligned} P_S(\gamma) &= 2\left(\frac{1}{2}\right)^m |Q_m^\gamma| - \left(\frac{1}{2}\right)^{2m} \left(|Q_m^\gamma|\right)^2 \\ &\leq 2^{(1-m)}|Q_m^\gamma| \\ &\leq 2^{(1-m)} 2^{mh(\gamma)} \\ &= 2^{\left[1-m(1-h(\gamma))\right]}, \end{aligned} \qquad (4)$$

where in the third line we used that $|Q_m^\gamma| \leq 2^{mh(\gamma)}$, which is shown in Sec. 1.4 of Ref. [31], and where $h(\gamma) = -\gamma \log_2 \gamma - (1-\gamma)\log_2(1-\gamma)$ is the binary entropy of γ.

For example, even with a high error tolerance, $\gamma = 0.05$ (giving $h(0.05) = 0.2864$) and taking $n = 88$, we obtain from (4) that $P_S(0.05) < 10^{-9}$.

We have assumed the keys are perfectly random, i.e., that S has zero information about them. In practice this will not be quite correct, but keys can be made close enough to random to make corrections negligible.

C. Obtaining the keys

S could try to learn the keys k_{ij} before they are used, i.e., before B sends the k_{ij}'s to Alice's agents. But by assumption the scheme is secure against these attacks: we assume Alice and Bob generate and distribute the keys secretly, and store them secretly until Bob communicates the secret keys.

D. Adding time delays

S can add time delays in any communications between any of Alice's agents and B. This can increase the uncertainty in B's location authenticated by Alice and/or delay Alice's verification. If S thereby causes the time delays between the A_i and B to be larger than acceptable thresholds, or for the communications in one or both directions to become out of sequence, then this causes the position verification to fail. We assume in this case Alice responds, for example by inspecting B's location with other physical means.

A limiting case is that S can jam the communications altogether. These delay or jamming attacks are unavoidable in practice unless the communication channels cannot be accessed by S. Inaccessible private channels is a strong assumption not generally made in quantum cryptography. One practical reason not to make this assumption is that it requires secure laboratories linked by a network of securely hardened channels. In position verification applications, these channels might typically be $\sim 10 - 10^5$km long (ranging from small scale networks on Earth to high Earth orbit satellites) and would need to be approximately straight line. A theoretical reason not to make it is that it trivialises position verification (PV) as a task. Given inaccessible private channels, PV can be securely implemented simply by exchanging messages, without using secret keys or any quantum communications, provided the channel transmission times are reliably known.

If S adds suitably short time delays, A can verify B's location within tolerable error bounds. If she adds longer time delays, she prevents A from verifying B's position, but alerts A to her interference. So the protocol is secure (in the sense claimed) against delay or jamming attacks.

E. Altering Bob's records

If S can, without detection, alter Bob's record of whether previous queries were authenticated, she can send repeated queries of the form query-message-ij, altering the record so that Bob has no record of each failed authentication. Bob will thus continue the protocol after failed authentication. S can thus continue until she successfully guesses the query string q_{ij}, and Bob's response will provide her with r_{ij}. If she is able thus to obtain r_{ij} before the authentic query-message-ij is sent, she can spoof a response to this challenge. If she is able to do this for all ij, she can systematically and indefinitely mislead the A_i as to B's location.

Timing constraints may restrict the scope of this attack, since as described it requires S to make $\sim 2^m$ guesses at q_{ij} to obtain r_{ij}. However, if S is also able to alter the data in Bob's register R_i, she can set it so that Bob will accept a query-message-ij for some value of j that may not authentically be sent until some (perhaps far) future time. This enlarges the time window during which she can send guesses at query-message-ij.

Also, if S can, without detection, alter Bob's records of the q_{ij}, in a way that allows her to choose the altered string (although not read the original string), she can create new query keys q_{ij}^S that she knows. If she is able to do this before the authentic query-message-ij is sent, she can use q_{ij}^S to send a spoof query-message-ij, obtain the response $_{ij}$, and use this to spoof responses to authentic queries. If she is able to do this for all ij, she can systematically and indefinitely mislead the A_i as to B's location.

The protocol thus requires that B can keep classical data secure against alteration, as well as keeping the key strings private (i.e. secure against reading). The ability to ensure that classical data within a secured site is unalterable is also a standard cryptographic assumption. However it is worth noting that it neither necessarily implies nor is necessarily implied by data privacy.

VI. QUANTITATIVE CONSIDERATIONS FOR SCHEME 1

We consider for simplicity a 1D implementation in which Alice has two agents (case $M = 2$), A_1 and A_2. Let A_1, A_2 and B be on the same line, with B between Alice's agents at equal distance from each of them.

We assume that the communication channel between A_1 (A_2) and B is optical and in free space, transmitting at the speed of light c.

A. Bob performs information processing with electronic circuits

Steps 6 and 7 comprise B receiving Alice's query signal encoded in light or other electromagnetic signals, converting these to electronic signals, authenticating the request originated from Alice, and then encoding the reply in light or other electromagnetic signals and transmitting to A_i, for $i = 1, 2$. In practice, a circuit comprising FPGAs could be used to perform these computations as fast as possible. Note that the signals exchanged between Alice and Bob in the position verification protocol are classical. Hence they can be sufficiently intense to deal with losses and errors. This is a significant practical advantage compared to position authentication schemes that need to transmit quantum states between Alice and Bob (e.g., [2–4, 32, 33]).

As an illustration, we take $n \sim 62$, with $\gamma = 0$. We note that because our scheme only involves classical communication and classical processing, it is sensible to assume zero errors, in contrast to schemes that require quantum communication or quantum information processing. An FPGA simply needs to compare received and stored key strings. Ref. [28] performed in 2016 completed a round including more complex computations and communication between adjacent FPGAs with a string of 128 bits in 1.8 μs. With these devices, assuming processing time is approximately linear in string length, our simpler computation with $n = 62$ bits should be completed within $\leq 0.88\mu$s, giving uncertainty of $\leq$ 264m in B's location.

With state of the art FPGAs, we estimate that B's verification might be completed within $\sim$ 10ns, giving an uncertainty of $\sim$ 3m in B's location.

If verification rounds take place every μs, the light speed signalling bound implies that the tag can move $\leq$ 300m between rounds. For 4 verifiers, this round frequency consumes $\approx 4 \times 124 \times 10^6 \approx 5 \times 10^8$ key bits per second.

If we assume, perhaps plausibly in many scenarios, that the tag will not move faster than the speed of sound (in air at sea level) from its expected location, verification rounds every μs mean that the tag cannot move more than $\approx 3 \times 10^{-4}$m between rounds. With rounds every ms, this becomes $\approx 3 \times 10^{-1} m$. This round frequency consumes $\approx 5 \times 10^5$ key bits per second. While still demanding, these resource requirements seem achievable with present technology, and give (modulo assumptions) good enough location precision to be useful in many scenarios.

VII. SCHEME 2: BOB HAS A TRUSTED SYNCHRONIZED CLOCK

Our second scheme introduces the assumption that B possesses a clock synchronised with Alice's clocks. This allows Alice to specify a signalling schedule in advance so B can transmit at specified times. Of course, it makes extra technological demands on B and on the size and security of his laboratory.

The main difference between Schemes 1 and 2, is that Scheme 2 does not require Alice to send a query signal every time she wishes to verify B's location. Instead, she shares an authenticated signalling schedule with B in advance, with B relying on his synchronised clock to follow the schedule. This removes the need for B to authenticate each individual query from Alice in real time, as he can authenticate the whole signalling schedule in advance. This removes one source of delay in the protocol, namely B's authentication time, denoted as δ_1 in the description of Scheme 1. It also potentially removes a second source of delay, B's transmission time δ_2, since if Bob knows δ_2 he can adjust for it by starting the transmission so that it *completes* (rather than starts) at the time T_j stipulated for his round j communication in A's schedule. More precisely, it potentially replaces δ_2 by the uncertainty Δ_2 in Bob's transmission time, and typically we expect $\Delta_2 \ll \delta_2$. We assume this adjustment below.

(We consider schemes involving only classical communication between A and B here, but it is worth noting that removing these delays is potentially even more valuable for schemes involving quantum communications from A and B and quantum measurement and/or information processing by B, since the latter steps are potentially significantly slower than their classical counterparts. It thus seems potentially advantageous, in scenarios in which it is justifiable, also to allow B and A to share synchronized clocks in such schemes. However, the advantage is lost if B is not able to keep information secret, since storing information for later use exposes it to spoofers. And if B is able to keep secret, the protocols discussed here using classical queries and responses may generally be more efficient. So this option may perhaps be useful only in the restricted scenario where B is able to keep quantum information secret but not classical information.)

Scheme 2 again assumes that Alice has M agents $A_1, \ldots, A_M$ surrounding the location L of B. Alice and B agree on a sufficiently large integer n, and on a sufficiently small error rate $0 \leq \gamma << 1$, which act as security parameters. We also assume that all communications take place at the speed of light through vacuum, which we denote by c. For all $i = 1, 2, \ldots, M$, Alice's agent A_i and B perform the following actions.

1. A and B share a secret key k that is used to authenticate communications and may also be used as a one-time pad to keep communications secret. This key may be expanded as and when needed by QKD.

2. At some time prior to the position verification protocol, A_i and B share a secret key $k_i = \{r_{i1}, \ldots, r_{iN}\}$, where each substring r_{ij} has n bits, and N is as large as required. They keep this secret from spoofers, although A_i may share it securely with other A_j. The key sharing may be done arbitrarily far in advance. For simplicity, we assume the key-sharing is error-free, i.e. that A_i and B have identical versions of k_i. This can be achieved, with high probability, by standard key reconciliation methods. A small allowed key sharing error rate can also be incorporated in the error-tolerant ($\gamma > 0$) versions of the position verification protocol, as described below.

3. A sends an authenticated message to B, specifying the times at which he is required to verify his location. This can be done arbitrarily far in advance of step 3, and possibly after or concurrent with step 2. In the simplest version, this message is public. Alternatively, it could be encrypted, to prevent S from learning the verification schedule.

4. If T_j is the j-th time B is required to verify his location, then to each A_i he sends the plain text 'Reply ij' followed by r_{ij} , completing his transmission at time T_j, according to his clock. As in Scheme 1, B may either broadcast or narrowcast his replies. We describe the narrowcast version below; the minor modifications required for the broadcast version are as for Scheme 1.

   Timing: this takes place by the time $T_j + \delta_d + \Delta_2$, where Δ_2 is the uncertainty in the time it takes B to transmit (consistently defined as in Scheme 1) and δ_d is the time difference between Alice and B's clocks, which may be non-zero if they are not perfectly synchronised. Note that we cannot assume $\delta_d > 0$. We assume that A_i and B are confident that their clock technology will ensure, in the absence of adversarial attacks on their clocks, there is some bound $\delta_d^{\max} > 0$ such that $|\delta_d| \leq \delta_d^{\max}$. In practice, this bound will be time-dependent. For simplicity here we consider a single bound that is valid throughout the duration of the protocol.

5. A_i receives ('Reply $i'j'$', $r'_{i'j'}$). She verifies that $i' = i$, that $j' = j$ (where j is the current round, i.e. A_i has received and authenticated replies from all rounds $k < j$), that the Hamming distance $d(r'_{ij}, r_{ij}) \leq \gamma(n - m)$ and that she has received the reply r'_{ij} not later than the time $T_j + \frac{d_i}{c} + \tilde{\delta}_L$, where $\tilde{\delta}_L$ has been agreed in advance by Bob and Alice, and which must satisfy $\tilde{\delta}_L \geq \delta_d^{\max} + \Delta_2$. If so, she sends the confirmation message '$s_{ij} = 1$' together with the time that she received r'_{ij} to A_0. Otherwise she sends the message '$s_{ij} = 0$'.

   Timing: If B is indeed at L, then A_i authenticates his reply by the time $T_j + \frac{d_i}{c} + \delta_d + \Delta_2 + \delta_3$, where d_i is the distance from L to A_i and δ_3 is the time taken for A_i to authenticate. She sends her confirmation message at time $T_j + \frac{d_i}{c} + \delta_d + \Delta_2 + \delta_3 + \delta_4$, where δ_4 is the time taken by Alice to generate and transmit the confirmation message.

6. If A_0 receives $s_{ij} = 1$ and authenticates it as a message from A_i for all $i = 1, 2, \ldots, M$, then she authenticates that the location of B was L, within some uncertainty given by $c(\tilde{\delta}_L - \delta_d^{\max})$, at some time T'_j, where $|T'_j - T_j| \leq \delta_d^{\max}$. This implies that the location of B at time T_j was L, within some uncertainty given by $c\tilde{\delta}_L$.

   Timing: Suppose that the authenticated channel from A_i to A_0 had length d'_i and that messages travel on it at speed $c'_i \leq c$. A_0 completes the authentication by the time

$$T_A = T_j + \max_i \left\{ \frac{d_i}{c} + \frac{d'_i}{c'_i} \right\} + \delta_d + \Delta_2 + \delta_3 + \delta_4 + \delta_5 \, ,$$

   where δ_5 is the time taken for A_0 to compute whether all confirmation messages satisfy $s_{ij} = 1$.

VIII. FURTHER ATTACKS ON SCHEME 2

As in section V, our security analysis here applies for spoofers who may have arbitrarily advanced quantum technology and share an arbitrarily large amount of entanglement, given our assumption that Bob can keep classical information secure from the spoofers.

A. Acting outside schedule

S may gain knowledge of the signalling schedule, potentially providing her with information about ΔR, the time difference between subsequent location requests. This exacerbates the problem illustrated in point 3 in section III, as S would know when she is able to move B (or encourage him to move, by spoofed GPS or other means) without risking a location check. This risk could be mitigated either by keeping the schedule suitably secret (by sending it encrypted) and unpredictable, or by ensuring the scheduled times are frequent enough that S could not move B a significant distance before the next verification is due. Note that the first option consumes a potentially large amount of shared secret key and the second requires a potentially high key refresh rate.

B. Clock desynchronization

Bob's clock may become desynchronized, either naturally or as a result of S's interference, introducing a time difference δ_d between Alice and Bob's clocks. At least theoretically, this is a significant concern: if S is able to move B physically at speeds arbitrarily close to c, she can cause his clock to run arbitrarily slowly with respect to A's lab frame. However, slowing B's clock delays his responses, which means that A will not incorrectly verify his position as guaranteed to be close to L. In principle, S could also desynchronize B's clock by altering the gravitational field in his vicinity. Such attacks are usually ignored in relativistic cryptography, given that it is impractical to create any significant effect. In most applications of relativistic cryptography, security is threatened only if the effect is large enough that points believed by one party to be spacelike separated are in fact timelike separated. In this case, though, any degree of desynchronization affects the precision of the position verification. However, in practice any effect seems likely negligible compared to other uncertainties.

A and B might attempt to counter accidental or deliberate desynchronization by exchanging authenticated messages to keep their clocks synchronized. This is complicated by the fact that a simple synchronisation protocol requires knowledge of B's position, or at least his distance from the relevant A_i. Synchronization schemes involving exchanges with several A_i in parallel still appear useful, but we will not pursue their analysis here.

IX. CONCLUSION

We have presented schemes for position verification in which the position verification queries and responses are purely classical, involving no quantum communication or quantum information processing. Quantum information transmission and measurement is required only to refresh the key via QKD. Our schemes are practical to implement with current technology. Their security is based on a standard assumption in quantum cryptography, also made in QKD, that a classical key can be stored securely, as initially proposed in Ref. [1].

When QPV schemes use position verification queries and/or responses that involve quantum communications, they typically use photons to encode quantum states. This poses challenges, including errors in state preparation, processing and measurement, losses, and security problems due to imperfect single-photon sources and single-photon detectors (e.g., photon-number splitting attacks [34, 35] and multiphoton attacks [36]) and side-channel attacks (e.g., [36]). The problem of losses is particularly challenging in schemes with large distances between the tagging device and the verifiers. An advantage of our schemes is that the queries and responses are purely classical. Quantum communications are needed only to replenish the key via QKD, which is secure against errors and losses. Moreover, the QKD communications, unlike the position verification queries and responses, are not tightly time constrained.

Given our assumptions, our schemes are secure against arbitrarily powerful quantum spoofers, who may share an arbitrary amount of entanglement. This is also an advantage compared to the best known quantum schemes, which have only been proved secure against spoofers that share an amount of entanglement linear in the classical information) [32, 33].

ACKNOWLEDGMENTS

We thank Daniel Oi, Jasminder S. Sidhu and Siddharth Joshi for helpful discussions. We acknowledge financial support from the UK Quantum Communications Hub grant no. EP/T001011/1. G.C. is supported by a studentship from the Engineering and Physical Sciences Research Council. A.K. and D.P.-G. were supported in part by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development and by the Province of Ontario through the Ministry of Research, Innovation and Science.

Author contributions. A.K conceived the project. A.K and D.P.-G. did the majority of the theoretical work, with input from G.C. A.K. and D.P.-G. wrote the manuscript with input from G.C.

[1] A. Kent, Quantum tagging for tags containing secret classical data, Physical Review A **84(2)**, 022335 (2011).

[2] A.Kent, R.Beausoleil, W. Munro, and T. Spiller, Tagging systems (U.S. Patent US20060022832A1, 2006).

[3] R. A. Malaney, Location-dependent communications using quantum entanglement, Physical Review A **81**, 042319 (2010).

[4] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, Position based cryptography, in *Annual International Cryptology Conference* (Springer, 2009) pp. 391–407.

[5] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).

[6] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, Position-based quantum cryptography: Impossibility and constructions, SIAM Journal on Computing **43**, 150 (2014).

[7] A. Kent, Unconditionally secure bit commitment, Phys. Rev. Lett. **83**, 1447 (1999).

[8] A. Kent, Coin tossing is strictly weaker than bit commitment, Phys. Rev. Lett. **83**, 5382 (1999).

[9] A. Kent, A no-summoning theorem in relativistic quantum theory, Quantum Inf. Process. **12**, 1023 (2013).

[10] D. Pitalúa-García, Spacetime-constrained oblivious transfer, Phys. Rev. A **93**, 062346 (2016).

[11] P. Hayden and A. May, Summoning information in spacetime, or where and when can a qubit be?, J. Phys. A: Math. Theor. **49**, 175304 (2016).

[12] E. Adlam and A. Kent, Quantum paradox of choice: More freedom makes summoning a quantum state harder, Physical Review A **93**, 062327 (2016).

[13] A. Kent, Unconstrained summoning for relativistic quantum information processing, Physical Review A **98**, 062332 (2018).

[14] D. Pitalúa-García and I. Kerenidis, Practical and unconditionally secure spacetime-constrained oblivious transfer, Phys. Rev. A **98**, 032327 (2018).

[15] D. Pitalúa-García, One-out-of-m spacetime-constrained oblivious transfer, Phys. Rev. A **100**, 012302 (2019).

[16] D. Pitalúa-García, Unconditionally secure relativistic multi-party biased coin flipping and die rolling, Proc. R. Soc. A **477**, 20210203 (2021).

[17] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).

[18] D. Dieks, Communication by EPR devices, Physics Letters A **92**, 271 (1982).

[19] D. Mayers, Unconditionally secure quantum bit commitment is impossible, Physical Review Letters **78**, 3414 (1997).

[20] H.-K. Lo and H. F. Chau, Is quantum bit commitment really possible?, Physical Review Letters **78**, 3410 (1997).

[21] H.-K. Lo and H. F. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible, Physica D: Nonlinear Phenomena **120**, 177 (1998).

[22] H.-K. Lo, Insecurity of quantum secure computations, Phys. Rev. A **56**, 1154 (1997).

[23] D. Gottesman, Theory of quantum secret sharing, Physical Review A **61**, 042311 (2000).

[24] L. Vaidman, Instantaneous measurement of nonlocal variables, Physical Review Letters **90(1)**, 010402 (2003).

[25] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Experimental bit commitment based on quantum communication and special relativity, Phys. Rev. Lett. **111**, 180504 (2013).

[26] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li, H.-F. Zhang, Y. Zhao, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, Experimental unconditionally secure bit commitment, Phys. Rev. Lett. **112**, 010504 (2014).

[27] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, Practical relativistic bit commitment, Phys. Rev. Lett. **115**, 030502 (2015).

[28] E. Verbanis, A. Martin, R. Houlmann, G. Boso, F. Bussières, and H. Zbinden, 24-hour relativistic bit commitment, Phys. Rev. Lett. **117**, 140506 (2016).

[29] P. Alikhani, N. Brunner, C. Crépeau, S. Designolle, R. Houlmann, W. Shi, N. Yang, and H. Zbinden, Experimental relativistic zero-knowledge proofs, Nature **599**, 47 (2021).

[30] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, On the requirements for successful GPS spoofing attacks, in *Proceedings of the 18th ACM Conference on Computer and Commun* CCS '11 (Association for Computing Machinery, New York, NY, USA, 2011) p. 75–86.

[31] J. H. van Lint, *Introduction to Coding Theory* (Springer, Berlin, 1999).

[32] A. Bluhm, M. Christandl, and F. Speelman, A single-qubit position verification protocol that is secure against multi-qubit attacks, Nat. Phys. **18**, 623 (2022).

[33] L. m. c. Escolà-Farràs and F. Speelman, Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers, Phys. Rev. Lett. **131**, 140802 (2023).

[34] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

[35] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[36] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent, and D. Pitalúa-García, Multiphoton and side-channel attacks in mistrustful quantum cryptography, PRX Quantum **2**, 030338 (2021).

Extended Abstract (Arxiv Preprint available in [1]):

Classically Spoofing System Linear Cross Entropy Score Benchmarking

Andrew Tanggara[1 2 *] Mile Gu[2 1 †] Kishor Bharti[3 4 ‡]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543.*
[2] *Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 639673.*
[3] *A*STAR Quantum Innovation Centre (Q.InC), Institute of High Performance Computing (IHPC), Agency for Science, Technology and Research (A*STAR), 1 Fusionopolis Way, #16-16 Connexis, Singapore, 138632, Republic of Singapore.*
[4] *Centre for Quantum Engineering, Research and Education, TCG CREST, Sector V, Salt Lake, Kolkata 700091, India.*

Abstract. Many "quantum supremacy" claims, notably by Google in 2019, rest upon the Linear Cross Entropy Benchmarking (Linear XEB) verification metric. However, the hardness of classically spoofing Linear XEB depends on the Cross-Entropy Quantum Threshold (XQUATH) assumption, which has been disproven for sublinear depth circuits. System Linear Cross Entropy Score (sXES), a Linear XEB variant, is a promising quantum supremacy verification metric for quantum Hamiltonian simulations as it relies on a different assumption called the System Linear Cross-Entropy Quantum Threshold (sXQUATH). Here, we disprove sXQUATH for sublinear depth circuits and construct an efficient spoofing algorithm for sXES of sufficiently noisy experiments.

Keywords: Quantum computation benchmarking, Quantum computational complexity, Linear cross-entropy benchmarking, Random quantum circuit sampling, Classical simulation of quantum computation

In 2019, the Google quantum AI team claimed the first experimental demonstration of "quantum supremacy," [2] or computational quantum advantage using a 53 qubits superconducting circuit [3], signifying a major leap forward in practical quantum computing and challenging the extended Church-Turing thesis [4]. In verifying that their circuit is correctly performing a task called quantum random circuit sampling (RCS), they tested their samples using a metric called "Linear Cross-Entropy Benchmarking (Linear XEB)" [5–10]. Since then, multiple RCS experiments [11–13] have their quantum supremacy claims verified by Linear XEB method, or a variant thereof. Skepticism on these claims have been raised, particularly by classical simulations of Google's RCS experiment [14–19] showing significantly shorter classical runtime compared to their initial estimation of $10,000$ years. Moreover, theoretical results on classical simulation of different RCS variants [20–25] cast doubts on the complexity-theoretic hardness of spoofing Linear XEB that rests on the cross entropy quantum threshold assumption (XQUATH) conjecture proposed by Aaronson and Gunn [26]. Recent demonstration that XQUATH does not hold for sublinear depth RCS [24], further diminishes the legitimacy of Linear XEB as a benchmark for quantum supremacy.

In the ongoing pursuit of quantum supremacy by the way of near-term quantum Hamiltonian simulation, a variant of Linear XEB called the System Linear Cross Entropy Score (sXES) has been proposed [27]. Structural difference between the circuits assessed by sXES and other Linear XEB variants renders it unclear whether existing Linear XEB spoofing methods such as [20, 22, 24] can be used for sXES. Moreover the hardness of spoofing sXES lies upon a complexity-theoretic conjecture known as the System Linear Cross-Entropy Quantum Threshold Assumption (sXQUATH), the formal relationship of which to XQUATH is unknown. These fundamental distinctions from other Linear XEB variants thus renders sXES a promising verification method in future claims of quantum supremacy experiments.

In this work, we go beyond the technique in [24] to show that there exists an efficient classical algorithm that approximates the experiment sufficiently well to refute sXQUATH (see Theorem 1). At the same time, we also show explicitly that our algorithm spoofs the sXES benchmark (see Theorem 2) for noisy experiments. Our algorithm approximates the output probability distribution of a family of quantum circuits known as the Minimal Quantum Singular Value Transform (mQSVT) circuit [27], which sXES assessed upon. While the mQSVT circuits bear the power to implement any quantum algorithm that falls into the Quantum Singular Value Transform (QSVT) framework [28] (such as Szegedy quantum walk [29] and quantum solver for system of linear equations [30] and Hamiltonian simulation tasks [31, 32]), our results suggest that a more robust benchmarking method is necessary for any claim of quantum supremacy experiment.

1 Hardness of spoofing mQSVT circuit benchmarking

An mQSVT circuit $\texttt{mQSVT}(U)$ (see Fig. 1) consists of d "blocks", each containing a copy of $n+1$ qubit uni-

[*] andrew.tanggara@gmail.com
[†] mgu@quantumcomplexity.org
[‡] kishor.bharti1@gmail.com

tary U and a copy of its conjugate $U^\dagger$. Denote the depth of U as d_U so that we can write $U = U_{d_U} \dots U_1$ where U_j is the j-th layer of U. These unitaries are interleaved by phase shift gates $R(\varphi)$ at the top register with carefully chosen phases (as discussed in the supplementary material of [27]). Samples from an mQSVT circuit are obtained from measuring the bottom n registers conditioned on measurement of the top register being 0. The outcome probability of an n-bit string x is therefore $p(U,x) = |\langle 0x|\texttt{mQSVT}(U)|0^{n+1}\rangle|^2$. Here we consider unitaries U consisting only of two-qubit gates such that in each layer, every qubit register is evolved by precisely one two-qubit gate without any geometric locality assumption (hence $n+1$ is even). This is the unitary architecture assumed for the RCS simulation result in [24].

For a noisy mQSVT Hamiltonian simulation experiment, a benchmarking scheme similar to XEB benchmarking used in RCS experiment [3, 11, 12], called the average system linear cross-entropy score (sXES) [27] was proposed. For a given ideal mQSVT circuit $\texttt{mQSVT}(U)$ and (empirically approximated) experimental probability $p_{\text{exp}}(U,x)$ of output x, its sXES is given by

$$\mathbb{E}_U[\text{sXES}(U)] = \sum_{x \neq 0^n} \mathbb{E}_U[p(U,x)\, p_{\text{exp}}(U,x)] \,, \qquad (1)$$

where $\mathbb{E}_U$ is expectation over random U. An experiment with high sXES indicates a high circuit fidelity as it assigns a high probability $p_{\text{exp}}(U,x)$ to string x with high ideal probability $p(U,x)$, hence higher sXES.

Computational hardness of classically spoofing sXES can be reduced to a statement which essentially says that: The average error of any efficient classical algorithm that takes a description of unitary U and output bit string x as input and outputs an approximation of $p(U,x)$ cannot be exponentially smaller than the average error of uniformly sampling x. This is a statement captured by the System Linear Cross-entropy Quantum Threshold Assumption (sXQUATH) [27], which the hardness of spoofing sXES relies upon. More precisely, sXQUATH conjecture states that there is no polynomial-time classical algorithm taking an efficient description of $n+1$-qubit unitary U and n bit string x as inputs and outputs an approximation $q(U,x)$ of mQSVT output probability $p(U,x)$ such that

$$\text{sXQ} = \mathcal{E}\Big(p(U,X), \frac{1}{2^n}\Big) - \mathcal{E}\Big(p(U,X), q(U,X)\Big) \geq c2^{-3n} \qquad (2)$$

for some constant c and large enough n. Here, $\mathcal{E}(f,g) := \mathbb{E}_{U,X}[(f(U,X) - g(U,X))^2]$ is the mean-squared error (MSE) between functions f and g and $\mathbb{E}_{U,X}$ is expectation over uniformly random variable $X \in \{0,1\}^n \backslash \{0^n\}$ and over Haar-random two-qubit gates in $n+1$-qubit unitary U.

Now we present the first main result below in Theorem 1, which states that sXQUATH generally does not hold. Particularly for a single-block mQSVT circuit (i.e. with $d = 1$) and a sublinear depth unitary U, one can construct a classical algorithm running in time polynomial in n with a non-negligibly less MSE than the trivial approximation.

Theorem 1 *There exists an efficient classical algorithm taking an efficient description of $n+1$-qubit unitary U with sublinear depth $d_U = o(n)$ and n bit string x as inputs and outputs an approximation $q(U,x)$ of a single-block mQSVT circuit output probability $p(U,x)$ that satisfies eqn. (2).*

Our second result further shows that the same algorithm spoofs sXES for mQSVT circuits with sufficiently large noise. As mQSVT circuits with completely depolarizing noise have uniform output probability, its sXES is $\mathbb{E}_U[\text{sXES}(U)] = 2^{-n}\sum_{x\neq 0}\mathbb{E}_U[p(U,x)]$, indicating no correlation with the ideal probability $p(U,x)$. Our algorithm spoofs sXES of all mQSVT circuits with depolarizing noise above a certain threshold (such that it is close to $2^{-n}\sum_{x\neq 0}\mathbb{E}_U[p(U,x)]$).

Theorem 2 *There exists an efficient classical algorithm spoofing sXES for all noisy single-block mQSVT circuit with $n+1$-qubit unitary U such that its sXES is at most $2^{-n}(\sum_{x\neq 0}\mathbb{E}_U[p(U,x)] + c^{d_U})$ for some constant $c > 0$.*

If we consider mQSVT circuit corrupted with depolarizing noise with noise strength $\gamma \in [0,1]$ on each of its register in each layer, then for sufficiently large γ its sXES score is going to be less than $2^{-n}(\sum_{x\neq 0}\mathbb{E}_U[p(U,x)] + c^{d_U})$. Theorem 2 indicates that the sXES all such noisy mQSVT circuit is spoofed by our algorithm.

Classical algorithm that refutes sXQUATH and spoofs sXES benchmark in Theorem 1 and Theorem 2 above is from a family of algorithms called the Pauli path algorithms. Below we discuss how the Pauli path algorithm works in showing the theorems above. Additionally we discuss how the existing instances of Pauli path algorithm used to classically simulate quantum circuits [20, 24, 33] are not directly applicable to mQSVT circuit, mainly due to the existence of multiple copies of random unitaries.

2 Pauli path algorithm for disproving sXQUATH and spoofing sXES

This section is slightly more technical as we define the Pauli path algorithm, how existing results using Pauli paths are not applicable in our case, and how can we make the Pauli path algorithm work to show Theorem 1 and Theorem 2. Nevertheless here we only outline the steps, for which a more rigorous treatment can be found in the full manuscript [1].

Given an n-qubit quantum circuit $C = C_d C_{d-1} \dots C_1$ (where C_j is its j-th layer), Pauli path algorithm classically computes its output probabilities by expanding density matrices at every layer in terms of normalized n-qubit Pauli matrices $\mathcal{P}_n = \{I/\sqrt{2}, X/\sqrt{2}, Y/\sqrt{2}, Z/\sqrt{2}\}^{\otimes n}$. At the input, we get $|0^n\rangle\langle 0^n| = \sum_{s_1 \in \mathcal{P}_n} s_1 \text{Tr}(s_1|0^n\rangle\langle 0^n|)$. We can substitute this expansion to the density matrix after the first layer, $\rho_1 := C_1|0^n\rangle\langle 0^n|C_1^\dagger$ then expand it in the same manner to get $\rho_1 = \sum_{s_1,s_2 \in \mathcal{P}_n} s_2 \text{Tr}(s_2 C_1 s_1 C_1^\dagger)\text{Tr}(s_1|0^n\rangle\langle 0^n|)$. Repeating this for the remaining layers and for measurement $|x\rangle\langle x|$, we obtain *transition amplitudes* defined by $\langle\!\langle s_1|0^n\rangle\!\rangle := \text{Tr}(s_1|0^n\rangle\langle 0^n|)$ and $\langle\!\langle s_{j+1}|C_j|s_j\rangle\!\rangle := \text{Tr}(s_{j+1}C_j s_j C_j^\dagger)$ and

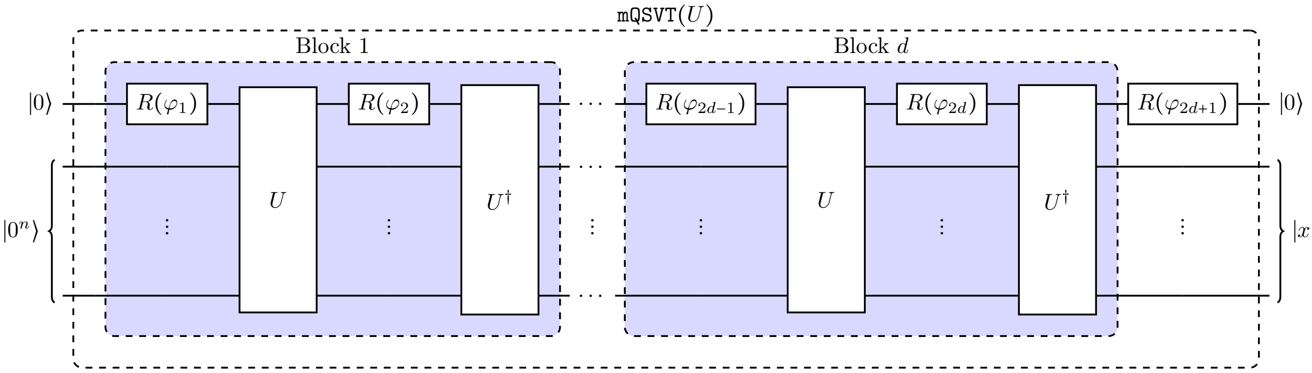


Figure 1: mQSVT circuit `mQSVT(`U`)` where U is a random $n+1$ qubit unitary made out of 2 qubit Haar-random unitaries and $R(\varphi)$ is Z-rotation gate with angle φ.

$\langle\!\langle x|s_{d+1}\rangle\!\rangle := \mathrm{Tr}(|x\rangle\!\langle x|s_{d+1})$. For transition amplitude $\langle\!\langle s_{j+1}|C_j|s_j\rangle\!\rangle$, we call s_j an *input Pauli* and s_{j+1} an *output Pauli.* A sequence of normalized n-qubit Paulis $\mathbf{s} = s_1, s_2, \ldots, s_{d+1}$ is called a *Pauli path.* Then, the probability of n bit string x is

$$|\langle x|C|0^n\rangle|^2 = \sum_{\mathbf{s}\in\mathcal{P}_n^{d+1}} f(C,\mathbf{s},x)\ , \tag{3}$$

where each Pauli path defines a *Fourier coefficient* $f(C,\mathbf{s},x) = \langle\!\langle x|s_{d+1}\rangle\!\rangle\langle\!\langle s_{d+1}|C_d|s_d\rangle\!\rangle \ldots \langle\!\langle s_2|C_1|s_1\rangle\!\rangle\langle\!\langle s_1|0^n\rangle\!\rangle$.

In computing the output probabilities of mQSVT circuit, a Pauli path algorithm expands density matrices at each layer in the copies of $n+1$-qubit random unitary U and its conjugate $U^\dagger$, as well as the single-qubit rotation gates $R(\varphi)$ interleaving them. So for a Pauli path $\mathbf{s}$ through a mQSVT circuit with unitary U and n-bit string output x, we denote an mQSVT circuit Fourier coefficient as $F(U,\mathbf{s},x)$, which consists of $2d(d_U+1)$ transition amplitudes. Hence the probability of output x from an mQSVT circuit with unitary U is

$$p(U,x) = \sum_{\mathbf{s}} F(U,\mathbf{s},x)\ . \tag{4}$$

Computing the *exact* output probabilities $p(U,x)$ using Pauli paths is exponentially hard due to exponentially many Fourier coefficients (one for each Pauli path $\mathbf{s}$). However it has been shown in [24] that for a unitary random circuit C, a carefully chosen *single* Pauli path can approximate $p(C,0^n)$ sufficiently well to refute XQUATH and spoof Linear XEB for sublinear depth circuits. The performance of this carefully chosen Pauli path approximation is due to the so-called "orthogonality property" of Pauli paths [24, 34] which states that the expectation of product of Fourier coefficient between distinct Pauli paths is equal to zero. Namely, $\mathbb{E}_C[f(C,\mathbf{s},x)f(C,\mathbf{r},x)] = 0$ if $\mathbf{s} \neq \mathbf{r}$. This value appears in both eqn. (2) and eqn. (1) when one expands the ideal probability $p(U,x)$ as in eqn. (4) and if $q(U,x)$ is a Pauli path approximation.

Unfortunately, orthogonality condition does not hold in general for mQSVT circuits due to a random unitary U appearing $2d$ number of times in a d-block mQSVT circuit. In fact it can take positive and negative values, complicating the analysis even more. But as noted in [34] on how the expectation of product between Fourier coefficients are closely related to Haar-random unitary moment matrix, we can use the random matrix theory of unitary Weingarten calculus [35–38] to compute this quantity for mQSVT circuits. This allows us to show that there is a Pauli path approximation using only a single Pauli path that disproves sXQUATH as stated in Theorem 1, as well as spoofs sXES in the sense of Theorem 2. This approximation for unitary U and outcome x takes the form of

$$q(U,x) = \frac{1}{2^n} + F(U,\mathbf{r},x)\ , \tag{5}$$

for Pauli path $\mathbf{r} = (Z\otimes I^{\otimes l-1}\otimes Z\otimes I^{\otimes n-l}, Z\otimes I^{\otimes n}, \ldots, Z\otimes I^{\otimes n})$ (up to normalization). With the chosen Pauli path $\mathbf{r}$, giving Fourier coefficient $F(U,\mathbf{r},x)$, the MSE error $\mathcal{E}(p(U,X),q(U,X))$ in the left-hand side of eqn. (2) turns out to be c^{d_U} smaller than the MSE error of the uniform-random sampling $\mathcal{E}(p(U,X),2^{-n})$ for some constant c. By taking depth d_U of unitary U to be sublinear, $d_U = o(n)$ eqn. (2) is then satisfied. Similarly for eqn. (1), using approximation $q(U,x)$ in place of experimental probability $p_{\exp}(U,x)$ gives a nontrivial sXES score stated in Theorem 2.

3 Future work and open questions

Our results along with [24], highlight the need for a novel benchmarking task with a stronger complexity-theoretic guarantee for future quantum supremacy experiments. In particular, such guarantee needs to rule out any possibility of spoofing by the Pauli algorithms. Moreover, one can also ask the question: What is the hardness relationship between different benchmarking methods, such as sXES, Linear XEB, XHOG, and their predecessor HOG [5]? What is the complexity theoretic relationship between their assumptions, sXQUATH, XQUATH, and QUATH [5] (assumption for the hardness of HOG)? Can one also disprove QUATH for sublinear-depth circuits using Pauli paths? To understand how to construct a more robust benchmarking method, it would be insightful to explore these questions.

References

[1] Andrew Tanggara, Mile Gu, and Kishor Bharti. "Classically Spoofing System Linear Cross Entropy Score Benchmarking". In: (2024). arXiv: 2405.00789 [quant-ph].

[2] John Preskill. "Quantum computing and the entanglement frontier". In: arXiv preprint arXiv:1203.5813 (2012).

[3] Frank Arute et al. "Quantum supremacy using a programmable superconducting processor". In: Nature 574.7779 (Oct. 2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5. URL: https://doi.org/10.1038%2Fs41586-019-1666-5.

[4] Sanjeev Arora and Boaz Barak. Computational complexity: a modern approach. Cambridge University Press, 2009.

[5] Scott Aaronson and Lijie Chen. "Complexity-Theoretic Foundations of Quantum Supremacy Experiments". In: (2016). arXiv: 1612.05903 [quant-ph].

[6] Sergio Boixo et al. "Characterizing quantum supremacy in near-term devices". In: Nature Physics 14.6 (Apr. 2018), pp. 595–600. DOI: 10.1038/s41567-018-0124-x. URL: https://doi.org/10.1038%2Fs41567-018-0124-x.

[7] Charles Neill et al. "A blueprint for demonstrating quantum supremacy with superconducting qubits". In: Science 360.6385 (2018), pp. 195–199.

[8] Dominik Hangleiter et al. "Sample complexity of device-independently certified "quantum supremacy"". In: Physical review letters 122.21 (2019), p. 210502.

[9] Jens Eisert et al. "Quantum certification and benchmarking". In: Nature Reviews Physics 2.7 (2020), pp. 382–390.

[10] Dominik Hangleiter and Jens Eisert. "Computational advantage of quantum random sampling". In: Reviews of Modern Physics 95.3 (2023), p. 035001.

[11] Yulin Wu et al. "Strong quantum computational advantage using a superconducting quantum processor". In: Physical review letters 127.18 (2021), p. 180501.

[12] Qingling Zhu et al. "Quantum computational advantage via 60-qubit 24-cycle random circuit sampling". In: Science bulletin 67.3 (2022), pp. 240–245.

[13] Lars S Madsen et al. "Quantum computational advantage with a programmable photonic processor". In: Nature 606.7912 (2022), pp. 75–81.

[14] Feng Pan and Pan Zhang. "Simulation of quantum circuits using the big-batch tensor network method". In: Physical Review Letters 128.3 (2022), p. 030501.

[15] Cupjin Huang et al. "Classical simulation of quantum supremacy circuits". In: arXiv preprint arXiv:2005.06787 (2020).

[16] Yong Liu et al. "Closing the" quantum supremacy" gap: achieving real-time simulation of a random quantum circuit using a new sunway supercomputer". In: Proc. of the Int'l Conference for HPC. 2021, pp. 1–12.

[17] Feng Pan, Keyang Chen, and Pan Zhang. "Solving the sampling problem of the sycamore quantum circuits". In: Physical Review Letters 129.9 (2022), p. 090502.

[18] Gleb Kalachev et al. "Classical sampling of random quantum circuits with bounded fidelity". In: arXiv preprint arXiv:2112.15083 (2021).

[19] Alexis Morvan et al. "Phase transition in random circuit sampling". In: arXiv preprint arXiv:2304.11119 (2023).

[20] Xun Gao and Luming Duan. "Efficient classical simulation of noisy quantum computation". In: arXiv preprint arXiv:1810.03176 (2018).

[21] Boaz Barak, Chi-Ning Chou, and Xun Gao. "Spoofing linear cross-entropy benchmarking in shallow quantum circuits". In: arXiv preprint arXiv:2005.02421 (2020).

[22] Xun Gao et al. "Limitations of linear cross-entropy as a measure for quantum advantage". In: arXiv preprint arXiv:2112.01657 (2021).

[23] Changhun Oh, Liang Jiang, and Bill Fefferman. "Spoofing cross-entropy measure in boson sampling". In: Physical Review Letters 131.1 (2023), p. 010401.

[24] Dorit Aharonov et al. "A polynomial-time classical algorithm for noisy random circuit sampling". In: Proceedings of the 55th ACM STOC. 2023, pp. 945–957.

[25] Joel Rajakumar, James D Watson, and Yi-Kai Liu. "Polynomial-Time Classical Simulation of Noisy IQP Circuits with Constant Depth". In: arXiv preprint arXiv:2403.14607 (2024).

[26] Scott Aaronson and Sam Gunn. "On the Classical Hardness of Spoofing Linear Cross-Entropy Benchmarking". In: (2020). arXiv: 1910.12085 [quant-ph].

[27] Yulong Dong, K. Birgitta Whaley, and Lin Lin. "A quantum hamiltonian simulation benchmark". In: npj Quantum Information 8.1 (Nov. 2022). DOI: 10.1038/s41534-022-00636-x. URL: https://doi.org/10.1038%2Fs41534-022-00636-x.

[28] András Gilyén et al. "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics". In: Proceedings of the 51st ACM STOC. 2019, pp. 193–204.

[29] Mario Szegedy. "Quantum speed-up of Markov chain based algorithms". In: 45th IEEE symposium on found. of CS. IEEE. 2004, pp. 32–41.

[30] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. "Quantum Algorithm for Linear Systems of Equations". In: Physical Review Letters 103.15 (Oct. 2009). ISSN: 1079-7114. DOI: 10.1103/physrevlett.103.150502. URL: http://dx.doi.org/10.1103/PhysRevLett.103.150502.

[31] Richard P Feynman. "Simulating physics with computers". In: Feynman and computation. CRC Press, 2018, pp. 133–153.

[32] Seth Lloyd. "Universal quantum simulators". In: Science 273.5278 (1996), pp. 1073–1078.

[33] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. "Achieving quantum supremacy with sparse and noisy commuting quantum computations". In: Quantum 1 (2017), p. 8.

[34] Aram W Harrow and Richard A Low. "Random quantum circuits are approximate 2-designs". In: Communications in Mathematical Physics 291 (2009), pp. 257–302.

[35] Benoıt Collins, Sho Matsumoto, and Jonathan Novak. "The Weingarten Calculus". In: NOTICES OF THE AMS 69.5 (2022).

[36] Yinzheng Gu. "Moments of random matrices and weingarten functions". PhD thesis. 2013.

[37] Daniel A Roberts and Beni Yoshida. "Chaos and complexity by design". In: Journal of High Energy Physics 2017.4 (2017), pp. 1–64.

[38] Yinchen Liu. "Moments of random quantum circuits and applications in random circuit sampling". MA thesis. University of Waterloo, 2021.

Robust and efficient verification of measurement-based quantum computation

Zihao Li[1] Huangjun Zhu[1] * Masahito Hayashi[2] †

[1] *Department of Physics and State Key Laboratory of Surface Physics, Institute for Nanoelectronic Devices and Quantum Computing, Center for Field Theory and Particle Physics, Fudan University*

[2] *School of Data Science, The Chinese University of Hong Kong, Shenzhen, International Quantum Academy (SIQA), and Graduate School of Mathematics, Nagoya University*

Abstract. To achieve reliable measurement-based quantum computation, it is crucial to verify whether the resource graph states are accurately prepared in the adversarial scenario. Previous verification protocols for this task are resource consuming or noise susceptible. Here, we propose a robust and efficient protocol for verifying arbitrary graph states with any prime local dimension in the adversarial scenario, which can be applied immediately to verifying measurement-based quantum computation. Our protocol requires only local Pauli measurements and is easy to realize with current technologies. It achieves the optimal scaling behaviors with respect to the system size and the target precision, and exponentially enhances the scaling behavior with the significance level.

Keywords: robust verification, MBQC, graph state, adversarial scenario

The technical version of this work is available on arXiv:2305.10742.

1 Introduction

Quantum computation offers the promise of exponential speedups over classical computation on certain important problems [1–3]. The very power of quantum computation raises the challenging problem of verifying the correctness of computation results. This problem lies at the heart of the active research field of quantum characterization, verification, and validation (QCVV) [4–9]. However, it is extremely difficult to construct robust and efficient verification protocols that apply to noisy, intermediate-scale quantum (NISQ) devices [3, 10, 11].

Measurement-based quantum computation (MBQC) [12–16] is a powerful and flexible model of quantum computation, where graph states are used as resources and local projective measurements on qudits are used to drive the computation. Compared with the preparation of multipartite entangled states, it is in general much easier to perform local projective measurements accurately. So the main challenge in the verification of MBQC lies in the verification of the underlying resource states.

In this paper, we consider the problem of verifying the resource graph states in the following adversarial scenario [17–23], which is pertinent to blind and cloud quantum computing [19, 24–26]: Alice is a client who can only perform single-qudit projective measurements, and Bob is a server who can prepare arbitrary quantum states. To perform MBQC, Alice delegates the preparation of the resource graph state $|G\rangle \in \mathcal{H}$ to Bob, who then prepares a state ρ on the whole system $\mathcal{H}^{\otimes M}$ and sends it to Alice qudit by qudit. If Bob is honest, then he is supposed to generate M copies of $|G\rangle$; while if he is malicious, then he can mess up the computation of Alice by generating an arbitrary correlated or even entangled state. To obtain reliable computation results, Alice needs to verify the resource state prepared by Bob with suitable tests on some systems of ρ. If the test results satisfy certain conditions, then she can guarantee that the reduced state on the remaining system is close enough to $|G\rangle$, and can safely use it for MBQC; otherwise, she rejects Bob's state. Since there is no communication from Alice to Bob after the preparation of ρ, the client's privacy is kept against the server by the no-signaling principle [24]. Hence, the procedure above is also suitable to verifying blind MBQC.

According to the above discussion, the problem of verifying MBQC reduces to the problem of verifying the resource graph state in the adversarial scenario [17, 19, 27]. However, it is highly nontrivial to construct robust and efficient verification protocols in the adversarial scenario. Although various protocols have been proposed [17–23], most protocols known so far are too resource consuming. Moreover, most protocols are not robust to experimental noise: the state prepared by Bob will be rejected with a high probability even if it has a very small deviation from the ideal state $|G\rangle$. However, in practice, it is unrealistic to ask honest Bob to generate the perfect resource state. In addition, if the state deviation from $|G\rangle$ is small enough, then it is still useful for MBQC [21, 22]. Therefore, a practical protocol should accept nearly ideal quantum states with a sufficiently high probability. Otherwise, Alice needs to repeat the verification protocol many times to accept such states, which may substantially increase the sampling complexity. Unfortunately, no protocol known in the literature can achieve this goal. A fault-tolerant verification protocol [26] that accepts noisy but still error-correctable states has been proposed, but it is robust only to certain correctable errors, and is difficult to realize in the current era of NISQ devices [3, 10, 11].

In this work, we propose a robust and efficient protocol for verifying blind MBQC. To achieve this goal we propose a robust and efficient protocol for verifying general qudit graph states with a prime local dimension in the

[*] zhuhuangjun@fudan.edu.cn

[†] hmasahito@cuhk.edu.cn

adversarial scenario. Our protocol is appealing to practical applications because it only requires stabilizer tests based on local Pauli measurements, which are easy to implement with current technologies. It is robust against arbitrary types of noise in state preparation, as long as the fidelity is sufficiently high. Moreover, our protocol can achieve optimal scaling behaviors with respect to the system size and target precision, and the sampling cost is comparable to the counterpart in the nonadversarial scenario. As far as we know, such a high efficiency has never been achieved before when robustness is taken into account. In addition to verifying MBQC, our approach can also be applied to verifying many other important quantum states in the adversarial scenario.

2 Verification of MBQC

Recently, a homogeneous strategy [17, 27] for testing qudit stabilizer states was proposed [17, 28]. Here we use a variant strategy for testing qudit graph states (d is a prime), which serves as an important subroutine of our verification protocol. The strategy is based on stabilizer tests with local Pauli measurements (see the technical version for details), and can be characterized by a two-outcome measurement $\{\Omega, \mathbb{I}-\Omega\}$, where the outcome Ω corresponds to passing the test, and the outcome $\mathbb{I}-\Omega$ corresponds to the failure. The operator Ω is called a strategy, and can be constructed as the form

$$\Omega = |G\rangle\langle G| + \lambda(\mathbb{I} - |G\rangle\langle G|) \qquad (1)$$

for any $1/d \leq \lambda < 1$. We denote by $\nu := 1-\lambda$ the spectral gap of Ω from the largest eigenvalue.

Suppose Alice intends to perform MBQC on the graph state $|G\rangle$ prepared by Bob. Our verification protocol runs as follows. First, Bob produces a state ρ on the whole space $\mathcal{H}^{\otimes(N+1)}$ with $N \geq 1$ and sends it to Alice. After receiving the state, Alice randomly permutes the $N+1$ systems of ρ (due to this procedure, we can assume that ρ is permutation invariant without loss of generality) and applies the strategy Ω in Eq. (1) to the first N systems. If at most k failures are observed among the N tests, Alice accepts the reduced state σ_{N+1} on the remaining system and uses it for MBQC; otherwise, she rejects it. Here the integer k is called the number of allowed failures, which is chosen by Alice before performing the tests.

With this verification protocol, Alice aims to achieve three goals: completeness, soundness, and robustness. The completeness means Alice does not reject the correct state. Since $|G\rangle$ can always pass each test, this goal is automatically guaranteed. The soundness means the following: once accepting, Alice needs to ensure with a small significance level δ that her state σ_{N+1} for MBQC has a sufficiently high fidelity (at least $1-\epsilon$) with $|G\rangle$. The threshold ϵ is called the target infidelity, which together with δ characterize the target verification precision. Among all known verification protocols, only the protocol of Refs. [17, 27] achieves the optimal sampling complexity with respect to all δ, ϵ, and the qudit number n of $|G\rangle$, even without considering the robustness. Although the condition of soundness looks simple, it is highly nontrivial to determine the degree of soundness. Even in the special case $k=0$, this problem was resolved only very recently after quite a lengthy analysis [17, 27].

To characterize the robustness of a protocol, we need to consider the case in which honest Bob prepares independent and identically distributed (i.i.d.) quantum states, that is, $\rho = \tau^{\otimes(N+1)}$ with $\tau \in \mathcal{D}(\mathcal{H})$. Due to inevitable noise, τ may not equal the ideal state $|G\rangle\langle G|$. Nevertheless, if the infidelity $\epsilon_\tau := 1 - \langle G|\tau|G\rangle$ is smaller than ϵ, then τ is still useful for MBQC. For a robust verification protocol, such a state should be accepted with a high probability. On the other hand, the probability that Alice accepts τ reads

$$p^{\mathrm{iid}}_{N,k}(\tau) = B_{N,k}\big(1-\mathrm{tr}(\Omega\tau)\big) = B_{N,k}(\nu\epsilon_\tau), \qquad (2)$$

where N is the number of tests, k is the number of allowed failures, and $B_{N,k}(p) := \sum_{j=0}^{k}\binom{N}{j}p^j(1-p)^{N-j}$ is the binomial cumulative distribution function.

To construct a robust verification protocol, k should be sufficiently large, so that $p^{\mathrm{iid}}_{N,k}(\tau)$ is sufficiently high. However, most previous protocols can only reach a meaningful conclusion when $k=0$ [17–20, 27], in which case the probability $p^{\mathrm{iid}}_{N,k=0}(\tau) = (1-\nu\epsilon_\tau)^N$ decreases exponentially with N, which is not satisfactory. Consequently, many repetitions are necessary to ensure that Alice accepts the state τ at least once. When $\epsilon_\tau = \epsilon/2$ for example, the number of repetitions is at least $\Theta(\exp[1/(4\delta)])$ for the protocol in [19] and $\Theta(\delta^{-1/2})$ for the protocol in [17, 27] as shown in the technical version, which substantially increases the actual sampling cost. Therefore, although some protocols known in the literature are reasonably efficient in achieving the soundness, they are not useful in verifying blind MBQC in a realistic scenario.

3 Results

3.1 Guaranteed infidelity

Suppose ρ is permutation invariant. Then the probability that Alice accepts ρ reads

$$p_k(\rho) = \sum_{i=0}^{k}\binom{N}{i}\mathrm{tr}\Big(\big[\Omega^{\otimes(N-i)}\otimes\overline{\Omega}^{\otimes i}\otimes\mathbb{I}\big]\rho\Big), \qquad (3)$$

where $\overline{\Omega} := \mathbb{I}-\Omega$. Denote by σ_{N+1} the reduced state on the remaining system when at most k failures are observed. The fidelity between σ_{N+1} and the ideal state $|G\rangle$ reads $F_k(\rho) = f_k(\rho)/p_k(\rho)$ [assuming $p_k(\rho) > 0$], where

$$f_k(\rho) = \sum_{i=0}^{k}\binom{N}{i}\mathrm{tr}\Big(\big[\Omega^{\otimes(N-i)}\otimes\overline{\Omega}^{\otimes i}\otimes|G\rangle\langle G|\big]\rho\Big). \qquad (4)$$

The actual verification precision can be characterized by the following figure of merit with $0 < \delta \leq 1$,

$$\bar{\epsilon}_\lambda(k,N,\delta) := 1 - \min_\rho\{F_k(\rho)\,|\,p_k(\rho) \geq \delta\}, \qquad (5)$$

where λ is determined by Eq. (1), and the minimization is taken over permutation-invariant states ρ on $\mathcal{H}^{\otimes(N+1)}$.

If Alice accepts the state prepared by Bob, then she can guarantee (with significance level δ) that the reduced state σ_{N+1} has infidelity at most $\bar{\epsilon}_\lambda(k,N,\delta)$ with $|G\rangle$. Consequently, the deviation of any measurement outcome probability from the ideal value is not larger than $\sqrt{\bar{\epsilon}_\lambda(k,N,\delta)}$. In the technical version we present the analytical formula and many useful properties of $\bar{\epsilon}_\lambda(k,N,\delta)$.

3.2 Verification with a fixed error rate

Now we set the number k to be proportional to the number of tests, that is, $k = \lfloor s\nu N\rfloor$, where $0 \le s < 1$ is the error rate. In this case, when Bob prepares i.i.d. states τ with infidelity $\epsilon_\tau < s$, the acceptance probability approaches one as N increases. In addition, we have the following theorems as proved in the technical version.

Theorem 1 *Suppose* $0 < s, \lambda < 1$, $0 < \delta \le 1/4$. *Then*

$$s - \frac{1}{\nu N} < \bar{\epsilon}_\lambda(\lfloor \nu s N\rfloor, N, \delta) \le s + \frac{1}{\nu\lambda}\sqrt{\frac{s\ln\delta^{-1}}{N}} + \frac{\ln\delta^{-1}}{2\nu^2\lambda N} + \frac{2}{\lambda N}. \qquad (6)$$

Theorem 1 implies that $\bar{\epsilon}_\lambda(\lfloor \nu s N\rfloor, N, \delta)$ converges to s when the number N of tests gets large. To achieve a given ϵ and δ, which means $\bar{\epsilon}_\lambda(\lfloor \nu s N\rfloor, N, \delta) \le \epsilon$, it suffices to set $s < \epsilon$ and choose a sufficiently large N.

Theorem 2 *Suppose* $0 < \delta \le 1/2$, $0 \le s < \epsilon < 1$, *and* $0 < \lambda < 1$. *Then we have* $\bar{\epsilon}_\lambda(\lfloor \nu s N\rfloor, N, \delta) \le \epsilon$ *as long as*

$$N \ge \frac{\epsilon}{[\lambda\nu(\epsilon - s)]^2}\left(\ln\delta^{-1} + 4\lambda\nu^2\right). \qquad (7)$$

Notably, if the ratio s/ϵ is a constant, then the sampling cost is only $O(\epsilon^{-1}\ln\delta^{-1})$, which is optimal with respect to all parameters ϵ, δ, and the qudit number n.

3.3 Sampling complexity of robust verification

Let ρ be the state on $\mathcal{H}^{\otimes(N+1)}$ prepared by Bob and σ_{N+1} be the reduced state after Alice performs suitable tests and accepts the state ρ. To verify the target state within infidelity ϵ, significance level δ, and robustness r (with $0 \le r < 1$) entails the following two conditions.

1. (Soundness) If the infidelity of σ_{N+1} with the $|G\rangle$ is larger than ϵ, then the acceptance probability $< \delta$.

2. (Robustness) If $\rho = \tau^{\otimes(N+1)}$ with $\tau \in \mathcal{D}(\mathcal{H})$ and $\epsilon_\tau \le r\epsilon$, then the acceptance probability $\ge 1 - \delta$.

Let k be the number of allowed failures; then the conditions of soundness and robustness can be expressed as

$$\bar{\epsilon}_\lambda(k,N,\delta) \le \epsilon, \qquad B_{N,k}(\nu r\epsilon) \ge 1 - \delta. \qquad (8)$$

Denote by $N_{\min}(\epsilon,\delta,\lambda,r)$ the minimum positive integer N such that Eq. (8) holds for some $k \le N - 1$. Then $N_{\min}(\epsilon,\delta,\lambda,r)$ is the minimum number of tests required for robust verification; it can be calculated numerically by using Algorithm 1 presented in the technical version.

Our following theorem provides an informative upper bound for $N_{\min}(\epsilon,\delta,\lambda,r)$ and clarifies the sampling complexity of robust verification.

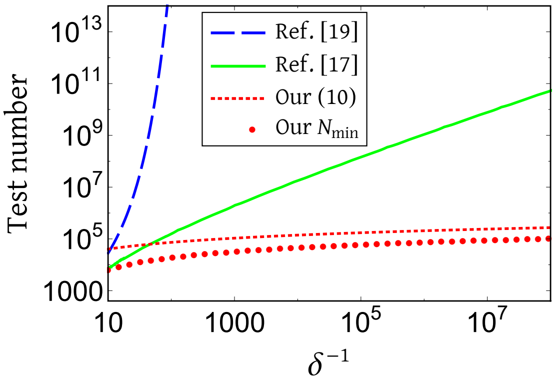


Figure 1: Number of tests required to verify a qudit graph state in the adversarial scenario within infidelity $\epsilon = 0.01$, significance level δ, and robustness $r = 1/2$. The red dots correspond to $N_{\min}(\epsilon,\delta,\lambda,r)$ with $\lambda = 1/2$; the red dashed curve corresponds to the RHS of Eq. (10), which is an upper bound for $N_{\min}(\epsilon,\delta,\lambda,r)$. The blue curve corresponds to the protocol in [19]; and the green curve corresponds to the protocol in [17] with $\lambda = 1/2$. The performances of the protocols in [21, 22] are not shown since the numbers of tests required are too large.

Theorem 3 *Suppose* $0 < \lambda, \epsilon < 1$, $0 < \delta \le 1/2$, *and* $0 \le r < 1$. *Then the conditions in Eq.* (8) *hold as long as*

$$k = \left\lfloor \left(\frac{\lambda\sqrt{2\nu} + r}{\lambda\sqrt{2\nu} + 1}\right)\nu\epsilon N\right\rfloor, \qquad (9)$$

$$N \ge \left\lceil \left[\frac{\lambda\sqrt{2\nu} + 1}{\lambda\nu(1 - r)}\right]^2 \frac{\ln\delta^{-1} + 4\lambda\nu^2}{\epsilon}\right\rceil. \qquad (10)$$

For given λ and r, the minimum number of tests is only $O(\epsilon^{-1}\ln\delta^{-1})$, which is independent of the qudit number n of $|G\rangle$ and achieves the optimal scaling behaviors with respect to the infidelity ϵ and significance level δ. If we choose $r = \lambda = 1/2$ for example, then Theorem 3 implies that $N_{\min}(\epsilon,\delta,\lambda,r) \le \lceil 144\,\epsilon^{-1}(\ln\delta^{-1} + 0.5)\rceil$, while numerical calculation shows $N_{\min}(\epsilon,\delta,\lambda,r) \le 67\,\epsilon^{-1}\ln\delta^{-1}$. Compared with previous protocols [17, 19, 27], our protocol improves the scaling behavior with respect to the significance level δ exponentially and even doubly exponentially, as illustrated in Fig. 1.

4 Discussion

We have proposed a highly robust and efficient protocol for verifying qudit (d is a prime) graph states in the adversarial scenario, which can be applied immediately to verifying blind MBQC. In addition to graph states, our protocol can also be used to verify many other important pure quantum states in the adversarial scenario (see the technical version for details), where the state preparation is controlled by a potentially malicious adversary, who can produce an arbitrary correlated or entangled state ρ on the whole system $\mathcal{H}^{\otimes(N+1)}$. Therefore, our verification protocol is of interest not only to blind MBQC, but also to many other tasks in quantum information processing that entail high-security.

References

[1] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th annual symposium on foundations of computer science* (IEEE, 1994) pp. 124-134.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).

[3] J. Preskill, Quantum Computing in the NISQ Era and Beyond. *Quantum* **2**, 79 (2018).

[4] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking. *Nat. Rev. Phys.* **2**, 382-390 (2020).

[5] J. Carrasco, A. Elben, C. Kokail, B. Kraus, and P. Zoller, Theoretical and Experimental Perspectives of Quantum Verification. *PRX Quantum* **2**, 010102 (2021).

[6] I. Šupić and J. Bowles, Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).

[7] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches. *Theory of Computing Systems* **63**, 05 (2019).

[8] M. Kliesch and I. Roth, Theory of quantum system certification. *PRX Quantum* **2**, 010201 (2021).

[9] X.-D. Yu, J. Shang, and O. Gühne, Statistical methods for quantum state verification and fidelity estimation. *Adv. Quantum Technol.* **5**, 2100126 (2022).

[10] F. Arute *et al.*, Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505 (2019).

[11] H.-S. Zhong *et al.*, Quantum computational advantage using photons. *Science* **370**, 1460 (2020).

[12] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer. *Phys. Rev. Lett.* **86**, 5188 (2001).

[13] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states. *Phys. Rev. A* **68**, 022312 (2003).

[14] D. L. Zhou, B. Zeng, Z. Xu, and C. P. Sun, Quantum computation based on d-level cluster state. *Phys. Rev. A* **68**, 062303 (2003).

[15] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia Measurement-based quantum computation beyond the one-way model. *Phys. Rev. A* **76**, 052315 (2006).

[16] H. J. Briegel, W. Dür, R. Raussendorf, and M. Van den Nest, Measurement-based quantum computation. *Nature Physics* **5**, 19 (2009).

[17] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario. *Phys. Rev. A* **100**, 062335 (2019).

[18] H. Zhu and M. Hayashi, Efficient verification of hypergraph states. *Phys. Rev. Appl.* **12**, 054047 (2019).

[19] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing. *Phys. Rev. Lett.* **115**, 220502 (2015).

[20] T. Morimae, Y. Takeuchi, and M. Hayashi, Verification of hypergraph states. *Phys. Rev. A* **96**, 062321 (2017).

[21] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States. *Phys. Rev. X* **8**, 021060 (2018).

[22] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, Resource-efficient verification of quantum computing using Serfling's bound. *npj Quantum Inf.* **5**, 27 (2019).

[23] Q. Xu, X. Tan, R. Huang, and M. Li, Verification of blind quantum computation with entanglement witnesses. *Phys. Rev. A* **104**, 042412 (2021).

[24] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements. *Phys. Rev. A* **87**, 050301(R) (2013).

[25] Y. Takeuchi, T. Morimae, and M. Hayashi, Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements. *Sci. Rep.* **9**, 13585 (2019).

[26] K. Fujii and M. Hayashi, Verifiable fault tolerance in measurement-based quantum computation. *Phys. Rev. A* **96**, 030301(R) (2017).

[27] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).

[28] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).

Unconditional quantum magic advantage in shallow circuit computation

Xingjian Zhang[1 2 *] Zhaokai Pan[1 †] Guoding Liu[1 ‡]

[1] *CQI, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084 China*
[2] *QICI, Department of Computer Science, University of Hong Kong, Pokfulam Road, Hong Kong*

Abstract. In this work, we discover a quantum pseudo-telepathy phenomenon that requires quantum magic, the essential ingredient for universal quantum computation. Translating the nonlocal phenomenon into a relation task, we provide the first unconditional proof of quantum magic advantage in computation. With recent experimental progress, we expect the computational task in this work to be faithfully realized on an upcoming early fault-tolerant quantum computing platform. We hope our results can inspire further explorations in this direction, eventually going beyond shallow circuits and solidifying the "magic" of universal quantum computation.

Keywords: quantum magic, shallow circuit computation, binary constraint system, quantum nonlocality

1 Introduction

Quantum theory promises computational speed-ups than classical means. The celebrated Gottesman-Knill Theorem implies that the full power of quantum computation resides in the specific resource of "magic" states — the secret sauce to establish universal quantum computation [1–3]. However, it is still questionable whether "magic" indeed brings the believed quantum advantage, ridding unproven complexity assumptions or black-box oracles. In this work, we study this issue and demonstrate the first unconditional magic advantage: a separation between the power of generic constant-depth or "shallow" quantum circuits and magic-free counterparts.

To establish the unconditional separation, we link the shallow circuit computation with the strongest form of quantum nonlocality — quantum "pseudo-telepathy," [4] where distant non-communicating observers generate perfectly synchronous statistics. Inspired by the linear binary constraint system [5], for the first time, we explicitly construct a quantum pseudo-telepathy correlation requiring magic resources and prove strict upper bounds on the correlation strength of solely magic-free operations. Then, we design a computational task that requires the output and the input to satisfy the constructed magic-necessary pseudo-telepathy correlations. This task separates the capabilities of generic quantum shallow circuits and their magic-free counterparts. We summarized our approach in Fig. 1.

As a by-product, we provide an efficient algorithm to solve a general linear binary constraint system over the Pauli group, in contrast to the broad undecidability in constraint systems [6, 7].

2 Basic Notions

2.1 Quantum magic

Quantum magic originates from the study of the classical simulation of quantum computation, closely related to the stabilizer formalism [1]. Consider an n-qubit quantum system. The Clifford group $\mathbb{C}_n$ is defined as the normalizer group of the Pauli group $\mathbb{P}_n$, namely the set of unitary operators that map a Pauli operator $P \in \mathbb{P}_n$ to a Pauli operator. Elements in the Clifford group are called Clifford operators or gates. A quantum circuit initialized in a computational-basis state and containing only Clifford gates and Pauli measurements is called a stabilizer circuit. Clearly, some unitary operators do not belong to the Clifford group, termed non-Clifford gates. Correspondingly, there are quantum states that cannot be prepared by any stabilizer circuit, even allowing post-selecting a subsystem upon Pauli measurement results. We call such states "magic" states [2].

2.2 Circuit classes

To realize universal quantum computation and achieve quantum advantage, some sort of "magic" must be involved, which can be either some magic states or non-Clifford gates [2, 3, 8–10]. In later discussions, we consider a model where all the magic comes from the non-Clifford gates. That is, the quantum state is initialized in $|0\rangle^{\otimes n}$, and the quantum measurement is performed on the computational basis. Depending on the type of computational resources, we categorize the circuits into three types. In a generic quantum circuit, the state undergoes operations in a universal gate set. Without quantum subsystems, the circuit degenerates into a classical one. In between, we define the Clifford or magic-free circuit, in which the quantum gates must be Clifford.

When the circuit is restricted to a constant depth, we call it a "shallow circuit." Furthermore, we consider the fan-in of gates to be bounded. Corresponding to a generic quantum circuit [11], a Clifford circuit, and a classical circuit [12, 13], we categorize the shallow circuits into classes of QNC^0, ClifNC^0, and NC^0, respectively.

2.3 Binary constraint systems (BCS)

Our starting point will be a special nonlocal game originating from the linear BCS [5]. A BCS comprises a set of Boolean functions, namely constraints, over binary variables $v_\gamma \in \{+1, -1\}$. For a linear BCS, the constraints are given in the form of $\prod_{\gamma\in\mathcal{S}_\alpha} v_\gamma = c_\alpha \in \{+1, -1\}$, where $\mathcal{S}_\alpha$ defines a subset of the variables. We say the

[*] zxj24@hku.hk
[†] pzk20@mails.tsinghua.edu.cn
[‡] lgd22@mails.tsinghua.edu.cn

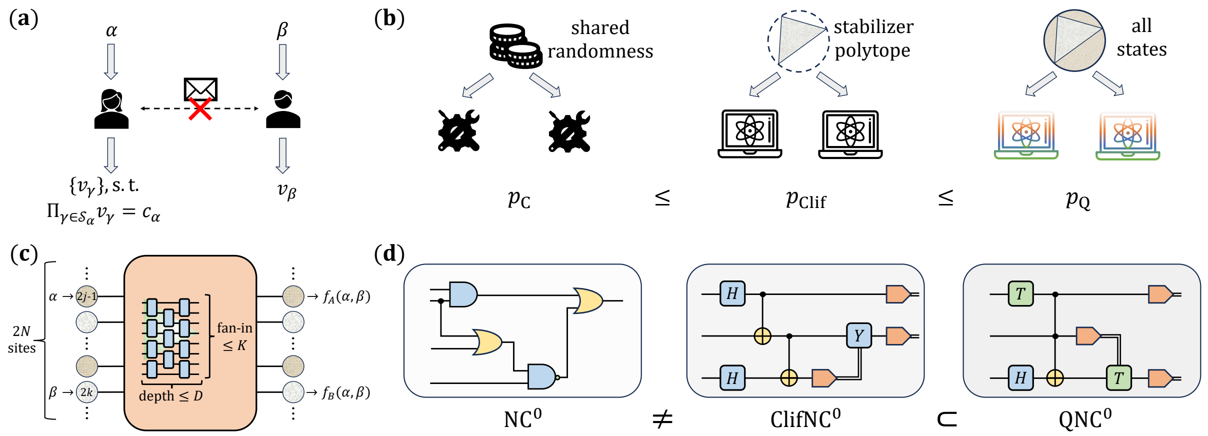


Figure 1: **(a)** A general BCS nonlocal game with non-communicating players. **(b)** Different game strategies. The three subfigures correspond to classical strategies, Clifford strategies, and general quantum strategies. **(c)** Solving a relation problem via a shallow circuit with bounded fan-in gates. **(d)** Categories of shallow circuits. Roughly speaking, the shallow circuit power corresponds to the corresponding strategies in nonlocal games given in (b).

BCS has a classical solution iff there exists a satisfying assignment to all the variables. The BCS can be generalized to an operator-valued set of functions, where the scalar variables are replaced with Hermitian operators A_γ with eigenvalues $\{+1,-1\}$, and the constraints are given in terms of $\prod_{\gamma\in\mathcal{S}_\alpha} A_\gamma = c_\alpha \mathbb{I}$ with $\mathbb{I}$ an identity operator of a finite dimension. In addition, the operators in each constraint need to be simultaneously measurable. We say the BCS has an operator-valued solution iff there exists an operator-valued satisfying assignment to all the Hermitian operators with an appropriate dimension.

2.4 BCS-based nonlocal games

Given a linear BCS, consider a corresponding nonlocal game with two non-communicating parties, Alice and Bob [Fig. 1(a)]. In each round of the game, a referee picks a constraint from the BCS labelled by α and a variable labelled by $\beta \in \mathcal{S}_\alpha$. The referee asks Alice to assign values to the variables satisfying the constraint and Bob to assign a value for v_β. The players win the game if and only if Alice gives a satisfying assignment for the constraint, and her assignment to v_β coincides with Bob's. Alice and Bob can agree on a game strategy in advance. We consider a hierarchy of their capabilities [Fig. 1(b)]:

1. *Classical strategies:* Players share common randomness and apply local classical operations;

2. *Clifford strategies:* Players share entanglement created by Clifford circuits and apply local Clifford operations and Pauli measurements;

3. *General strategies:* Players share general entanglement and apply general local quantum operations.

In the field of nonlocality, a perfect winning quantum strategy is termed "quantum pseudo-telepathy" [4]. The existence of a perfect winning classical/quantum strategy in the nonlocal game is equivalent to the existence of a classical/operator-valued solution to the underlying BCS [5, 14]. Specifically, a perfect winning Clifford strategy corresponds to a Pauli-string solution.

3 Main Results

Previously, a strict inclusion between NC^{0}and QNC^{0}was proved [15, 16]. In this work, we unconditionally confirm magic makes a strict hierarchy among shallow circuits [Fig. 1(d)]:

$$\mathsf{ClifNC}^0 \subset \mathsf{QNC}^0. \tag{1}$$

We take the following steps toward this main result: (1) Find a BCS that does not have classical or Pauli-string solutions but has generic observable solutions; (2) Based on the above BCS, construct a nonlocal game in which magic is necessary to win perfectly; (3) Transform the magic-necessary BCS nonlocal game to a relation problem separating ClifNC^{0}and QNC^0(Sec. 3.3).

For step (1), we develop an efficient approach to solving a linear BCS over the Pauli group (Sec. 3.1), which can then rule out BCS nonlocal games with perfect-winning Clifford/classical strategies. Afterward, we construct a BCS that has a non-trivial magic-necessary operator-valued solution and complete step (2) (Sec. 3.2).

3.1 Solving linear BCS over the Pauli group

To study Clifford strategies in the BCS nonlocal game, note that the Pauli strings are either anti-commuting, like $\{X, Z\} = 0$, or commuting, like $[X \otimes X, Z \otimes Z] = 0$. In addition, for two Pauli strings A, B, we have $\langle \Phi^+ | A \otimes B | \Phi^+ \rangle = \mathrm{tr}(AB^{\mathrm{T}})/d \in \{0, \pm 1\}$, where d is the system dimension. When restricting solving the BCS over the Pauli group, we can transform the original operator-valued BCS into a classically valued BCS for the commutators between the variables. We prove the following results for general linear BCS.

Theorem 1 *Given a linear BCS with l variables and m constraints, there exists a classical algorithm that finishes* *in* poly(l, m) *steps to determine whether the BCS has a Pauli-string operator-valued solution. If the answer is affirmative, the algorithm returns one such solution.*

Theorem 2 *Suppose a linear BCS does not have a Pauli-string solution. Then, for its associated nonlocal game, if Alice and Bob are restricted to Clifford strategies, either Alice fails to give satisfying assignments for all the constraints, or there exists one pair of questions (α, β), where the probability that Alice and Bob's assignments to v_β coincide does not exceed $1/2$.*

3.2 Magic-necessary BCS

Next, we construct a BCS family, some of which have a general quantum solution but no Pauli-string solution. This result explicitly falsifies a previous conjecture [17].

We present the BCS family in the language of graph theory. Consider an undirected complete graph $G = (V, E)$ with n vertices. The BCS contains the following variables: (1) Each vertex $v \in V$ corresponds to one variable a_v; (2) Each undirected edge $e = (u, v) \in E$ corresponds to three variables x_{uv}, y_{uv}, and z_{uv}; (3) Every two disjoint edges $e_1 = (u, v) \in E$ and $e_2 = (s, t) \in E$, where s, t, u, and v are different vertices, correspond to (i) variable $b_{e_1e_2} \equiv b_{uv|st}$, where $b_{e_1e_2} = b_{e_2e_1}$; (ii) variables $c_{e_1e_2} \equiv c_{uv|st}$ and $c_{e_2e_1} \equiv c_{st|uv}$, where $c_{e_1e_2} \neq c_{e_2e_1}$ in general. The smallest non-trivial BCS is defined on a graph with four vertices (Fig. 2). Based on these variables, the BCS contains the following constraints,

$$\begin{aligned} a_u a_v y_{uv} &= 1, \forall (u, v) \in E, \\ x_{uv} y_{uv} z_{uv} &= 1, \forall (u, v) \in E, \\ x_{uv} x_{st} b_{uv|st} &= 1, \forall (u, v), (s, t) \in E, \\ x_{uv} z_{st} c_{uv|st} &= 1, \forall (u, v), (s, t) \in E, \\ b_{uv|st} b_{vs|ut} b_{su|vt} &= 1, \forall u, v, s, t \in V, \\ c_{uv|st} c_{vs|ut} c_{su|vt} &= 1, \forall u, v, s, t \in V, \\ \prod_{v \in V} a_v &= -1. \end{aligned} \tag{2}$$

This BCS family exhibits a hierarchy among classical, Clifford, and general quantum resources. Based on the BCS nonlocal game construction, we state the result in terms of perfect winning strategies in the nonlocal games.

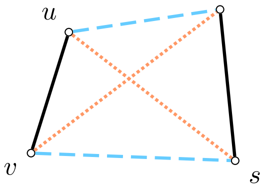


Figure 2: A subgraph illustrating the variables in Eq. (2).

Theorem 3 *For the nonlocal game defined through the BCS in Eq. (2),*

1. *$n = 4$: $\exists$ perfect-winning Clifford strategy, but it does not have a perfect-winning classical strategy;*
2. *$n \in 2\mathbb{N} + 5$: $\exists$ perfect-winning classical strategy;*
3. *$n \in 2\mathbb{N}+6$: $\exists$ strategies that exploit quantum magic to win perfectly, but it does not have a perfect-winning Clifford or classical strategy.*

As a corollary of Theorem 2, for the nonlocal game with $n \in 2\mathbb{N} + 6$, with uniformly distributed random questions, the winning probabilities of all Clifford and classical strategies can be upper-bounded by

$$p_{\text{Clif}} \leq 1 - \frac{1}{2|\mathcal{Q}|}, \tag{3}$$

where $\mathcal{Q}$ denotes the set of questions.

Here, we present one operator-valued solution to the BCS when $n = 8$. Labelling the vertices from 1 to 8, a realization of a_v and x_{uv} in the above BCS is

$$\begin{aligned} &a_v = \mathbb{I}_8 - 2\mathbf{e}_{vv}, v = 1, \cdots, 8, \\ &x_{uv} = \mathbb{I}_8 - \mathbf{e}_{uu} - \mathbf{e}_{vv} + \mathbf{e}_{uv} + \mathbf{e}_{vu}, u, v = 1, \cdots, 8, u \neq v, \end{aligned} \tag{4}$$

where $\mathbb{I}_8$ is an eight-dimensional identity operator, and $\mathbf{e}_{ij}$ denotes an elementary matrix. The other operators can be determined via a_v's and x_{uv}'s. The measurements corresponding to x_{uv} require non-Clifford operations, which can be realized by applying a Toffoli gate up to a local unitary operation, which is a non-Clifford gate, followed by the computational-basis measurement.

3.3 Magic advantage in shallow circuits

Building on the BCS nonlocal game defined through Eq. (2), we design a computational task that requires the output and the input to satisfy the constructed magic-necessary pseudo-telepathy correlations. Roughly speaking, consider a relation problem with $2N$ sites: two randomly chosen computing sites $2j-1$ and $2k$ are input with α and β and required to output the desired nonlocal outputs up to an allowed transformation depending on other sites [Fig. 1(c)]. Using a light-cone-type argument [15, 16], we prove that the only way a shallow circuit solves the relation problem is to apply the quantum pseudo-telepathy strategy as a subroutine, which necessarily requires magic.

Theorem 4 (Informal) *Given the nonlocal game defined by the BCS in Eq. (2) with size $n \in 2\mathbb{N} + 6$, $\exists$ relation problem R_N^n and a constant K, such that for circuits restricted to K-bounded fan-in gates,*

- *R_N^n can be perfectly solved by a* QNC^0 *circuit, where some gates are non-Clifford operations;*
- *Any Clifford circuit that solves R_N^n with probability larger than $(1 + p_{\text{Clif}})/2$ with p_{Clif} given in Eq. (3) must have a circuit depth $\Omega(\log N)$.*

References

[1] D. Gottesman, *Stabilizer codes and quantum error correction* (California Institute of Technology, 1997).

[2] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005), URL `https://link.aps.org/doi/10.1103/PhysRevA.71.022316`.

[3] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004), URL `https://link.aps.org/doi/10.1103/PhysRevA.70.052328`.

[4] G. Brassard, A. Broadbent, and A. Tapp, Found. Phys. **35**, 1877 (2005).

[5] R. Cleve and R. Mittal, in *Automata, Languages, and Programming: 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I 41* (Springer, 2014), pp. 320–331.

[6] W. Slofstra, in *Forum Math. Pi* (Cambridge University Press, 2019), vol. 7, p. e1.

[7] W. Slofstra, J. Am. Math. Soc. **33**, 1 (2020).

[8] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001), URL `https://link.aps.org/doi/10.1103/PhysRevLett.86.5188`.

[9] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003), URL `https://link.aps.org/doi/10.1103/PhysRevA.68.022312`.

[10] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016), URL `https://link.aps.org/doi/10.1103/PhysRevX.6.021043`.

[11] P. Høyer and R. Špalek, in *STACS 2003*, edited by H. Alt and M. Habib (Springer Berlin Heidelberg, Berlin, Heidelberg, 2003), pp. 234–246, ISBN 978-3-540-36494-8.

[12] N. Pippenger, in *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)* (1979), pp. 307–311.

[13] S. A. Cook, Inf. Control. **64**, 2 (1985), ISSN 0019-9958, URL `https://www.sciencedirect.com/science/article/pii/S0019995885800413`.

[14] R. Cleve, L. Liu, and W. Slofstra, J. Math. Phys. **58**, 012202 (2017).

[15] S. Bravyi, D. Gosset, and R. König, Science **362**, 308 (2018), URL `https://www.science.org/doi/abs/10.1126/science.aar3106`.

[16] S. Bravyi, D. Gosset, R. König, and M. Tomamichel, Nat. Phys. **16**, 1040 (2020), ISSN 1745-2481, URL `https://doi.org/10.1038/s41567-020-0948-z`.

[17] A. Arkhipov, arXiv:1209.3819 (2012).

Unconditional quantum magic advantage in shallow circuit computation

Xingjian Zhang,[1, 2, 3, 4, *] Zhaokai Pan,[1, †] and Guoding Liu[1, ‡]

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[2] *Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*

[3] *Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[4] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

(Dated: May 20, 2024)

Quantum theory promises computational speed-ups than classical means. The celebrated Gottesman-Knill Theorem implies that the full power of quantum computation resides in the specific resource of “magic” states — the secret sauce to establish universal quantum computation. However, it is still questionable whether “magic” indeed brings the believed quantum advantage, ridding unproven complexity assumptions or black-box oracles. In this work, we demonstrate the first unconditional magic advantage: a separation between the power of generic constant-depth or “shallow” quantum circuits and magic-free counterparts. For this purpose, we link the shallow circuit computation with the strongest form of quantum nonlocality — quantum “pseudo-telepathy,” where distant non-communicating observers generate perfectly synchronous statistics. We prove quantum magic is indispensable for such correlated statistics in a specific nonlocal game inspired by the linear binary constraint system. Then, we translate generating quantum pseudo-telepathy into a relation problem, where magic is necessary for a shallow circuit to solve it perfectly. As a by-product, we provide an efficient algorithm to solve a general linear binary constraint system over the Pauli group, in contrast to the broad undecidability in constraint systems. We anticipate our results will enlighten the final establishment of the unconditional advantage of universal quantum computation.

I. INTRODUCTION

Starting from Richard Feynman’s proposal of simulating physics with quantum means [1], it has been an appealing quest to exploit phenomena unique to quantum theory to accelerate computation. A series of results, such as Shor’s factoring algorithm [2] and Grover’s search [3], strengthen the belief in the power of quantum computation. Notwithstanding the prosperity in the zoo of quantum algorithms, it is still intriguing to answer the basic questions: Does quantum theory really bring a computational advantage over classical means, and if yes, what is the origin of such power? A well-known statement that seems to respond to both questions is quantum “magic” [4]. The so-called quantum magic states are beyond the reach of stabilizer circuits, the ones initialized in the computational-basis state and composed of only Clifford gates and Pauli measurements. The Gottesman-Knill Theorem shows that stabilizer circuits can be perfectly simulated by classical computers in a polynomial time of the input size, deemed as efficient [5–7]. On the other hand, attempts from the simulation field suggest a strong relevance between the quantity of magic and the extent of quantum advantage [8–16]. Quantum algorithms richer in magic are often more difficult for a classical computer to simulate.

Indeed, considering the structure of quantum state space, magic states, or equivalently non-Clifford operations, is indispensable for a complete picture [4, 17]. In contrast, whether they bring a super-polynomial or even an exponential quantum computational advantage as promised remains to be proved. Despite numerous good reasons to believe in its validity [18, 19], unfortunately, explorations to date have not got rid of assumptions of unproven hardness for classical algorithms, such as factoring a large number in Shor’s algorithm [2], or reliance on queries to a black-box oracle as in Grover’s search [3], where the oracle construction may be hard work.

To firmly establish the quantum advantage, one may alternatively start from a more restrictive regime in complexity. Instead of defining “efficient” as a polynomially growing time, a notable regime is the set of shallow circuits [20, 21], where the circuit depth, or equivalently the computing time, is restricted to a constant irrelevant to the problem size. The consideration of quantum shallow circuits was partly attributed to an experimental perspective, as it is relatively simpler to deal with system decoherence within a fixed time [22]. More importantly, theorists have rich toolkits from quantum information theory to aid the investigations. A particular instrument is quantum nonlocality, a most distinguishing property of quantum theory [23, 24]. As shown by the renowned Bell theorem [25], entanglement leads to purely quantum

[*] zxj24@hku.hk

[†] pzk20@mails.tsinghua.edu.cn

[‡] lgd22@mails.tsinghua.edu.cn

correlations between nonlocal observers beyond the scope of classical physics [26]. One can translate quantum nonlocality into a computational task to generate nonlocal statistics among distant computing sites [27–30]. While classical circuits require a growing time with respect to the input size to scramble the information for computation, quantum shallow circuits are competent to the task, bringing an unconditional advantage.

Despite the recent progress in shallow circuits, a vague question arises: Is "magic" indispensable for the full power of quantum computation in the low-complexity regime? Indeed, among all the existing explorations of quantum shallow circuits, the essential ingredient for the quantum advantage — long-range entanglement, can be generated with Clifford circuits without using the magic resource [31]. On the other hand, though not rigorous, with our experiences in the complexity theory such as the padding argument [32], we may be inclined to think of a collapse of the power of universal quantum computation if magic makes no difference in the low-complexity regime. Following the logic of relating nonlocality with shallow circuit computation, a relevant question is the role of quantum magic in nonlocality, which is much unexplored compared to the more prevalent quantum features like entanglement.

In this work, we unconditionally confirm that quantum magic brings an advantage, at least in a shallow circuit. For this purpose, we consider the strongest form of nonlocality, where nonlocal observers generate perfectly synchronous statistics, namely quantum "pseudo-telepathy" [23]. For the first time, we explicitly construct a quantum pseudo-telepathy correlation requiring magic resources and prove strict upper bounds on the correlation strength of solely magic-free operations. Then, we design a computational task that requires the output and the input to satisfy the constructed magic-necessary pseudo-telepathy correlations. This task separates the capabilities of generic quantum shallow circuits and their magic-free counterparts. We summarize our approach in Fig. 1.

II. BASIC NOTIONS AND MAIN RESULT

The concept of quantum magic originates from the study of the classical simulation of quantum computation, closely related to the stabilizer formalism [5]. Consider an n-qubit quantum system on which the Pauli group is defined as the set of operators

$$\mathbb{P}_n = \{\pm 1, \pm i\} \times \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}^{\otimes n}, \tag{1}$$

together with operator multiplication. Here, $\mathbb{I}$ is the two-dimensional identity operator, and $\sigma_x, \sigma_y, \sigma_z$ are the qubit Pauli matrices. The Clifford group is defined as the normalizer group of the Pauli group $\mathbb{P}_n$:

$$\mathbb{C}_n = \{C \in \mathbb{U}_n | \forall P \in \mathbb{P}_n, CPC^\dagger \in \mathbb{P}_n\}, \tag{2}$$

where $\mathbb{U}_n$ is the set of all n-qubit unitary operators. Elements in the Clifford group are called Clifford operators or gates. A quantum circuit initialized in the computational-basis state and containing only Clifford gates and Pauli measurements is called a stabilizer circuit. Note that the Pauli measurements are equivalent to applying some Clifford gates, followed by computational-basis measurements. The Gottesman-Knill theorem states that the measurement results can be well-simulated by a classical circuit running in a time that is polynomial in the number of qubits [5, 6].

Clearly, there are unitary operators that do not belong to the Clifford group. Well-known non-Clifford operations include the T-gate, which adds a non-trivial relative phase to basis state superposition:

$$a|0\rangle + b|1\rangle \to a|0\rangle + e^{i\pi/4} b|1\rangle, \tag{3}$$

and the Toffoli gate, the quantum generalization of the NAND gate:

$$|c_1\rangle|c_2\rangle|t\rangle \to |c_1\rangle|c_2\rangle|t \oplus (c_1 \cdot c_2)\rangle, \tag{4}$$

where $c_1, c_2, t \in \{0, 1\}$ represent the values in the two control qubits and the target qubit, respectively. Correspondingly, there are quantum states that cannot be prepared by any stabilizer circuit, even allowing post-selecting a subsystem upon Pauli measurement results. We call such states "magic" states. As an example, the state

$$|H\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle \tag{5}$$

is a qubit magic state.

To realize universal quantum computation and achieve quantum advantage, some sort of "magic" must be involved, which can be either some magic states or non-Clifford gates [4, 6, 9, 33, 34]. In later discussions, we consider a model where all the magic comes from the gates. That is, the quantum state is initialized in $|0\rangle^{\otimes n}$, and the quantum measurement is performed on the computational basis. Depending on the type of computational resources, we categorize the circuits into three types. In a generic quantum circuit, the state undergoes operations in a universal gate set. Without quantum subsystems, the circuit degenerates into a classical one. We further define the Clifford or magic-free circuit, in which the quantum gates must be Clifford. Note that in generic quantum circuits or magic-free circuits, we also allow intermediate quantum measurements for feedback and classically controlled operations for assistance. In Clifford circuits, we restrict the classical feedback to perform the logical operations of parity and negation and controlled-Pauli operations [35].

Besides the accessible computational resources, the power of a circuit is also influenced by the circuit depth and the gate fan-in. The circuit depth is defined as the number of steps to perform all the gates and measurements. Note that in one step, multiple gates acting on

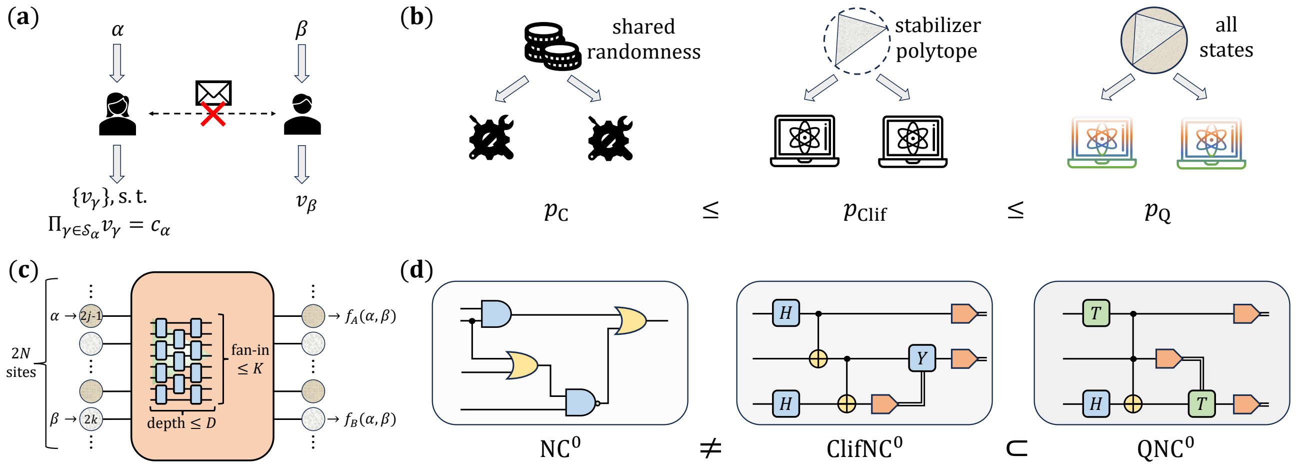


FIG. 1: **(a)** A general BCS nonlocal game with non-communicating players. Given a BCS, the input or the question to Alice is a constraint indexed by α, and the question to Bob is a variable indexed by β, with $\beta \in \mathcal{S}_\alpha$, where $\mathcal{S}_\alpha$ corresponds to the set of variables in constraint labeled with α. The players win the game if and only if Alice outputs an assignment to the variables $\{v_\gamma\}_\gamma$ satisfying the constraint $\prod_{\gamma\in\mathcal{S}_\alpha} v_\gamma = c_\alpha$, and Alice and Bob give an identical assignment to v_β. **(b)** Different game strategies. (1) Classical strategy: players share randomness and apply local classical operations. (2) Clifford strategy: players share entanglement prepared by stabilizer circuits and apply local Clifford operations and local Pauli measurements. The set of stabilizer states forms a convex polytope [7, 8]. (3) General strategy: players share a general entangled state and apply general local quantum operations. The set of all quantum states is a convex set. There is a hierarchy among the maximum winning probabilities in each level: $p_{\mathrm{C}} \leq p_{\mathrm{Clif}} \leq p_{\mathrm{Q}}$. We present a family of nonlocal games via Eq. (9), which manifest levelled quantum pseudo-telepathy, namely $p_{\mathrm{C}} < p_{\mathrm{Clif}} = 1$ and $p_{\mathrm{Clif}} < p_{\mathrm{Q}} = 1$ under different game parameters. **(c)** Solving a relation problem via a shallow circuit with bounded fan-in gates. The circuit depth D and the maximum gate fan-in K are both fixed constants. The BCS nonlocal game can be translated to a relation problem on $2N$ sites: two randomly chosen computing sites $2j-1$ and $2k$ are input with α and β and required to output $f_A(\alpha,\beta)$ and $f_B(\alpha,\beta)$, respectively, up to a transformation depending on other sites. The bounded fan-in and constant depth conditions restrict each output site to be affected only by a constant number of input sites, as shown by the lightcone shaded in green. **(d)** Categories of shallow circuits. (1) NC^0: classical shallow circuits with bounded fan-in gates, comprising classical gates like $\mathsf{AND}, \mathsf{OR}, \mathsf{NOT}, \mathsf{NAND}$. (2) ClifNC^0: magic-free shallow circuits with bounded fan-in gates, comprising a magic-free initial quantum state, Clifford gates like $\mathsf{H}, \mathsf{S}, \mathsf{CNOT}$, and (intermediate) Pauli measurements. Classical feedback is allowed. (3) QNC^0: general quantum shallow circuits with bounded fan-in gates, allowing a generic initial state and non-Clifford gates like the T gate and the Toffoli gate. In this work, we prove the strict inclusion of $\mathsf{ClifNC}^0 \subset \mathsf{QNC}^0$.

different subsystems can be implemented in parallel. The gate fan-in is defined as the number of input (quantum) bits a gate can act on. For instance, the T gate has fan-in 1, and the Toffoli gate has fan-in 3. In our definition, the fan-in includes both classical bits and qubits, as depicted and explained in Fig. 2, e.g., a T gate controlled by a classical bit has fan-in 2. In this way, we unify the discussions for classical logical gates, quantum gates, classically controlled quantum gates, and measurements.

In this work, we are interested in the computational power of shallow circuits with bounded fan-in gates. That is, the circuit depth is a constant, and the fan-in of all the operations in the circuit has a constant upper bound. Within this restriction, we denote the classes of classical circuits [20, 36], Clifford circuits, and generic quantum circuits [37] as NC^0, ClifNC^0, and QNC^0, respectively. We depict examples of these circuits in Fig. 1(d). As a remark, we overuse the complexity class notations for the associated circuits, like previous works in the field.

Previously, a strict inclusion between $\mathsf{NC}^0$and $\mathsf{QNC}^0$was proved [27, 28]. Here, we show magic makes a strict hierarchy among shallow circuits:

$$\mathsf{ClifNC}^0 \subset \mathsf{QNC}^0. \tag{6}$$

III. BINARY-CONSTRAINT-SYSTEM-BASED NONLOCAL GAMES

A. Preliniminaries of binary constraint systems

To prove the main result in Eq. (6), essentially, we manifest nonlocal correlations where magic states or non-Clifford operations play a non-trivial role. Our starting point is a special nonlocal game originating from the lin-

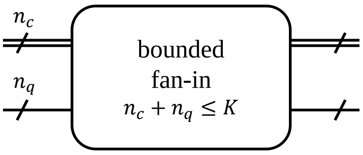


FIG. 2: A general K-bounded fan-in gate. In general, it acts on n_c bits and n_q qubits, with $n_c + n_q \le K$. When $n_c = 0$, it becomes a normal quantum gate characterized by a unitary operation. When $n_q = 0$, it becomes a normal classical gate.

ear binary constraint system (BCS) [38]. A BCS comprises a set of Boolean functions, namely constraints, over binary variables v_γ. We take the variable values over $\{+1, -1\}$ for later convenience. For a linear BCS, the constraints are given by functions in the form of $\prod_{\gamma \in \mathcal{S}_\alpha} v_\gamma = c_\alpha \in \{+1, -1\}$, where $\mathcal{S}_\alpha$ defines a subset of the variables. Given a linear BCS, consider a corresponding nonlocal game with two parties, Alice and Bob, as shown in Fig. 1(a). In each round of the game, a referee picks a constraint from the BCS labeled by α and a variable labeled by $\beta \in \mathcal{S}_\alpha$. The referee asks Alice to assign values to the variables satisfying the constraint and Bob to output a value for v_β. The nonlocal players win the game if and only if

1. Alice gives a satisfying assignment for the constraint c_α, and
2. Alice's assignment to v_β coincides with Bob's.

Alice and Bob cannot communicate with each other once the game starts. Nevertheless, they can agree on a game strategy in advance.

Naturally, the existence of a perfect winning strategy is related to the properties of the underlying linear BCS. If and only if the linear BCS has a solution where a fixed value assignment to the variables satisfies all the constraints, Alice and Bob can win the associated nonlocal game with certainty by classical means [38]. Otherwise, the winning probability by any classical strategy, where the players are restricted to shared randomness and local classical operations, is strictly upper-bounded from 1.

Notwithstanding, even if a fixed satisfying assignment does not exist, the nonlocal players may still win the game perfectly by exploiting quantum strategies. For a systematic study, we first generalize the BCS to a set of operator-valued functions. The scalar variables are replaced with Hermitian operators A_γ of a finite dimension with eigenvalues $\{+1, -1\}$, and the constraints become $\prod_{\gamma \in \mathcal{S}_\alpha} A_\gamma = c_\alpha \mathbb{I}$ with $\mathbb{I}$ an identity operator. In addition, the observables corresponding to the variables in each constraint are required to be compatible, namely jointly measurable. The existence of a quantum perfect winning strategy is equivalent to the operator-valued BCS having a solution [38]. Suppose the solution to the operator-valued BCS is given by a set of d-dimensional operators, $\{A_\gamma\}_\gamma$, then the perfect winning strategy in the corresponding nonlocal game goes as follows:

1. Alice and Bob first share a maximally entangled state, $|\Phi^+\rangle = \sum_{i=0}^{d-1} |ii\rangle / \sqrt{d}$;
2. After the game starts, Alice measures the observables $\{A_\gamma\}_\gamma$, and Bob measures the observables $\{A_\gamma^{\mathrm{T}}\}_\gamma$ to assign values to the variables, where T denotes the operator transpose.

By construction, Alice's measurement results satisfy the constraint. Also, as the maximally entangled state has the property

$$\langle \Phi^+ | A_\gamma \otimes A_\gamma^{\mathrm{T}} | \Phi^+ \rangle = \frac{1}{d} \mathrm{tr}\left(A_\gamma^2\right) = 1, \tag{7}$$

the assignments of Alice and Bob to the same variable thus coincide.

Due to the intrinsic randomness in quantum measurements, an observable may take different outcomes in each constraint, hence assigning a different value to the same variable. Such flexibility brings an advantage over classical means, where quantum resources bring Alice and Bob "pseudo-telepathy" as if they knew what was going on at the other side via a "spooky action" [23]. We shall further discuss this issue and review relevant existing results in the Supplementary Information (SI) Sec. IB, such as the famous Mermin-Peres nonlocal game [39, 40].

B. Clifford strategies in BCS-based nonlocal games

Among quantum strategies for the nonlocal game, there are different levels of capabilities, as shown in Fig. 1(b). Instead of having access to all quantum states and operations, we consider constraining the players to apply only Clifford strategies. Specifically, Alice and Bob can apply Clifford operations to a state initialized in $|0\rangle$ before the nonlocal game to create entanglement. Afterward, they each take a share of the state and apply only Pauli-string measurements to the state for the game. If the nonlocal game has a Clifford strategy that wins perfectly, then the underlying BCS has a Pauli-string solution, and *vice versa*. Notably, we derive the following results for general linear BCS. We prove Theorem 1 in SI Sec. VB and Theorem 2 in SI Sec. III.

Theorem 1. *Given a linear BCS with l variables and m constraints, there exists a classical algorithm that finishes in* $\mathrm{poly}(l, m)$ *steps to determine whether the BCS has a Pauli-string operator-valued solution. If the answer is affirmative, the algorithm returns one such solution.*

Theorem 2. *Suppose a linear BCS does not have a Pauli-string solution. Then, for its associated nonlocal game, if Alice and Bob are restricted to Clifford strategies, either Alice fails to give satisfying assignments for all the constraints, or there exists one pair of questions (α, β), where the probability that Alice and Bob's assignments to v_β coincide does not exceed $1/2$.*

Theorem 1 improves previous attempts of searching for a Pauli-string solution to a linear BCS [41, 42], which poses additional requirements on the appeared times of each variable. Besides, Theorem 1 sharply contrasts the common undecidability in the field of constraint systems, such as determining the existence of an operator-valued solution to a general BCS, which may not be Pauli strings [43].

Theorem 2 constraints the capability of Clifford strategies when the underlying BCS does not have Pauli-string solutions. In later discussions, we will apply Theorem 2 to compute the maximum winning probability of Clifford strategies playing magic-necessary BCS nonlocal games.

Here, we describe the algorithm for finding Pauli-string solutions to a general linear BCS. The algorithm highly relies on the following properties of Pauli operators, as shown by the following lemma.

Lemma 1. *Suppose $A_1, A_2, \cdots, A_l$ are Pauli-string observables. For $j, k = 1, \cdots, l$, define $C_{jk} = A_j A_k A_j A_k$ as the commutator between A_j and A_k. Then, C_{jk}'s have the following properties:*

1. *$C_{jk} \in \{\pm\mathbb{I}\}$. Specifically, $C_{jk} = \mathbb{I}$ when $A_j A_k - A_k A_j = 0$, and $C_{jk} = -\mathbb{I}$ when $A_j A_k + A_k A_j = 0$;*
2. *$C_{jk} = C_{kj}$ and $C_{jj} = \mathbb{I}$;*
3. *$A_j A_k = C_{jk} A_k A_j$.*

The proof of Lemma 1 is straightforward. Now, suppose there exists a Pauli-string solution to the BCS with l variables and m constraints. Using this lemma, we can apply variable substitution and exchange the order between variables A_j and A_k similarly as solving a classical linear BCS, up to a sign change due to the Pauli operator commutation. In the end, we can express each variable A_i in the BCS via a set of independent variables $\{A_r\}_r$ and sign variables C_i's. In SI Sec. VB, we prove that with a further substitution of the expressions into the original BCS, we can transform the BCS into a linear BCS of solely the sign variables C_i's and commutators C_{jk}'s between independent variables. The substitution thus far is efficient, namely in poly(l, m) steps. Since the new BCS is defined over $\mathbb{Z}_2$, it can be efficiently solved. If the new BCS does not have a solution, then by contradiction, the original BCS does not have a Pauli-string solution.

If the new BCS has a solution, we can assign Pauli-string operators to the independent variables $\{A_r\}_r$ in the original BCS, which satisfies the required commutation conditions. Here, we give an explicit construction. Suppose there are p commutators equal to -1, given by $C_{j_1k_1}, C_{j_2k_2}, \cdots, C_{j_pk_p}$. Then, we can construct Pauli strings over p qubits according to the following rule: For every q'th qubit in each Pauli string, where $1 \leq q \leq p$, assign σ_x for A_{j_q} and σ_z for A_{k_q}; assign all the other qubits as $\mathbb{I}$. That is,

$$\text{the } q\text{'th qubit of } A_r = \begin{cases} \sigma_x, & \text{if } r = j_q, \\ \sigma_z, & \text{if } r = k_q, \\ \mathbb{I}, & \text{otherwise.} \end{cases} \tag{8}$$

It can be directly checked that this construction satisfies the requirements. The rest of the variables are then determined by the independent variables and sign variables C_i's. This finishes the algorithm.

IV. MAGIC-NECESSARY QUANTUM PSEUDO-TELEPATHY

A. Magic-necessary BCS

Previously, it was conjectured that whenever a linear BCS nonlocal game has a perfect winning strategy, it is either a Clifford or a classical one [41]. Recent group embedding results evidence the falseness of the above conjecture [43, 44]. Here, we take a relevant yet different approach and directly present a linear BCS nonlocal game to disprove the conjecture. To make it illustrative, we state the underlying BCS in the language of graph theory. Consider an undirected complete graph $G = (V, E)$ with n vertices. An undirected graph indicates that for any two connected vertices, u and v, the tuples (u, v) and (v, u) represent the same edge. The BCS contains the following variables:

1. Each vertex $v \in V$ corresponds to one variable a_v.
2. Each undirected edge, denoted by $e = (u, v) \in E$, corresponds to three variables x_{uv}, y_{uv}, and z_{uv}.
3. Every two disjoint edges, denoted by $e_1 = (u, v) \in E$ and $e_2 = (s, t) \in E$, where s, t, u, and v are different vertices, correspond to
   (a) one variable $b_{e_1e_2} \equiv b_{uv|st}$, where $b_{e_1e_2} = b_{e_2e_1}$;
   (b) two variables $c_{e_1e_2} \equiv c_{uv|st}$ and $c_{e_2e_1} \equiv c_{st|uv}$, where $c_{e_1e_2} \neq c_{e_2e_1}$ in general.

For clarity, we express the variables with respect to the underlying vertices and denote the BCS (nonlocal game) size with the number of vertices. The smallest non-trivial BCS is defined on a graph with four vertices, as shown in Fig. 3. Based on these variables, the BCS contains the following constraints,

$$\begin{aligned} a_u a_v y_{uv} &= 1, \forall (u, v) \in E, \\ x_{uv} y_{uv} z_{uv} &= 1, \forall (u, v) \in E, \\ x_{uv} x_{st} b_{uv|st} &= 1, \forall (u, v), (s, t) \in E, \\ x_{uv} z_{st} c_{uv|st} &= 1, \forall (u, v), (s, t) \in E, \\ b_{uv|st} b_{vs|ut} b_{su|vt} &= 1, \forall u, v, s, t \in V, \\ c_{uv|st} c_{vs|ut} c_{su|vt} &= 1, \forall u, v, s, t \in V, \\ \prod_{v \in V} a_v &= -1. \end{aligned} \tag{9}$$

This family of BCS's exhibits a hierarchy among classical, Clifford, and general quantum resources, as shown by the following theorem.

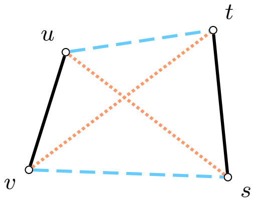


FIG. 3: A subgraph with four vertices to illustrate the BCS variables in Eq. (9). Each vertex v corresponds to one variable a_v, and there are four such variables in the subgraph. Each undirected edge $e = (u, v)$ corresponds to three variables x_{uv}, y_{uv}, z_{uv}. With six edges in the subgraph, there are six variables for each kind. Every two disjoint edges $e_1 = (u, v), e_2 = (s, t)$ correspond to two kinds of variable $b_{uv|st} = b_{st|uv}$ and $c_{uv|st}, c_{st|uv}$. The subgraph has three sets of disjoint edges, denoted by black solid lines, blue dashed lines, and orange dotted lines, respectively. Consequently, there are three variables of the kind $b_{uv|st}$ and six variables of the kind $c_{uv|st}$.

Theorem 3. *For the nonlocal game defined through the BCS in Eq.* (9),

1. *when $n = 4$, it has a perfect-winning Clifford strategy, but it does not have a perfect-winning classical strategy;*
2. *when $n \in 2\mathbb{N} + 5 = \{5, 7, 9, \cdots\}$, it has a perfect-winning classical strategy;*
3. *when $n \in 2\mathbb{N} + 6 = \{6, 8, 10, \cdots\}$, it has strategies that exploit quantum magic to win perfectly, but it does not have a perfect-winning Clifford strategy or classical strategy.*

The full proof of Theorem 3 is presented in SI Sec. II. One can apply Theorem 1 to check that the BCS defined in Eq. (9) with $n \in 2\mathbb{N}+6$ does not have Pauli-string solutions. As a consequence, the associated nonlocal game does not have a perfect-winning Clifford strategy or classical strategy.

As a corollary of Theorem 2, for the nonlocal game with $n \in 2\mathbb{N} + 6$, with uniformly distributed random questions, the winning probabilities of all Clifford and classical strategies can be upper-bounded by

$$p_{\text{Clif}} \leq 1 - \frac{1}{2|\mathcal{Q}|}, \tag{10}$$

where $\mathcal{Q}$ denotes the set of questions in the nonlocal game. For the BCS given in Eq. (9), we denote the set of questions for Alice as $\tilde{\mathcal{Q}}_A$, namely the BCS constraints, and the set of questions for Bob as $\tilde{\mathcal{Q}}_B$, namely the BCS variables. In Table I and II, we give the expressions to calculate the set sizes. We also provide the concrete numbers for the case of $n = 8$. For the BCS game of size n with uniformly distributed questions, by applying Theorem 2, we obtain a direct upper bound on the average winning probability of Clifford strategies as $1 - 1/(2[3(|\tilde{\mathcal{Q}}_A| - 1) + n])$. Note that the constraint $\prod_{v\in V} a_v = -1$ comprises n variables, while every other constraint consists of three variables.

constraint format	expression	number $(n = 8)$
$aa'y = 1$	$\binom{n}{2}$	28
$xyz = 1$	$\binom{n}{2}$	28
$xx'b = 1$	$\binom{n}{4} \cdot 3$	210
$xzc = 1$	$\binom{n}{4} \cdot 3 \cdot 2$	420
$bb'b'' = 1$	$\binom{n}{4}$	70
$cc'c'' = 1$	$\binom{n}{4} \cdot 4$	280
$\prod a = -1$	1	1
total	$\lvert\tilde{\mathcal{Q}}_A\rvert$	1037

TABLE I: Number of constraints in the BCS game.

variable type	expression	number $(n = 8)$
a	n	8
x	$\binom{n}{2}$	28
y	$\binom{n}{2}$	28
z	$\binom{n}{2}$	28
b	$\binom{n}{4} \cdot 3$	210
c	$\binom{n}{4} \cdot 3 \cdot 2$	420
total	$\lvert\tilde{\mathcal{Q}}_B\rvert$	722

TABLE II: Number of variables in the BCS game.

B. Non-Clifford gates to realize the magic-necessary BCS

In SI Sec. II, we present a group-theoretic method to determine the magic-necessary perfect-winning strategies [45, 46] when $n \in 2\mathbb{N} + 6$. A notable property is that there are non-unique solutions to the BCS and thus nonequivalent perfect winning quantum strategies in general. Here, we present one operator-valued solution to the BCS when $n = 8$. Labelling the vertices from 1 to 8, a realization of a_v and x_{uv} in the above BCS is

$$\begin{aligned} a_v &= \mathbb{I}_8 - 2\mathbf{e}_{vv}, v = 1, \cdots, 8, \\ x_{uv} &= \mathbb{I}_8 - \mathbf{e}_{uu} - \mathbf{e}_{vv} + \mathbf{e}_{uv} + \mathbf{e}_{vu}, u, v = 1, \cdots, 8, u \neq v \end{aligned} \tag{11}$$

where $\mathbb{I}_8$ is an eight-dimensional identity operator, and $\mathbf{e}_{ij}$ denotes an elementary matrix, of which the element in the i'th row and j'th column is one, and all the other elements are zero. The other operators can be determined via a_v's and x_{uv}'s. The perfect winning strategy of the nonlocal game thus takes three pairs of the Einstein-Podolsky-Rosen (EPR) state, $(|00\rangle + |11\rangle)/\sqrt{2}$. In this strategy, the measurements corresponding to x_{uv} require non-Clifford operations, which can be realized by applying a Toffoli gate up to a local unitary operation followed by the computational-basis measurement.

To illustrate the circuit operations for the nonlocal game, in Fig. 4, we depict the observables of x_{78}, y_{78}, z_{78} and the implementation for the constraint $x_{78}y_{78}z_{78} = 1$. The observable x_{78} is the same as the Toffoli gate. To measure this observable, one can use the Hadamard test, in which the required non-Clifford gate is the controlled-controlled-controlled-X (CCCX) gate. Similarly, the non-Clifford gates required to measure y_{78} and z_{78} are the controlled-controlled-Z (CCZ) and controlled-controlled-controlled-(-X) gates, respectively.

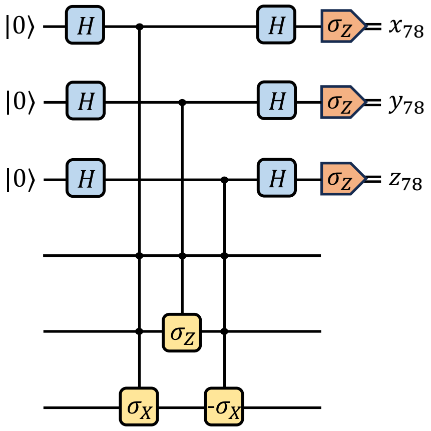


FIG. 4: The circuit with non-Clifford gates to realize the simultaneous measurement of x_{78}, y_{78}, and z_{78} by using the Hadamard test. The Hadamard test uses an ancilla initialized in $|0\rangle$, followed by a Hadamard gate, applying controlled-O and again a Hadamard gate, and measuring in the computational basis to get measurement results of O. Here, the non-Clifford gates are CCCX, CCZ, and CCC(-X) for x_{78}, y_{78}, and z_{78}, respectively.

C. Modified BCS for shallow circuit computation

For the convenience of the shallow circuit computational task, we slightly modify the BCS in Eq. (9). For the n-variable constraint $\prod_{v\in V} a_v = -1$, we can introduce $(n-3)$ new variables and turn them into an equivalent set of $(n-2)$ constraints with three variables each. That is, we introduce new variables $a_{12}, a_{123}, \cdots, a_{1\cdots n-2}$ and convert the constraint as

$$a_1a_2a_3\cdots a_n = -1 \Longleftrightarrow \begin{cases} a_1a_2a_{12} &= 1 \\ a_{12}a_3a_{123} &= 1 \\ \cdots & \\ a_{1\cdots n-3}a_{n-2}a_{1\cdots n-2} &= 1 \\ a_{1\cdots n-2}a_{n-1}a_n &= -1. \end{cases} \tag{12}$$

Note that the commutation requirement between variables a_u and a_v in the original constraint is preserved, since they also need to satisfy the constraint of $a_ua_vy_{uv} = 1$. Denote the set of constraints in the modified BCS as $\mathcal{Q}_A$. Suppose the original BCS with size n consists of $|\tilde{\mathcal{Q}}_A|$ constraints. In correspondence with Eq. (10) in the main text, there are $|\mathcal{Q}| = 3|\mathcal{Q}_A|$ sets of questions in the modified BCS nonlocal game, with

$$\begin{aligned} |\mathcal{Q}_A| &= |\tilde{\mathcal{Q}}_A| + n - 3 \\ &= 2\binom{n}{2} + 14\binom{n}{4} + n - 2. \end{aligned} \tag{13}$$

V. MAGIC COMPUTATIONAL ADVANTAGE IN SHALLOW CIRCUITS

A. Outline

As shown in Theorem 3, the nonlocal game defined through the BCS in Eq. (9) separates the capabilities between a generic quantum world and the magic-free world to generate correlations. Now, we translate correlation generation into a computational task of a relation problem and show the magic advantage. As a reminder, the computational task is a single-user one. "Alice" and "Bob" in the nonlocal game now refer to parts of the circuit, which is merely for intuitive thinking. In particular, one should not consider the task as a distributed computation.

Briefly speaking, a relation problem randomly selects an input bit string z_{in} from a set and asks the computation to output a bit string z_{out}, such that z_{out} *always* satisfies a certain relation with respect to z_{in}. The high-level idea to analyze the shallow circuit capabilities is as follows: In a circuit comprising K-bounded fan-in gates, where each gate can act on at most K inputs, the value K mimics the light speed for information scrambling [47]. Furthermore, if the circuit is shallow, where the circuit depth is a constant independent of the problem size, it restricts the "time" for information scrambling; hence, many sites in the circuit are "space-like" separated from each other. If the relation problem is defined via a nonlocal game, where randomly chosen computing sites of "Alice" and "Bob" are required to generate nonlocal correlations, then the circuit must be capable of winning the game between "space-like" separated sites without communication. Suppose the underlying nonlocal game cannot be won perfectly without a particular resource. In that case, the players must communicate to exchange information and generate the desired correlation, which takes "time." Therefore, the shallow circuit should fail in the task. On the contrary, things become different if the nonlocal game can be won perfectly. Entanglement can be created and distributed between two arbitrary sites via entanglement swapping with bounded fan-in quantum gates in constant steps [28, 30], and quantum "pseudo-telepathy" completes the remaining task.

B. Relation problem separating $\mathsf{QNC}^0$and ClifNC^0

Given a nonlocal game with size n, we can define a relation problem labeled by n, R_N^n. In the following discussions, we focus on the relation problem R_N^8, namely the problem that embeds the BCS nonlocal game with size $n = 8$. Other values of n can be studied similarly. We describe the task by giving the quantum circuit that perfectly solves the computational problem. As shown in Fig. 5(b), consider a quantum circuit containing $2N$ computing sites labeling from 1 to $2N$. Imagine the circuit is divided into two parts, Alice and Bob, where Alice holds the odd-valued sites, and Bob holds the even-valued sites. Each site consists of a set of classical wires to receive the input of R_N^8 and quantum wires initialized in $|0\rangle$ for three qubits. Throughout this work, we denote the classical systems by double wires and quantum systems by single wires.

In the computation, Alice and Bob first prepare three pairs of the EPR state, $(|00\rangle + |11\rangle)/\sqrt{2}$, between their adjacent sites $(2i-1, 2i), i \in \mathbb{N}^+$, as shown by the blue boxes. Next, given an input instance (j, k, α, β), Alice and Bob perform three Bell-state measurements (BSM) between the three pairs of qubits on their adjacent sites $(2j, 2j+1), \cdots, (2k-2, 2k-1)$ in a concatenated manner, as shown by the white boxes. A BSM projects two qubits into one of the four orthogonal Bell states,

$$\begin{aligned}
|\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \\
|\Phi^-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\
|\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \\
|\Psi^-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}},
\end{aligned} \tag{14}$$

and the measurement can be realized by a CNOT gate with Pauli measurements. When the BSM is performed jointly on one qubit of two Bell states each, the remaining two qubits become one of the Bell states with equal probability conditioned on the measurement outcome, a phenomenon called entanglement swapping [48]. Afterward, Alice and Bob perform the perfect-winning strategy for the nonlocal game at sites $2j-1$ and $2k$ with respect to the questions α and β, respectively, as shown by the orange boxes.

To win the BCS nonlocal game, we hope the post-measurement state after entanglement swapping is $|\Phi^+\rangle^{\otimes 3}$, three pairs of the EPR state, such that $\langle\Phi^+|^{\otimes 3} A_\gamma \otimes A_\gamma^{\mathrm{T}} |\Phi^+\rangle^{\otimes 3} = 1$. However, a subtle issue is the so-called bit and phase flips in entanglement swapping. Due to the randomness in BSM, the post-measurement state may differ from the EPR state $|\Phi^+\rangle$, experiencing a rotation of a Pauli operator. Note that different from the case of Pauli measurements, where for any $|\psi\rangle \in \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ and any Pauli operator P, $\langle\psi| P \otimes P^{\mathrm{T}} |\psi\rangle = \pm 1$, such a Pauli error totally ruins the measurement statistics of Alice and Bob in the nonlocal game and results in random outcomes. To fix this issue, we compromise by embedding the circuit outcomes in these cases to the allowed relation for the computational problem while requiring the circuit to generate the desired nonlocal game statistics with a non-negligible probability. For the quantum circuit that takes the pseudo-telepathy as a sub-routine, the desired statistics can be generated with probability 1/64. On the contrary, any magic-free is incompetent to generate the desired statistics with any constant probability. We give the proof in SI Sec. IV.

With the above quantum circuit, we define the computational problem, as rigorously stated in Fig. 5(a). Strictly speaking, our problem not only requires the circuit to return an output that satisfies certain criteria but also to return one specific output with a non-negligible probability. This differs from the standard relation problem, where it suffices for the algorithm to return a valid output. A more accurate statement of our results can be given in terms of a sampling problem. Nevertheless, we shall keep using the term "a relation problem," which is more intuitive.

Building on the nonlocal games defined through Eq. (9), the following theorem illustrates the separation between $\mathsf{QNC}^0$and ClifNC^0circuits in solving the BCS relation computational problem. We provide the analysis details in SI Sec. IV.

Theorem 4. *Given the nonlocal game defined by the BCS in Eq. (9) with size $n \in 2\mathbb{N} + 6$, there is a relation problem R_N^n and a constant K_{th} independent of N, such that for any integer $K > K_{\mathrm{th}}$,*

- *R_N^n can be perfectly solved by a QNC^0circuit with K-bounded fan-in geometrically local gates, where some gates are non-Clifford operations.*
- *Any Clifford circuit with K-bounded fan-in gates that solves R_N^n with probability larger than $(1 + p_{\mathrm{Clif}})/2$ with p_{Clif} given in Eq. (10) must have a circuit depth at least increasing logarithmically with respect to the problem size N, where the gates can be non-geometrically local.*

By this, we prove the main result in Eq. (6). In the second part of the theorem, the logarithmic separation is tight. That is, a magic-free circuit with bounded fan-in gates can solve the problem, of which the depth grows logarithmically. For a straightforward solution, all the computing sites send their input to a fixed ancilla, which performs the nonlocal game calculation and sends back the result to the specified sites.

VI. DISCUSSIONS AND OUTLOOK

In summary, we discover a family of nonlocal games that require quantum magic to win perfectly and trans-

Input of R_N^8:
An instance of (j,k,α,β) defining

$$\alpha_i = \begin{cases} \alpha, & \text{if } i = j, \\ \perp, & \text{if } i \neq j, \end{cases}$$

$$\beta_i = \begin{cases} \beta, & \text{if } i = k, \\ \perp, & \text{if } i \neq k, \end{cases}$$

where $1 \leq j < k \leq N,\ \alpha \in \mathcal{Q}_A,\ \beta \in \mathcal{Q}_B$.

Valid outputs of R_N^8:
Bit strings $\{r_i^A(l)\}_i$ and $\{r_i^B(l)\}_i, l \in \{1,2,3\}$,
Case I: Long-range nonlocal game

$$\prod_{j<i\leq k} r_i^A(l) = +1, \forall l \in \{1,2,3\},$$
$$\prod_{j\leq i<k} r_i^B(l) = +1, \forall l \in \{1,2,3\},$$
$$(\mathbf{r}_j^A, \mathbf{r}_k^B) = f(\alpha,\beta),$$

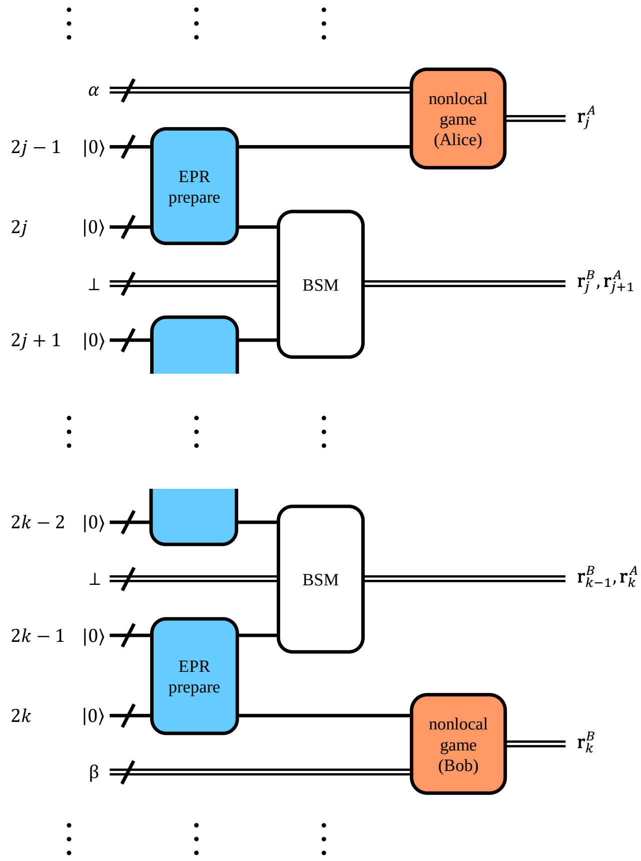
where $\mathbf{r}_i^A = (r_i^A(1), r_i^A(2), r_i^A(3)) \in \{\pm 1\}^3$ and similar to $\mathbf{r}_i^B$, $f(\alpha,\beta)$ is the satisfying assignment in the nonlocal game.

Case II: Entanglement swapping flips
There exists $l \in \{1,2,3\}$, such that

$$\prod_{j<i\leq k} r_i^A(l) = -1, \quad \text{or} \quad \prod_{j\leq i<k} r_i^B(l) = -1.$$

Additional requirement:
Both cases occur with a non-negligible probability, for all (j,k,α,β)

(a)



(b)

FIG. 5: (a) Description of the shallow-circuit computation task R_N^8. (b) A quantum shallow circuit that realizes R_N^8.

late it into an unconditional proof of magic computational advantage. While not being the purpose of this work, by applying the “game gluing” technique [46, 49], one can combine games with different sizes in the family and construct a nonlocal game with a strict separation between the winning probabilities of classical, Clifford, and general quantum strategies. We consider this to be of independent interest to some research. In addition, we believe other nonlocal games exist that can demonstrate magic advantage. For instance, following the method of embedding a general group into a BCS in Ref. [43], one can obtain candidate BCS nonlocal games. In SI Sec. VA, we review the procedure. Combined with Theorem 1, one can efficiently check whether they have perfect-winning Clifford strategies.

To compute the relation problem in a realistic experiment, one shall further consider the noise. For this purpose, noise-tolerant methods, such as error correction and mitigation in a shallow circuit, need to be developed. With recent experimental progress, preparing magic states and implementing a few layers of non-Clifford gates are becoming easy [50, 51]. We expect that the computational task in this work can be faithfully realized on an upcoming early fault-tolerant quantum computing platform [52–54].

This work takes the first step in proving the computation necessity of quantum magic unconditioned on any complexity assumption. We hope our results can inspire further explorations in this direction, eventually going beyond the regime of shallow circuits and solidifying the “magic” of universal quantum computation.

ACKNOWLEDGMENTS

We acknowledge Zhengfeng Ji and Honghao Fu for the insightful discussions on the binary constraint systems and the group embedding results, Qi Zhao, Zhaohui Wei, and Yilei Chen for leading us to the consideration of non-Clifford quantum operations, Yu Cai for introducing to us the results in Ref. [46, 55], Yuwei Zhu, Boyang Chen, and Yuxuan Yan for helpful discussions on the group representation theory and quantum magic. We express special thanks to Tian Ye for his vital and generous help during early stages of this project in a weekly discussion. All the authors acknowledge support by the National Natural Science Foundation of China Grant No. 12174216 and the Innovation Program for Quantum Science and Technology Grant No. 2021ZD0300804. X.Z. acknowledges additional support by the National Natural Science Foundation of China through Grant No. 11975222 and support by the Hong Kong Research Grant Council through grant number R7035-21 of the Research Impact Fund.

[1] R. P. Feynman, Int. J. Theor. Phys. **21** (1982).
[2] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[3] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[4] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[5] D. Gottesman, *Stabilizer codes and quantum error correction* (California Institute of Technology, 1997).
[6] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[7] C. Cormick, E. F. Galvão, D. Gottesman, J. P. Paz, and A. O. Pittenger, Phys. Rev. A **73**, 012301 (2006).
[8] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, New J. Phys. **16**, 013009 (2014).
[9] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016).
[10] M. Howard and E. Campbell, Phys. Rev. Lett. **118**, 090501 (2017).
[11] J. R. Seddon and E. T. Campbell, Proc. Math. Phys. Eng. Sci. **475**, 20190251 (2019).
[12] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Quantum **3**, 181 (2019).
[13] X. Wang, M. M. Wilde, and Y. Su, New J. Phys. **21**, 103002 (2019).
[14] J. R. Seddon, B. Regula, H. Pashayan, Y. Ouyang, and E. T. Campbell, PRX Quantum **2**, 010345 (2021).
[15] Z.-W. Liu and A. Winter, PRX Quantum **3**, 020333 (2022).
[16] J. Chen, Y. Yan, and Y. Zhou, arXiv:2308.01886 (2023).
[17] H. Zhu, R. Kueng, M. Grassl, and D. Gross, arXiv:1609.08172 (2016).
[18] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and quantum computation*, 47 (American Mathematical Soc., 2002).
[19] J. Preskill, in *Feynman Lectures on Computation* (CRC Press, 2023) pp. 193–244.
[20] S. A. Cook, Inf. Control. **64**, 2 (1985).
[21] P. Høyer and R. Špalek, Theory Comput. **1**, 81 (2005).
[22] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, Science **270**, 1633 (1995).
[23] G. Brassard, A. Broadbent, and A. Tapp, Found. Phys. **35**, 1877 (2005).
[24] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[25] J. S. Bell, Physics Physique Fizika **1**, 195 (1964).
[26] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[27] S. Bravyi, D. Gosset, and R. König, Science **362**, 308 (2018).
[28] S. Bravyi, D. Gosset, R. König, and M. Tomamichel, Nat. Phys. **16**, 1040 (2020).
[29] L. Caha, X. Coiteux-Roy, and R. Koenig, arXiv:2312.09209 (2023).
[30] K. Bharti and R. Jain, arXiv:2310.01540 (2023).
[31] J. Barrett, C. M. Caves, B. Eastin, M. B. Elliott, and S. Pironio, Phys. Rev. A **75**, 012103 (2007).
[32] S. Arora and B. Barak, *Computational complexity: a modern approach* (Cambridge University Press, 2009).
[33] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[34] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[35] N. Delfosse, M. E. Beverland, and M. A. Tremblay, Bounds on stabilizer measurement circuits and obstructions to local implementations of quantum ldpc codes (2021), arXiv:2109.14599 [quant-ph].
[36] N. Pippenger, in *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)* (1979) pp. 307–311.
[37] P. Høyer and R. Špalek, in *STACS 2003*, edited by H. Alt and M. Habib (Springer Berlin Heidelberg, Berlin, Heidelberg, 2003) pp. 234–246.
[38] R. Cleve and R. Mittal, in *Automata, Languages, and Programming: 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I 41* (Springer, 2014) pp. 320–331.
[39] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[40] A. Peres, Phys. Lett. A **151**, 107 (1990).
[41] A. Arkhipov, arXiv:1209.3819 (2012).
[42] S. Trandafir, P. Lisoněk, and A. Cabello, Phys. Rev. Lett. **129**, 200401 (2022).
[43] W. Slofstra, in *Forum Math. Pi*, Vol. 7 (Cambridge University Press, 2019) p. e1.
[44] W. Slofstra, J. Am. Math. Soc. **33**, 1 (2020).
[45] R. Cleve, L. Liu, and W. Slofstra, J. Math. Phys. **58**, 012202 (2017).
[46] A. Coladangelo and J. Stark, arXiv:1709.09267 (2017).
[47] E. H. Lieb and D. W. Robinson, Commun. Math. Phys. **28**, 251 (1972).
[48] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[49] Z. Ji, arXiv:1310.3794 (2013).
[50] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, Nature **574**, 505 (2019).
[51] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, *et al.*, Phys. Rev. Lett. **127**, 180501 (2021).
[52] V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, A. Miano, B. Brock, A. Ding, L. Frunzio, *et al.*, Nature **616**, 50 (2023).
[53] Z. Ni, S. Li, X. Deng, Y. Cai, L. Zhang, W. Wang, Z.-B. Yang, H. Yu, F. Yan, S. Liu, *et al.*, Nature **616**, 56 (2023).
[54] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, *et al.*, Nature **626**, 58 (2024).
[55] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Phys. Rev. A **93**, 062121 (2016).

Supplementary Information: Unconditional quantum magic advantage in shallow circuit computation

Xingjian Zhang,[1, 2, 3, 4, *] Zhaokai Pan,[1, †] and Guoding Liu[1, ‡]

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[2] *Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*

[3] *Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[4] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

(Dated: May 20, 2024)

We prove the results presented in the main text in this Supplementary Information. In Sec. I, we present the necessary preliminaries for the notions in this work. In Sec. II, we analyze the new binary constraint system (BCS) proposed in this work along a group-theoretic approach. In Sec. III, we analyze the capabilities of Clifford strategies in the BCS-based nonlocal game. In Sec. IV, we introduce the relation problem based on the BCS nonlocal game, construct a shallow circuit solution that requires quantum magic, and prove the complexity hardness for magic-free circuits. In Sec. V, we review a group embedding result in Ref. [1] and provide an efficient algorithm to solve a linear BCS over the Pauli group.

I. PRELIMINARIES

In this section, we review preliminary concepts for this work. We assume readers are familiar with the basic notions of linear algebra, graph theory, and group theory, and the basic description of quantum systems. For completeness, we restate some basic notions that are listed in the main text.

In the Appendix, we overuse some letters such as n and i when expressing the total number of items or labelling the variables; nevertheless, their meaning can be specified from the context.

A. Quantum magic and non-Clifford operations

We first briefly review the concept of quantum magic and related notions. For simplicity, we only consider the n-qubit system based on the Pauli group. Nevertheless, the results can be easily generalized to systems with a prime dimension by using the Weyl-Heisenberg algebra. Readers who are interested in the topic may refer to the Ph.D. thesis of Gottesman [2] and its following works for a more in-depth discussion.

Let us start with the definition of the Pauli observables on a single qubit:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1}$$

where $\mathbb{I}$ is the identity operator, and the other three observables σ_x, σ_y, and σ_z are always named nontrivial Pauli observables. The n-qubit Pauli group is defined as the set of operators

$$\mathbb{P}_n = \{\pm 1, \pm i\} \times \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}^{\otimes n}, \tag{2}$$

together with the operator multiplication. The Clifford group is defined as the normalizer of the Pauli group $\mathbb{P}_n$:

$$\mathbb{C}_n = \{C \in \mathbb{U}_n | \forall P \in \mathbb{P}_n, CPC^\dagger \in \mathbb{P}_n\}, \tag{3}$$

where $\mathbb{U}_n$ is the n-qubit unitary group. Operators in the Clifford group are called Clifford operations or gates. A highly related concept is the stabilizer state, which is generated by applying Clifford gates on the computational basis states, or equivalently the eigenstates of $\sigma_z^{\otimes n}$. If a state cannot be prepared in this way or by mixing stabilizer states, the state is said to contain quantum "magic" [3].

[*] zxj24@hku.hk

[†] pzk20@mails.tsinghua.edu.cn

[‡] lgd22@mails.tsinghua.edu.cn

B. General binary constraint systems

In this section, we review the definition of a binary constraint system (BCS). A BCS consists of n binary variables $v_1, \cdots, v_n$ and m constraints $c_1, \cdots, c_m$, where each c_j is a Boolean equation with respect to a subset of v_i's, $v_i \in \mathcal{S}_j$. In later discussions, we shall specify a constraint by c_j. Note that BCS with general Boolean constrains can describe general systems of equations [4]. In a linear BCS, all the constraints are given by addition over $\mathbb{Z}_2$, or the parity operation over Boolean variables ranging in $\mathbb{Z}_2 = \{0, 1\}$. In the literature, such a BCS is also called a parity BCS. For convenience of a quantum generalization, it is equivalent to define the BCS over sign variables ranging in $\{+1, -1\}$. In this case, a Boolean function can be equivalently given by a multilinear function of a subset of variables on $\mathbb{R}$. For a linear BCS, the parity constraint becomes a product of the variables. In accordance with the notations in the main text, we mainly use the sign variables and denote each constraint c_j as a multilinear function of a set of variables $\{v_i : i \in \mathcal{S}_j\}$, namely in the form of $\prod_{i\in\mathcal{S}_j} v_i = c_j \in \{+1, -1\}$. Nevertheless, it is sometimes more convenient to use the Boolean variables to represent a BCS. In correspondence to the sign variables,

$$\begin{aligned} v_i v_j = +1 \Leftrightarrow v_i \oplus v_j = 0, \\ v_i v_j = -1 \Leftrightarrow v_i \oplus v_j = 1, \end{aligned} \tag{4}$$

where the LHS are the notations using sign variables and the RHS are the notations using Boolean variables. We shall specify the notations if we resort to the Boolean variables.

If a BCS has a satisfying assignment, namely a fixed assignment to the variables that satisfies all the constraint, we say it has a classical solution. Note that if all the constraints are $c_j = +1$, the BCS can be trivially satisfied by assigning all the variables to be $+1$. With respect to the BCS size, searching for a classical solution to a general BCS is NP-hard. On the other hand, the problem is in P for linear BCS, where one can apply Gaussian elimination or the replacement method to efficiently solve the system.

The quantum generalization of a BCS is an operator-valued constraint system. The variables v_j's are replaced with linear operators A_j's acting on a Hilbert space $\mathcal{H}$ with a finite dimension, such that

1. Each A_j is Hermitian with eigenvalues in $\{1, -1\}$, i.e., $A_j = A_j^\dagger$ and $A_j^2 = \mathbb{I}$ for all j.

2. A_j's satisfy all the constraints with c_i replaced with $c_i\mathbb{I}$, where $\mathbb{I}$ is the identity operator on $\mathcal{H}$.

3. If A_i and A_j appear in the same constraint, they commute with each other, i.e., $A_iA_j = A_jA_i$.

If there exists a Hilbert space $\mathcal{H}$ with dimension d and a set of linear operators following the above requirements, we say the BCS has a d-dimensional quantum satisfying assignment, or simply a quantum solution. As a side remark, the requirement that the operator variable acts on a finite-dimensional Hilbert space can be relaxed in several directions, including allowing an infinite dimension and limits of finite-dimensional systems. We do not discuss such generalizations and refer readers to Ref. [1, 5] for a more detailed definition.

If a BCS has a quantum solution, one can apply quantum measurements to realize it in an experiment, where they prepare independently and identically many copies of a quantum state and measure the observables in each constraint. For each constraint, the measurement results shall satisfy the relation in the fashion of classical variables. Note that the requirement for a quantum solution guarantees the validity of a joint measurement for each constraint. Due to the intrinsic randomness in quantum measurements, the same variable may take different values in different constraints. It is worth mentioning that measuring the set of observables on any state, including a maximally mixed state, generates the desired statistics for the constraints. The quantum satisfying assignment is also called a state-independent contextuality of the observables [6].

As the dimension can be arbitrary, searching for a quantum solution is undecidable [1, 7]. A helpful way of thinking is to regard the BCS as a group presentation statement [8, 9].

Definition 1 (Group presentation)**.** *Given a set $\mathcal{S}$, let $\mathcal{F}(\mathcal{S})$ be the free group on $\mathcal{S}$ and $\mathcal{R}$ a set of words on $\mathcal{S}$, and denote the quotient group of $\mathcal{F}(\mathcal{S})$ by the smallest normal subgroup containing each element in $\mathcal{R}$ as $\langle \mathcal{S} : \mathcal{R} \rangle$. A group G is said to have the presentation $\langle \mathcal{S} : \mathcal{R} \rangle$ if it is isomorphic to $\langle \mathcal{S} : \mathcal{R} \rangle$.*

In the group presentation, the elements in $\mathcal{S}$ are called generators, and the elements in $\mathcal{R}$ are called relators. Given a linear BCS, one can regard the constraints as a group presentation.

Definition 2 (Solution group of a linear BCS)**.** *Given a linear BCS with n binary variables $\{v_i\}$ and m constraints*

$\{c_j\}$, the solution group of the BCS is defined as the group with the following presentation:

$$\begin{aligned}\Gamma = \{\{J, g_i : i \in [n]\} : \{g_i^2 &= e, \forall i \in [n],\\ J^2 &= e,\\ \forall j \in [m], g_k g_l &= g_l g_k, \forall k, l \in \mathcal{S}_j,\\ J g_i &= g_i J, \forall i \in [n],\\ \prod_{i \in \mathcal{S}_j} g_i &= J^{\chi(c_j=-1)}, \forall j \in [m]\}\},\end{aligned} \tag{5}$$

where the group element J corresponds to -1 in the BCS, e defines the identity operator of the group, and $\chi(\cdot)$ is the indicator function that takes the value 1 if the argument is true and 0 if the argument is false.

Note that if $J = e$, the solution group is trivial, as the assignment of all the group elements to be e satisfies all the relators. On the contrary, should $J \neq e$, the solution group is non-trivial, and the group presentation corresponds to a valid operator-valued solution to the underlying BCS, as stated by the following lemma.

Lemma 1 ([9, 10])**.** *Given a linear BCS that defines a solution group with the group element J corresponding to -1, if J is non-trivial in some finite-dimensional representation of the solution group, then the BCS has a finite-dimensional quantum satisfying assignment. The converse is also true.*

The irreducible representation of the generators in the solution group determines the quantum realization [9, 11]. Here, a representation of the group refers to a group homomorphism of the group to a set of unitary operators on a Hilbert space, and an irreducible representation refers to a representation that does not have a non-trivial group-invariant subspace [12]. For a classical solution, it can be described by the Abelian group, where all the group elements commute with each other.

As an example of linear BCS, we review the Mermin-Peres BCS, also widely known as the "magic-square" system [13, 14]. Note that one should not mistake the name "magic" for the quantum resource of magic states. The Mermin-Peres BCS involves $n = 9$ variables and $m = 6$ constraints. In terms of sign variables ranging in $\{+1, -1\}$, the BCS is defined as follows:

$$\begin{aligned} v_1 v_2 v_3 &= 1,\\ v_4 v_5 v_6 &= 1,\\ v_7 v_8 v_9 &= 1,\\ v_1 v_4 v_7 &= 1,\\ v_2 v_5 v_8 &= 1,\\ v_3 v_6 v_9 &= -1.\end{aligned} \tag{6}$$

This BCS does not have a classical solution. On the other hand, it has a unique quantum solution over the Pauli group. We denote the operator that corresponds to v_i as A_i in accordance with the notations above. The quantum solution is given as follows [10, 15]:

$$\begin{aligned} A_1 &= \sigma_z \otimes \mathbb{I},\\ A_2 &= \mathbb{I} \otimes \sigma_z,\\ A_3 &= \sigma_z \otimes \sigma_z,\\ A_4 &= \mathbb{I} \otimes \sigma_x,\\ A_5 &= \sigma_x \otimes \mathbb{I},\\ A_6 &= \sigma_x \otimes \sigma_x,\\ A_7 &= \sigma_z \otimes \sigma_x,\\ A_8 &= \sigma_x \otimes \sigma_z,\\ A_9 &= \sigma_y \otimes \sigma_y,\end{aligned} \tag{7}$$

where $\otimes$ stands for the tensor product operation.

Given a BCS, one can define an associated nonlocal game [8]. In the nonlocal game, there are two cooperating players, Alice and Bob, who cannot communicate with each other once the game starts. With respect to a probability distribution, a referee randomly selects one constraint, c_s, and one variable, v_t, contained in the constraint. In our work, we always take the probability distribution to be uniform. The referee send s to Alice and t to Bob. Then, Alice returns an assignment to each variable v_i in c_s that satisfies the constraint and Bob returns an assignment to variable v_t. They win the game if and only if the assignments of Bob and Alice to v_t are the same. This type of nonlocal game extends the well-known Clauser-Horne-Shimony-Holt (CHSH) game [16], where the underlying BCS involves two binary variables and two multi-linear constraints,

$$\begin{aligned} v_1 v_2 &= 1, \\ v_1 v_2 &= -1. \end{aligned} \tag{8}$$

This BCS game is equivalent to the CHSH game in the sense of the probability distribution that Alice and Bob can achieve. Note that this BCS does not have either a classical solution or a quantum solution. Still, quantum strategies for the game can bring a higher winning probability than classical ones.

To maximize the winning probability, Alice and Bob can agree on a strategy for playing the game. We call a strategy is *perfect* if it wins with probability 1. We say Alice and Bob apply a classical strategy if they can access only shared and local randomness. In quantum theory, Alice and Bob can pre-share entanglement and apply local quantum operations. In general, when a BCS does not have a solution, it is possible that Alice assigns different values to the same variable upon different questions of constraint. However, it brings limited advantages. For classical strategies, using basic linear algebra analysis, it is not hard to prove that a BCS game has a perfect classical strategy if and only if the corresponding BCS has a solution. It follows that to decide whether a general BCS game has a perfect classical strategy is in NP-hard for general Boolean constraints and in P for linear constraints with respect to the BCS size. In the above examples, the CHSH game has a maximal winning probability of 3/4, and the Mermin-Peres game has a maximal winning probability of 8/9. In the quantum case, if the BCS does not have an operator-valued solution, then there does not exist a perfect winning strategy for the associated nonlocal game, and *vice versa*. This fact is first proved in Ref. [8]. If the BCS has a quantum solution, it is linked to a perfect quantum winning strategy in a one-to-one correspondence. Suppose the quantum solution to the BCS is given by observables $\{A_i\}_i$ acting on a d-dimensional system. Alice and Bob first share a maximally entangled state, $|\Phi^+\rangle = \sum_{i=0}^{d-1} |ii\rangle / \sqrt{d}$. When the nonlocal game starts, upon receiving the constraint c_s, Alice measures the observables A_i belonging to the constraint, and upon receiving the variable v_t, Bob measures the transpose of the observable A_t, denoted by A_t^{T}. The measurement statistics satisfy the winning condition.

For the well-known existing BCS that are solvable, it either has a classical solution, which corresponds to an Abelian group, or a quantum solution of Pauli strings as in the case of the Mermin-Peres magic square, which corresponds to the Pauli group. In Ref. [17], the author provides an efficient algorithm to determine perfect quantum solutions to a special type of linear BCS, where each variable shows up in exactly two constraints. Moreover, if such a BCS has a solution, the solution is necessarily given by Pauli strings, i.e., the solution is in the Pauli group. Following this result, it was conjectured that any linear BCS with an operator-valued satisfying assignment belongs to either of the two cases [17]. As mentioned in the main text, this conjecture has been suggested false [1, 7]. In the next section, we directly disprove this conjecture with a specific linear BCS.

II. GROUP-THEORETIC ANALYSIS OF THE BINARY CONSTRAINT SYSTEM

In this section, we apply group-theoretic tools to analyse the properties of the proposed linear BCS in the main text. We first review the BCS proposed in this work. Given an undirected complete graph $G = (V, E)$ with n vertices, it defines the following variables:

1. Each vertex $v \in V$ corresponds to one variable a_v.

2. Each undirected edge, denoted by $e = (u, v) \in E$, corresponds to three variables x_{uv}, y_{uv}, z_{uv}.

3. Every two disjoint edges, denoted by $e_1 = (u, v) \in E$ and $e_2 = (s, t) \in E$, where s, t, u, v are different vertices, correspond to

   (a) one variable $b_{uv|st} \equiv b_{st|uv}$, where $b_{e_1 e_2} = b_{e_2 e_1}$;

   (b) two variables $c_{e_1 e_2} \equiv c_{uv|st}$ and $c_{e_2 e_1} \equiv c_{st|uv}$, where $c_{e_1 e_2} \neq c_{e_2 e_1}$ in general.

Based on these variables, the BCS contains the following constraints,

$$\begin{aligned}
a_u a_v y_{uv} &= 1, \forall (u,v) \in E, \\
x_{uv} y_{uv} z_{uv} &= 1, \forall (u,v) \in E, \\
x_{uv} x_{st} b_{uv|st} &= 1, \forall (u,v),(s,t) \in E, \\
x_{uv} z_{st} c_{uv|st} &= 1, \forall (u,v),(s,t) \in E, \\
b_{uv|st} b_{vs|ut} b_{su|vt} &= 1, \forall (u,v),(s,t) \in E, \\
c_{uv|st} c_{vs|ut} c_{su|vt} &= 1, \forall (u,v),(s,t) \in E, \\
\prod_{v \in V} a_v &= -1.
\end{aligned} \tag{9}$$

For a nontrivial BCS, the system size is at least $n = 4$. If the BCS has a solution, then the other variables can be generated by a's and x's. For convenience, we label the vertices with natural numbers from 1 to n. For each vertex v and each edge $(u,v), u \neq v$, we can use transpositions between elements in the set $[2n]$ to represent the generators, where $a_v = (2v-1\ 2v)$ and $x_{uv} = (2u-1\ 2v-1)(2u\ 2v)$. Here, $(i\ j)$ represents a transposition between i and j. We have the following results for the BCS.

Theorem 1. *For any BCS of the above form with $n \in 2\mathbb{N}+5 = \{5,7,9,\cdots\}$, it has a classical solution.*

Proof. When $n \in 2\mathbb{N}+5$, the BCS can be satisfied by assigning all the variables a_v's to be -1 and all the other variables to be 1. □

Theorem 2. *When $n = 4$, this BCS has a two-qubit Pauli-string solution. On the other hand, the BCS does not have a classical solution or a single-qubit Pauli solution in this case.*

Proof. The BCS having no classical solution can be directly checked by solving the BCS on the binary field. By using the fact that there is no state-independent contextuality in a qubit system, one can prove that the BCS does not have a single-qubit Pauli solution either [18–20]. Later, we prove this statement under the context of linear BCS.

For the former statement, here is one construction of the two-qubit Pauli-string solution. We abbreviate the Pauli operators $\mathbb{I}, \sigma_x, \sigma_y, \sigma_z$ as I, X, Y, Z, respectively, and omit the tensor-product operator in the expressions.

a_1	a_2	a_3	a_4		
$-ZZ$	II	ZI	IZ		
x_{12}	x_{13}	x_{14}	x_{23}	x_{24}	x_{34}
$-YY$	XI	IX	II	II	ZZ
y_{12}	y_{13}	y_{14}	y_{23}	y_{24}	y_{34}
$-ZZ$	$-IZ$	$-ZI$	ZI	IZ	ZZ
z_{12}	z_{13}	z_{14}	z_{23}	z_{24}	z_{34}
$-XX$	$-XZ$	$-ZX$	ZI	IZ	II
$b_{12\|34}$	$b_{13\|24}$	$b_{14\|23}$			
XX	XI	IX			
$c_{12\|34}$	$c_{13\|24}$	$c_{14\|23}$	$c_{34\|12}$	$c_{24\|13}$	$c_{23\|14}$
$-YY$	XZ	ZX	YY	$-XZ$	$-ZX$

TABLE I: A two-qubit Pauli-string solution for the BCS when $n = 4$.

□

Theorem 3 (A special case of the results in Ref. [18–20])**.** *If a linear BCS has a single-qubit operator-valued solution, then it has a classical solution.*

Proof. Two-dimensional matrices have such a special property: Suppose $A, B \in \mathbb{C}^{2\times 2}$ and $[A,B] = AB - BA = 0$. At least one of the following cases would happen (1) $A = c\mathbb{I}$ for some $c \in \mathbb{C}$; (2) $B = c\mathbb{I}$ for some $c \in \mathbb{C}$; (3) $A = cB$ for some $c \in \mathbb{C}$. Therefore, all two-dimensional matrices that are not proportional to the identity matrix $\mathbb{I}$ can be classified into different equivalence classes, with elements in a class proportional to each other.

Given a single-qubit operator-valued solution, denote the first equivalent class as $\{c_1 O, c_2 O, \cdots | c_1, c_2, \cdots = \pm 1\}$ where $O \neq \pm \mathbb{I}$ and $O^2 = \mathbb{I}$. Substituting $\{c_1 O, c_2 O, \cdots | c_1, c_2, \cdots = \pm 1\}$ with $\{c_1 \mathbb{I}, c_2 \mathbb{I}, \cdots | c_1, c_2, \cdots = \pm 1\}$ and not changing other variables also provides a solution. This is because (1) variables in different equivalent classes do not show up in the same constraint; (2) the constraints among the variables proportional to $\mathbb{I}$ and in the first equivalent class are not violated after the substitution. Similarly, we can set all variables proportional to $\mathbb{I}$ to give a solution. The proportional coefficient is a valid classical solution. □

Theorem 4. *For any BCS of the above form with $n \in 2\mathbb{N}+6 = \{6, 8, 10, \cdots\}$, it does not have a Pauli-string solution.*

Proof. Later we shall present a general method to determine whether a general linear BCS has a Pauli-string solution, where the current result can be regarded as a special case. Nevertheless, here we present a graph-based proof specific to this BCS, which is more illustrative.

We first specify the commutation properties of Pauli strings. The Pauli group elements are either anti-commuting, like $\{X, Z\} = XZ + ZX = 0$, or commuting, like $[X \otimes X, Z \otimes Z] = (X \otimes X)(Z \otimes Z) - (Z \otimes Z)(X \otimes X) = 0$. Therefore, if we swap any two operators in a multiplication of some Pauli-string operators, the operator value of the multiplication would at most differ with a sign.

Now we prove the theorem by contradiction. Assume the BCS described in the theorem has a Pauli-string solution. Without loss of generality, with respect to the correspondence between the BCS variables and vertices in a fully connected undirected graph, let us consider the sets of variables and constraints corresponding to a subgraph with five vertices, labeled with 1 through 5. For the quadrangle $\{1, 2, 4, 5\}$, we have the equation $b_{12|45} b_{24|15} b_{41|25} = \mathbb{I}$. Substituting all the b-type variables by $x_{uv} x_{st} b_{uv|st} = \mathbb{I}$, we have

$$x_{12} x_{45} x_{24} x_{15} x_{41} x_{25} = \mathbb{I}. \tag{10}$$

Similarly, for the quadrangles $\{1, 3, 4, 5\}$ and $\{2, 3, 4, 5\}$, we have the equations

$$x_{13} x_{45} x_{34} x_{15} x_{41} x_{35} = \mathbb{I}. \tag{11}$$

$$x_{23} x_{45} x_{34} x_{25} x_{42} x_{35} = \mathbb{I}. \tag{12}$$

Next, by multiplying the left and right sides of Eqs. (10)(11) and (12), respectively, swapping the order of the variables, and eliminating the adjacent two variables that are the same, we get

$$x_{12} x_{13} x_{23} x_{45} = \pm \mathbb{I}, \tag{13}$$

where "±" denotes that either case would happen. In this step, we have used the commutation properties of Pauli strings. In other words,

$$x_{45} \in \{\pm x_{12} x_{13} x_{23}\}. \tag{14}$$

As a reminder, x_{uv} and x_{vu} represent the same variable. Note that there is nothing special about the choice of x_{45} among the variables, and a similar result can be obtained with an arbitrary specification of a subgraph with five vertices. For instance, we can get

$$x_{46} \in \{\pm x_{12} x_{13} x_{23}\}. \tag{15}$$

Combining the above two equations, we have $x_{45} = \pm x_{46}$. For $n \geq 6$, following the above procedure and enumerating all such identities, one shall find that all the x-type variables differ from each other up to a sign, i.e., $x_{uv} \in \{\pm x\}$ for all $(u, v) \in E$. Thus we can assume that $x_{uv} = x'_{uv} x$ where $x'_{uv} \in \{\pm 1\}$.

Following the specification of the x-type variables, for any four distinct vertices $u, v, s, t \in V$, we have the following expressions:

$$\begin{aligned} b_{uv|st} &= x_{uv} x_{st} = x'_{uv} x'_{st} \mathbb{I}, \\ c_{uv|st} &= x_{uv} z_{st} = x_{uv} x_{st} y_{st} = x'_{uv} x'_{st} y_{st} = x'_{uv} x'_{st} a_s a_t. \end{aligned} \tag{16}$$

Consequently,

$$\begin{aligned} b_{uv|st} b_{vs|ut} b_{su|vt} &= x'_{uv} x'_{st} x'_{vs} x'_{ut} x'_{su} x'_{vt} = 1, \\ c_{uv|st} c_{vs|ut} c_{su|vt} &= x'_{uv} x'_{st} x'_{vs} x'_{ut} x'_{su} x'_{vt} a_s a_t a_u a_t a_v a_t = 1. \end{aligned} \tag{17}$$

Note that all the a-type variables commute with each other, since they simultaneously appear in the last equation of the BCS. We hence derive that $a_u a_v a_s a_t = 1$ for all four distinct vertices $u, v, s, t \in V$, which is equivalent to

$$a_u = a_v a_s a_t. \tag{18}$$

By applying a similar argument as for the x-type variables, we shall find that all the a-type variables are identical, i.e., $a_v \equiv a, \forall v \in V$. This contradicts the constraint $\prod_{v\in V} a_v = -1$ when n, the number of vertices, is even. Therefore, the BCS of the above form with $n \in 2\mathbb{N} + 6$ does not have a Pauli-string solution. □

Theorem 5. *For any BCS of the above form with $n \geq 4$, label the vertices from 1 to n. The BCS has a solution over the centralizer group of element $J = (1\ 2)(3\ 4)\cdots(2n-1\ 2n)$ in the permutation group S_{2n}.*

Proof. Consider $x_{(u,v)} = (2u-1\ 2v-1)(2u\ 2v)$, $a_v = (2v-1\ 2v)$, and all the other variables generated by them. One can easily check that the assignment satisfies the constraints. As J does not map to the identity element of the group, this is a non-trivial quantum solution following Lemma 1. The solution group corresponds to the centralizer of J in the permutation group, given by

$$C_J = S_n \ltimes \mathbb{Z}_2^n, \tag{19}$$

which is the semi-product of the permutation group S_n generated by $x_{(u,v)}$, and an Abelian group $\mathbb{Z}_2^n$ generated by a_v. □

Now we solve the irreducible representations of the solution, which gives the quantum realizations. We have the following theorem.

Theorem 6. *An irreducible representation of $S_n \ltimes \mathbb{Z}_2^n$ can be labeled by $\left(m, \theta^{(m)}, \rho^{(n-m)}\right)$ where m is an integer in $[0, n]$, $\theta^{(m)}$ and $\rho^{(n-m)}$ are two irreducible representations of permutation groups S_m and S_{n-m}, respectively. Given label $\left(m, \theta^{(m)}, \rho^{(n-m)}\right)$, we first get an irreducible representation of group $S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n$, which is given by*

$$\begin{aligned} &\phi^{(m,\theta,\rho)} : S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n \to M_{\dim\theta^{(m)}\times\dim\rho^{(n-m)}}(\mathbb{R}) \\ &x \in S_m, y \in S_{n-m}, z \in \mathbb{Z}_2^n, (x, y, z) \mapsto \theta^{(m)}(x) \otimes \rho^{(n-m)}(y) \otimes \varphi^{(m)}(z). \end{aligned} \tag{20}$$

Here, $\varphi^{(m)}$ is an irreducible representation of $\mathbb{Z}_2^n$ such that for any element $z = (z_1, z_2, \cdots, z_n) \in \mathbb{Z}_2^n$ where $\forall j, z_j \in \{0, 1\}$,

$$\varphi^{(m)}(z) = \prod_{j=1}^{m} (-1)^{z_j}. \tag{21}$$

The irreducible representation of $S_n \ltimes \mathbb{Z}_2^n$ labeled by $\left(m, \theta^{(m)}, \rho^{(n-m)}\right)$, denoted as $\Phi^{(m,\theta,\rho)}$, is the induced representation of $\phi^{(m,\theta,\rho)}$. Specifically, one first finds the left coset of $S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n$ in $S_n \ltimes \mathbb{Z}_2^n$, given by

$$\left\{g_1 S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n, g_2 S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n, \cdots, g_{\binom{n}{m}} S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n\right\}, \tag{22}$$

where $\left\{g_1, g_2, \cdots, g_{\binom{n}{n}}\right\}$ are representative elements and g_1 is the identity. Then, the induced representation $\Phi^{(m,\theta,\rho)}$ is defined on the bases $\left\{g_i \vec{e}_j | 1 \leq i \leq \binom{n}{m}, 1 \leq j \leq \dim\phi^{(m,\theta,\rho)}\right\}$ where $\vec{e}_j$ is a basis of the representation space of $\phi^{(m,\theta,\rho)}$. That is, for any element $g \in S_n \ltimes \mathbb{Z}_2^n$, suppose that $gg_i \in g_{\sigma(i)} S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n$ and set $h_i = g_{\sigma(i)}^{-1} g g_i$ where σ is a permutation on $\left\{1, 2, \cdots, \binom{n}{m}\right\}$, then

$$\Phi^{(m,\theta,\rho)}(g) = \left(\Pi_\sigma \otimes \mathbb{I}_{\dim\phi^{(m,\theta,\rho)}}\right) \left(\bigoplus_{i=1}^{n} \phi^{(m,\theta,\rho)}(h_i)\right). \tag{23}$$

Here, Π_σ is a permutation matrix defined on the computational basis $|1\rangle, |2\rangle, \cdots, \left|\binom{n}{m}\right\rangle$ and transforms $|i\rangle$ to $|\sigma(i)\rangle$.

Proof. This theorem is a direct corollary of Proposition 25 in [12]. To get an irreducible representation of $C_J = S_n \ltimes \mathbb{Z}_2^n$, we start from the irreducible representation of $\mathbb{Z}_2^n$. Note that $\mathbb{Z}_2^n = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$ is generated by n two-order elements $a_1, a_2, \cdots, a_n$. Any irreducible representation of $\mathbb{Z}_2^n$ can be labeled by a vector with length n, like $(1, -1, \cdots, 1)$, denoting the values that n generators would be mapped to in the representation. Meanwhile, we call two irreducible representations equivalent if they can be mutually transformed via S_n. In other words, two irreducible representations are equivalent if and only if the corresponding vectors have the same number of -1. To obtain an irreducible representation of C_J, we only need to consider inequivalent irreducible representations of $\mathbb{Z}_2^n$ under the transformation of S_n. Without loss of generality, we choose these irreducible representations as $(1, 1, \cdots, 1)$, $(-1, 1, \cdots, 1)$, $(-1, -1, \cdots, 1)$, and $\cdots$, $(-1, -1, \cdots, -1)$ and label them with the number of -1, that is, $\{0, 1, \cdots, n\}$.

For a number $m \in \{0, 1, \cdots, n\}$, we get an irreducible representation of $\mathbb{Z}_2^n$, denoted as $\varphi^{(m)}$, mapping the generators a_i to $\varphi^{(m)}(a_i) = (-1)^{\mathbb{1}_{i \leq m}}$. Then, we consider a subgroup of S_n, such that any element h in this subgroup satisfies $\forall z \in \mathbb{Z}_2^n$,

$$\varphi^{(m)}(gzg^{-1}) = \varphi^{(m)}(z), \tag{24}$$

or equivalently, $1 \leq i \leq n$,

$$\varphi^{(m)}(ga_ig^{-1}) = \varphi^{(m)}(a_i). \tag{25}$$

Clearly, this subgroup must be $S_m \times S_{n-m}$. Then, one can define the irreducible representation of $S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n$ as

$$\begin{aligned} \phi^{(m,\theta,\rho)} &: S_m \times S_{n-m} \ltimes \mathbb{Z}_2^n \to M_{\dim \theta^{(m)} \times \dim \rho^{(n-m)}}(\mathbb{R}) \\ x \in S_m, y \in S_{n-m}, z \in \mathbb{Z}_2^n&, (x, y, z) \mapsto \theta^{(m)}(x) \otimes \rho^{(n-m)}(y) \otimes \varphi^{(m)}(z), \end{aligned} \tag{26}$$

where $\theta^{(m)}$ and $\rho^{(n-m)}$ are two irreducible representations of permutation groups S_m and S_{n-m}, respectively. Note that $\phi^{(m,\theta,\rho)}$ is a well-defined group homomorphism due to the condition of Eq. (24). Proposition 25 in [12] tells us that any irreducible representation of $S_n \ltimes \mathbb{Z}_2^n$ can be constructed by the induced representation of $\phi^{(m,\theta,\rho)}$ by traversing m, θ, and ρ. Proof is done. □

For a perfect strategy of the non-local game, the element J must be mapped to a non-identity element. Note that any element in C_J commutes with J. Via Theorem 6, one can obtain the following result:

$$\begin{aligned} \Phi^{(m,\theta,\rho)}(J) &= \varphi^{(m)}(J)\mathbb{I}_{\dim \Phi} \\ &= \varphi^{(m)}\left(\prod_{i=1}^{n} a_i\right)\mathbb{I}_{\dim \Phi} \\ &= \prod_{i=1}^{n} \varphi^{(m)}(a_i)\mathbb{I}_{\dim \Phi} \\ &= (-1)^{\text{mod}(m,2)}\mathbb{I}_{\dim \Phi}, \end{aligned} \tag{27}$$

where $\dim \Phi = \binom{n}{m} \dim \phi = \binom{n}{m} \dim \theta^{(m)} \dim \rho^{(n-m)} \geq \binom{n}{m}$. Thus, $\Phi^{(m,\theta,\rho)}(J)$ corresponds to a perfect measurement strategy if and only if m is odd. The smallest dimension of the quantum system for a perfect strategy is n when $m = 1$ or $m = n - 1$ and $\dim \theta^{(m)} = \dim \rho^{(n-m)} = 1$.

The quantum realization of the BCS in Eq. (9) is not unique. The underlying reason is that unlike the Pauli group, the permutation group has more than one inequivalent irreducible representations [12]. For $n = 8$, which is the smallest size for a non-trivial result where there is not a Pauli-string solution to the BCS, we consider the case where $m = 1$ and θ and ρ are both trivial representations, in which the dimension of the quantum system is 8. It implies that the corresponding non-local game can be realized with only 3 EPR pairs. The representations of the generators are given by the following:

$$a_1 = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, a_2 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, \cdots, a_8 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix}, \tag{28}$$

$$x_{12} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, x_{13} = \begin{pmatrix} 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \cdots, x_{18} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{29}$$

The value of x_{uv} equals $x_{1u}x_{1v}x_{1u} = \mathbb{I}_8 - \mathbf{e}_{uu} - \mathbf{e}_{vv} + \mathbf{e}_{uv} + \mathbf{e}_{vu}$, where $\mathbb{I}_8$ is an eight-dimensional identity operator, and $\mathbf{e}_{ij}$ denotes an elementary matrix, of which the element in the i'th row and j'th column is one, and all the other elements are zero.

From the expression of the generators, we can see that the measurement observables do not belong to the Pauli group and need magic to realize. Following the same derivation, one can prove that the smallest non-trivial irreducible representation of the solution to the BCS defined over n vertices requires an n-dimensional system. Thus, we obtain an upper bound of the smallest number of qubits to win the non-local game.

Corollary 1. *The smallest number of qubits to win the associated nonlocal game of Eq. (9) is $O(\log n)$.*

III. CAPABILITIES OF CLIFFORD STRATEGIES IN THE NONLOCAL GAME

In proving the "magic" advantage in shallow circuit quantum computation, we need to specify the capabilities of Clifford strategies in the nonlocal BCS game. Thanks to the algebraic structure of BCS, we can use mature techniques from linear algebra to obtain quantitative results.

Suppose the players in a nonlocal game are restricted to Clifford operations only, or that they do not have access to quantum magic resources. In this case, the most general strategy they can apply to playing the nonlocal game is as follows:

- Before the nonlocal game starts:
  1. Alice and Bob prepares an n-qubit state and initialize it in $|0\rangle$.
  2. Alice and Bob apply joint Clifford operations and Pauli-string measurements to the state and evolve it into an entangled state ρ_{AB}, where the subscripts denote the subsystems they each will hold in the game.
- After the nonlocal game starts: Alice and Bob each applies Pauli-string measurements to their own quantum system.

In our discussions, we allow an arbitrarily large n. Using a convexity argument, we know that a mixed state does not bring any advantage to Alice and Bob in winning the nonlocal game, and we can hence take ρ_{AB} as a pure state $|\psi\rangle$ without loss of generality. By further applying the Schmidt decomposition result, a pure state can be written as

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |ii\rangle , \tag{30}$$

where $\forall i, \alpha_i \geq 0$, and $\sum_{i=0}^{d-1} \alpha_i^2 = 1$. Note that the maximally entangled state, which is

$$\left|\Phi^+\right\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |ii\rangle , \tag{31}$$

can be prepared by applying control-NOT operations to $|0\rangle$, which is a Clifford operation. Therefore, a general bipartite entangled state $|\psi\rangle$ shared by Alice and Bob can only be linked with $|\Phi^+\rangle$ with a Clifford operation, i.e., $|\psi\rangle = U_C |\Phi^+\rangle$.

Based upon the above observations, we discuss the capabilities of Clifford operations in playing a parity BCS nonlocal game. In demonstrating the magic advantage, we are interested in the parity BCS that do not have a Pauli-string quantum satisfying assignment. We have the following result for these instances.

Theorem 7. *Suppose a parity BCS does not have a satisfying assignment with Pauli-string observables. Then, for any Clifford strategy, there exist a constraint labelled by c_s and a variable in it labelled by v_t, where the probability that the assignments of Alice and Bob to v_t under the constraint c_s are identical does not exceed $1/2$.*

Proof. In the first part of the proof, we prove the case where Alice and Bob initially share a maximally entangled state $|\Phi^+\rangle$ in Eq. (31) of an arbitrary dimension and then generalize the result to general Clifford strategies. In the BCS nonlocal game, without loss of generality, upon receiving the constraint labelled by s, Alice shall measure a set of commuting Pauli-string observables that return a satisfying assignment to the constraint, since a failure in satisfying the constraint results in a loss in the nonlocal game. On the other hand, the observables that she measures for the same variable, e.g., v_t, in different constraints can be different. To specify her strategy, we denote the observable Alice measures for vairable v_t in the constraint c_s as $A_t^{(s)}$. On Bob's side, we denote the observable he measures for variable v_t as B_t.

Now, suppose Alice and Bob initially share the maximally entangled state $|\Phi^+\rangle$. Assume there exists a Clifford strategy, such that $\forall s, t$,

$$\left\langle\Phi^+\right| A_t^{(s)} \otimes B_t \left|\Phi^+\right\rangle > 0. \tag{32}$$

Since Alice and Bob apply a Clifford strategy, $A_t^{(s)}$ and B_t are both Pauli strings, so is $A_t^{(s)} B_t^{\mathrm{T}}$. Using the property of $|\Phi^+\rangle$, the left-hand side of the above equation equals $\langle\Phi^+| A_t^{(s)} B_t^{\mathrm{T}} \otimes \mathbb{I} |\Phi^+\rangle = \mathrm{tr}\Big(A_t^{(s)} B_t^{\mathrm{T}}\Big)/d$, where d is the system dimension. Since $A_t^{(s)} B_t^{\mathrm{T}}$ is a Pauli string, we have $\mathrm{tr}\Big(A_t^{(s)} B_t^{\mathrm{T}}\Big)/d \in \{0, \pm 1\}$. According to our assumption, we conclude that $A_t^{(s)} = B_t^{\mathrm{T}}$ and $\langle\Phi^+| A_t^{(s)} \otimes B_t |\Phi^+\rangle = 1$ for all s, t. Besides,

$$\begin{aligned}
\left\langle\Phi^+\right| A_t^{(s_1)} A_t^{(s_2)} \otimes \mathbb{I} \left|\Phi^+\right\rangle &= \left\langle\Phi^+\right| (A_t^{(s_1)} \otimes \mathbb{I})(A_t^{(s_2)} \otimes \mathbb{I}) \left|\Phi^+\right\rangle \\
&= \left\langle\Phi^+\right| (A_t^{(s_1)} \otimes \mathbb{I})(A_t^{(s_2)} \otimes \mathbb{I}) \left|\Phi^+\right\rangle \left\langle\Phi^+\right| (\mathbb{I} \otimes B_t)(\mathbb{I} \otimes B_t) \left|\Phi^+\right\rangle \\
&\geq \left\langle\Phi^+\right| A_t^{(s_1)} \otimes B_t \left|\Phi^+\right\rangle \left\langle\Phi^+\right| A_t^{(s_2)} \otimes B_t \left|\Phi^+\right\rangle \\
&> 0,
\end{aligned} \tag{33}$$

which holds for all s_1, s_2 and t. In the third line, we apply the Cauchy-Schwarz inequality. The only value that the above equation can take is hence 1, indicating that $A_t^{(s_1)} = A_t^{(s_2)}$. Thus we can omit the superscript (s).

Since the linear BCS does not have a satisfying assignment with Pauli-string observables, we can use the commutation properties of Pauli operators and the substitution method and derive an expression $A_{t_1} A_{t_2} \cdots A_{t_m} = -\mathbb{I}$ for a set of variables that leads to a contradiction of $\mathbb{I} = -\mathbb{I}$. The proof of this statement shall be given in Corollary 2 in Appendix V B. Therefore, for any Clifford strategy, there exists a particular pair of inputs s, t such that $\langle\Phi^+| A_t^{(s)} \otimes B_t |\Phi^+\rangle \leq 0$. Consequently,

$$\Pr[\text{win} \mid s, t] = \frac{1}{2}\left(1 + \left\langle\Phi^+\right| A_t^{(s)} \otimes B_t \left|\Phi^+\right\rangle\right) \leq \frac{1}{2}. \tag{34}$$

Therefore, the average winning probability of the game is

$$\Pr[\text{win}] = \sum_{s',t'} \Pr[\text{win}|s', t'] \Pr[s', t'] \leq 1 - \frac{1}{2}\Pr[s, t]. \tag{35}$$

In the second part of the proof, we use the definition of Clifford operations that map a Pauli-string observable to a Pauli-string observable. For any initial state $|\psi\rangle$ that Alice and Bob may share in advance, it is linked with $|\Phi^+\rangle$ via a Clifford operation U_C. Then for any Pauli-string observables A_t, B_t,

$$\langle\psi| A_t \otimes B_t |\psi\rangle = \left\langle\Phi^+\right| U_C^\dagger (A_t \otimes B_t) U_C \left|\Phi^+\right\rangle \equiv \left\langle\Phi^+\right| A_t' \otimes B_t' \left|\Phi^+\right\rangle, \tag{36}$$

where A_t' and B_t' are also Pauli-string observables that adapt to the systems of Alice and Bob, respectively. Then, either $\{A_t'\}$ fails in yielding a satisfying assignment to one of the constraints, or the proof dates back to the first part. This finishes the proof. □

IV. 1D MAGIC BCS RELATION PROBLEM

In this part, we introduce the relation problem in detail by embedding the BCS nonlocal game into a one-dimensional grid. We will prove Theorem 4 in the main text, showing this problem can be solved by a generic constant-depth quantum circuit with only bounded fan-in gates, while any magic-free circuit requires a circuit depth that increases at least logarithmically to the input size. For simplicity, we consider the non-trivial BCS game with size $n = 8$. Three pairs of qubits suffice to realize the nonlocal game associated with this BCS, as shown in Section II. One can consider other values of n, where the proofs are similar.

In the shallow circuit computation, we apply the modified BCS given in Methods. That is, the constraint of $\prod_{v \in \mathcal{V}} a_v = -1$ is replaced with the set of constraints

$$\begin{cases}
a_1 a_2 a_{12} &= 1 \\
a_{12} a_3 a_{123} &= 1 \\
\cdots & \\
a_{1\cdots n-3} a_{n-2} a_{1\cdots n-2} &= 1 \\
a_{1\cdots n-2} a_{n-1} a_n &= -1.
\end{cases} \tag{37}$$

For the modified BCS with size $n = 8$, by applying Theorem 7, we have the following result.

Lemma 2. *In the modified BCS game with $n = 8$, suppose the questions are picked up uniformly at random. Then, the maximal winning probability for all Clifford strategies is upper-bounded by*

$$p_{\text{Clif}} \leq 1 - \frac{1}{6252}. \tag{38}$$

Now we introduce the relation problem R_N, which is labeled with a number N representing the problem size. One can assume that two players, Alice and Bob, collaborate with each other to solve R_N. The input and output of R_N are given as follows.

1. Input: in each round, Alice and Bob are given a question,
$$q = (\alpha_1, \beta_1, \cdots, \alpha_N, \beta_N), \alpha_i \in \mathcal{Q}^A \cup \{\perp\}, \beta_i \in \mathcal{Q}^B \cup \{\perp\}, \tag{39}$$
where q stands for "question", α_i is the input on Alice's side at site $i \in [N]$, and β_i is the input on Bob's side at site $i \in [N]$. $\mathcal{Q}^A$ consists of the set of constraints in the BCS, and $\mathcal{Q}^B$ consists of the set of variables in the BCS. Here, $\{\perp\}$ represents a null input.
2. Output: in each round, Alice and Bob need to return a reaction to the question,
$$r = (\mathbf{r}_1^A, \mathbf{r}_1^B, \cdots, \mathbf{r}_N^A, \mathbf{r}_N^B), \tag{40}$$
where r stands for "reaction", $\mathbf{r}_i^A = (r_i^A(1), r_i^A(2), r_i^A(3)) \in \{\pm 1\}^3$ is the output on Alice's side at site i, and similarly on Bob's side.

Now, we define the 1D magic BCS relation problem R_N. In the computation task, Alice and Bob are promised to receive an instance given by a tuple $(j, k, \alpha, \beta), 1 \leq j < k \leq N$, which defines the input as

$$\alpha_i = \begin{cases} \alpha, & \text{if } i = j, \\ \perp, & \text{if } i \neq j, \end{cases} \qquad \beta_i = \begin{cases} \beta, & \text{if } i = k, \\ \perp, & \text{if } i \neq k. \end{cases} \tag{41}$$

That is, we require the sites j on Alice's side and k on Bob's side to play the BCS nonlocal game with questions α and β, respectively. Alice and Bob are required to give an output satisfying either of the following requirements:

Case 1 For any $l \in \{1, 2, 3\}$,

$$\begin{aligned} \prod_{j < i \leq k} r_i^A(l) &= +1, \\ \prod_{j \leq i < k} r_i^B(l) &= +1, \end{aligned} \tag{42}$$

and

$$(\mathbf{r}_j^A, \mathbf{r}_k^B) = f(\alpha, \beta), \tag{43}$$

where f is the relation defined by the BCS nonlocal game.

Case 2 There exists $l \in \{1, 2, 3\}$ such that,

$$\prod_{j < i \leq k} r_i^A(l) = -1, \tag{44}$$

or

$$\prod_{j \leq i < k} r_i^B(l) = -1. \tag{45}$$

In addition, we require that **Case 1** occurs with a probability no smaller than a positive constant value $p \in (0, 1/64]$. By constant, we mean that p cannot be negligibly small, where there exists a sequence of positive values $\{p_1, \cdots, p_t, \cdots\}$ such that $p = \lim_{t \to \infty} p_t = 0^+$.

Below, we show that the 1D magic relation problem R_N can be solved by a QNC^0circuit but cannot be solved by any ClifNC^0circuit. We first show that there exists a shallow circuit with generic bounded fan-in quantum gates that perfectly completes this task. Now consider the following strategy:

1. Alice and Bob share $3N$ pairs of EPR states, $|\Phi^+\rangle^{\otimes 3N}$, where $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and arrange them in three layers, denoted by $q_{2i-1}(l), q_{2i}(l), i \in [N], l \in \{1,2,3\}$, where qubits $q_{2i-1}(l)$ and $q_{2i}(l)$ reside in the state $|\Phi^+\rangle$. Alice holds the qubits $q_{2i-1}(l)$ and Bob holds the qubits $q_{2i}(l)$.

2. For any $j \leq i \leq k-1$, perform an entanglement swapping operation between pairs of EPRs with a BSM on qubits $q_{2i}(l)$ and $q_{2i+1}(l)$. Denote the Bell state measurement results on the pair of adjacent qubits $q_{2i}(l)$ and $q_{2i+1}(l)$ as $r_i^B(l)$ and $r_{i+1}^A(l)$, respectively.

3. On the three pairs of qubits $q_{2j-1}(l)$ and $q_{2k}(l)$, Alice and Bob perform the measurements corresponding to the winning strategy in the BCS nonlocal game and obtain outputs $(r_j^A(l), r_k^B(l))$.

4. Take an arbitrary measurement on the qubits that are not measured and record the measurement results with respect to the site indices.

Note that at the end of the entanglement swapping operations, qubits $q_{2j-1}(l)$ and $q_{2k}(l)$ reside in $|\Phi^+\rangle$ with probability $1/4$ for each $l \in \{1,2,3\}$. By construction, this strategy naturally meets the problem requirements, and the first requirement defined through Eq. (42) and (43) is met with probability $1/64$. One can also see the reason that we modify the underlying BCS game: Alice needs to output an assignment to all the variables that appear in the constraint. As Alice can only output 3 bits in the relation problem, we need to decompose the original n-variable constraint into smaller ones. Measuring the observables in the winning strategy of the BCS nonlocal game thus results in the desired statistics. Moreover, the above strategy can be realized in a constant depth with finite fan-in operations and a computational basis measurement. Nevertheless, there is a minimal fan-in size of the gates to realize the above strategy. The following theorem gives a sufficient gate fan-in size.

Theorem 8. *Suppose the quantum computation circuits act on qubits or bits. Then, the fan-in size $K = 14$ is sufficient for the above strategy.*

Proof. As counted in Methods, in the modified BCS nonlocal game for the relation problem R_N^8, the number of variables is $727 + 1 < 2^{10}$, and the number of constraints is $1042 + 1 < 2^{11}$, where we also need to consider the null input $\perp$. Thus, all possible inputs α_i, β_i at site $i \in [N]$ can be encoded as 11 bits.

Next, we prove that all the operations in the above strategy can be implemented by K-bounded fan-in gates with $K = 14$. Note that all constant input size boolean function can be computed in NC^0, so we only care about the classically controlled quantum gates [Fig. 1(b)] and quantum measurements [Fig. 1(c)]. We analyze the algorithm step by step:

1. EPR preparation: No classical bit is involved. The quantum circuit involves simply one or two-qubit quantum gates, hence $K \geq 0 + 2 = 2$ in this step.

2. BSM: First determine whether the input is $\perp$ through classical computing. Then perform BSM if it so and do nothing if not. This step requires $K \geq 1 + 2 = 3$.

3. Nonlocal game: 11 classical bits are needed to control 3-qubit quantum gates. This step requires $K \geq 11+3 = 14$.

Therefore, all the operations in the shallow-circuit strategy to solve the computational problem can be implemented using K bounded fan-in gates with $K = 14$. This finishes the proof. □

As a side remark, note that a classically controlled quantum gate with a constant number of classical control bits can be decomposed into compositions of single-bit classically controlled quantum gates within a constant depth where the quantum part acts on up to two qubits [21]. Thus, actually, $K = 3$ is sufficient, albeit a compromise of a few circuit layers.

Below, we prove the hardness of the problem for a ClifNC^0circuit with only bounded fan-in classical gates and Clifford gates, including classically controlled Clifford gates and constant-weight Pauli-string measurements. We illustrate these two types of bounded fan-in gates in Fig. 1. The bounded fan-in classically controlled quantum gates require the numbers of classical input bits and the controlled qubits to be both finite, and the controlled gate is Clifford in a ClifNC^0circuit. The circuit allows intermediate measurements, and the measurement results can be used to control subsequent quantum gates. The constant-weight Pauli measurement measures a Pauli observable on a constant number of qubits, where the POVM element is a stabilizer state. As a constant-weight Pauli measurement is equivalent to implementing a constant-depth Clifford gate followed by the computational basis measurement on the first qubit and implementing the inverse of the Clifford gate, we can take all measurements as computational basis measurements, or σ_z measurements.

Now, consider a magic-free circuit with depth D, and the gates within it have fan-in bounded by K, which means the total number of input classical bits and qubits of the gates is no larger than K. Denote the qubit or bit value at

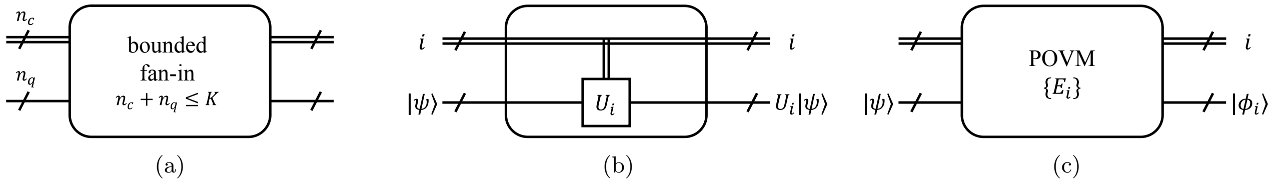


FIG. 1: (a) A general K-bounded fan-in gate acting on n_c bits and n_q qubits, with $n_c + n_q \le K$. There are two types of gates with $n_q > 0$: (b) Classically controlled quantum gates. The classical input i controls whether to apply the quantum gate U_i to the quantum input state $|\psi\rangle$; (c) Quantum measurement characterized by a positive operator-valued measure (POVM). The classical system acts as a register to record the measurement result. In a ClifNC^0circuit, U_i within the classically controlled gate is restricted to a Clifford operation. Meanwhile, in a ClifNC^0circuit, each measurement element E_i should be a mixture of stabilizer states. Equivalently, for a magic-free quantum input state $|\psi\rangle$, the post-measurement state $|\phi_i\rangle$ in a ClifNC^0circuit still does not contain quantum magic. In this work, we simply consider projective measurements. Both (b) and (c) are special cases of (a).

index v as i_v and suppose $\mathcal{E}_1$ is the gate of the first layer that contains i_v as an input. Then, $\mathrm{supp}(\mathcal{E}_1(i_v))$ determines a set of qubits and bits after the first layer of the circuit that may be affected by i_v. Similarly, we can consider the qubits and bits that may be affected in the next layer of the circuit. Denote the gates in each circuit layer are given by $\{\mathcal{E}_1, \mathcal{E}_2, \cdots, \mathcal{E}_D\}$. In the end, we call the set of qubits and bits

$$L_C^{\rightarrow}(i_v) = \mathrm{supp}(\mathcal{E}_D(\mathrm{supp}(\cdots \mathrm{supp}(\mathcal{E}_2(\mathrm{supp}(\mathcal{E}_1(i_v))))))) \tag{46}$$

the forward light cone of i_v.

The backward light cone of an output bit or qubit, o_w, at index b can be defined with the reverse of the forward light cone of the input and given by

$$L_C^{\leftarrow}(o_w) := \{i_v | o_w \in L_C^{\rightarrow}(i_v)\}. \tag{47}$$

The backward light cone of an output set, O, is defined as

$$L_C^{\leftarrow}(O) := \bigcup_{o \in O} L_C^{\leftarrow}(o). \tag{48}$$

Note that if a depth-D quantum circuit, $\mathcal{C}$, only comprises gates with fan-in bounded by K, then

$$|L_C^{\leftarrow}(o)| \le K^D, \tag{49}$$

and

$$|L_C^{\leftarrow}(O)| \le |O| K^D. \tag{50}$$

Note that the input of the relation problem R_N is classical and given by $q = (\alpha_1, \beta_1, \cdots, \alpha_N, \beta_N)$. Before acting gates, there are also an arbitrary number of classical ancillas with value 0 and quantum ancillas at state $|0\rangle$, which do not contain any input information. With the circuit's evolution, the input information will spread among classical bits and qubits via classically controlled quantum gates. Nonetheless, due to the gates being bounded fan-in and the circuit being at constant depth, the input information cannot spread a lot. The output of R_N can be read out from the classical bits after constant-depth circuit evolution. Without loss of generality, we can assume the output of R_N is read out from the first $6N$ bits at the last step of the circuit, which is $r = (\mathbf{r}_1^A, \mathbf{r}_1^B, \cdots, \mathbf{r}_N^A, \mathbf{r}_N^B)$ as mentioned above. We depict this procedure in Fig. 2(a).

Using the idea of information not spreading a lot, we will show that with high probability, an input value α_j (β_k) is independent of the output $\mathbf{r}_k^B$ ($\mathbf{r}_j^A$), as presented in Lemma 4. Before proving it, we first present the following lemma.

Lemma 3. *Let $\mathcal{C}$ be a depth-D circuit with classical inputs and an arbitrary number of quantum and classical ancillas, which comprises gates with fan-in upper bounded by K. The output of $\mathcal{C}$ is read out from the classical bits at the end of the circuit. Then, the following holds:*

Let O be a fixed subset of output bit indices, and suppose I is a randomly chosen subset of input bit indices such that for any input bit index v,

$$\Pr_I[v \in I] \le \eta. \tag{51}$$

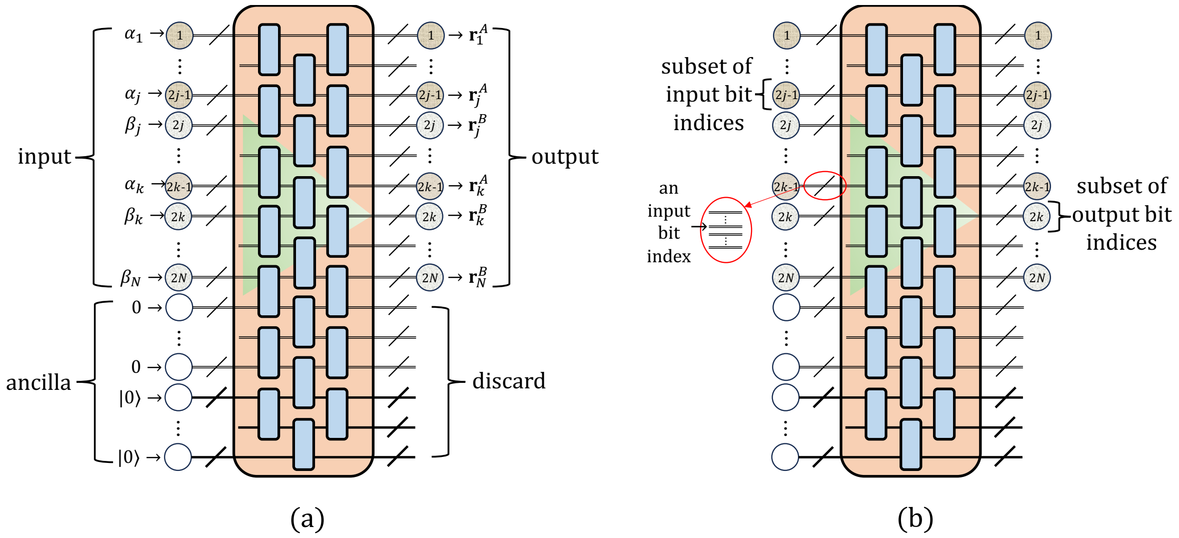


FIG. 2: (a) A circuit to solve relation problem R_N. The input comprises classical bits $(\alpha_1, \beta_1, \cdots, \alpha_N, \beta_N)$. Note that α_i takes value from $\mathcal{Q}^A \cup \{\perp\}$ and contains $\log\big(|\mathcal{Q}^A| + 1\big)$ bits. The case is similar for β_i. Besides, the circuit also has an arbitrary number of bits 0 and qubits $|0\rangle$ as ancillas. The output of the relation problem comprises classical bits $(\mathbf{r}_1^A, \mathbf{r}_1^B, \cdots, \mathbf{r}_N^A, \mathbf{r}_N^B)$. Each $\mathbf{r}_i^A$ or $\mathbf{r}_i^B$ contains three bits. Other qubits and bits within the circuit are discarded. (b) Diagram to label a subset of the input bits, a subset of the output bits, and an input bit. In Lemma 4, the subset of the input bits I is the set that takes value in $\mathcal{Q}^A$ or $\mathcal{Q}^B$ and does not take value of $\perp$. The subset of the output bits O is the set of bits outputting $\mathbf{r}_j^A$ or $\mathbf{r}_k^B$.

Then

$$\Pr_I[O \cap L_C^{\rightarrow}(I) \neq \emptyset] \leq \eta |O| 2^{|O|} K^D. \tag{52}$$

Proof.

$$\begin{aligned}
\Pr_I[O \cap L_C^{\rightarrow}(I) \neq \emptyset] &= \sum_{P \subseteq O, P \neq \emptyset} \Pr_I[O \cap L_C^{\rightarrow}(I) = P] \\
&\leq \sum_{P \subseteq O, P \neq \emptyset} \Pr_I[I \cap L_C^{\leftarrow}(P) \neq \emptyset] \\
&\leq \sum_{P \subseteq O, P \neq \emptyset} \sum_{v \in L_C^{\leftarrow}(P)} \Pr_I[v \in I] \\
&\leq \sum_{P \subseteq O, P \neq \emptyset} \sum_{v \in L_C^{\leftarrow}(P)} \eta \\
&\leq \sum_{P \subseteq O, P \neq \emptyset} |L_C^{\leftarrow}(P)| \eta \\
&\leq \sum_{P \subseteq O, P \neq \emptyset} |P| K^D \eta \\
&\leq 2^{|O|} |O| K^D \eta.
\end{aligned} \tag{53}$$

□

Lemma 4. *Consider a depth-D circuit composed of gates of fan-in at most K. The input of the circuit $q = (\alpha_1, \beta_1, \cdots, \alpha_N, \beta_N)$ is determined by a tuple (j, k, α, β) with $1 \leq j < k \leq N$ and given by Eq. (41). We denote the set of all possible inputs as S. The output of the circuit is given by $r = (\mathbf{r}_1^A, \mathbf{r}_1^B, \cdots, \mathbf{r}_N^A, \mathbf{r}_N^B)$. Define the event $E_\mathcal{C} \subset S$ in which the input parameters satisfy*

$$\mathrm{supp}(\mathbf{r}_j^A) \cap L_C^{\rightarrow}(\mathrm{supp}(\beta_k)) = \emptyset \text{ and } \mathrm{supp}(\mathbf{r}_k^B) \cap L_C^{\rightarrow}(\mathrm{supp}(\alpha_j)) = \emptyset. \tag{54}$$

Here, $\mathrm{supp}(x)$ *means the bits carrying on the value x. Under a uniform choice of input from S, the event $E_{\mathcal{C}}$ occurs with probability* $\Pr[E_{\mathcal{C}}] \geq 1 - \frac{48K^D}{N}$.

Proof. We consider a random input from the set S, which is constructed by a randomly generated tuple (j, k, α, β). Note that j and k are two different numbers uniformly and randomly picked from $\{1, 2, \cdots, N\}$ while α and β are randomly and uniformly picked from $\mathcal{Q}^A$ and $\mathcal{Q}^B$, respectively. Consider the input bit set as $I = \mathrm{supp}(\alpha_j)$ as the set that takes value in $\mathcal{Q}^A$ and does not take value of $\perp$ in Lemma 3 and suppose the input bit v is located at site j^*, as shown in Fig. 2(b). We have

$$\Pr_{\mathrm{supp}(\alpha_j)}[v \in \mathrm{supp}(\alpha_j)] = \Pr_{1 \leq j \leq N}[j = j^*] = \frac{1}{N}. \tag{55}$$

Meanwhile, consider the subset of the output bits O is the set of bits outputting $\mathbf{r}_k^B$, based on Lemma 3, we obtain

$$\Pr_{\mathrm{supp}(\alpha_j)}[\mathrm{supp}(\mathbf{r}_k^B) \cap L_C^{\rightarrow}(\mathrm{supp}(\alpha_j)) \neq \emptyset] \leq 2^{|\mathbf{r}_k^B|}|\mathbf{r}_k^B|K^D\frac{1}{N}. \tag{56}$$

Note that $\mathbf{r}_k^B$ only has 3 output bits, then

$$\Pr_{\mathrm{supp}(\alpha_j)}[\mathrm{supp}(\mathbf{r}_k^B) \cap L_C^{\rightarrow}(\mathrm{supp}(\alpha_j)) \neq \emptyset] \leq \frac{24K^D}{N}. \tag{57}$$

Similarly, we get

$$\Pr_{\mathrm{supp}(\beta_k)}[\mathrm{supp}(\mathbf{r}_j^A) \cap L_C^{\rightarrow}(\mathrm{supp}(\beta_k)) \neq \emptyset] \leq \frac{24K^D}{N}. \tag{58}$$

Thus,

$$\begin{aligned}\Pr_q[E_{\mathcal{C}}] &= \Pr_{\mathrm{supp}(\alpha_j),\mathrm{supp}(\beta_k)}[\mathbf{r}_j^A \cap L_C^{\rightarrow}(\beta_k) = \emptyset \cap \mathbf{r}_k^B \cap L_C^{\rightarrow}(\alpha_j) = \emptyset] \\ &= 1 - \Pr_{\mathrm{supp}(\alpha_j),\mathrm{supp}(\beta_k)}[\mathbf{r}_j^A \cap L_C^{\rightarrow}(\beta_k) \neq \emptyset \cup \mathbf{r}_k^B \cap L_C^{\rightarrow}(\alpha_j) \neq \emptyset] \\ &\geq 1 - \Pr_{\mathrm{supp}(\beta_k)}[\mathbf{r}_j^A \cap L_C^{\rightarrow}(\beta_k) \neq \emptyset] - \Pr_{\mathrm{supp}(\alpha_j)}[\mathbf{r}_k^B \cap L_C^{\rightarrow}(\alpha_j) \neq \emptyset] \\ &\geq 1 - \frac{48K^D}{N}.\end{aligned} \tag{59}$$

□

With Lemma 4, we are able to achieve our ultimate goal to prove the hardness of R_N for magic-free shallow circuits. The main idea is that with high probability, the event defined in Lemma 4 would happen, and if this event happens, the magic-free circuit cannot give a correct output as the nonlocal game requires magic to win with certainty.

Theorem 9. *Let $\mathcal{C}$ be a depth-D circuit with classical input values and classical and quantum ancillas, which only comprises magic-free operations with fan-in upper bounded by K. Now, consider the classical input $q = (\alpha_1, \beta_1, \cdots, \alpha_N, \beta_N)$ determined by Eq. (41) with α_j and β_k selected uniformly at random from $\mathcal{Q}^A$ and $\mathcal{Q}^B$. Then for any constant value $p \in (0, 1)$, the average probability that $\mathcal{C}$ outputs $r = (\mathbf{r}_1^A, \mathbf{r}_1^B, \cdots, \mathbf{r}_N^A, \mathbf{r}_N^B)$ such that*

(1) r and q satisfy the requirements in ***Case 1*** *and* ***Case 2****,*

(2) outputs ***Case 1*** *with probability no smaller than p,*

is at most $\frac{48K^D}{N} + p_{\mathrm{Clif}}$, with p_{Clif} given in Lemma 2. To meet the requirements with a success probability larger than $(1 + p_{\mathrm{Clif}})/2$, the circuit depth requirement is $\Theta(\log N)$.

Proof. The average success probability of $\mathcal{C}$ to output a correct relation between r and q is

$$\begin{aligned}
\Pr_q[\text{success}] =& \Pr_q[\textbf{Case 1}] \Pr_q[\text{success}|\textbf{Case 1}] + \Pr_q[\textbf{Case 2}] \Pr_q[\text{success}|\textbf{Case 2}] \\
=& \Pr_q[\textbf{Case 1}](\Pr_q[E_{\mathcal{C}}|\textbf{Case 1}] \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}] + \Pr_q[E_{\mathcal{C}}^C|\textbf{Case 1}] \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}^C]) \\
&+ \Pr_q[\textbf{Case 2}] \Pr_q[\text{success}|\textbf{Case 2}] \\
\leq& \Pr_q[\textbf{Case 1}](\Pr_q[E_{\mathcal{C}}|\textbf{Case 1}] \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}] + 1 - \Pr_q[E_{\mathcal{C}}|\textbf{Case 1}]) + \Pr_q[\textbf{Case 2}] \\
=& 1 - \Pr_q[\textbf{Case 1}] \Pr_q[E_{\mathcal{C}}|\textbf{Case 1}](1 - \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}]) \\
=& 1 - \Pr_q[E_{\mathcal{C}}](1 - \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}]) \\
=& 1 - \Pr_q[E_{\mathcal{C}}] + \Pr_q[E_{\mathcal{C}}] \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}] \\
\leq& \frac{48K^D}{N} + \Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}].
\end{aligned} \tag{60}$$

Here, $E_{\mathcal{C}}$ is the event defined in Lemma 4 and $E_{\mathcal{C}}^C$ is the complementary set of $E_{\mathcal{C}}$. From the above inequality, notice that the upper bound on the average success probability is irrelevant with the probability for **Case 1** to occur, i.e., the value of p. Now, we only need to investigate the value of $\Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}]$.

When **Case 1** happens, the success condition is making the inputs α_j and β_k and the outputs $\mathbf{r}_j^A$ and $\mathbf{r}_k^B$ satisfy the relation defined by the BCS game, i.e., Eq. (43). Also, when $E_{\mathcal{C}}$ happens, the output $\mathbf{r}_j^A$ only depends on α_j and does not depend on β_k. And the reverse is true for $\mathbf{r}_k^B$. It reduces to the case that Alice and Bob are trying to win the BCS non-local game without classical communication. As the circuit only comprises $|0\rangle$ as input quantum states, Clifford gates, and Pauli measurements, it means that Alice and Bob need to win this non-local game with Pauli measurements and magic-free states, whose winning probability is upper-bounded by p_{Clif}. That is, $\Pr_q[\text{success}|\textbf{Case 1}, E_{\mathcal{C}}] \leq p_{\text{Clif}}$. Then, we conclude that the average success probability of $\mathcal{C}$ to output a correct relation between r and q is

$$\Pr_q[\text{success}] \leq \frac{48K^D}{N} + p_{\text{Clif}}. \tag{61}$$

To output the correct relation with a success probability larger than $(1 + p_{\text{Clif}})/2$, the circuit depth D has a lower bound as below.

$$\frac{48K^D}{N} + p_{\text{Clif}} \geq \frac{1 + p_{\text{Clif}}}{2} \Leftrightarrow D \geq \frac{\log N + \log \frac{1-p_{\text{Clif}}}{96}}{\log K} = \Omega(\log N). \tag{62}$$

On the other hand, as stated in the main text, there is a classical circuit with circuit depth $O(\log N)$ that solves the problem. Therefore, the bound on the circuit depth for magic-free circuits to solve the problem is tight. This finishes the proof. □

V. FINDING POTENTIAL MAGIC-NECESSARY LINEAR BINARY CONSTRAINT SYSTEMS

In this section, we discuss finding other instances of linear BCS that require magic for a perfect quantum solution. It is challenging to develop a general procedure for this target. Instead, we provide a "guess-and-check" procedure: (1) First, obtain a potential BCS, and (2) Second, verify whether the BCS has a solution over the Pauli group. For the first step, one can use the group embedding results in Ref. [1]. Building on the group-theoretic results, including Ref. [8, 9], Ref. [1] provides an efficient procedure to embed a group into a BCS, which is a group homomorphism of the original group to a non-trivial BCS solution group; hence the procedure constructs a BCS that necessarily has a (quantum) solution. In particular, the output solution group inherits the representation properties of the original group. However, such a BCS may have a classical solution or a quantum solution over the Pauli group, where magic is absent. We develop an efficient classical algorithm for this issue to decide whether a linear BCS has a Pauli-string solution. Besides aiding the search for non-trivial linear BCS, we hope this result can help explore the decidability problems for general BCS and nonlocal games [5].

A. Slofstra's group embedding procedure

A group G is said to be embedded into group K if there exists an injective group homomorphism $\phi : G \to K$. One can pose additional requirements to the group embedding to guarantee the inheritance of group representation properties; see Definitions 10 and 14 in Ref. [1] for example. This is also one of the core issues in the group embedding procedure in Ref. [1]. For our purpose of finding magic-necessary BCS, some analysis on the group representation inheritance issue may be redundant. Nevertheless, we faithfully review the group embedding results of Ref. [1] here and leave the problem of simplifying the procedure to future work. For the convenience of stating the group embedding results, we use the Boolean variables and parity constraints instead of the sign variables and multilinear constraints in this subsection. The conversion between sign variables and Boolean variables is given in Eq. (4).

As we now use the Boolean variable notation, a BCS can be compactly written as $M\vec{v} = \vec{c}$, where M is an $m \times n$ Boolean matrix, $\vec{v} = (v_1, \cdots, v_n)^{\mathrm{T}}$ is the vector of variables, and $\vec{c} = (c_1, \cdots, c_m)^{\mathrm{T}}$ is the vector of constraints. The non-zero elements in the j'th row of M define the set of variables presented in the j'th constraint, $\mathcal{S}_j$. We first define several classes of groups, including a restatement of the BCS solution group with the current notations.

Definition 3 (Solution group of a linear BCS using Boolean variables)**.** *Given a linear BCS with n binary variables $\{v_i\}$ and m constraints $\{c_j\}$ specified by $M\vec{v} = \vec{c}$, the solution group of the BCS is defined as the group with the following presentation:*

$$\begin{aligned}\Gamma(M, \vec{c}) = \{\{J, g_i : i \in [n]\} : \{&g_i^2 = e, \forall i \in [n],\\ &J^2 = e,\\ \forall j \in [m], &g_k g_l = g_l g_k, \forall k, l \in \mathcal{S}_j,\\ &J g_i = g_i J, \forall i \in [n],\\ &\prod_{i \in \mathcal{S}_j} g_i = J^{c_j}, \forall j \in [m]\}\},\end{aligned} \tag{63}$$

where e defines the identity operator of the group. We take the convention that $J^0 = e$.

Definition 4 (Linear-plus-conjugacy group)**.** *Given a linear BCS with n binary variables $\{v_i\}$ and m constraints $\{c_j\}$ specified by $M\vec{v} = \vec{c}$, and $\mathcal{C} \subseteq [n] \times [n] \times [n]$ with $[n] = \{1, \cdots, n\}$, the linear-plus-conjugacy group $\Gamma(M, \vec{c}, \mathcal{C})$ is defined as*

$$\Gamma(M, \vec{c}, \mathcal{C}) \equiv \langle \Gamma(M, \vec{c}) : g_i g_j g_i = g_k, \forall (i, j, k) \in \mathcal{C} \rangle, \tag{64}$$

where the relators $g_i g_j g_i = g_k$ are additionally posed to the solution group $\Gamma(M, \vec{c})$.

Definition 5 (Homogeneous linear-plus-conjugacy group)**.** *Given an $m \times n$ Boolean matrix M where the set of non-zero elements in the j'th row is given by $\mathcal{S}_j$, and $\mathcal{C} \subseteq [n] \times [n] \times [n]$, the homogeneous linear-plus-conjugacy group $\Gamma_0(M, \mathcal{C})$ is defined as*

$$\begin{aligned}\Gamma_0(M, \mathcal{C}) = \{\{g_i : i \in [n]\} : \{&g_i^2 = e, \forall i \in [n],\\ \forall j \in [m], &g_k g_l = g_l g_k, \forall k, l \in \mathcal{S}_j,\\ &\prod_{i \in \mathcal{S}_j} g_i = e, \forall j \in [m],\\ &g_i g_j g_i = g_k, \forall (i, j, k) \in \mathcal{C}\}\}.\end{aligned} \tag{65}$$

Definition 6 (Extended homogeneous linear-plus-conjugacy group)**.** *Given an $m \times n$ Boolean matrix M, $\mathcal{C}_0 \subseteq [n] \times [n] \times [n]$, $\mathcal{C}_1 \subseteq [l] \times [n] \times [n]$, and L an $l \times l$ lower-triangular matrix with non-negative integer entries, the extended homogeneous linear-plus-conjugacy group $E\Gamma_0(M, \mathcal{C}_0, \mathcal{C}_1, L)$ is defined as*

$$\begin{aligned}E\Gamma_0(M, \mathcal{C}_0, \mathcal{C}_1, L) \equiv \langle \Gamma_0(M, \mathcal{C}_0), h_1, \cdots, h_l : &h_i g_j h_i^{-1} = g_k, \forall (i, j, k) \in \mathcal{C}_1,\\ &h_i h_j h_i^{-1} = h_j^{L_{ij}}, \forall i > j \wedge L_{ij} > 0\rangle,\end{aligned} \tag{66}$$

where L_{ij} refers to the element on the i'th row and j'column of matrix L.

With the above definition, Ref. [1] proves the following embedding results:

Theorem 10 ([1])**.** *Suppose a group G has a presentation in the form of an extended homogeneous linear-plus-conjugacy group given by $E\Gamma_0(M, \mathcal{C}_0, \mathcal{C}_1, L)$. Then there are the following group embedding results:*

1. *There exists a group embedding of $E\Gamma_0(M, \mathcal{C}_0, \mathcal{C}_1, L)$ into a homogeneous linear-plus-conjugacy group (Proposition 33 in Ref. [1]):*
$$E\Gamma_0(M, \mathcal{C}_0, \mathcal{C}_1, L) \to \Gamma_0(M', \mathcal{C}), \tag{67}$$
where $\Gamma_0(M', \mathcal{C})$ is a homogeneous linear-plus-conjugacy group.

2. *The extended $\Gamma_0(M', \mathcal{C})$ can be transformed into a linear-plus-conjugacy group (see the remark after Definition 31 in Ref. [1]):*
$$\Gamma_0(M', \mathcal{C}) \times \mathbb{Z}_2 = \Gamma(M', 0, \mathcal{C}). \tag{68}$$

3. *By adding relations with respect to one group element $J \in \Gamma(M', 0, \mathcal{C}), J \neq e$, which extends the matrix M' into N and adds non-homogeneous linear constraints that involve J, extend the linear-plus-conjugacy group:*
$$\Gamma(M', 0, \mathcal{C}) \to \Gamma(N, \vec{c}, \mathcal{C}'), \tag{69}$$
where $\vec{c} \neq 0$, with some entries equal to J.

4. *There exists a group embedding of $\Gamma(N, \vec{c}, \mathcal{C}')$ into a linear group (Proposition 27 in Ref. [1]):*
$$\Gamma(N, \vec{c}, \mathcal{C}) \to \Gamma(N', \vec{c}'), \tag{70}$$
which defines a BCS solution group that has a non-trivial group element $J \neq e$.

The proof is constructive, thus one can derive the concrete groups in each step. In brief, as long as a group can be presented in the form of Def. 6, which is an extended homogeneous linear-plus-conjugacy group, it can be converted into a BCS solution group after a series of group embeddings and a proper construction of non-trivial relators with respect to a group element $J \neq e$, which is set to correspond to -1 in the BCS. As promised by Lemma 1, the underlying BCS of the solution group has an (operator-valued) solution.

B. Efficient algorithm for finding perfect Pauli-string solutions to linear BCS

Next, we provide an efficient algorithm to determine the existence of a Pauli-string solution to a general linear BCS. Combined with Slofstra's group embedding procedure, one can guess and test BCS instances to search for a potential BCS that has a non-trivial solution group other than the Pauli group.

We first present some fundamental properties of Pauli-string observables.

Lemma 5. *Suppose $A_1, A_2, \cdots, A_n$ are Pauli-string observables. For $i, j \in [n]$, define $C_{ij} = A_iA_jA_iA_j$ as the commutator between A_i and A_j. Then, C_{ij}'s have the following properties:*

1. *$C_{ij} \in \{\pm\mathbb{I}\}$. Specifically, $C_{ij} = \mathbb{I}$ when $A_iA_j - A_jA_i = 0$, and $C_{ij} = -\mathbb{I}$ when $A_iA_j + A_jA_i = 0$;*
2. *$C_{ij} = C_{ji}$ and $C_{ii} = \mathbb{I}$;*
3. *$A_iA_j = C_{ij}A_jA_i$.*

The proof of Lemma 5 is straightforward, and we leave it to the readers as an exercise. According to the first property, C_{ij} is always proportional to $\mathbb{I}$ and thus commute with all the A_i's. We can treat C_{ij}'s as numbers ± 1 for simplicity. The second property shows that for a group of n A_i's, the number of independent commutators C_{ij}'s among them is at most $n(n-1)/2$. The third property shall be vital for our later discussions, as it allows us to swap two adjacent variables A_i and A_j in a product of Pauli strings up to an additional coefficient C_{ij}. Together with the first property, for a product of Pauli-string variables, we can arbitrarily rearrange their order up to a change in the sign.

Given a linear BCS, we first determine if it has a classical solution, i.e., $A_i \in \{\pm 1\}$ for all $i \in [n]$. This is equivalent to solving a system of linear equations over $\mathbb{Z}_2$, which can be done in poly(n) steps through, for example, the Gaussian elimination method. Going back to determine if the BCS has a Pauli-string solution, if we hope to apply a similar procedure, the only obstacle is that the variables might not commute with each other. Nevertheless, thanks to the nice properties of Pauli strings in Lemma 5, we can do the same thing as finding a classical solution with at most a difference in sign, which we record as a sign variable C_i. Should the BCS have a Pauli-string solution, at the end of the elimination, we can express each variable A_i as a product of some variables, which we term the "free variables," multiplied by a plus or minus sign $C_i \in \{\pm 1\}$. We use the terminology "free variables" as they are allowed to take any value, while the remaining variables depend on their values. Now we give the rigorous statement and prove it.

Lemma 6. *For a linear BCS with n variables $A_1, \cdots, A_n$ and m constraints, if it has a Pauli-string solution, then there exists a set of free variables $\{A_{i_k}\}_k$, such that each variable in the BCS can be represented in the form of $A_i = C_i A_{i_1} A_{i_2} \cdots A_{i_k} \cdots$, where $C_i \in \{\pm 1\}$ and A_{i_k}'s are arranged with the subscript k from small to large. This result can be obtained in* poly(n, m) *steps.*

Proof. When finding an operator-valued solution to a linear BCS, we require the variables in the same constraint to be compatible, as discussed in Appendix I B. Now we prove a stronger statement that does not rely on this requirement.

We prove the lemma by mathematical induction on m. The statement holds when $m = 1$, where $A_1 A_2 \cdots A_n = \pm 1$. Clearly, $A_1 = \pm A_2 \cdots A_n$, and we can take $A_2 \cdots A_n$ as free variables. We use the first property in Lemma 5 when there is a need to change the order of two variables, which finishes in poly(n) steps using a sorting algorithm. Now assume the statement holds for $m = k$. When $m = k + 1$, without loss of generality, suppose the first constraint is the added constraint with $A_1 A_2 \cdots A_l = \pm 1$. Thus, $A_1 = \pm A_2 \cdots A_l$. Substitute this expression into the other equations and simplify them using Lemma 5, which finishes in poly(n, m) steps using Gaussian elimination. Then, we get a set of k constraints. According to the induction hypothesis, every variable A_i can be represented as a product of free variables up to a sign. So we can plug the free variables into the added constraint $A_1 = \pm A_2 \cdots A_l$ and get the expression for A_1 in terms of free variables. Therefore, the statement holds for $m = k + 1$. □

Now, we get the expression for each variable in terms of a set of free variables, resulting in a linear BCS over A_i's and additional sign variables C_i's.

We further consider the conditions in the original linear BCS and eliminate all the non-free variable A_i's. Using Lemma 6, we find a set of free variables and use them to express all the other variables. Then, we substitute the expressions into the original BCS and obtain a new BCS containing the free variables and C_i's. By the definition of the free variable, every free variable occurs for an even number of times in each constraint of the new BCS by this step, otherwise, it is determined by the other variables through their commutators. By further applying Lemma 5, we can get rid of all the A_i variables and obtain a set of equations of C_i's and C_{kl}'s where k, l are the commutators of the free variables A_k and A_l. In addition, if A_i and A_j appear in the same constraint of the original BCS, they commute with each other, i.e., $A_i A_j A_i A_j = 1$. For each pair of A_i and A_j, by applying Lemma 6, replace them in the equation $A_i A_j A_i A_j = 1$ via their expressions in terms of the free variables and obtain the other equations of C_{kl}'s where k, l are indices of free variables. In the end, we convert the original linear BCS to an equivalent set of equations of C_i's ($i \in [n]$) and C_{kl}'s (k, l are indices of free variables), which is just a system of linear equations over $\mathbb{Z}_2$. Note that all the procedures are simply substitutions and the order swaps between variables, which finish in poly(n, m) steps. Should the original BCS have a Pauli-string solution, we can efficiently solve the newly derived linear equations and get a set of valid values for C_i's and C_{kl}'s.

Note that by this step, we have not finished solving the original BCS over the Pauli group, as we have not determined the operator values of A_i's. The following lemma gives a systematic method to assign legitimate Pauli-string values for all the free variables and, hence, all the variables in the original BCS.

Lemma 7. *For any given set of sign variables $\{C_{ij} = \pm 1\}_{1 \le i < j \le n}$, there exists a set of Pauli strings $\{A_i\}_{1 \le i \le n}$, such that for any $1 \le i < j \le n$, $A_i A_j A_i A_j = C_{ij}$. That is, the commutator between A_i and A_j is C_{ij}.*

Proof. We give an explicit construction. Suppose there are p sign variables equal to -1, given by $C_{i_1 j_1}, C_{i_2 j_2}, \cdots, C_{i_p j_p}$. Then, we can construct Pauli strings over p qubits according to the following rule: for every q'th qubit in each Pauli string, where $1 \le q \le p$, assign σ_x for A_{i_q} and σ_z for A_{j_q}; assign all the other qubits as $\mathbb{I}$. That is,

$$\text{the } q\text{'th qubit of } A_k = \begin{cases} \sigma_x, & \text{if } k = i_q, \\ \sigma_z, & \text{if } k = j_q, \\ \mathbb{I}, & \text{otherwise.} \end{cases} \tag{71}$$

It can be directly checked that this construction satisfies the requirements.

□

Later, we take the Mermin-Peres magic square BCS as an example to exhibit the entire procedure. As a side note, the correspondence between traceless symmetric matrices over $\mathbb{Z}_2^{n \times n}$ and Pauli strings was implicitly used in Lemma 7 in Ref. [4].

Now we summarize the results for determining the Pauli-string solution to a linear BCS.

Theorem 11. *For a linear BCS with n variables and m constraints, there exists a classical algorithm that determines whether it has a perfect quantum strategy on the Pauli group in* poly(n, m) *steps.*

The procedures can be summarized as follows:

1. Solve the BCS as if it is a classical one, with a recording of the commutator and sign changes in each step. Get an expression for each variable in terms of a set of free variables.
2. Substitute the expressions into the original BCS. Get a system of linear functions of C_i's and C_{kl}'s and solve them over $\mathbb{Z}_2$.
3. Assign a Pauli string to every free variable. Then derive the operator values of all the variables according to the expressions in step 1.

On the other hand, if there is not a Pauli-string solution to the linear BCS, we shall come to a contradiction somewhere in the procedures.

Corollary 2. *Suppose a linear BCS does not have a satisfying assignment with Pauli-string observables. On the one hand, we can use the substitution method of solving a BCS and obtain a relation for a subset of variables,*

$$A_{t_1}A_{t_2}\cdots A_{t_k} = -\mathbb{I}. \tag{72}$$

On the other hand, by posing the commutation properties of Pauli strings to the BCS variables, the left-hand side can be eliminated to $\mathbb{I}$, resulting in a contradiction.

The proof of this corollary is similar to Lemma 6. In brief, in the algorithm for finding Pauli-string solutions, we only use two operations throughout the process: (1) substitution of expressions and (2) swapping two variables in an expression according to Lemma 5. If the algorithm cannot find a Pauli-string solution, it must result in a contradiction. As we keep the right-hand side of each formula to be $\pm\mathbb{I}$, the contradiction is thus the form of the statement in the corollary.

As an example, we apply the algorithm to find a Pauli-string solution to the Mermin-Peres magic square BCS. The original BCS is given by

$$\begin{aligned} A_1A_2A_3 &= 1,\\ A_4A_5A_6 &= 1,\\ A_7A_8A_9 &= 1,\\ A_1A_4A_7 &= 1,\\ A_2A_5A_8 &= 1,\\ A_3A_6A_9 &= -1. \end{aligned} \tag{73}$$

After the first step, we find that the BCS variables can be determined by a set of free variables $\{A_5, A_6, A_8, A_9\}$:

$$\begin{aligned} A_1 &= C_1A_5A_6A_8A_9,\\ A_2 &= C_2A_5A_8,\\ A_3 &= C_3A_6A_9,\\ A_4 &= C_4A_5A_6,\\ A_7 &= C_7A_8A_9. \end{aligned} \tag{74}$$

Substituting these expressions into the original BCS, we obtain the set of equations

$$\begin{aligned} A_1A_2A_3 &= C_1C_2C_3C_{59}C_{56}C_{58}C_{69}C_{89} = 1,\\ A_4A_5A_6 &= C_4C_{56} = 1,\\ A_7A_8A_9 &= C_7C_{89} = 1,\\ A_1A_4A_7 &= C_1C_4C_7C_{59}C_{68}C_{56}C_{58}C_{69}C_{89} = 1,\\ A_2A_5A_8 &= C_2C_{58} = 1,\\ A_3A_6A_9 &= C_3C_{69} = -1. \end{aligned} \tag{75}$$

Using the commutation conditions between variables in the same constraint as the original BCS, we have the equations

$$\begin{aligned} A_1A_2A_1A_2 &= C_{69} = 1,\\ &\cdots\\ A_4A_7A_4A_7 &= C_{59}C_{68}C_{56}C_{58}C_{69}C_{89} = 1,\\ &\cdots\\ A_8A_9A_8A_9 &= C_{89} = 1. \end{aligned} \tag{76}$$

Solving Eq. (75) and (76) over $\mathbb{Z}_2$, we have

$$\begin{aligned} &C_1 = C_2 = C_4 = C_7 = 1, \\ &C_3 = -1, \\ &C_{56} = C_{58} = C_{69} = C_{89} = 1, \\ &C_{59} = C_{68} = -1. \end{aligned} \tag{77}$$

With respect to the commutators among the free variables, we obtain two commutators that are equal to -1. Assign the free variables as two-qubit Pauli strings,

$$\begin{aligned} A_5 &= \sigma_x \otimes \mathbb{I}, \\ A_6 &= \mathbb{I} \otimes \sigma_x, \\ A_8 &= \mathbb{I} \otimes \sigma_z, \\ A_9 &= \sigma_z \otimes \mathbb{I}, \end{aligned} \tag{78}$$

and the other variables are then determined as

$$\begin{aligned} A_1 &= -\sigma_y \otimes \sigma_y, \\ A_2 &= \sigma_x \otimes \sigma_z, \\ A_3 &= -\sigma_z \otimes \sigma_x, \\ A_4 &= \sigma_x \otimes \sigma_x, \\ A_7 &= \sigma_z \otimes \sigma_z. \end{aligned} \tag{79}$$

This solution is equivalent to the solution in Eq. (7) in the sense of a unitary transformation, or a relabelling of the variables.

[1] W. Slofstra, in *Forum Math. Pi*, Vol. 7 (Cambridge University Press, 2019) p. e1.
[2] D. Gottesman, *Stabilizer codes and quantum error correction* (California Institute of Technology, 1997).
[3] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[4] Z. Ji, arXiv:1310.3794 (2013).
[5] H. Fu, C. A. Miller, and W. Slofstra, arXiv:2101.11087 (2021).
[6] A. Cabello, Phys. Rev. Lett. **101**, 210401 (2008).
[7] W. Slofstra, J. Am. Math. Soc. **33**, 1 (2020).
[8] R. Cleve and R. Mittal, in *Automata, Languages, and Programming: 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I 41* (Springer, 2014) pp. 320–331.
[9] R. Cleve, L. Liu, and W. Slofstra, J. Math. Phys. **58**, 012202 (2017).
[10] A. Coladangelo and J. Stark, arXiv:1709.09267 (2017).
[11] C. Paddock, W. Slofstra, Y. Zhao, and Y. Zhou, arXiv:2301.11291 (2023).
[12] J.-P. Serre *et al.*, *Linear representations of finite groups*, Vol. 42 (Springer, 1977).
[13] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[14] A. Peres, Phys. Lett. A **151**, 107 (1990).
[15] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Phys. Rev. A **93**, 062121 (2016).
[16] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[17] A. Arkhipov, arXiv:1209.3819 (2012).
[18] E. Specker, Dialectica **14**, 239 (1960).
[19] S. Kochen and E. Specker, J. Math. Mech. **17**, 59 (1967).
[20] R. Renner and S. Wolf, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.* (IEEE, 2004) pp. 322–322.
[21] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge university press, 2010).

Unmasking the Polygamous Nature of Quantum Nonlocality

Paweł Cieśliński[1] Lukas Knips[2 3 4] Mateusz Kowalczyk[1] Wiesław Laskowski[1 *]
Tomasz Paterek[1 5] Tamás Vértesi[6] Harald Weinfurter[1 2 3 4]

[1] *University of Gdańsk, Gdańsk, Poland*
[2] *Max Planck Institute for Quantum Optics, Garching, Germany*
[3] *Ludwig Maximilian University, Munich, Germany*
[4] *Munich Center for Quantum Science and Technology, Munich, Germany*
[5] *Xiamen University Malaysia, Sepang, Malaysia*
[6] *Institute for Nuclear Research, Debrecen, Hungary*

Abstract. Quantum mechanics imposes limits on the statistics of certain observables. The most famous example is the uncertainty principle. Similar trade-offs exist for the simultaneous violation of multiple Bell inequalities. In the simplest case of three observers, violating one inequality precludes the violation of any other inequality, a property called monogamy of Bell violations. We show that the Bell-monogamy does not hold universally and the only monogamous situation exists only for three observers. Consequently, the nature of quantum nonlocality is truly polygamous. The identified polygamous inequalities are experimentally violated and may be exploited for quantum cryptography or simultaneous self-testing of multiple nodes in a quantum network.

Keywords: quantum correlations, Bell inequalities, Bell monogamy, self-testing, quantum network

1 Introduction

Quantum nonlocality is one of the most intriguing features of quantum theory. Starting from its beginnings and the famous EPR argument [1], through the first works of John Bell [2] to various experiments [3–12], it reveals the impossibility of a local-realistic description of quantum phenomena. Violation of a Bell inequality serves now not only as fundamental test for the statements about the nature of reality but also finds applications in many areas of modern quantum technologies [13–19]. One crucial concept in the study of quantum nonlocality is the monogamy principle, which states that it is impossible to simultaneously violate all k-partite ($k < N$) two-setting Bell inequalities among N different parties. After the early findings by Scarani and Gisin [20], and later by Toner and Verstraete [21] (see also [22, 23]), it became a fundamental result in the field and the subject of many extensive studies [24–38].

However, as shown here, the monogamy principle is not fundamental. Rather, it is a mere consequence of the specific mathematical structure of certain inequalities, which are not universal. To support our claim, we develop a systematic method to construct Bell inequalities among $N-1$ observers that do not adhere to the monogamy principle for all $N > 3$. Furthermore, we provide an interesting minimalistic polygamous scenario based only on bipartite correlations between all pairs of observers. We show that the simultaneous violation of all inequalities is possible if the number of parties is $N = 18$. Recognising the practical challenges associated with generating high-fidelity quantum states in experimental setups, we could still identify inequalities that are violated experimentally by noisy six-qubit Dicke states. The polygamous nature of quantum nonlocality is therefore proven theoretically and confirmed in experiments.

2 Three parties and strict monogamy

We begin by recalling the standard results on Bell monogamy between three observers. Consider a scenario in which party A tries to simultaneously violate the CHSH inequalities [39] with parties B and C using a three-qubit quantum state. We denote the value of the CHSH-Bell parameters by $\mathcal{B}_{AB}$ and $\mathcal{B}_{AC}$, respectively. Quantum mechanics predicts that these parameters obey the relation [20, 21]

$$\mathcal{B}_{AB}^2 + \mathcal{B}_{AC}^2 \leq 8. \tag{1}$$

Note that if one of the inequalities is violated, e.g. $\mathcal{B}_{AB} > 2$, then the other one cannot be violated, $\mathcal{B}_{AC} < 2$. This is the statement of monogamy of Bell inequality violations.

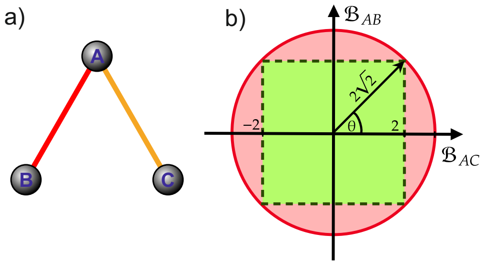


Figure 1: Visual representation of monogamy between CHSH inequality violations for three parties. *a*) Schematic of the arrangement where three observers (A, B, C) try to violate two inequalities (red and orange edges). *b*) Accessible values of Bell parameters $\mathcal{B}_{AB}$ and $\mathcal{B}_{AC}$ for parties AB and AC. According to local realistic models, the bound on each inequality is given by 2 and hence its predictions are confined to the square with a side length of 4. Quantum predictions lie within a circle of a radius $2\sqrt{2}$.

[*] wieslaw.laskowski@ug.edu.pl

3 Polygamy of Bell violation

To demonstrate the polygamous nature of Bell nonlocality, we generalise the Toner-Verstraete scenario [21] to the case of N observers where each of them can perform measurements of two dichotomic observables $A_1^{(i)}, A_2^{(i)}$ $(i = 1, \ldots, N)$. Then, we analyze the simultaneous violation of Bell inequalities between $N-1$ observers in all possible N configurations. One strategy to find Bell inequalities that do not satisfy the monogamy principle is by imposing permutation symmetry. Let N observers share an N-qubit quantum state that is permutationally invariant, and they perform measurements of the same observables on it, i.e., $A_j^{(i)} = A_j^{(1)} (j = 1, 2; i = 2, ..., N)$. In such a situation, if we find a Bell inequality that is violated by the reduced state, it immediately implies that all inequalities under consideration are violated. This does not necessarily exclude correlation trade-offs, but it clearly rules out monogamy.

Polygamy of Mermin inequalities ($N \geq 5$). Let us now use this framework to show that the violation of multi-particle Mermin inequalities is polygamous. Let each of the N observers simultaneously measure a Mermin parameter $\mathcal{M}_{N-1}$ [40] involving $N-1$ parties. Correspondingly, there are N such parameters. The violation of all N $(N-1)$-qubit Mermin inequalities is the highest for the state $|\psi_{\max}\rangle = \frac{1}{\sqrt{2}}(|D_N^1\rangle + |1...1\rangle)$ and achieves the value equal to

$$\mathcal{M}_{N-1}^{\max} = \frac{2^{(N-2)/2}}{\sqrt{N}}. \quad (2)$$

Note that for $N = 3$ and $N = 4$ our result is consistent with [21] and [29], and we do not observe simultaneous violation of the Mermin inequalities. However, already from $N = 5$ onwards such a violation is possible and it increases exponentially with the number of qubits. Remarkably, in the limit of many particles, not only is there no monogamy of violations, but in fact every inequality is violated maximally.

Polygamy for four parties ($N = 4$). As shown in the previous section, it is not possible to violate all four three-qubit Mermin inequalities for observers (ABC, ABD, ACD, BCD) in a four-party system (A,B,C,D), where for simplicity $A^{(1)} \equiv A, A^{(2)} \equiv B$, etc. However, it is possible to find another set of two-setting Bell inequalities that have this feature.

Using an original method based on linear programming we found a three-qubit inequality $\langle I_{ABC}\rangle \leq 6$, where

$$\begin{aligned} I_{ABC} &= 2\ \mathrm{sym}[A_1] - \mathrm{sym}[A_1B_1] - \mathrm{sym}[A_1B_2] \quad (3)\\ &+ \mathrm{sym}[A_2B_2] + 2A_1B_1C_1 + \mathrm{sym}[A_2B_1C_1]\\ &- 2\ \mathrm{sym}[A_2B_2C_1] - A_2B_2C_2. \end{aligned}$$

We use here a compact notation for symmetrising over different observers

$$\mathrm{sym}[A_kB_lC_m] = \sum_{\pi(k,l,m)} A_kB_lC_m, \quad (4)$$

where the sum is over all permutations of (k, l, m), denoted as $\pi(k, l, m)$, assuming $A_0 = B_0 = C_0 = 1$, e.g., $\mathrm{sym}[A_1B_1] = A_1B_1 + A_1C_1 + B_1C_1$ being the permutations of $k = 1, l = 1, m = 0$. Analogous expressions can be formulated for I_{ABD}, I_{ACD}, I_{BCD} inequalities. It can be directly verified that all of them are simultaneously violated by the four-qubit state of the form $|\psi\rangle = \cos\theta|D_4^1\rangle + \sin\theta|1111\rangle$. The maximal violation of $6.154 > 6$ is observed for $\theta = 0.144$, and observables lying in the xz plane. We emphasise the relative simplicity, as every observer measures the same set of two observables. The above example shows that, already for a system of four particles, one can define inequalities involving three observers such that all of them are simultaneously violated.

Polygamy with two-body correlators. The violation of monogamy is by no means limited to the case of higher-order correlations. Here we focus on a minimalist scenario based on the measurements between each pair of observers. Again, we approach this problem through the linear programming technique described in Methods. As a result, the $(N-1)$-partite two-body Bell inequality was found to be $\langle I_{N-1}\rangle \geq 0$. The corresponding Bell operator is given as

$$\begin{aligned} I_{N-1} &= L + \alpha\,(\mathrm{sym}[A_1] + \mathrm{sym}[A_2]) \quad (5)\\ &+ \mathrm{sym}[A_1B_1] + 4\ \mathrm{sym}[A_1B_2] + \mathrm{sym}[A_2B_2], \end{aligned}$$

where L and α are defined by $L = 3((N-4)^2 + N - 2)$ and $\alpha = -3(N-4)$, respectively.

To determine the violation of (5) one has to minimize the Bell expression in (5) for the $(N-1)$-partite reduced state of some N-partite symmetric state, e.g., $|D_N^1\rangle$, using observables in the xz plane. By substituting $N = 18$ and plugging in the optimal observables we obtain

$$\langle I_{A_1A_2}\rangle_{\rho_2} = -\frac{4}{99}. \quad (6)$$

Therefore, the two-body Bell inequality (5) is clearly violated. This implies that the 18-qubit state $|D_{18}^1\rangle$ can simultaneously violate all 17-qubit two-body Bell inequalities and thus the monogamy principle does not hold. Note that here any exchange of information happens only between the pairs of observers.

Experimental demonstration of Bell polygamy. Although the polygamous character of Bell inequality violations is already present in four-qubit systems, an experimental demonstration of such phenomena would require an experiment with very low experimental errors. For this reason, we construct five-party inequalities for $N = 6$ observers with far less demanding visibility requirement and demonstrate in an optical experiment that they are violated in all six five-party subsystems. Again, by the linear programming method used before we arrive at the five-qubit inequality $\langle I_{ABCDE}\rangle \leq 6$ with

$$\begin{aligned} I_{ABCDE} &= -\,\mathrm{sym}[A_1B_1] - \mathrm{sym}[A_2B_2] \quad (7)\\ &+ \mathrm{sym}[A_1B_1C_1D_1] + \mathrm{sym}[A_1B_1C_1D_2]\\ &- \mathrm{sym}[A_1B_2C_2D_2] + \mathrm{sym}[A_2B_2C_2D_2]. \end{aligned}$$

It is worth noting that although these inequalities are defined for five qubits (they constitute the facet of a five-party Bell-Pitovsky polytope), they do not involve five-qubit correlations.

We experimentally demonstrate the existence of polygamous Bell-type correlations using five-party subsystems of a six-qubit Dicke state $|D_6^3\rangle$ prepared with polarisation entangled photons. A detailed description of the experimental setup can be found in Refs. [41, 42]. All six five-party Bell inequalities are simultaneously violated (see Table 1) by at least one standard deviation using the same settings. The observed average violation is $37.5787/6 > 6$.

Table 1: Experimental polygamy of nonlocality. Simultaneous violation of all six five-party Bell inequalities (7), with the local realistic bound of 6, where each observer measures the same settings in the xz plane. All inequalities are violated by at least one standard deviation.

Partition	Violation	Std. dev.
ABCDE	6.315	0.133
ABCDF	6.204	0.131
ABCEF	6.479	0.137
ABDEF	6.307	0.137
ACDEF	6.146	0.125
BCDEF	6.128	0.128

Figure 2 shows how the violation depends on the choice of measurement settings (the same for every observer) both for the theoretical prediction as well as for the experimentally prepared and measured state. A small, yet clearly visible, region of settings shows where the simultaneous violation of all inequalities is indeed possible.

The full manuscript is available at `https://arxiv.org/abs/2312.04373`.

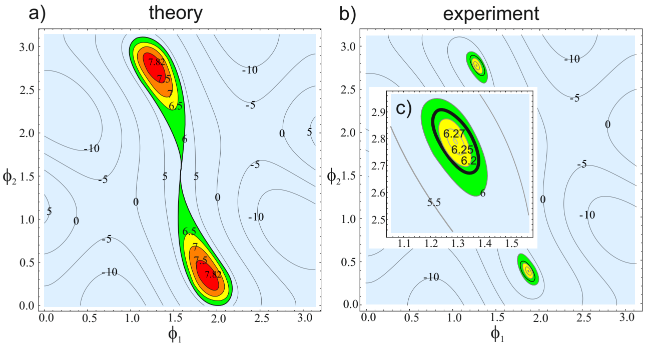


Figure 2: The average violation of inequalities (7) plotted as a function of measurement angles α and β. Panel *a*) shows the theoretical predictions arising from calculating the violation of inequalities using ideal state. Due to the symmetry of the six-qubit Dicke state, the average violation is equivalent to the violation obtained by any set of five parties. The average violation of all inequalities based on the experimental data is presented in panel *b*). Despite the apparent symmetry, due to the imperfections and statistics, not all inequalities are simultaneously violated in the coloured region. It is the area inside the bold line in panel *c*) where all six inequalities are violated simultaneously.

References

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[2] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.*, 1(3):195–200, 1964.

[3] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 1982.

[4] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043,1998.

[5] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409(6822):791–794, 2001.

[6] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. *Nature*, 403(6769):515–519, 2000.

[7] P. Walther, M. Aspelmeyer, K. J. Resch, and A. Zeilinger. Experimental violation of a cluster state Bell inequality. *Phys. Rev. Lett.*, 95:020403, 2005.

[8] B. Hensen, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[9] M. Giustina, et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115(25), 2015.

[10] L. K. Shalm, et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115(25), 2015.

[11] W. Rosenfeld, et. al. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.*, 119(1), 2017.

[12] D. Rauch, et. al. Cosmic Bell test using random measurement settings from high-redshift quasars. *Phys. Rev. Lett.*, 121(8), 2018.

[13] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[14] D. Mayers and A. Chi-Chih Yao. Self testing quantum apparatus. *Quantum Inf. Comput.*, 4:273–286, 2003.

[15] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, 2005.

[16] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[17] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, 2010.

[18] N. Brunner, et. al. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, 2014.

[19] I. Šupić and J. Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, 2020.

[20] V. Scarani and N. Gisin. Quantum communication between N partners and Bell's inequalities. *Phys. Rev. Lett.*, 87:117901, 2001.

[21] B. Toner and F. Verstraete. Monogamy of Bell correlations and Tsirelson's bound. Preprint at https://arxiv.org/abs/quant-ph/0611001, 2006.

[22] B. Toner. Monogamy of non-local quantum correlations. *Proc.R.Soc.A*, 465(2101):59–69, 2009.

[23] B. F. Toner. *Quantifying quantum nonlocality.* PhD thesis, California Institute of Technology, 2007.

[24] D. Collins and N. Gisin. A relevant two qubit Bell inequality inequivalent to the CHSH inequality. *J. Phys. A*, 37(5):1775, 2004.

[25] J. Barrett, A. Kent, and S. Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, 97:170409, 2006.

[26] M. Seevinck. Classification and monogamy of three-qubit biseparable Bell correlations. *Phys. Rev. A*, 76:012106, 2007.

[27] M. Pawłowski and C. Brukner. Monogamy of Bell's inequality violations in nonsignaling theories. *Phys. Rev. Lett.*, 102:030403, 2009.

[28] M. Pawłowski. Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations. *Phys. Rev. A*, 82:032313, 2010.

[29] P. Kurzyński, T. Paterek, R. Ramanathan, W. Laskowski, and D. Kaszlikowski. Correlation complementarity yields Bell monogamy relations. *Phys. Rev. Lett.*, 106:180402, 2011.

[30] L. Aolita, R. Gallego, A. Cabello, and A. Acín. Fully nonlocal, monogamous, and random genuinely multipartite quantum correlations. *Phys. Rev. Lett.*, 108:100401, 2012.

[31] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, and A. Acín. Elemental and tight monogamy relations in nonsignaling theories. *Phys. Rev. A*, 90:052323, 2014.

[32] R. Ramanathan and P. Horodecki. Strong monogamies of no-signaling violations for bipartite correlation Bell inequalities. *Phys. Rev. Lett.*, 113:210403, 2014.

[33] M. C. Tran, R. Ramanathan, M. McKague, D. Kaszlikowski, and T. Paterek. Bell monogamy relations in arbitrary qubit networks. *Phys. Rev. A*, 98:052325, 2018.

[34] R. Augusiak. Simple and tight monogamy relations for a class of Bell inequalities. *Phys. Rev. A*, 95:012113, 2017.

[35] M. Wieśniak. Symmetrized persistency of Bell correlations for Dicke states and GHZ-based mixtures: studying the limits of monogamy, 2021. Preprint at https://arxiv.org/abs/2102.08141.

[36] R. Silva, N. Gisin, Y. Guryanova, and S. Popescu. Multiple observers can share the nonlocality of half of an entangled pair by using optimal weak measurements. *Phys. Rev. Lett.*, 114:250401, 2015.

[37] S. Cheng, L. Liu, T. J. Baker, and M. J. W. Hall. Limitations on sharing Bell nonlocality between sequential pairs of observers. *Phys. Rev. A*, 104:L060201, 2021.

[38] S. Sundar M. and A. K. Pan. Sharing nonlocality in a quantum network by unbounded sequential observers. *Phys. Rev. A*, 106:042218, 2022.

[39] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[40] N. D. Mermin Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838-1840, 1991.

[41] W. Wieczorek, et. al. Experimental entanglement of a six-photon symmetric dicke state. *Phys. Rev. Lett.*, 103:020504, 2009.

[42] R. Krischek, et. al. Ultraviolet enhancement cavity for ultrafast nonlinear optics and high-rate multiphoton entanglement experiments. *Nat. Photonics*, 4(3):170–173, 2010.

Postselected quantum Shannon theory

Kaiyuan Ji[1] * Bartosz Regula[2] † Ludovico Lami[3] [4] ‡ Mark M. Wilde[1] §

[1] *School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA*
[2] *Mathematical Quantum Information RIKEN Hakubi Research Team, RIKEN Cluster for Pioneering Research (CPR) and RIKEN Center for Quantum Computing (RQC), Wako, Saitama 351-0198, Japan*
[3] *QuSoft, Science Park 123, 1098 XG Amsterdam, the Netherlands*
[4] *Korteweg–de Vries Institute for Mathematics and Institute for Theoretical Physics, University of Amsterdam, Amsterdam, the Netherlands*

Abstract. The characterisation of rates of quantum information-theoretic tasks underlies the efficient use of quantum systems in information processing. Such tasks typically rely on the involved parties making a measurement and attempting to distinguish different states or communicated messages. Here we investigate a modified setting in which the parties are allowed an additional 'inconlusive' measurement outcome, which indicates that they do not make a guess, and the error probabilities are conditioned on conclusive attempts only. Such a scenario is equivalent to quantum information processing assisted by the resource of *postselection.*

We completely characterise two of the most important quantum information-theoretic tasks — quantum hypothesis testing and entanglement-assisted communication over quantum channels — in the postselected setting, giving exact solutions already in the single-shot cases and establishing computable, single-letter expressions for the asymptotic rates. Notably, we show that postselection considerably simplifies the framework of quantum information theory, resulting in markedly simplified solutions and properties. We prove in particular that the asymptotic error exponent of discriminating any two quantum states ρ and σ is given by the Hilbert projective metric $D_{\max}(\rho\|\sigma)+D_{\max}(\sigma\|\rho)$ in asymmetric hypothesis testing, and by the Thompson metric $\max\{D_{\max}(\rho\|\sigma), D_{\max}(\sigma\|\rho)\}$ in symmetric hypothesis testing. This endows these two quantities with fundamental operational interpretations in quantum state discrimination. Similarly, we show that the entanglement- and nonsignalling-assisted capacities of quantum channels are given by a variant of mutual information based on the Hilbert projective metric. Our hypothesis testing results extend to very general settings of composite hypotheses and channel discrimination, allowing for solutions to be obtained even in cases where the rates are not known in conventional quantum Shannon theory. Our achievability bounds for communication make use of a novel postselected teleportation-based protocol.

We thus obtain fundamental limits on the performance of quantum information processing even under the powerful resource of postselection. Joint submission of arXiv:2209.10550 and arXiv:2308.02583.

Keywords: Postselection; hypothesis testing; quantum state discrimination; quantum channel discrimination; entanglement-assisted communication; quantum channel capacity.

1 Background

The main aim of quantum information science is to understand how quantum physical resources can be used to enhance our ability to manipulate and transmit information. This study has been particularly fruitful in delineating the ultimate limits of such advantages: for instance, the standard approach of quantum Shannon theory is to study asymptotic transformation rates, which describe the limit where one has access to an unbounded number of quantum state or channel uses. Although idealised, such limits led to a substantial simplification of the evaluation of many operational quantities, while at the same time precisely characterising the extent of advantages that quantum resources can provide even under permissive assumptions. They have thus formed the foundation of quantum communication theory and are the bedrock of our understanding of quantum information processing. It was further realised that providing additional resources — for instance, allowing two communicating parties to share quantum entanglement [1, 2, 3] — not only can significantly enhance our ability to perform quantum information processing tasks, but also, again, drastically simplify the computation of the operational quantities, overcoming problems such as the (in)famous nonadditivity [4, 5] and superactivation [6, 7] phenomena which hinder the evaluation of quantum channel capacities.

It thus becomes a fundamental problem to understand two aspects of this question: on the one hand, how allowing additional resources can enhance quantum information processing, and on the other, how it can simplify the complex mathematical problems underlying its operational characterisation.

2 Summary

To gain insight into the limits of quantum advantages in communication and information processing, here we initiate the study of quantum Shannon theory enhanced by the resource of *postselection.* In its basic form, it simply corresponds to a situation where a party in a given task is allowed an additional 'inconclusive' measurement outcome — representing, for example, situations in which a given process does not conclusively distinguish between some states in consideration, resulting in no guess being made. Crucially, we only consider results conditioned on a conclusive outcome — that is, postselected — and do

*kj264@cornell.edu
†bartosz.regula@gmail.com
‡ludovico.lami@gmail.com
§wilde@cornell.edu

not penalise the parties for an inconclusive result.

Focusing on the tasks of quantum hypothesis testing as well as communication over quantum channels assisted by shared correlations, our main finding is the **exact evaluation of the optimal performance of these tasks in all relevant settings**. In particular: we obtain not only asymptotic results but also tightly characterise the one-shot and many-copy performance of the tasks; we characterise hypothesis testing error probabilities in both symmetric and asymmetric discrimination settings, for both quantum states and channels; we evaluate quantum channel capacities, both quantum and classical, in both one-shot and asymptotic cases, assisted by both entanglement and nonsignalling resources. The framework is shown to enjoy **remarkably simplified properties** compared to conventional quantum Shannon theory, allowing us to give **closed-form, single-letter, SDP-computable expressions for all considered quantities**. Our methods extend even to settings where results in conventional Shannon theory are not known: for instance, composite hypothesis testing, strong converse channel discrimination rates, or an exact one-shot characterisation of entanglement-assisted channel capacities and their equivalence with nonsignalling-assisted ones. Here we focus in particular on applications to communication, discussing achievable protocols in detail and devising a postselected teleportation-based coding scheme.

The price to pay in our approach is the need to allow one communicating party arbitrary access to postselection. Such a concession is known to significantly enhance the power of quantum mechanics in many contexts such as computation and metrology [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19], even being equivalent to having access to postselected closed timelike curves [20, 21, 22]. However, due to the remarkable simplifications that follow, postselection can be very useful in understanding the ultimate power of quantum information processing, and it has already found use, e.g., as the conceptual foundation of the hardness arguments that underlie quantum supremacy experiments [23]. In a similar manner, we hope that our results can find use both in the formalisation of the foundations of quantum theory, as well as in the study of the limits of practical information processing protocols even in permissive settings.

3 Framework

Postselected hypothesis testing. Given a state that is promised to be either ρ or σ, the experimenter's goal is to guess which one the state actually is, with an additional option of making no guess. In this situation, the experimenter's strategy can in general be described by a three-outcome measurement $\{P, Q, \mathbb{1} - P - Q\}$, such that the first two outcomes correspond to guessing ρ and guessing σ, respectively, and the last outcome corresponds to being inconclusive. In the asymmetric setting, no prior probabilities of ρ or σ are assumed. The postselected type I error probability (for mistaking ρ as σ) is given by $\mathrm{Tr}[Q\rho]/\mathrm{Tr}[(P+Q)\rho]$, and the postselected type II error probability (for mistaking σ as ρ) is given by $\mathrm{Tr}[P\sigma]/\mathrm{Tr}[(P+Q)\sigma]$. The optimal type II error with constraints on the type I error is represented by the *postselected ε-hypothesis testing relative entropy*:

$$D^{\varepsilon}_{\mathrm{pH}}(\rho\|\sigma) :=$$
$$-\log_2 \inf_{P,Q\geq 0}\left\{\frac{\mathrm{Tr}[P\sigma]}{\mathrm{Tr}[(P+Q)\sigma]} : \frac{\mathrm{Tr}[Q\rho]}{\mathrm{Tr}[(P+Q)\rho]} \leq \varepsilon,\ P+Q \leq \mathbb{1}\right\}.$$

In the symmetric setting, the prior probabilities of ρ and σ are known to be p and $q \equiv 1-p$, respectively. Then the minimum postselected error probability is given by $\overline{p}_{\mathrm{err}}(\rho,\sigma|p,q) := \inf_{P,Q\geq 0}\left\{\frac{p\mathrm{Tr}[Q\rho]+q\mathrm{Tr}[P\sigma]}{\mathrm{Tr}[(P+Q)(p\rho+q\sigma)]} : P+Q\leq\mathbb{1}\right\}.$

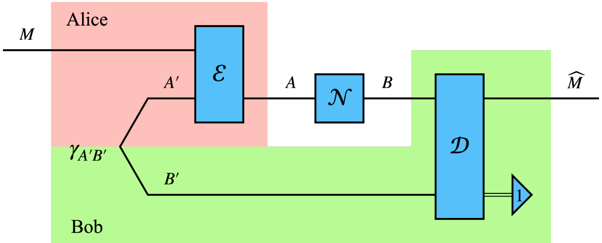


Figure 1: *Postselected entanglement-assisted (pEA) communication.*

Postselected entanglement-assisted (pEA) communication. In pEA communication, Alice (the sender) and Bob (the receiver) aim at transmitting a quantum or classical message from her system M to his system $\widehat{M} \cong M$ through a given quantum channel $\mathcal{N}_{A\to B}$. See Fig. 1. As in conventional entanglement-assisted communication [1, 24, 25], they are allowed to share an unbounded amount of entanglement to assist the transmission. What differs from the conventional setting is that we now assume that Bob's decoding operation has the additional option of being inconclusive about the message being transmitted. The postselected error probability of the transmission is then defined to be conditioned on him being conclusive. We define the *one-shot ε-error postselected entanglement-assisted (pEA) quantum capacity* and the *asymptotic pEA quantum capacity* of the channel $\mathcal{N}_{A\to B}$, respectively, as

$$Q^{\varepsilon}_{\mathrm{pEA}}(\mathcal{N}) := \sup_{\Theta\in\mathrm{pEA}} \left\{\log_2 d_M : P_{\mathrm{err}}(\Theta;\mathcal{N}) \leq \varepsilon\right\},$$
$$Q_{\mathrm{pEA}}(\mathcal{N}) := \inf_{\varepsilon\in(0,1)} \liminf_{n\to\infty} \frac{1}{n} Q^{\varepsilon}_{\mathrm{pEA}}(\mathcal{N}^{\otimes n}),$$

where, in the first equation, d_M is the dimensionality of the system M, $P_{\mathrm{err}}(\Theta;\mathcal{N})$ is the worst-case postselected error probability with respect to a protocol Θ over the channel $\mathcal{N}$, and the supremum is over all pEA protocols. If we only consider transmission of classical messages (i.e., if M is classical), the capacities similarly defined are called the *one-shot* and *asymptotic pEA classical capacities*, denoted by $C^{\varepsilon}_{\mathrm{pEA}}(\mathcal{N})$ and $C_{\mathrm{pEA}}(\mathcal{N})$, respectively.

Postselected nonsignalling-assisted (pNA) communication. The only difference with pEA communication is that now Alice and Bob can be assisted by general nonsignalling correlations, which is a broader class of correlations than shared entanglement. The resulting one-shot quantum and classical capacities are denoted by $Q^{\varepsilon}_{\mathrm{pNA}}(\mathcal{N})$ and $C^{\varepsilon}_{\mathrm{pNA}}(\mathcal{N})$, and the resulting asymptotic quantum and classical capacities are denoted by $Q_{\mathrm{pNA}}(\mathcal{N})$ and $C_{\mathrm{pNA}}(\mathcal{N})$. Nonsignalling-assisted communication was studied in the conventional (non-postselected) framework in [26, 27, 28].

4 Results

Our results are expressed in terms of the following information-theoretic measures. Denoting the max-relative entropy [29] between two states ρ and σ by $D_{\max}(\rho\|\sigma)$, the *Hilbert projective metric* [30, 17] between ρ and σ is defined as $D_\Omega(\rho\|\sigma) := D_{\max}(\rho\|\sigma) + D_{\max}(\sigma\|\rho)$, and the *Thompson metric* [31] between ρ and σ is defined as $D_\Xi(\rho\|\sigma) := \max\{D_{\max}(\rho\|\sigma), D_{\max}(\sigma\|\rho)\}$. We define the *projective mutual information* of a channel $\mathcal{N}_{A\to B}$ as

$$I_\Omega(\mathcal{N}) := \sup_{\rho_{RA}} I_\Omega(R;B)_{\mathcal{N}_{A\to B}[\rho_{RA}]},$$

where $I_\Omega(R;B)_{\omega_{RB}} := \inf_{\sigma_B} D_\Omega(\omega_{RB}\|\omega_R \otimes \sigma_B)$ is a variant of the mutual information of a bipartite state ω_{RB} derived from the Hilbert projective metric. We note that all the above measures can be evaluated using semidefinite programs (SDPs).

Postselected hypothesis testing. In the asymmetric setting, we show that the error exponent in postselected hypothesis testing can be precisely characterised in terms of the Hilbert projective metric:

$$D^\varepsilon_{\mathrm{pH}}(\rho\|\sigma) = \log_2\left(\tfrac{\varepsilon}{1-\varepsilon}2^{D_\Omega(\rho\|\sigma)} + 1\right) \quad \forall \varepsilon \in (0,1). \quad (1)$$

By the additivity of $D_\Omega(\rho\|\sigma)$, the one-shot characterisation readily gives rise to the counterpart of quantum Stein's lemma [32, 33] in the postselected framework: $\lim_{n\to\infty} \frac{1}{n} D^\varepsilon_{\mathrm{pH}}(\rho^{\otimes n}\|\sigma^{\otimes n}) = D_\Omega(\rho\|\sigma)$ $\forall \varepsilon \in (0,1)$. In the symmetric setting, we show that the minimum postselected error probability is precisely characterised by the Thompson metric: $\overline{p}_{\mathrm{err}}(\rho,\sigma|p,q) = (2^{D_\Xi(\rho\|\sigma)} + 1)^{-1}$. This helps establish the counterpart of the quantum Chernoff bound [34, 35] in the postselected framework: $\lim_{n\to\infty} -\frac{1}{n}\log_2 \overline{p}_{\mathrm{err}}(\rho^{\otimes n}, \sigma^{\otimes n}|p,q) = D_\Xi(\rho\|\sigma)$ $\forall p \equiv 1-q \in (0,1)$. These results in particular endow D_Ω and D_Ξ with explicit operational meanings in state discrimination.

It is noteworthy that in both the asymmetric and symmetric settings of postselected hypothesis testing, the one-shot results imply that the multi-shot postselected error probabilities contain no terms of order lower than linear in n, which strongly contrasts with the situation encountered in the conventional framework [36, 37].

Furthermore, all our results for postselected hypothesis testing are straightforwardly extended to more general settings such as composite hypothesis testing and strong converse channel hypothesis testing, contrasting with the extraordinary complications of similar settings in the conventional framework [38, 39, 40, 41, 42, 43, 44, 45]. In the discrimination of channels, we show in particular that parallel protocols are always optimal: both in non-asymptotic and asymptotic channel discrimination, no advantage can be gained by using adaptive or even more general discrimination schemes, such as those involving indefinite causal order.

Postselected entanglement & nonsignalling-assisted (pEA & pNA) communication. Our main results are tight upper and lower bounds on the one-shot ε-error quantum and classical capacities of any channel $\mathcal{N}_{A\to B}$ in both the pEA and pNA scenarios. Our bounds show that all these capacities are approximately characterised by an analytical expression in terms of the postselected error probability ε and the channel's projective mutual information $I_\Omega(\mathcal{N})$:

$$\begin{aligned} C^\varepsilon_{\mathrm{pEA}}(\mathcal{N}) &\approx C^\varepsilon_{\mathrm{pNA}}(\mathcal{N}) \approx 2Q^\varepsilon_{\mathrm{pEA}}(\mathcal{N}) \approx 2Q^\varepsilon_{\mathrm{pNA}}(\mathcal{N}) \\ &\approx \log_2\left(\tfrac{\varepsilon}{1-\varepsilon}2^{I_\Omega(\mathcal{N})} + 1\right) \quad \forall \varepsilon \in (0,1). \end{aligned} \quad (2)$$

Our proof technique is sketched as follows. First of all, we propose a postselected entanglement-assisted coding scheme based on probabilistic teleportation, and this constructively proves the lower bound on $Q^\varepsilon_{\mathrm{pEA}}(\mathcal{N})$. Diverging from typical coding schemes in the conventional framework, the postselected teleportation-based coding follows the idea of (1) teleporting the message entirely through the shared entangled systems and (2) encoding the classical information of whether the teleportation succeeded into the input system A of the channel $\mathcal{N}$. As Bob decodes this classical information, he would gain insight into whether the message was teleported successfully, and he makes a guess about the message only if he believes there was a success. We then prove a non-trivial connection between the optimal performance of this scheme and $I_\Omega(\mathcal{N})$. For the converse direction, we establish an upper bound on $C^\varepsilon_{\mathrm{pNA}}(\mathcal{N})$ based on the postselected hypothesis testing relative entropy, which, by invoking Eq. (1), is given by the rightmost terms in Eq. (2). By linking the one-shot quantum and classical capacities via superdense coding, we observe that the derived upper and lower bounds match, resulting in Eq. (2).

We then prove that the projective mutual information of channels is additive, using which our one-shot results give rise to a single-letter characterisation of the asymptotic capacities in both the pEA and pNA scenarios:

$$C_{\mathrm{pEA}}(\mathcal{N}) = C_{\mathrm{pNA}}(\mathcal{N}) = 2Q_{\mathrm{pEA}}(\mathcal{N}) = 2Q_{\mathrm{pNA}}(\mathcal{N}) = I_\Omega(\mathcal{N}).$$

The simplicity of our asymptotic results parallels that of Shannon's celebrated noisy-channel coding theorem for classical channels [46] and the entanglement-assisted capacity theorem for quantum channels in the conventional framework [1, 24], but the postselected results enjoy significantly simpler proofs. Furthermore, we find that the strong converses of all the capacities above are the same as the capacities themselves, and that feedback assistance does not provide any additional advantage in both the asymptotic and non-asymptotic regimes. Analogies of such findings are known for both classical channels [47, 48] and quantum channels in the conventional framework [2, 49, 50, 51, 52, 53], although they were much more difficult to establish there. In addition, the optimum rates of pEA and pNA communication feature only the capacity term and another $O(\frac{1}{n})$ term, which echoes the same property in postselected hypothesis testing and contrasts with the non-trivial second-order asymptotics in the conventional framework [54].

References

[1] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48:2637–2655, 2002.

[2] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter. The Quantum Reverse Shannon Theorem and Resource Tradeoffs for Simulating Quantum Channels. *IEEE Transactions on Information Theory*, 60:2926–2959, 2014.

[3] Mario Berta, Matthias Christandl, and Renato Renner. The Quantum Reverse Shannon Theorem Based on One-Shot Information Theory. *Communications in Mathematical Physics*, 306:579, 2011.

[4] P. W. Shor. The additivity conjecture in quantum information theory. *Current Developments in Mathematics*, 2005:173–190, 2005.

[5] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5:255–257, 2009.

[6] Graeme Smith and Jon Yard. Quantum communication with zero-capacity channels. *Science*, 321(5897):1812–1815, September 2008. arXiv:0807.4935.

[7] Graeme Smith, John A. Smolin, and Jon Yard. Quantum communication with Gaussian channels of zero quantum capacity. *Nature Photonics*, 5:624–627, 2011.

[8] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A*, 461:3473–3482, 2005.

[9] Jaromír Fiurášek. Optimal probabilistic estimation of quantum states. *New Journal of Physics*, 8:192–192, 2006.

[10] Bernat Gendra, Elio Ronco-Bonvehi, John Calsamiglia, Ramon Muñoz-Tapia, and Emilio Bagan. Beating noise with abstention in state estimation. *New Journal of Physics*, 14:105015, 2012.

[11] Joshua Combes, Christopher Ferrie, Zhang Jiang, and Carlton M. Caves. Quantum limits on postselected, probabilistic quantum metrology. *Physical Review A*, 89:052117, 2014.

[12] Joshua Combes and Christopher Ferrie. Cost of postselection in decision theory. *Physical Review A*, 92:022117, 2015.

[13] David R. M. Arvidsson-Shukur, Nicole Yunger Halpern, Hugo V. Lepage, Aleksander A. Lasek, Crispin H. W. Barnes, and Seth Lloyd. Quantum advantage in postselected metrology. *Nature Communications*, 11:3775, 2020.

[14] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Physics Letters A*, 210:151–156, 1996.

[15] Adrian Kent. Entangled Mixed States and Local Purification. *Physical Review Letters*, 81:2839–2841, 1998.

[16] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60:1888–1898, 1999.

[17] David Reeb, Michael J. Kastoryano, and Michael M. Wolf. Hilbert's projective metric in quantum information theory. *Journal of Mathematical Physics*, 52:082201, 2011.

[18] Bartosz Regula. Probabilistic Transformations of Quantum Resources. *Physical Review Letters*, 128:110505, 2022.

[19] Bartosz Regula. Tight constraints on probabilistic convertibility of quantum states. *Quantum*, 6:817, 2022.

[20] Seth Lloyd, Lorenzo Maccone, Raul Garcia-Patron, Vittorio Giovannetti, Yutaka Shikano, Stefano Pirandola, Lee A. Rozema, Ardavan Darabi, Yasaman Soudagar, Lynden K. Shalm, and Aephraim M. Steinberg. Closed Timelike Curves via Postselection: Theory and Experimental Test of Consistency. *Physical Review Letters*, 106:040403, 2011.

[21] Seth Lloyd, Lorenzo Maccone, Raul Garcia-Patron, Vittorio Giovannetti, and Yutaka Shikano. Quantum mechanics of time travel through post-selected teleportation. *Physical Review D*, 84(2):025007, July 2011.

[22] Todd A. Brun and Mark M. Wilde. Perfect State Distinguishability and Computational Speedups with Postselected Closed Timelike Curves. *Foundations of Physics*, 42:341–361, 2012.

[23] Aram W. Harrow and Ashley Montanaro. Quantum computational supremacy. *Nature*, 549:203–209, 2017.

[24] A. S. Holevo. On entanglement-assisted classical capacity. *Journal of Mathematical Physics*, 43(9):4326–4333, August 2002.

[25] N. Datta and M. H. Hsieh. One-Shot Entanglement-Assisted Quantum and Classical Communication. *IEEE Transactions on Information Theory*, 59:1929–1939, 2013.

[26] Runyao Duan and Andreas Winter. No-Signalling-Assisted Zero-Error Capacity of Quantum Channels and an Information Theoretic Interpretation of the Lovász Number. *IEEE Transactions on Information Theory*, 62:891–914, 2016.

[27] K. Fang, X. Wang, M. Tomamichel, and M. Berta. Quantum Channel Simulation and the Channel's Smooth Max-Information. *IEEE Transactions on Information Theory*, 66:2129–2140, 2020.

[28] Ryuji Takagi, Kun Wang, and Masahito Hayashi. Application of the Resource Theory of Channels to Communication Scenarios. *Physical Review Letters*, 124:120502, 2020.

[29] N. Datta. Min- and Max-Relative Entropies and a New Entanglement Monotone. *IEEE Transactions on Information Theory*, 55:2816–2826, 2009.

[30] P. J. Bushell. Hilbert's metric and positive contraction mappings in a Banach space. *Archive for Rational Mechanics and Analysis*, 52:330–338, 1973.

[31] A. C. Thompson. On certain contraction mappings in a partially ordered vector space. *Proc. Amer. Math. Soc.*, 14:438–443, 1963.

[32] Fumio Hiai and Dénes Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143:99–114, 1991.

[33] T. Ogawa and H. Nagaoka. Strong converse and Stein's lemma in quantum hypothesis testing. *IEEE Transactions on Information Theory*, 46:2428–2433, 2000.

[34] Michael Nussbaum and Arleta Szkoła. The Chernoff lower bound for symmetric quantum hypothesis testing. *Ann. Stat.*, 37:1040–1057, 2009.

[35] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acin, and F. Verstraete. Discriminating States: The Quantum Chernoff Bound. *Physical Review Letters*, 98:160501, 2007.

[36] Ke Li. Second-order asymptotics for quantum hypothesis testing. *Ann. Stat.*, 42:171–189, 2014.

[37] M. Tomamichel and M. Hayashi. A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks. *IEEE Transactions on Information Theory*, 59:7693–7710, 2013.

[38] Fernando G. S. L. Brandão and Martin B. Plenio. A Generalization of Quantum Stein's Lemma. *Communications in Mathematical Physics*, 295:791–828, 2010.

[39] Mario Berta, Fernando G. S. L. Brandão, Gilad Gour, Ludovico Lami, Martin B. Plenio, Bartosz Regula, and Marco Tomamichel. On a gap in the proof of the generalised quantum Stein's lemma and its consequences for the reversibility of quantum resources. *Quantum*, 7:1103, 2023.

[40] Aram W. Harrow, Avinatan Hassidim, Debbie W. Leung, and John Watrous. Adaptive versus nonadaptive strategies for quantum channel discrimination. *Physical Review A*, 81:032339, 2010.

[41] Farzin Salek, Masahito Hayashi, and Andreas Winter. Usefulness of adaptive strategies in asymptotic quantum channel discrimination. *Physical Review A*, 105:022419, 2022.

[42] Nengkun Yu and Li Zhou. When is the Chernoff Exponent for Quantum Operations Finite? *IEEE Transactions on Information Theory*, 67:4517–4523, 2021.

[43] Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, and Benoit Valiron. Quantum computations without definite causal structure. *Physical Review A*, 88:022318, 2013.

[44] Xin Wang and Mark M. Wilde. Resource theory of asymmetric distinguishability for quantum channels. *Phys. Rev. Research*, 1:033169, 2019.

[45] Kun Fang, Omar Fawzi, Renato Renner, and David Sutter. Chain Rule for the Quantum Relative Entropy. *Physical Review Letters*, 124:100501, 2020.

[46] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27:379–423, 1948.

[47] C. E. Shannon. The zero error capacity of a noisy channel. *IRE Transactions on Information Theory*, 2(3):8–19, 1956.

[48] J. Wolfowitz. The coding of messages subject to chance errors. *Illinois Journal of Mathematics*, 1(4):591 – 606, 1957.

[49] Manish K. Gupta and Mark M. Wilde. Multiplicativity of completely bounded p-norms implies a strong converse for entanglement-assisted capacity. *Communications in Mathematical Physics*, 334(2):867–887, October 2014.

[50] Garry Bowen. Quantum feedback channels. *IEEE Transactions on Information Theory*, 50(10):2429–2434, October 2004. arXiv:quant-ph/0209076.

[51] Garry Bowen and Rajagopal Nagarajan. On feedback and the classical capacity of a noisy quantum channel. *IEEE Transactions on Information Theory*, 51:320–324, January 2005.

[52] Dawei Ding and Mark M. Wilde. Strong converse for the feedback-assisted classical capacity of entanglement-breaking channels. *Problems of Information Transmission*, 54:1–19, 2018.

[53] Tom Cooney, Milán Mosonyi, and Mark M. Wilde. Strong Converse Exponents for a Quantum Channel Discrimination Problem and Quantum-Feedback-Assisted Communication. *Communications in Mathematical Physics*, 344:797–829, 2016.

[54] Nilanjana Datta, Marco Tomamichel, and Mark M. Wilde. On the second-order asymptotics for entanglement-assisted communication. *Quantum Information Processing*, 15(6):2569–2591, March 2016.

Optimal protocols for universal adjointation of isometry operations

Satoshi Yoshida[1] * Akihito Soeda[2] [3] [1] Mio Murao[1] [4]

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan*

[2] *Principles of Informatics Research Division, National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

[3] *Department of Informatics, School of Multidisciplinary Sciences, SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

[4] *Trans-scale Quantum Science Institute, The University of Tokyo, Bunkyo-ku, Tokyo 113-0033, Japan*

Abstract. Identification of possible transformations of quantum objects including quantum states and quantum operations is indispensable in developing quantum algorithms. Universal transformations, defined as input-independent transformations, appear in various quantum applications. Such is the case for universal transformations of unitary operations. However, extending these transformations to non-unitary operations is nontrivial and largely unresolved. Addressing this, we introduce *isometry adjointation* protocols that convert an input isometry operation into its adjoint operation, which include both unitary operation and quantum state transformations. The paper details the construction of parallel and sequential isometry adjointation protocols, derived from unitary inversion protocols using quantum combs, and achieving optimal approximation error. This error is shown to be independent of the output dimension of the isometry operation. In particular, we explicitly obtain an asymptotically optimal parallel protocol achieving an approximation error $\epsilon = \Theta(d^2/n)$, where d is the input dimension of the isometry operation and n is the number of calls of the isometry operation. The research also extends to isometry inversion and universal error detection, employing semidefinite programming to assess optimal performances. The findings suggest that the optimal performance of general protocols in isometry adjointation and universal error detection is not dependent on the output dimension, and that indefinite causal order protocols offer advantages over sequential ones in isometry inversion and universal error detection. The full paper of this work is on arXiv [1].

Keywords: Higher-order quantum transformations, Quantum supermaps, Isometry operations, Adjoint operations, Encoding and decoding of quantum information

1 Problem setting and main results

Quantum protocols dealing with unknown quantum states have been extensively studied, such as state cloning [2]. Possibility and impossibility of such protocols have played an important role in implementing cryptographic protocols [3, 4]. Unknown quantum operations are also utilized in various quantum protocols, such as oracle quantum computation [5], unitary property testing [6], and higher-order quantum transformations [7]. In general, it is difficult to utilize unknown quantum states and operations in quantum protocols since we require an extra resource overhead to estimate their description via process tomography [8, 9]. Previous works have invented subroutines to deal with unknown quantum states or unitary operations such as swap test [10], amplitude amplification [11], and transformations of unknown unitary operations [12–19]. However, their extension to general quantum operations are not well investigated. One of the most important class of quantum operations are isometry operations, which represent encoding of quantum information into a higher-dimensional system. Mathematically, they include unitary operations and pure quantum states as special cases, namely, $\mathbb{V}_{\rm iso}(d,D) \simeq \mathbb{U}(d)$ for $D = d$ and $\mathbb{V}_{\rm iso}(d,D) \simeq \mathbb{C}^D$ for $d = 1$ hold, where $\mathbb{V}_{\rm iso}(d,D)$ is the set of isometry operators $V : \mathbb{C}^d \to \mathbb{C}^D$ and $\mathbb{U}(d)$ is the set of d-dimensional unitary operators. In this work, we define the task *isometry adjointation* given as follows.

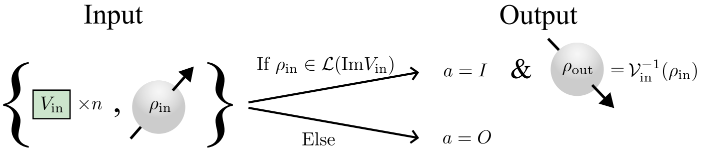

Input
Output
$V_{\rm in}$ $\times n$
$\rho_{\rm in}$
If $\rho_{\rm in} \in \mathcal{L}(\mathrm{Im} V_{\rm in})$
$a = I$
&
$\rho_{\rm out} = \mathcal{V}_{\rm in}^{-1}(\rho_{\rm in})$
Else
$a = O$

Figure 1: Definition of the task isometry adjointation.

Definition 1 (Isometry adjointation)**.** *Given n calls of an unknown isometry operation $V_{\rm in} \in \mathbb{V}_{\rm iso}(d,D)$, the task is to implement a quantum instrument $\{\Phi_I, \Phi_O\}$*[1] *such that Φ_I approximates the adjoint operation $V_{\rm in}^{\dagger}$*[2]*.*

The adjoint operation can be written as $V_{\rm in}^{\dagger}\rho_{\rm in}V_{\rm in} = \mathcal{V}_{\rm in}^{-1}(\Pi_{\mathrm{Im}\, V_{\rm in}}\rho_{\rm in}\Pi_{\mathrm{Im}\, V_{\rm in}})$, where $\mathcal{V}_{\rm in}^{-1}$ is a CPTP map satisfying $\mathcal{V}_{\rm in}^{-1} \circ \mathcal{V}_{\rm in} = \mathbb{1}_d$, and $\Pi_{\mathrm{Im}\, V_{\rm in}}$ is an orthogonal projector onto the image $\mathrm{Im}\, V_{\rm in}$. Thus, an isometry adjointation protocol checks whether the input quantum state is within the subspace $\mathrm{Im}\, V_{\rm in}$ specified by the unknown isometry operation $V_{\rm in}$, and if the input state is in the subspace, it applies the

*satoshiyoshida.phys@gmail.com

[1] The measurement outcomes I and O stand for "in $\mathrm{Im}\, V_{\rm in}$" and "out of $\mathrm{Im}\, V_{\rm in}$", respectively (see also Fig. 1).

[2] We also demand that the one-side error condition $\Phi_O \circ \mathcal{V}_{\rm in} = 0$, i.e., when $\rho_{\rm in} \in \mathcal{L}(\mathrm{Im}\, V_{\rm in})$, we obtain the measurement outcome $a = I$ with a unit probability.

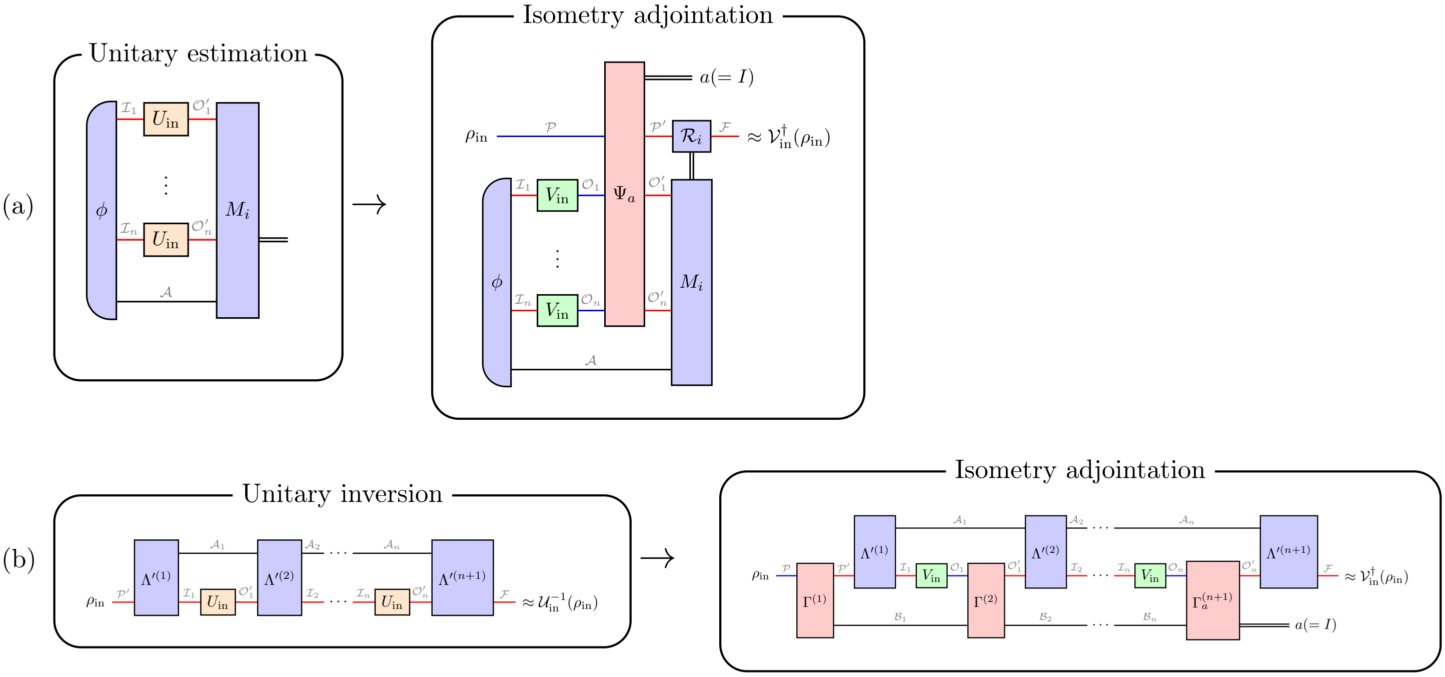


Figure 2: (a) Construction of a parallel isometry adjointation protocol from a covariant unitary estimation protocol. (b) Construction of a sequential isometry adjointation protocol from a unitary inversion protocol.

inverse operation $\mathcal{V}_{\rm in}^{-1}$ on the input state (Fig. 1). This task reduces to unitary inversion [15–19] ($U \in \mathbb{U}(d) \mapsto U^{-1}$) for $D = d$ and swap test [10], or programmable projective measurement [20] ($|\psi\rangle \in \mathbb{C}^D \mapsto \{|\psi\rangle\langle\psi|, \mathbb{1} - |\psi\rangle\langle\psi|\}$) for $d = 1$. We show two ways to construct isometry adjointation protocols, one of which utilizes the input isometry operations in parallel, and the other utilizes them in sequence. The parallel protocol is constructed from a unitary estimation protocol, and the sequential protocol is from a unitary inversion protocol (Fig. 2). Both of them achieve the optimal performances among all parallel or sequential protocols.

Theorem 2. *The parallel or sequential protocols shown in Fig. 2 implement the quantum instrument $\{\Phi_I, \Phi_O\}$ satisfying*

$$\begin{aligned}\Phi_I(\rho_{\rm in}) =&(1-p)V_{\rm in}^\dagger \rho_{\rm in} V_{\rm in}\\ &+ \frac{\mathbb{1}_d}{d}\operatorname{Tr}\{[p\Pi_{\operatorname{Im} V_{\rm in}} + \alpha(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\rm in}})]\rho_{\rm in}\}, \quad (1)\end{aligned}$$

where $p, \alpha \in [0,1]$ are obtained from the original unitary estimation or unitary inversion protocol. The worst-case diamond-distance error is given by $\epsilon = \frac{1}{2}\sup_{V_{\rm in}\in\mathbb{V}_{\rm iso}(d,D)} \|\Phi - \mathcal{V}_{\rm adjoint}\|_\diamond = \max\{\frac{1}{2}(1-d^{-2})p, \alpha\}$, where Φ and $\mathcal{V}_{\rm adjoint}$ are CPTP maps defined by $\Phi := \Phi_I \otimes |0\rangle\langle 0| + \Phi_O \otimes |1\rangle\langle 1|$ and $\mathcal{V}_{\rm adjoint} := \mathcal{V}^\dagger \otimes |0\rangle\langle 0| + \frac{\mathbb{1}_d}{d}\operatorname{Tr}[(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\rm in}})\cdot] \otimes |1\rangle\langle 1|$.

Theorem 3. *For given d, D, n, the protocols shown in Figs. 2 achieve the optimal worst-case diamond-distance error among all parallel or sequential protocols, respectively.*

In particular, p, α in (1) is given in Theorems 5 and 6 of the technical manuscript [1], which do not depend on the output dimension D of the isometry. Thus, we obtain the following Lemma.

Lemma 4. *The optimal approximation error ϵ of parallel or sequential isometry adjoinattion using n calls of the input isometry operation $V_{\rm in} \in \mathbb{V}_{\rm iso}(d, D)$ do not depend on D.*

2 Construction of parallel and sequential isometry adjointation protocols

We construct a quantum instrument $\{\Psi_a : \mathcal{L}(\mathbb{C}^D)^{\otimes n+1} \to \mathcal{L}(\mathbb{C}^d)^{\otimes n+1}\}_{a\in\{I,O\}}$ using the quantum Schur transform [21–24] satisfying the following equation [25]:

$$\begin{aligned}\Psi_I[\mathcal{V}_{\rm in}^{\otimes n}(\phi)\otimes\rho] = &\int_{\mathbb{U}(d)} \mathrm{d}U \mathcal{U}^{\otimes n}(\phi)\otimes(\mathcal{U}\circ\mathcal{V}_{\rm in}^\dagger)(\rho)\\ &+\operatorname{Tr}\left[(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\rm in}}))\rho\right]\Psi_I(\phi), \quad (2)\end{aligned}$$

where $\mathcal{V}_{\rm in}(\cdot) := V_{\rm in}\cdot V_{\rm in}^\dagger$, $\mathcal{U}(\cdot) := U \cdot U^\dagger$, $\mathrm{d}U$ is the Haar measure on $\mathbb{U}(d)$, and Ψ_I is a completely positive trace non-increasing (CPTNI) map. To cancel out $\mathcal{U}$ after $\mathcal{V}_{\rm in}^\dagger$ in (2), a unitary estimation protocol is combined as shown in Fig. 2 (a). The left panel of Fig. 2 (a) shows a parallel protocol for unitary inversion using a unitary estimation protocol. The input unitary operation $U_{\rm in}$ is estimated as $\hat{U}_i$ from the measurement outcome i of a POVM $\{M_i\}$ on the state $\mathcal{U}_{\rm in}^{\otimes n} \otimes \mathbb{1}(\phi)$. The inverse operation $R_i := \hat{U}_i^{-1}$ of the estimated operation is applied to the input quantum state $\rho_{\rm in}$. Assuming that the unitary estimation protocol is covariant, we can show that the quantum circuit shown in the right panel of Fig. 2 (a) implements a quantum operation (1) with $p = \frac{d^2}{d^2-1}(1 - F_{\mathrm{est}})$ and $\alpha = \operatorname{Tr} \Psi_I[\operatorname{Tr}_{\mathcal{A}}(\phi)]$ where F_{est} is the entanglement fidelity of unitary estimation and ϕ is shown in Fig. 2. From covariant unitary estimation protocols presented in Refs. [26–29], we show the isometry adjointation protocol achieving $p = O(d^4/n^2)$, $\alpha = O(d^2/n)$ in (1). Thus, for $n \gg d^2$, this protocol achieves $\epsilon = O(d^2/n)$, and in particular for the case of $d = 2$, this is given by $\epsilon = 6.2287/n + O(n^{-2})$. Therefore, we can achieve an approximation error ϵ by $n = O(d^2/\epsilon)$ calls of the input isometry operation. We also show that this scaling is optimal among all possible parallel protocols, i.e., $\inf_{\text{parallel protocol}} \epsilon = \Theta(d^2/n)$.

From a given sequential unitary inversion protocol, we construct an isometry adjointation protocol as shown in Fig. 2 (b). This construction is done by inserting the set of quantum operations $\Gamma^{(i)}$ (red one) to the unitary inversion protocol composed of $\Lambda'^{(i)}$ (blue one). The sequence of $\Lambda'^{(i)}$ transforms the action of n calls of $\mathcal{V}_{\mathrm{in}}$ to $\mathcal{V}_{\mathrm{in}}^\dagger$ and randomized unitary operation, similarly to (2). We can show that the resulting protocol implements a quantum operation (1) if the original unitary inversion protocol is covariant [25].

Our constructions of isometry adjointation protocols are transformations from the unitary inversion protocols. Since the unitary inversion protocols are transformations of quantum operations, or quantum supermaps [30], such transformations are called quantum supersupermaps. Using the idea of quantum supersupermaps, the problem to design an isometry adjointation protocol reduces to designing a unitary inversion protocol, which is extensively studied in previous works [15–19]. Note that a similar idea is used in Ref. [31], which presents transformation of the function applied on block-encoding unitary operation in quantum singular value transformations.

3 Reduction to isometry inversion, universal error detection, and programmable projective measurement

By discarding the measurement outcome of isometry adjointation protocols in Fig. 2, we can implement *isometry inversion* [32]. Isometry inversion is the task to implement the inverse operation $\mathcal{V}_{\mathrm{in}}^{-1}$ of the input isometry operation $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$, where the inverse operation is defined as a CPTP map such that $\mathcal{V}_{\mathrm{in}}^{-1} \circ \mathcal{V}_{\mathrm{in}} = \mathbb{1}_d$. We can show that the obtained isometry inversion protocol has the approximation error ϵ that is the same as the original unitary inversion protocol. Since d-dimensional unitary inversion with approximation error ϵ can be done using $n = O(\mathrm{poly}(d)\epsilon^{-1/2})$ (parallel) or $n = O(\mathrm{poly}(d) \log \epsilon^{-1})$ calls of the input unitary operation [17], we can construct the isometry inversion protocol with the same number of the input operations. In particular for the case of $d = 2$, our construction with the deterministic exact unitary inversion [19] gives deterministic and exact isometry inversion.

By discarding the output state of isometry adjointation protocols in Fig. 2, we can implement *universal error detection*, which is a task to implement the POVM $\{\Pi_{\operatorname{Im} V_{\mathrm{in}}}, \mathbb{1}_D - \operatorname{Im} V_{\mathrm{in}}\}$ approximately. In particular, it implements the POVM $\{\Pi_{\operatorname{Im} V_{\mathrm{in}}} + \alpha(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\mathrm{in}}}), (1 - \alpha)(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\mathrm{in}}})\}$, where α is given in (1), which quantifies the approximation error of the protocol. The minimal value of α among parallel protocols is explicitly given in Theorem 12 of the technical manuscript [1], which scales as $\inf_{\text{paralell protocol}} \alpha = \Theta(d^2/n)$. The special case $(d = 1)$ of universal error detection reduces to a programmable projective measurement [20], which transforms an input unknown pure state $|\psi_{\mathrm{in}}\rangle \in \mathbb{C}^D$ to the corresponding POVM $\{|\psi_{\mathrm{in}}\rangle\langle\psi_{\mathrm{in}}|, \mathbb{1}_D - |\psi_{\mathrm{in}}\rangle\langle\psi_{\mathrm{in}}|\}$. The optimal approximation error is obtained in Ref. [20], which corresponds to the $d = 1$ case of our explicit expression of α [25].

References

[1] S. Yoshida, A. Soeda, and M. Murao, arXiv:2401.10137 (2024).

[2] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[3] C. H. Bennett and G. Brassard, arXiv:2003.06557 (2020).

[4] S. Wiesner, ACM Sigact News **15**, 78 (1983).

[5] J. Watrous, arXiv:0804.3401 (2008).

[6] A. Montanaro and R. de Wolf, arXiv:1310.2035 (2013).

[7] A. Bisio and P. Perinotti, Proc. R. Soc. A **475**, 20180706 (2019).

[8] I. L. Chuang and M. A. Nielsen, Journal of Modern Optics **44**, 2455 (1997).

[9] C. H. Baldwin, A. Kalev, and I. H. Deutsch, Phys. Rev. A **90**, 012110 (2014).

[10] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[11] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, Contemporary Mathematics **305**, 53 (2002).

[12] J. Miyazaki, A. Soeda, and M. Murao, Phys. Rev. Res. **1**, 013007 (2019).

[13] Q. Dong, S. Nakayama, A. Soeda, and M. Murao, arXiv:1911.01645 (2019).

[14] Q. Dong, M. T. Quintino, A. Soeda, and M. Murao, Phys. Rev. Lett. **126**, 150504 (2021).

[15] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Phys. Rev. A **100**, 062339 (2019).

[16] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Phys. Rev. Lett. **123**, 210502 (2019).

[17] M. T. Quintino and D. Ebler, Quantum **6**, 679 (2022).

[18] M. Navascués, Phys. Rev. X **8**, 031008 (2018).

[19] S. Yoshida, A. Soeda, and M. Murao, Phys. Rev. Lett. **131**, 120602 (2023).

[20] U. Chabaud, E. Diamanti, D. Markham, E. Kashefi, and A. Joux, Phys. Rev. A **98**, 062318 (2018).

[21] D. Bacon, I. L. Chuang, and A. W. Harrow, Phys. Rev. Lett. **97**, 170502 (2006).

[22] H. Krovi, Quantum **3**, 122 (2019).

[23] W. M. Kirby and F. W. Strauch, Quantum Inf. Comput. **18**, 0721 (2018).

[24] A. Wills and S. Strelchuk, arXiv:2305.04069 (2023).

[25] See Technical Manuscript [1] for the detail.

[26] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. A **69**, 050303 (2004).

[27] G. Chiribella, G. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. **93**, 180503 (2004).

[28] G. Chiribella, G. D'Ariano, and M. Sacchi, Phys. Rev. A **72**, 042338 (2005).

[29] Y. Yang, R. Renner, and G. Chiribella, Phys. Rev. Lett. **125**, 210501 (2020).

[30] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Europhys. Lett. **83**, 30004 (2008).

[31] Z. M. Rossi and I. L. Chuang, arXiv:2304.14392 (2023).

[32] S. Yoshida, A. Soeda, and M. Murao, Quantum **7**, 957 (2023).

Universal adjointation of isometry operations using transformation of quantum supermaps

Satoshi Yoshida[1], Akihito Soeda[2,3,1], and Mio Murao[1,4]

[1]Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan

[2]Principles of Informatics Research Division, National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

[3]Department of Informatics, School of Multidisciplinary Sciences, SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

[4]Trans-scale Quantum Science Institute, The University of Tokyo, Bunkyo-ku, Tokyo 113-0033, Japan

Identification of possible transformations of quantum objects including quantum states and quantum operations is indispensable in developing quantum algorithms. Universal transformations, defined as input-independent transformations, appear in various quantum applications. Such is the case for universal transformations of unitary operations. However, extending these transformations to non-unitary operations is nontrivial and largely unresolved. Addressing this, we introduce *isometry adjointation* protocols that convert an input isometry operation into its adjoint operation, which include both unitary operation and quantum state transformations. The paper details the construction of parallel and sequential isometry adjointation protocols, derived from unitary inversion protocols using quantum combs, and achieving optimal approximation error. This error is shown to be independent of the output dimension of the isometry operation. In particular, we explicitly obtain an asymptotically optimal parallel protocol achieving an approximation error $\epsilon = \Theta(d^2/n)$, where d is the input dimension of the isometry operation and n is the number of calls of the isometry operation. The research also extends to isometry inversion and universal error detection, employing semidefinite programming to assess optimal performances. The findings suggest that the optimal performance of general protocols in isometry adjointation and universal error detection is not dependent on the output dimension, and that indefinite causal order protocols offer advantages over sequential ones in isometry inversion and universal error detection.

1 Introduction

The possibility and impossibility of universal transformation of unknown quantum states have played a major role in quantum information and foundations (e.g., state cloning

Satoshi Yoshida: satoshiyoshida.phys@gmail.com

Akihito Soeda: soeda@nii.ac.jp

Mio Murao: murao@phys.s.u-tokyo.ac.jp

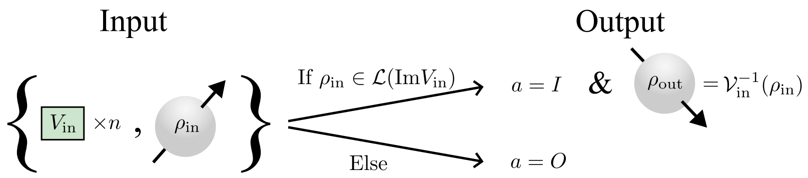

Input
Output
V_{in} $\times n$
ρ_{in}
If $\rho_{\text{in}} \in \mathcal{L}(\text{Im}V_{\text{in}})$
Else
$a = I$
$a = O$
&
ρ_{out} $= \mathcal{V}_{\text{in}}^{-1}(\rho_{\text{in}})$

Figure 1: Definition of the task isometry adjointation.

[1], universal NOT [2], and swap test [3] or programmable projective measurement [4]). Recently, transformations of quantum operations, namely, *quantum supermaps*, have been investigated to aim for *higher-order quantum computataion* [5], which is a candidate for the quantum generalization of higher-order functions [6], as well as its connections to channel resource theory [7], quantum thermodynamics [8], and causal structure [9]. Since universal transformation of quantum operations can be utilized as an elementary operation in higher-order quantum computation, the full characterization of possible universal transformations of quantum operations is indispensable. Although universal transformations of unitary operations have been extensively studied [10–33], their generalization to non-unitary operations have not been well investigated except for a few examples (Ref. [34] for POVM measurements and Ref. [35] for isometry operations). In particular, isometry operations represent encoding of quantum information, and universal transformation of them would be useful as an elementary building block in higher-order quantum computation.

This work extends one of the most important task of universal transformation of unitary operations, called *unitary inversion* [10, 25–33], to isometry operations. Unitary inversion is a task to transform an unknown unitary operation $\mathcal{U}_{\text{in}}$ into its inverse operation $\mathcal{U}_{\text{in}}^{-1}$, where $\mathcal{U}_{\text{in}}$ is given by $\mathcal{U}_{\text{in}}(\cdot) := U_{\text{in}} \cdot U_{\text{in}}^\dagger$ for a unitary operator U_{in}. Since the inverse of a unitary operator U_{in} can be given by the adjoint operator $U_{\text{in}}^\dagger$, one natural extension of unitary inversion to isometry operations is given by *isometry adjointataion*. We consider an isometry operation $\mathcal{V}_{\text{in}}(\cdot) := V_{\text{in}} \cdot V_{\text{in}}^\dagger$, where $V_{\text{in}} : \mathbb{C}^d \to \mathbb{C}^D$ is an isometry operator satisfying $V_{\text{in}}^\dagger V_{\text{in}} = \mathbb{1}_d$ for the identity operator $\mathbb{1}_d$. We denote the set of isometry operators $V_{\text{in}} : \mathbb{C}^d \to \mathbb{C}^D$ by $\mathbb{V}_{\text{iso}}(d, D)$, and the set of d-dimensional unitary operators by $\mathbb{U}(d) = \mathbb{V}_{\text{iso}}(d, d)$. Isometry adjointation is a task to transform an unknown isometry operation $\mathcal{V}_{\text{in}}$ to a quantum instrument $\{\Phi_a\}_{a \in \{I,O\}}$[1] such that Φ_I approximates the adjoint operation $\mathcal{V}_{\text{in}}^\dagger$, where $\mathcal{V}_{\text{in}}^\dagger$ is given by $\mathcal{V}_{\text{in}}^\dagger(\cdot) := V_{\text{in}}^\dagger \cdot V_{\text{in}}$. The adjoint operation $\mathcal{V}_{\text{in}}^\dagger(\cdot)$ is given as

$$\mathcal{V}_{\text{in}}^\dagger(\rho_{\text{in}}) = \mathcal{V}_{\text{in}}^{-1}(\Pi_{\text{Im}V_{\text{in}}} \rho_{\text{in}} \Pi_{\text{Im}V_{\text{in}}}), \tag{1}$$

where $\mathcal{V}_{\text{in}}^{-1}$ is the inverse operation satisfying $\mathcal{V}_{\text{in}}^{-1} \circ \mathcal{V}_{\text{in}}(\rho) = \rho$ for all $\rho \in \mathcal{L}(\mathbb{C}^d)$, and $\Pi_{\text{Im}V_{\text{in}}}$ is the orthogonal projector onto $\text{Im}V_{\text{in}}$. It implements the projective measurement $\{\Pi_{\text{Im}V_{\text{in}}}, \mathbb{1} - \Pi_{\text{Im}V_{\text{in}}}\}$ and the inverse operation $\mathcal{V}_{\text{in}}^{-1}$ at the same time (see Fig. 1). Isometry adjointation can be reduced to two relevant tasks called *isometry inversion* [35] and *universal error detection*, where the former is the task to implement the inverse operation $\mathcal{V}_{\text{in}}^{-1}$, and the latter is the task to implement the projective merasurement $\{\Pi_{\text{Im}V_{\text{in}}}, \mathbb{1} - \Pi_{\text{Im}V_{\text{in}}}\}$, from an unknown isometry operation $\mathcal{V}_{\text{in}}$.

We construct parallel and sequential protocols for isometry adjointation by transforming the corresponding unitary inversion protocol (Fig. 2 and Theorems 6 and 5). Isometry inversion and universal error detection protocols are constructed by discarding the measurement outcome and output quantum state, respectively, from the isometry adjointation

[1] Measurement outcomes $a \in \{I, O\}$ stand for "in $\text{Im}V_{\text{in}}$" and "out of $\text{Im}V_{\text{in}}$."

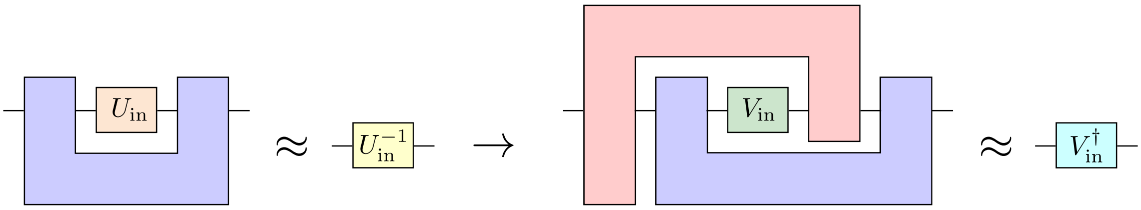


Figure 2: Left panel (unitary inversion): Transformation of a unitary operation U_{in} into its inverse operation U_{in}^{-1}. Right panel (isometry adjointation): Transformation of an isometry operation V_{in} into its adjoint operation $V_{\text{in}}^{\dagger}$. The isometry adjointation protocol is constructed by transforming the unitary inversion protocol (shown in blue) using a quantum comb shown in red.

protocol (Corollaries 7 and 8). We analyze the optimality of the constructed protocols, and we show the following properties:

- Our construction of parallel and sequential protocols gives the optimal performances among all parallel or sequential protocols (Theorem 10).
- Optimal parallel protocol for universal error detection is explicitly given (Theorem 12).
- A parallel protocol for isometry adjointation is given, which achieves an asymptotically optimal approximation error $\epsilon = \Theta(d^2 n^{-1})$ (Theorem 14).

We also give semidefinite programming (SDP) to obtain the optimal performances for these tasks using parallel, sequential, and general protocols including indefinite causal order [9, 36, 37] (Section 4.3).

The rest of this work is organized as follows. Section 2 defines the tasks isometry adjointation, isometry inversion, and universal error detection, and corresponding figures of merit. Section 3.1 introduces the technical details to obtain the main result of this paper (Theorem 5) in Section 3.2, constructing the isometry adjointation protocol. Section 3.3 constructs isometry inversion and universal error detection protocols from the isometry adjointation protocol. Section 4.1 introduces the Choi operator of the general quantum supermap and shows that the Choi operators corresponding to optimal protocols for isometry adjointation, isometry inversion, and universal error detection have the unitary group symmetry. Section 4.2 analyzes the optimal performances using analytical methods based on group theory. Section 4.3 numerically investigates the optimal performances using semidefinite programming. Section 5 concludes the work.

2 Problem setting

We consider the following tasks for the given unknown input state $\rho_{\text{in}} \in \mathcal{L}(\mathbb{C}^D)$ and the unknown isometry operation $\mathcal{V}(\cdot) \coloneqq V \cdot V^\dagger$ for $V \in \mathbb{V}_{\text{iso}}(d, D)$ (see Sections 2.1 – 2.3 for the detail):

- Probabilistic exact isometry inversion
  Promise: The input state ρ_{in} is within the code space $\mathcal{L}(\text{Im}V)$.
  Task: Output the quantum state $\mathcal{V}^{-1}(\rho_{\text{in}})$ with probability p.
- Deterministic isometry inversion
  Promise: The input state ρ_{in} is within the code space $\mathcal{L}(\text{Im}V)$.
  Task: Output a quantum state close to $\mathcal{V}^{-1}(\rho_{\text{in}})$.

- Universal error detection
  Task: Output the measurement outcome $a \in \{I, O\}$[2] with probability close to $\mathrm{Tr}(\Pi_{\mathrm{Im}V_{\mathrm{in}}}\rho_{\mathrm{in}})$ ($a = I$), and $\mathrm{Tr}[(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})\rho_{\mathrm{in}}]$ ($a = O$), where $\Pi_{\mathrm{Im}V_{\mathrm{in}}}$ is the orthogonal projectors onto the subspace $\mathrm{Im}V_{\mathrm{in}}$.

- Isometry adjointation
  Task: Output the quantum state probabilistically with the measurement outcome $a \in \{I, O\}$ with probability close to $\mathrm{Tr}(\Pi_{\mathrm{Im}V_{\mathrm{in}}}\rho_{\mathrm{in}})$ ($a = I$), and $\mathrm{Tr}[(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})\rho_{\mathrm{in}}]$ ($a = O$). When $\rho_{\mathrm{in}} \in \mathcal{L}(\mathrm{Im}V)$, the measurement outcome $a = I$ is obtained with a unit probability with an output quantum state close to $\mathcal{V}^{-1}(\rho_{\mathrm{in}})$. When the measurement outcome $a = O$ is obtained, an output quantum state is given by a fixed quantum state, e.g., the maximally mixed state.

We define the details of the task in the following subsections. To this, we introduce the notion of quantum supermaps, representing the transformations of quantum channels. We first consider a deterministic transformation from n quantum channels $\Phi_{\mathrm{in}}^{(i)} : \mathcal{L}(\mathcal{I}_i) \to \mathcal{L}(\mathcal{O}_i)$ for $i \in \{1, \cdots, n\}$ to a quantum channel $\Phi_{\mathrm{out}} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{F})$, where $\mathcal{I}_i$, $\mathcal{O}_i$, $\mathcal{P}$, and $\mathcal{F}$ are Hilbert spaces[3]. Such a transformation is represented as a linear supermap

$$\mathcal{C} : \bigotimes_{i=1}^{n} [\mathcal{L}(\mathcal{I}_i) \to \mathcal{L}(\mathcal{O}_i)] \to [\mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{F})], \tag{2}$$

where $[\mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)]$ is a set of linear maps from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$. A probabilistic transformation of quantum channels is represented as a set $\{\mathcal{C}_a\}_a$, where a corresponds to the classical outcome. We consider three classes of transformations, as shown below.

- Parallel protocol
  We call $\mathcal{C}$ is implemented by a parallel protocol when input operations are used in parallel as follows:

  $$\mathcal{C}\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right] = \Lambda^{(2)} \circ \left[\bigotimes_{i=1}^{n} \Phi_{\mathrm{in}}^{(i)} \otimes \mathbb{1}_{\mathcal{A}}\right] \circ \Lambda^{(1)}, \tag{3}$$

  where $\Lambda^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{I}^n \otimes \mathcal{A})$ and $\Lambda^{(2)} : \mathcal{L}(\mathcal{O}^n \otimes \mathcal{A}) \to \mathcal{L}(\mathcal{F})$ are quantum channels, $\mathcal{A}$ is an auxiliary Hilbert space, and $\mathcal{I}^n$ and $\mathcal{O}^n$ are joint Hilbert spaces defined by $\mathcal{I}^n := \bigotimes_{i=1}^{n} \mathcal{I}_i$ and $\mathcal{O}^n := \bigotimes_{i=1}^{n} \mathcal{O}_i$, respectively. Similarly, we consider the implementation of a probabilistic transformation of $\{\mathcal{C}_a\}_a$ in a parallel protocol given by

  $$\mathcal{C}_a\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right] = \Lambda_a^{(2)} \circ \left[\bigotimes_{i=1}^{n} \Phi_{\mathrm{in}}^{(i)} \otimes \mathbb{1}_{\mathcal{A}}\right] \circ \Lambda^{(1)}, \tag{4}$$

  where $\{\Lambda_a^{(2)}\}_a$ is a quantum instrument[4]. We also consider a subclass of parallel protocols called parallel delayed input-state protocols, which are realized as

  $$\mathcal{C}\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right](\rho_{\mathrm{in}}) = \Lambda\left[\rho_{\mathrm{in}} \otimes \left(\bigotimes_{i=1}^{n} \Phi_{\mathrm{in}}^{(i)} \otimes \mathbb{1}_{\mathcal{A}}\right)(\phi)\right], \tag{5}$$

[2] I stands for "in ImV" and O stands for "out of ImV."

[3] $\mathcal{P}$ stands for "global past" and $\mathcal{F}$ stands for "global future."

[4] A quantum instrument is a set of completely-positive maps that sum up to a completely-positive and trace-preserving map [38].

where $\rho_{\mathrm{in}} \in \mathcal{L}(\mathcal{P})$ is an input quantum state and $\phi \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{A})$ is a quantum state. Similarly, we consider the parallel delayed input-state protocol of a probabilistic transformation given by

$$\mathcal{C}_a\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right](\rho_{\mathrm{in}}) = \Lambda_a\left[\rho_{\mathrm{in}} \otimes \left(\bigotimes_{i=1}^{n} \Phi_{\mathrm{in}}^{(i)} \otimes \mathbb{1}_{\mathcal{A}}\right)(\phi)\right]. \tag{6}$$

- Sequential protocol (quantum comb [39])
We call $\mathcal{C}$ is implemented by a sequential protocol or a quantum comb [39] when input operations are used sequentially as follows:

$$\mathcal{C}\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right] = \Lambda^{(n+1)} \circ \left[\Phi_{\mathrm{in}}^{(n)} \otimes \mathbb{1}_{\mathcal{A}_n}\right] \circ \Lambda^{(n)} \circ \cdots \circ \Lambda^{(2)} \circ \left[\Phi_{\mathrm{in}}^{(1)} \otimes \mathbb{1}_{\mathcal{A}_1}\right] \circ \Lambda^{(1)}, \tag{7}$$

where $\Lambda^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{I}_1 \otimes \mathcal{A}_1), \Lambda^{(2)} : \mathcal{L}(\mathcal{O}_1 \otimes \mathcal{A}_1) \to \mathcal{L}(\mathcal{I}_2 \otimes \mathcal{A}_2), \cdots, \Lambda^{(n)} : \mathcal{L}(\mathcal{O}_{n-1} \otimes \mathcal{A}_{n-1}) \to \mathcal{L}(\mathcal{I}_n \otimes \mathcal{A}_n), \Lambda^{(n+1)} : \mathcal{L}(\mathcal{O}_n \otimes \mathcal{A}_n) \to \mathcal{L}(\mathcal{F})$ are quantum channels and $\mathcal{A}_1, \cdots, \mathcal{A}_n$ are auxiliary Hilbert spaces. Similarly, we consider the implementation of a probabilistic transformation of $\{\mathcal{C}_a\}_a$ in a sequential protocol given by

$$\mathcal{C}_a\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right] = \Lambda_a^{(n+1)} \circ \left[\Phi_{\mathrm{in}}^{(n)} \otimes \mathbb{1}_{\mathcal{A}_n}\right] \circ \Lambda^{(n)} \circ \cdots \circ \Lambda^{(2)} \circ \left[\Phi_{\mathrm{in}}^{(1)} \otimes \mathbb{1}_{\mathcal{A}_1}\right] \circ \Lambda^{(1)}, \tag{8}$$

where $\{\Lambda_a^{(n+1)}\}_a$ is a quantum instrument.

- General protocol
We consider the most general case, where $\mathcal{C}$ satisfies the following properties:

   1. Completely CP preserving: $(\mathcal{C} \otimes \mathbb{1})\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right]$ is completely positive (CP) for all CP maps $\Phi_{\mathrm{in}}^{(1)} : \mathcal{L}(\mathcal{I}_1 \otimes \mathcal{A}_1) \to \mathcal{L}(\mathcal{O}_1 \otimes \mathcal{B}_1), \cdots, \Phi_{\mathrm{in}}^{(n)} : \mathcal{L}(\mathcal{I}_n \otimes \mathcal{A}_n) \to \mathcal{L}(\mathcal{O}_n \otimes \mathcal{B}_n)$, where $\mathcal{A}_1, \cdots, \mathcal{A}_n$ and $\mathcal{B}_1, \cdots, \mathcal{B}_n$ are auxiliary Hilbert spaces and $\mathbb{1}$ is the identity supermap defined by $\mathbb{1}(\Phi) = \Phi$ for all $\Phi : \mathcal{L}\left[\bigotimes_{i=1}^n \mathcal{A}_i\right] \to \mathcal{L}\left[\bigotimes_{i=1}^n \mathcal{B}_i\right]$.
   2. TP preserving: $\mathcal{C}\left[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}\right]$ is trace preserving (TP) for all TP maps $\Phi_{\mathrm{in}}^{(1)} : \mathcal{L}(\mathcal{I}_1) \to \mathcal{L}(\mathcal{O}_1), \cdots, \Phi_{\mathrm{in}}^{(n)} : \mathcal{L}(\mathcal{I}_n) \to \mathcal{L}(\mathcal{O}_n)$.

We say that $\mathcal{C}$ is a *quantum superchannel* [39] if it satisfies the above conditions. For a probabilistic transformation, we consider the case when $\{\mathcal{C}_a\}_a$ is given by a *quantum superinstrument*, namely, $\mathcal{C}_a$ is completely CP preserving and $\sum_a \mathcal{C}_a$ is TP preserving. The classes of quantum superchannel and superinstrument include indefinite causal order [9, 36, 37], which is not realizable in a conventional quantum circuit model.

2.1 Isometry inversion

We consider a probabilistic exact or deterministic implementation of isometry inversion. For a probabilistic exact implementation, we require that the output state is $\mathcal{V}^{-1}(\rho_{\mathrm{in}})$ for all $\rho_{\mathrm{in}} \in \mathcal{L}(\mathrm{Im}V)$ with probability p. For a deterministic implementation, we require that the output state is obtained deterministically for all $\rho_{\mathrm{in}} \in \mathcal{L}(\mathrm{Im}V)$. We consider the worst-case channel fidelity defined by

$$F_{\mathrm{worst}} = \inf_{V \in \mathbb{V}_{\mathrm{iso}}(d,D)} F_{\mathrm{ch}}[\mathcal{C}[\mathcal{V}^{\otimes n}] \circ \mathcal{V}, \mathbb{1}_d], \tag{9}$$

where F_{ch} is the channel fidelity [40] and $\mathbb{1}_d$ is the identity operation. The channel fidelity between a quantum channel Λ on a d-dimensional system and a d-dimensional unitary operation $\mathcal{U}(\cdot) = U \cdot U^\dagger$ is given by

$$F_{\text{ch}}(\Lambda, \mathcal{U}) = \frac{1}{d^2} \operatorname{Tr}[J_\Lambda |U\rangle\!\rangle\langle\!\langle U|], \tag{10}$$

where J_Λ and $|U\rangle\!\rangle$ are the Choi operator of Λ and the Choi vector of U [41, 42], respectively, defined by

$$J_\Lambda \coloneqq \sum_{i,j} |i\rangle\langle j| \otimes \Lambda(|i\rangle\langle j|), \tag{11}$$

$$|U\rangle\!\rangle \coloneqq \sum_i |i\rangle \otimes U\,|i\rangle \tag{12}$$

using the computational basis $\{|i\rangle\}$ of the input system (see Section 3.1.1 for the detail of the Choi representation). Therefore, $F_{\text{ch}}(\Lambda, \mathcal{U})$ is linear with respect to Λ. The channel fidelity is invariant under the action of unitary operations, i.e.,

$$F_{\text{ch}}(\mathcal{U}' \circ \Lambda^{(1)} \circ \mathcal{U}, \mathcal{U}' \circ \Lambda^{(2)} \circ \mathcal{U}) = F_{\text{ch}}(\Lambda^{(1)}, \Lambda^{(2)}) \tag{13}$$

holds for any quantum channels $\Lambda^{(1)}$ and $\Lambda^{(2)}$ and unitary operations $\mathcal{U}$ and $\mathcal{U}'$. Therefore, when $D = d$, the definition (9) of the figure of merit for deterministic isometry inversion corresponds to the worst-case channel fidelity for deterministic unitary inversion introduced in Ref. [29] given by

$$F_{\text{worst}} = \inf_{U \in \mathbb{U}(d)} F_{\text{ch}}[\mathcal{C}(\mathcal{U}^{\otimes n}), \mathcal{U}^{-1}]. \tag{14}$$

We denote the optimal success probability of isometry inversion in parallel, sequential, and general protocols by $p_{\text{opt}}^{(x)}(d, D, n)$ for $x = \text{PAR}$ (parallel), $x = \text{SEQ}$ (sequential), and $x = \text{GEN}$ (general), respectively. Similarly, we denote the optimal fidelity of isometry inversion by $F_{\text{opt}}^{(x)}(d, D, n)$.

2.2 Universal error detection

We define the task to implement the POVM $\{\Pi_I, \Pi_O\}$ given by

$$\Pi_I = \Pi_{\operatorname{Im} V_{\text{in}}} + \alpha(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\text{in}}}), \tag{15}$$

$$\Pi_O = (1 - \alpha)(\mathbb{1}_D - \Pi_{\operatorname{Im} V_{\text{in}}}), \tag{16}$$

i.e., we require the one-sided error condition such that we obtain the measurement outcome $a = I$ with a unit probability when $\rho_{\text{in}} \in \mathcal{L}(\operatorname{Im} V_{\text{in}})$ holds. We denote the minimal value of α in parallel, sequential, and general protocols as $\alpha_{\text{opt}}^{(x)}(d, D, n)$ for $x = \text{PAR}$ (parallel), $x = \text{SEQ}$ (sequential), and $x = \text{GEN}$ (general), respectively.

2.3 Isometry adjointation

We demand the quantum superinstrument $\{\mathcal{C}_I, \mathcal{C}_O\}$ satisfies

$$\operatorname{Tr} \mathcal{C}_I[\mathcal{V}^{\otimes n}](\rho_{\text{in}}) = 1 \quad \forall \rho_{\text{in}} \in \mathcal{D}(\operatorname{Im} V), \tag{17}$$

which corresponds to the one-sided error condition in universal error detection. We define the quantum channels corresponding to the output quantum instrument and adjoint operation by

$$\mathcal{C}[\mathcal{V}^{\otimes n}](\cdot) := \mathcal{C}_I[\mathcal{V}^{\otimes n}](\cdot) \otimes |0\rangle\langle 0| + \mathcal{C}_O[\mathcal{V}^{\otimes n}](\cdot) \otimes |1\rangle\langle 1| \,, \tag{18}$$

$$\mathcal{V}_{\text{adjoint}}(\cdot) := V^\dagger \cdot V \otimes |0\rangle\langle 0| + \text{Tr}[(\mathbb{1}_D - \Pi_{\text{Im}V})\cdot]\frac{\mathbb{1}}{d} \otimes |1\rangle\langle 1| \,, \tag{19}$$

and define the figure of merit by the worst-case diamond-distance error:

$$\epsilon = \sup_{V \in \mathbb{V}_{\text{iso}}(d,D)} \frac{1}{2}\left\| \mathcal{C}[\mathcal{V}^{\otimes n}] - \mathcal{V}_{\text{adjoint}} \right\|_\diamond, \tag{20}$$

where $\|\cdot\|_\diamond$ is the diamond norm [43]. We denote the minimal value of ϵ in parallel, sequential, and general protocols by $\epsilon_{\text{opt}}^{(x)}(d, D, n)$ for $x = \text{PAR}$ (parallel), $x = \text{SEQ}$ (sequential), and $x = \text{GEN}$ (general), respectively.

3 Construction of isometry adjointation protocols and reduction to isometry inversion and universal error detection

In Section 3.1, we introduce the Choi representation to represent quantum channels and quantum supermaps. We also introduce the link product to represent their compositions. Then, we introduce the group theoretic technique called the Schur-Weyl duality. In Section 3.2, we construct isometry adjointation protocols by transforming unitary inversion protocols using the quantum comb derived from the Schur-Weyl duality. We also derive isometry inversion and universal error detection protocols from the isometry adjointation protocol.

In the following discussions, we suppose $\mathcal{I}_1 = \cdots \mathcal{I}_n = \mathcal{F} = \mathcal{O}'_1 = \cdots = \mathcal{O}'^n = \mathcal{P}' = \mathbb{C}^d$, $\mathcal{O}_1 = \cdots = \mathcal{O}_n = \mathcal{P} = \mathbb{C}^D$, and denote the joint Hilbert spaces by $\mathcal{I}^i := \bigotimes_{j=1}^i \mathcal{I}_j$, $\mathcal{O}'^i := \bigotimes_{j=1}^i \mathcal{O}'_j$, and $\mathcal{O}^i = \bigotimes_{j=1}^i \mathcal{O}_j$ for $j \in \{1, \cdots, n\}$. To illustrate the dimensions of the Hilbert spaces corresponding to the wires in the quantum circuits shown in this Section, we utilize the following color code of wires: a red wire corresponds to a d-dimensional Hilbert space, a blue wire corresponds to a D-dimensional Hilbert space, and a black wire corresponds to a Hilbert space with an arbitrary dimension. The dual wires in the quantum circuits represent classical information transmissions.

3.1 Preliminaries

3.1.1 Choi representation and link product

Any quantum channel $\Lambda : \mathcal{L}(\mathcal{I}) \to \mathcal{L}(\mathcal{O})$ can be represented by the Choi operator $J_\Lambda \in \mathcal{L}(\mathcal{I} \otimes \mathcal{O})$ defined by [41, 42]

$$J_\Lambda := \sum_{i,j} |i\rangle\langle j|_\mathcal{I} \otimes \Lambda(|i\rangle\langle j|)_\mathcal{O}, \tag{21}$$

where $\{|i\rangle\}$ is the computational basis of $\mathcal{I}$. In particular, the Choi operator $J_\mathcal{V}$ of an isometry operation $\mathcal{V}(\cdot) := V \cdot V^\dagger$ for an isometry operator $V : \mathcal{I} \to \mathcal{O}$ is represented as

$$J_\mathcal{V} = |V\rangle\rangle\langle\langle V|, \tag{22}$$

where $|V\rangle\rangle \in \mathcal{I} \otimes \mathcal{O}$ is the Choi vector of V defined by

$$|V\rangle\rangle := \sum_i |i\rangle_{\mathcal{I}} \otimes (V|i\rangle)_{\mathcal{O}}. \tag{23}$$

A composition of two quantum channels $\Lambda^{(1)} : \mathcal{L}(\mathcal{I}) \to \mathcal{L}(\mathcal{O}_1)$ and $\Lambda^{(2)} : \mathcal{L}(\mathcal{O}_1) \to \mathcal{L}(\mathcal{O}_2)$ can be represented in terms of the corresponding Choi operators as

$$J_{\Lambda^{(2)} \circ \Lambda^{(1)}} = J_{\Lambda^{(2)}} \star J_{\Lambda^{(1)}}, \tag{24}$$

where $\star$ is the link product [44] defined by

$$A \star B := \mathrm{Tr}_{\mathcal{B}}[(A^{T_{\mathcal{B}}} \otimes \mathbb{1}_{\mathcal{C}})(\mathbb{1}_{\mathcal{A}} \otimes B)] \tag{25}$$

for $A \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$ and $B \in \mathcal{L}(\mathcal{B} \otimes \mathcal{C})$, and $A^{T_{\mathcal{B}}}$ is the partial transpose of A with respect to the subsystem $\mathcal{B}$. The link product satisfies the commutativity and associativity relations by definition, given as

$$A \star B = B \star A, \tag{26}$$

$$(A \star B) \star C = A \star (B \star C) \tag{27}$$

for $A \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$, $B \in \mathcal{L}(\mathcal{B} \otimes \mathcal{C})$, and $C \in \mathcal{L}(\mathcal{C} \otimes \mathcal{D})$. If the two operators A and B does not have an overlap subsystem, i.e., $A \in \mathcal{L}(\mathcal{A})$ and $B \in \mathcal{L}(\mathcal{B})$ for $\mathcal{A} \neq \mathcal{B}$, the link product of A and B becomes the tensor product:

$$A \star B = A \otimes B. \tag{28}$$

Using the Choi operator and the link product, we can represent the quantum combs defined in Eq. (7). The Choi operator of the quantum channel shown in the right-hand side of Eq. (7) is given by

$$J_{\Lambda^{(n+1)}} \star J_{\Phi_{\mathrm{in}}^{(n)}} \star J_{\Lambda^{(n)}} \star \cdots \star J_{\Lambda^{(2)}} \star J_{\Phi_{\mathrm{in}}^{(1)}} \star J_{\Lambda^{(1)}}. \tag{29}$$

Using Eqs. (26)-(28), this can be rewritten as

$$C \star \bigotimes_{i=1}^{n} J_{\Phi_{\mathrm{in}}^{(i)}}, \tag{30}$$

where $C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ is the Choi operator of the quantum comb $\mathcal{C}$ defined by

$$C := J_{\Lambda^{(n+1)}} \star J_{\Lambda^{(n)}} \star \cdots \star J_{\Lambda^{(1)}}. \tag{31}$$

Therefore, the action of a quantum comb $\mathcal{C}$ on input quantum operations $\{\Phi_{\mathrm{in}}^{(1)}, \cdots, \Phi_{\mathrm{in}}^{(n+1)}\}$ is given in the Choi representation by

$$J_{\mathcal{C}[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}]} = C \star \bigotimes_{i=1}^{n} J_{\Phi_{\mathrm{in}}^{(i)}}. \tag{32}$$

The following Theorem characterizes the set of Choi operators of quantum combs.

Theorem 1. [44, 45] *Suppose $\mathcal{P}, \mathcal{F}, \mathcal{I}_i, \mathcal{O}_i$ for $i \in \{1, \cdots, n\}$ are Hilbert spaces and define the joint Hilbert spaces by $\mathcal{I}^n := \bigotimes_{i=1}^n \mathcal{I}_i$ and $\mathcal{O}^n := \bigotimes_{i=1}^n \mathcal{O}_i$. The operator $C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ can be written as Eq. (31) using quantum channels $\Lambda^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{I}_1 \otimes \mathcal{A}_1), \Lambda^{(2)} : \mathcal{L}(\mathcal{O}_1 \otimes \mathcal{A}_1) \to \mathcal{L}(\mathcal{I}_2 \otimes \mathcal{A}_2), \cdots, \Lambda^{(n)} : \mathcal{L}(\mathcal{O}_{n-1} \otimes \mathcal{A}_{n-1}) \to \mathcal{L}(\mathcal{I}_n \otimes \mathcal{A}_n), \Lambda^{(n+1)} :$*

$\mathcal{L}(\mathcal{O}_n \otimes \mathcal{A}_n) \to \mathcal{L}(\mathcal{F})$ and auxiliary Hilbert spaces $\mathcal{A}_1, \cdots, \mathcal{A}_n$ if and only if C satisfies the following equations:

$$C \geq 0, \tag{33}$$

$$\operatorname{Tr}_{\mathcal{I}_i} C^{(i)} = C^{(i-1)} \otimes \mathbb{1}_{\mathcal{O}_{i-1}} \quad \forall i \in \{1, \cdots, n+1\}, \tag{34}$$

where $\mathcal{O}_0$ and $\mathcal{I}_{n+1}$ are defined by $\mathcal{O}_0 := \mathcal{P}$ and $\mathcal{I}_{n+1} := \mathcal{F}$, and $C^{(i)}$ for $i \in \{0, \cdots, n+1\}$ are defined by $C^{(n+1)} := C$, $C^{(i-1)} := \operatorname{Tr}_{\mathcal{O}_{i-1}\mathcal{I}_i} C^{(i)} / \dim \mathcal{O}_{i-1}$ and $C^{(0)} := 1$.

The probabilistic transformation $\{\mathcal{C}_a\}_a$ in a sequential protocol given by Eq. (8) can be similarly represented by

$$J_{\mathcal{C}_a[\Phi_{\text{in}}^{(1)} \otimes \cdots \otimes \Phi_{\text{in}}^{(n)}]} = C_a \star \bigotimes_{i=1}^{n} J_{\Phi_{\text{in}}^{(i)}}, \tag{35}$$

where C_a is the Choi operator of the probabilistic transformation $\{\mathcal{C}_a\}_a$ defined by

$$C_a := J_{\Lambda_a^{(n+1)}} \star J_{\Lambda^{(n)}} \star \cdots \star J_{\Lambda^{(1)}}. \tag{36}$$

The following Theorem characterizes the set of Choi operators of probabilistic transformations implemented in sequential protocols.

Theorem 2. [44, 45] *Suppose $\mathcal{P}, \mathcal{F}, \mathcal{I}_i, \mathcal{O}_i$ for $i \in \{1, \cdots, n\}$ are Hilbert spaces and define the joint Hilbert spaces by $\mathcal{I}^n := \bigotimes_{i=1}^n \mathcal{I}_i$ and $\mathcal{O}^n := \bigotimes_{i=1}^n \mathcal{O}_i$. The set of operators $\{C_a\}_a \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ can be written as Eq. (31) using quantum channels $\Lambda^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{I}_1 \otimes \mathcal{A}_1), \Lambda^{(2)} : \mathcal{L}(\mathcal{O}_1 \otimes \mathcal{A}_1) \to \mathcal{L}(\mathcal{I}_2 \otimes \mathcal{A}_2), \cdots, \Lambda^{(n)} : \mathcal{L}(\mathcal{O}_{n-1} \otimes \mathcal{A}_{n-1}) \to \mathcal{L}(\mathcal{I}_n \otimes \mathcal{A}_n)$, a quantum instrument $\{\Lambda_a^{(n+1)}\}_a : \mathcal{L}(\mathcal{O}_n \otimes \mathcal{A}_n) \to \mathcal{L}(\mathcal{F})$ and auxiliary Hilbert spaces $\mathcal{A}_1, \cdots, \mathcal{A}_n$ if and only if C satisfies the following equations:*

$$C_a \geq 0, \tag{37}$$

$$\operatorname{Tr}_{\mathcal{I}_i} C^{(i)} = C^{(i-1)} \otimes \mathbb{1}_{\mathcal{O}_{i-1}} \quad \forall i \in \{1, \cdots, n+1\}, \tag{38}$$

where $\mathcal{O}_0$ and $\mathcal{I}_{n+1}$ are defined by $\mathcal{O}_0 := \mathcal{P}$ and $\mathcal{I}_{n+1} := \mathcal{F}$, and $C^{(i)}$ for $i \in \{0, \cdots, n+1\}$ are defined by $C^{(n+1)} := \sum_a C_a$, $C^{(i-1)} := \operatorname{Tr}_{\mathcal{O}_{i-1}\mathcal{I}_i} C^{(i)} / \dim \mathcal{O}_{i-1}$ and $C^{(0)} := 1$.

The link product also represents the composition of two quantum combs. We consider two quantum combs $\mathcal{C}'$ and $\mathcal{T}$ defined by

$$\mathcal{C}'\left[\Phi_{\text{in}}'^{(1)} \otimes \cdots \otimes \Phi_{\text{in}}'^{(n)}\right] := \Lambda'^{(n+1)} \circ (\Phi_{\text{in}}'^{(n)} \otimes \mathbb{1}_{\mathcal{A}_n}) \circ \cdots \circ \Lambda'^{(2)} \circ (\Phi_{\text{in}}'^{(1)} \otimes \mathbb{1}_{\mathcal{A}_1}) \circ \Lambda'^{(1)}, \tag{39}$$

$$\mathcal{T}\left[\Phi_{\text{in}}''^{(1)} \otimes \cdots \otimes \Phi_{\text{in}}''^{(n)}\right] := \Gamma^{(n+1)} \circ (\Phi_{\text{in}}''^{(n)} \otimes \mathbb{1}_{\mathcal{B}_n}) \circ \cdots \circ \Gamma^{(2)} \circ (\Phi_{\text{in}}''^{(1)} \otimes \mathbb{1}_{\mathcal{B}_1}) \circ \Gamma^{(1)}, \tag{40}$$

where $\mathcal{A}_i$ and $\mathcal{B}_i$ for $i \in \{1, \cdots, n\}$ are auxiliary Hilbert spaces and $\Lambda'^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{I}_1 \otimes \mathcal{A}_1)$, $\Lambda'^{(i)} : \mathcal{L}(\mathcal{O}'_{i-1} \otimes \mathcal{A}_{i-1}) \to \mathcal{L}(\mathcal{I}_i \otimes \mathcal{A}_i)$ for $i \in \{2, \cdots, n\}$, $\Lambda'^{(n+1)} : \mathcal{L}(\mathcal{O}'_n \otimes \mathcal{A}_n) \to \mathcal{L}(\mathcal{F})$, $\Gamma^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{P}' \otimes \mathcal{B}_1)$, $\Gamma^{(i)} : \mathcal{L}(\mathcal{O}_{i-1} \otimes \mathcal{B}_{i-1}) \to \mathcal{L}(\mathcal{O}'_{i-1} \otimes \mathcal{B}_i)$ for $i \in \{2, \cdots, n\}$, and $\Gamma^{(n+1)} : \mathcal{L}(\mathcal{O}_n \otimes \mathcal{B}_n) \to \mathcal{L}(\mathcal{O}'_n)$ are quantum channels. We define the composed quantum comb $\mathcal{C}$ by

$$\mathcal{C}\left[\Phi_{\text{in}}^{(1)}, \cdots, \Phi_{\text{in}}^{(n)}\right] := \Lambda^{(n+1)} \circ (\Phi_{\text{in}}^{(n)} \otimes \mathbb{1}_{\mathcal{A}_n\mathcal{B}_n}) \circ \cdots \circ \Lambda^{(2)} \circ (\Phi_{\text{in}}^{(1)} \otimes \mathbb{1}_{\mathcal{A}_1\mathcal{B}_1}) \circ \Lambda^{(1)}, \tag{41}$$

$$\Lambda^{(i)} := (\Lambda'^{(i)} \otimes \mathbb{1}_{\mathcal{B}_i}) \circ (\Gamma^{(i)} \otimes \mathbb{1}_{\mathcal{A}_{i-1}}) \quad \forall i \in \{1, \cdots, n+1\}. \tag{42}$$

In terms of the Choi operator, this composition can be written as

$$C = C' \star T, \tag{43}$$

where C', T, and C are Choi operators of $\mathcal{C}'$, $\mathcal{T}$, and $\mathcal{C}$, respectively.

3.1.2 Schur-Weyl duality

We introduce the Schur-Weyl duality as follows. We consider representations of the special unitary group $\mathbb{U}(d)$ and the permutation group $\mathfrak{S}_n$ on a n-fold Hilbert space $(\mathbb{C}^d)^{\otimes n}$ defined by

$$\mathbb{U}(d) \ni U \mapsto U^{\otimes n} \in \mathcal{L}(\mathbb{C}^d)^{\otimes n}, \tag{44}$$

$$\mathfrak{S}_n \ni \pi \mapsto P_\pi \in \mathcal{L}(\mathbb{C}^d)^{\otimes n}, \tag{45}$$

where P_π is a permutation operator on $(\mathbb{C}^d)^{\otimes n}$ defined by

$$P_\pi(|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle) := \left|\psi_{\pi^{-1}(1)}\right\rangle \otimes \cdots \otimes \left|\psi_{\pi^{-1}(n)}\right\rangle \quad \forall |\psi_1\rangle, \cdots, |\psi_n\rangle \in \mathbb{C}^d. \tag{46}$$

The Schur-Weyl duality asserts a simultaneous irreducible decomposition of the two representations $U^{\otimes n}$ and P_π given by

$$(\mathbb{C}^d)^{\otimes n} = \bigoplus_{\mu \in \mathbb{Y}_n^d} \mathcal{U}_\mu^{(d)} \otimes \mathcal{S}_\mu, \tag{47}$$

$$U^{\otimes n} = \bigoplus_{\mu \in \mathbb{Y}_n^d} (U_\mu)_{\mathcal{U}_\mu^{(d)}} \otimes \mathbb{1}_{\mathcal{S}_\mu}, \tag{48}$$

$$P_\pi = \bigoplus_{\mu \in \mathbb{Y}_n^d} \mathbb{1}_{\mathcal{U}_\mu^{(d)}} \otimes (\pi_\mu)_{\mathcal{S}_\mu}, \tag{49}$$

where μ runs in the set of Young diagrams with n boxes whose depth is less than or equal to d, denoted by $\mathbb{Y}_n^d$, and U_μ and π_μ are irreducible representations of $\mathbb{U}(d)$ and $\mathfrak{S}_n$ on the linear spaces $\mathcal{U}_\mu^{(d)}$ and $\mathcal{S}_\mu$, respectively.[5] We denote the dimensions of the irreducible representation spaces $\mathcal{U}_\mu^{(d)}$ and $\mathcal{S}_\mu$ by $m_\mu^{(d)}$ and d_μ, respectively.[6] They are given by [46]

$$d_\mu = \frac{n!}{\mathrm{hook}(\mu)}, \tag{50}$$

$$m_\mu^{(d)} = \frac{\prod_{(i,j)\in\mu}(d+j-i)}{\mathrm{hook}(\mu)}, \tag{51}$$

where $\mathrm{hook}(\mu)$ for $\mu \in \mathbb{Y}_n^d$ is defined by

$$\mathrm{hook}(\mu) = \prod_{(i,j)\in\mu} (\mu_i + \mu'_j - i - j + 1), \tag{52}$$

and (i,j) is the coordinate of a box in the Young diagram μ such that i represents the row number running from bottom to top and j represents the column number running from left to right. The numbers μ_i and μ'_j are the numbers of boxes in the i-th row and the j-th column, respectively. The n-fold isometry operator $V^{\otimes n}$ for $V \in \mathbb{V}_{\mathrm{iso}}(d,D)$ can also be decomposed as

$$V^{\otimes n} = \bigoplus_{\mu \in \mathbb{Y}_n^d} (V_\mu)_{\mathcal{U}_\mu^{(d)} \to \mathcal{U}_\mu^{(D)}} \otimes \mathbb{1}_{\mathcal{S}_\mu}, \tag{53}$$

[5] The superscript d is put on $\mathcal{U}_\mu^{(d)}$ since the properties of the representation space $\mathcal{U}_\mu^{(d)}$, e.g., the dimension, depends on the local dimension d. On the other hand, we do not put the superscript d on $\mathcal{S}_\mu$ like $\mathcal{S}_\mu^{(d)}$ since the representation space $\mathcal{S}_\mu^{(d)}$ is automorphic to $\mathcal{S}_\mu^{(d')}$ for an arbitrary local dimension d'.

[6] The dimension of $\mathcal{U}_\mu^{(d)}$ is denoted by $m_\mu^{(d)}$ since $\mathcal{U}_\mu^{(d)}$ is the multiplicity space corresponding to the irreducible representation space $\mathcal{S}_\mu$ [see Eq. (47)].

where $V_\mu : \mathcal{U}_\mu^{(d)} \to \mathcal{U}_\mu^{(D)}$ is an isometry operator, as shown in Ref. [35].

Due to Schur's lemma, any operator commuting with $U^{\otimes n}$ for all $U \in \mathbb{U}(d)$ can be written as a linear combination of the operators $E_{ij}^{\mu,d}$ defined by

$$E_{ij}^{\mu,d} := \mathbb{1}_{\mathcal{U}_\mu^{(d)}} \otimes |\mu, i\rangle\langle\mu, j|_{\mathcal{S}_\mu} \tag{54}$$

for $i, j \in \{1, \cdots, d_\mu\}$, where $\{|\mu, i\rangle\}$ is an orthonormal basis of $\mathcal{S}_\mu$. Then, the following relation holds:

$$\operatorname{Tr} E_{ij}^{\mu,d} = m_\mu^{(d)} \delta_{ij}, \quad E_{ij}^{\mu,d} E_{kl}^{\nu,d} = \delta_{\mu\nu}\delta_{jk} E_{il}^{\mu,d}, \tag{55}$$

where δ_{ij} is Kronecker's delta defined by $\delta_{ii} = 1$ and $\delta_{ij} = 0$ for $i \neq j$. In particular, $\{m_\mu^{(d)-1/2} E_{ij}^{\mu,d}\}$ forms an orthonormal basis of the set of operators commuting with $U^{\otimes n}$ for all $U \in \mathbb{U}(d)$ under the Hilbert-Schmidt inner product $\langle X, Y\rangle := \operatorname{Tr}\left(X^\dagger Y\right)$. Thus, any operator ρ commuting with $U^{\otimes n}$ for all $U \in \mathbb{U}(d)$ can be represented as

$$\rho = \sum_{\mu \in \mathbb{Y}_n^d} \sum_{i,j=1}^{d_\mu} \frac{\operatorname{Tr}\left(E_{ji}^{\mu,d} \rho\right)}{m_\mu^{(d)}} E_{ij}^{\mu,d}. \tag{56}$$

Also, we define the Young projector Π_μ by

$$\Pi_\mu^{(d)} := \sum_{i=1}^{d_\mu} E_{ii}^{\mu,d}, \tag{57}$$

which is an orthonormal projector onto the subspace $\mathcal{U}_\mu^{(d)} \otimes \mathcal{S}_\mu$.

In particular, we consider the Schur basis of $(\mathbb{C}^d)^{\otimes n}$ defined by

$$|\mu, u, i\rangle := |\mu, u\rangle_{\mathcal{U}_\mu^{(d)}} \otimes |\mu, i\rangle_{\mathcal{S}_\mu}, \tag{58}$$

where $\{|\mu, u\rangle\}$ is the Gelfand-Zetlin basis of $\mathcal{U}_\mu^{(d)}$ and $\{|\mu, i\rangle\}$ is the Young-Yamanouchi basis of $\mathcal{S}_\mu$. The change of the basis from the computational basis to the Schur basis is called the quantum Schur transform [47–52], denoted by V_{Sch}. The standard tableaux with frame μ is indexed by $i \in \{1, \cdots, d_\mu\}$ and the i-th standard tableau is denoted by s_i^μ. Each element in the Young-Yamanouchi basis $\{|\mu, i\rangle\}$ is associated with the standard tableaux s_i^μ. We also define the set of operators $\{E_{ab}^{\lambda,d}\}$ on $(\mathbb{C}^d)^{\otimes n-1}$ for $\lambda \in \mathbb{Y}_{n-1}^d$ and $a, b \in \{1, \cdots, d_\lambda\}$. To express the relation between $\{E_{ij}^{\mu,d}\}$ and $\{E_{ab}^{\lambda,d}\}$, we introduce the following notations on the Young diagrams. We denote the set of Young diagrams obtained by adding (removing) a box to λ by $\lambda + \square$ ($\lambda - \square$), and the index of the standard tableau $s_{a_\mu^\lambda}^\mu$ obtained by adding a box $\boxed{n}$ to a standard tableau s_a^λ by a_μ^λ. Then, the following Lemma holds.

Lemma 3. [21, 30, 53, 54] *The tensor product $E_{ab}^{\lambda,d} \otimes \mathbb{1}_d$ and the partial trace of $E_{ij}^{\mu,d}$ in the last system for $\lambda \in \mathbb{Y}_{n-1}^d$ and $\mu \in \mathbb{Y}_n^d$ are given by*

$$E_{ab}^{\lambda,d} \otimes \mathbb{1}_d = \sum_{\mu \in \lambda + \square} E_{a_\mu^\lambda b_\mu^\lambda}^{\mu,d}, \quad \operatorname{Tr}_n E_{a_\mu^\lambda b_\mu^\kappa}^{\mu,d} = \delta_{\lambda\kappa} \frac{m_\mu^{(d)}}{m_\lambda^{(d)}} E_{ab}^{\lambda,d}. \tag{59}$$

3.2 Construction of isometry adjointation protocol

3.2.1 Transformation from unitary inversion to isometry inversion

In this section, we derive a probabilistic quantum comb $\{\mathcal{T}_I, \mathcal{T}_O\}$ transforming a unitary inversion protocol to an isometry adjointation protocol as

$$\begin{aligned} &C' \star |U_{\mathrm{in}}\rangle\!\rangle\langle\!\langle U_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n} \approx |U_{\mathrm{in}}^{-1}\rangle\!\rangle\langle\!\langle U_{\mathrm{in}}^{-1}|_{\mathcal{P}'\mathcal{F}} \quad \forall U_{\mathrm{in}} \in \mathbb{U}(d) \\ &\implies T_I \star C' \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \approx |V_{\mathrm{in}}^{\dagger}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^{\dagger}|_{\mathcal{P}\mathcal{F}} \quad \forall V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D), \end{aligned} \tag{60}$$

where C' is the Choi operator corresponding to a quantum comb implementing unitary inversion, and T_I is the Choi operator corresponding to $\mathcal{T}_I$.

We define $T_I, T_O \in \mathcal{L}(\mathcal{P}' \otimes \mathcal{O}'^n \otimes \mathcal{P} \otimes \mathcal{O}^n)$ using the operators $\{E^{\mu,d}_{ij}\}$ introduced in Section 3.1.2 by

$$T_I := \sum_{\mu \in \mathbb{Y}^d_{n+1}} \sum_{i,j=1}^{d_\mu} \frac{(E^{\mu,d}_{ij})_{\mathcal{P}'\mathcal{O}'^n} \otimes (E^{\mu,D}_{ij})_{\mathcal{P}\mathcal{O}^n}}{m^{(d)}_\mu}, \tag{61}$$

$$T_O := \sum_{t=d}^{n} \sum_{\substack{\mu_{n+1} \in \cdots \in \mu_t \\ \mu_t \in \mathbb{Y}^d_t, \mu_{t+1} \notin \mathbb{Y}^d_{t+1}}} \sum_{a,b=1}^{d_{\mu_t}} \frac{(E^{\mu_t,d}_{ab})_{\mathcal{P}'\mathcal{O}'^{t-1}} \otimes \mathbb{1}_{\mathcal{O}'_t \cdots \mathcal{O}'_n} \otimes (E^{\mu_i,D}_{a^{\mu_t}_{\mu_{t+1}\cdots\mu_{n+1}} b^{\mu_t}_{\mu_{t+1}\cdots\mu_{n+1}}})_{\mathcal{P}\mathcal{O}^n}}{d^{n+1-t} m^{(d)}_{\mu_t}}, \tag{62}$$

where $\mu_j \in \mu_{j+1}$ for $j = t, \cdots, n$ represents that μ_{j+1} is a Young diagram obtained by adding a box to μ_j, and $a^{\mu_t}_{\mu_{t+1}\cdots\mu_{n+1}}$ is defined by $a^{\mu_t}_{\mu_{t+1}\cdots\mu_{n+1}} := (\cdots(a^{\mu_t}_{\mu_{t+1}})^{\mu_{t+1}}_{\mu_{t+2}})\cdots)^{\mu_n}_{\mu_{n+1}}$, namely, the index of the standard tableau obtained by recursively adding a box $\boxed{j+1}$ to $s^{\mu_j}_a$ for $j = t, \cdots, n$. Then, $\{\mathcal{T}_I, \mathcal{T}_O\}$ satisfies the quantum comb condition as shown in the following Lemma.

Lemma 4. *The set of operators $\{T_I, T_O\}$ defined in Eqs. (61) and (62) satisfies*

$$T_I \geq 0, \quad T_O \geq 0, \tag{63}$$

$$\mathrm{Tr}_{\mathcal{O}'_{i-1}} T^{(i)} = T^{(i-1)} \otimes \mathbb{1}_{\mathcal{O}_{i-1}} \quad \forall i \in \{1, \cdots, n+1\}, \tag{64}$$

where $\mathcal{O}_0$ and $\mathcal{O}'_0$ are defined by $\mathcal{O}'_0 := \mathcal{P}'$ and $\mathcal{O}_0 := \mathcal{P}$, and $T^{(i)}$ are defined by $T^{(n+1)} := T_I + T_O$, $T^{(i)} := \mathrm{Tr}_{\mathcal{O}'_i\mathcal{O}_i} T^{(i+1)}/D$ for $i \in \{1, \cdots, n+1\}$, and $T^{(0)} := 1$.

Proof. See Appendix A.1 for the proof. □

Lemma 4 imply the existence of quantum channels $\Gamma^{(1)} : \mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{I}_1 \otimes \mathcal{B}_1), \Gamma^{(2)} : \mathcal{L}(\mathcal{O}_1 \otimes \mathcal{B}_1) \to \mathcal{L}(\mathcal{O}'_2 \otimes \mathcal{B}_2), \cdots, \Gamma^{(n)} : \mathcal{L}(\mathcal{O}_{n-1} \otimes \mathcal{B}_{n-1}) \to \mathcal{L}(\mathcal{O}'_n \otimes \mathcal{B}_n)$, a quantum instrument $\{\Gamma^{(n+1)}_I, \Gamma^{(n+1)}_O\} : \mathcal{L}(\mathcal{O}_n \otimes \mathcal{B}_n) \to \mathcal{L}(\mathcal{F})$ and auxiliary Hilbert spaces $\mathcal{B}_1, \cdots, \mathcal{B}_n$ such that (see Theorem 2)

$$T_a = J_{\Gamma^{(n+1)}_a} \star J_{\Gamma^{(n)}} \star \cdots \star J_{\Gamma^{(1)}} \quad \forall a \in \{I, O\}, \tag{65}$$

where J_Γ is the Choi operator of $\Gamma \in \{\Gamma^{(1)}, \cdots, \Gamma^{(n)}, \Gamma^{(n+1)}_a\}$.

We compose the probabilistic quantum comb $\{\mathcal{T}_I, \mathcal{T}_O\}$ with the unitary inversion protocol to implement isometry adjointation. Suppose a quantum comb $\mathcal{C}' : \bigotimes_{i=1}^n [\mathcal{L}(\mathcal{I}_i) \to \mathcal{L}(\mathcal{O}'_i)] \to [\mathcal{L}(\mathcal{P}') \to \mathcal{L}(\mathcal{F})]$ given by [see Fig. 3 (a-1)]

$$\mathcal{C}'\left[\Phi^{(1)}_{\mathrm{in}}, \cdots, \Phi^{(n)}_{\mathrm{in}}\right] := \Lambda'^{(n+1)} \circ (\Phi^{(n)}_{\mathrm{in}} \otimes \mathbb{1}_{\mathcal{A}_n}) \circ \cdots \circ \Lambda'^{(2)} \circ (\Phi^{(1)}_{\mathrm{in}} \otimes \mathbb{1}_{\mathcal{A}_1}) \circ \Lambda'^{(1)} \tag{66}$$

implements deterministic unitary inversion approximately:

$$\mathcal{C}'(\mathcal{U}_{\mathrm{in}}^{\otimes n}) \approx \mathcal{U}_{\mathrm{in}}^{-1} \quad \forall U_{\mathrm{in}} \in \mathbb{U}(d). \tag{67}$$

Reference [29] shows that the optimal worst-case channel fidelity of unitary inversion is achieved with the protocol whose Choi operator C' satisfies the $\mathbb{U}(d) \times \mathbb{U}(d)$ symmetry given by

$$[C', U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}'\mathcal{O}'^n}] = 0 \quad \forall U', U'' \in \mathbb{U}(d). \tag{68}$$

From the sequential unitary inversion protocol satisfying the $\mathbb{U}(d) \times \mathbb{U}(d)$ symmetry (68), we define a probabilistic transformation as follows [see Fig. 3 (b)]:

$$\mathcal{C}_a\left[\Phi_{\mathrm{in}}^{(1)}, \cdots, \Phi_{\mathrm{in}}^{(n)}\right] := \Lambda_a^{(n+1)} \circ (\Phi_{\mathrm{in}}^{(n)} \otimes \mathbb{1}_{\mathcal{A}_n\mathcal{B}_n}) \circ \cdots \circ \Lambda^{(2)} \circ (\Phi_{\mathrm{in}}^{(1)} \otimes \mathbb{1}_{\mathcal{A}_1\mathcal{B}_1}) \circ \Lambda^{(1)}, \tag{69}$$

$$\Lambda^{(i)} := (\Lambda'^{(i)} \otimes \mathbb{1}_{\mathcal{B}_i}) \circ (\Gamma^{(i)} \otimes \mathbb{1}_{\mathcal{A}_{i-1}}) \quad \forall i \in \{1, \cdots, n\}, \tag{70}$$

$$\Lambda_a^{(n+1)} := (\Lambda'^{(n+1)} \otimes \mathbb{1}_{\mathcal{B}_{n+1}}) \circ (\Gamma_a^{(n+1)} \otimes \mathbb{1}_{\mathcal{A}_n}), \tag{71}$$

where $\Gamma^{(1)}, \cdots, \Gamma^{(n)}$ and $\{\Gamma_a^{(n+1)}\}_a$ are quantum channels and a quantum instrument composing the quantum supersupermap $\{\mathcal{T}_a\}_a$ and $\Lambda'^{(1)}, \cdots, \Lambda'^{(n+1)}$ are quantum channels composing the unitary inversion quantum comb $\mathcal{C}'$ [see Eqs. (65) and (66)]. The supermap $\{\mathcal{C}_a\}_a$ implements isometry adjointation as shown in the following Theorem.

Theorem 5. *The sequential protocol shown in Fig. 3 (b) implements an isometry adjointation with the worst-case diamond-norm error given by*

$$\epsilon = \max\{\alpha_{C'}, 1 - F_{\mathrm{UI}}\}, \tag{72}$$

where $\alpha_{C'}$ is defined by

$$\alpha_{C'} := \mathrm{Tr}[\mathrm{Tr}_{\mathcal{F}}(C')\Sigma], \tag{73}$$

Σ is defined by

$$\Sigma := \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\mu \in \lambda + \square} \sum_{a,b=1}^{d_\lambda} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes \frac{(E_{a_\mu^\lambda b_\mu^\lambda}^{\mu,d})_{\mathcal{O}'^n\mathcal{P}'}}{m_\mu^{(d)}}, \tag{74}$$

and F_{UI} is the worst-case channel fidelity of the unitary inversion.

Proof sketch. We show that the probabilistic quantum comb $\{\mathcal{T}_I, \mathcal{T}_O\}$ derived in this section satisfies

$$T_I \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \approx \int_{\mathbb{U}(d)} \mathrm{d}U |UV_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle UV_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{P}'} \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n}, \tag{75}$$

where $\mathrm{d}U$ is the Haar measure of $\mathbb{U}(d)$. Then, Eq. (60) holds since

$$T_I \star C' \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \approx C' \star \int_{\mathbb{U}(d)} \mathrm{d}U |UV_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle UV_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{P}'} \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n} \tag{76}$$

$$\approx \int_{\mathbb{U}(d)} \mathrm{d}U |UV_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle UV_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{P}'} \star |U^{-1}\rangle\!\rangle\langle\!\langle U^{-1}|_{\mathcal{P}'\mathcal{F}} \tag{77}$$

$$= |V_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{F}}. \tag{78}$$

See Appendix A.2 for the detail. □

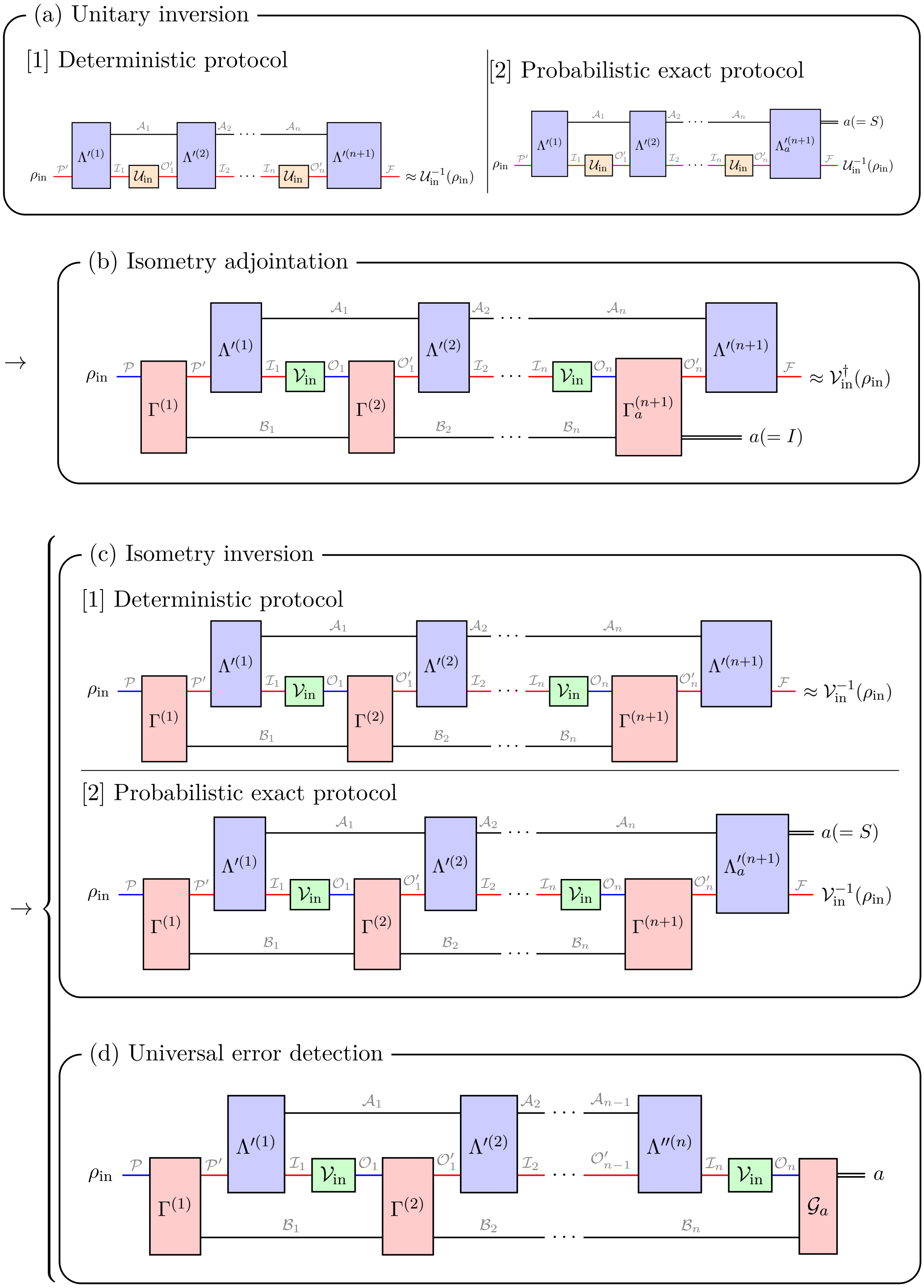


Figure 3: (a) Sequential protocols for deterministic and probabilistic exact unitary inversion. (b) A sequential isometry adjointation protocol is constructed by transforming the unitary inversion protocol using a quantum supersupermap. (c, d) Reduction to isometry inversion and universal error detection by discarding the measurement outcome and the output state of the isometry adjointation protocol, respectively.

3.2.2 Asymptotically optimal parallel protocol for isometry adjointation

We construct an asymptotically optimal parallel protocol for isometry adjointation by transforming the parallel protocol for unitary inversion. The optimal parallel protocol for deterministic unitary inversion is investigated in Ref. [29], which shows that the estimation-based protocol achieves the optimal worst-case channel fidelity among all parallel protocols. In the estimation-based unitary inversion protocol, one first estimates the input unitary operation U_{in} by applying U_{in} in parallel to a quantum state $\phi \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{A})$, and measure the output state by a POVM $\{M_i\} \subset \mathcal{L}(\mathcal{O}'^n \otimes \mathcal{A})$, where $\mathcal{A}$ is an auxiliary Hilbert space. We define the measurement channel $\{\mathcal{M}_i\}_i$ corresponding to the POVM $\{M_i\}$ defined by $\mathcal{M}_i(\cdot) \coloneqq \mathrm{Tr}(M_i \cdot)$. Then, one calculates the inverse operation $\mathcal{R}_i$ of the estimated unitary operation and applies $\mathcal{R}_i$ on the input quantum state ρ_{in}. This protocol can be expressed as [see Fig. 4 (a-1)]

$$\sum_i (\mathcal{R}_i \otimes \mathcal{M}_i)[\rho_{\text{in}} \otimes (\mathcal{U}_{\text{in}}^{\otimes n} \otimes \mathbb{1}_{\mathcal{A}})(\phi)] \approx \mathcal{U}_{\text{in}}^{-1}(\rho_{\text{in}}) \tag{79}$$

for all $U_{\text{in}} \in \mathbb{U}(d)$ and $\rho_{\text{in}} \in \mathcal{L}(\mathbb{C}^d)$. The worst-case channel fidelity of the unitary inversion is the same as the entanglement fidelity of the unitary estimation protocol given by

$$F_{\text{est}} \coloneqq \inf_{U_{\text{in}} \in \mathbb{U}(d)} F_{\text{ch}}[\mathcal{E}_{U_{\text{in}}}, \mathcal{U}_{\text{in}}]. \tag{80}$$

Here, $\mathcal{E}_{U_{\text{in}}}$ is the measure-and-prepare channel defined by

$$\mathcal{E}_{U_{\text{in}}} \coloneqq \sum_i p(\hat{U}_i | U_{\text{in}}) \hat{\mathcal{U}}_i, \tag{81}$$

where $p(\hat{U}_i | U_{\text{in}})$ is the probability to estimate the input unitary operation U_{in} as $\hat{U}_i$. The optimal estimation is shown to be done with the covariant protocol [55], satisfying

$$p(U' \hat{U}_i U'' | U' U_{\text{in}} U'') = p(\hat{U}_i | U_{\text{in}}) \quad \forall U', U'' \in \mathbb{U}(d). \tag{82}$$

By transforming the estimation-based protocol (79) using the covariant unitary estimation as shown in Eq. (60), we obtain an isometry adjointation protocol given by [see Fig. 4 (b)]

$$\mathcal{C}_a[\mathcal{V}_{\text{in}}^{\otimes n}](\rho_{\text{in}}) \coloneqq \sum_i (\mathcal{R}_i \otimes \mathcal{M}_i) \circ (\Psi_a \otimes \mathbb{1}_{\mathcal{A}})[\rho_{\text{in}} \otimes (\mathcal{V}_{\text{in}}^{\otimes n} \otimes \mathbb{1}_{\mathcal{A}})(\phi)] \tag{83}$$

for all $a \in \{I, O\}$, $V_{\text{in}} \in \mathbb{V}_{\text{iso}}(d, D)$ and $\rho_{\text{in}} \in \mathcal{L}(\mathbb{C}^D)$, where $\Psi_a : \mathcal{L}(\mathcal{O}^n \otimes \mathcal{P}) \to \mathcal{L}(\mathcal{O}'^n \otimes \mathcal{P}')$ is a quantum instrument implemented by Algorithm 1. The approximation error ϵ of isometry adjointation is given in the following Theorem.

Theorem 6. *The parallel protocol shown in Fig. 4 (b) implements an isometry adjointation with the worse-case diamond-norm error given by*

$$\epsilon = \max\{\alpha_\phi, 1 - F_{\text{est}}\}, \tag{84}$$

where α_ϕ is defined by

$$\alpha_\phi \coloneqq \sum_{\lambda \in \mathbb{Y}_n^d} \mathrm{Tr}\left[\mathrm{Tr}_{\mathcal{A}}(\phi) \Pi_\lambda^{(d)}\right] \sum_{\mu \in \lambda \cap \square \cap \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} \tag{85}$$

$$= \sum_{\lambda \in \mathbb{Y}_n^d} \mathrm{Tr}\left[\mathrm{Tr}_{\mathcal{A}}(\phi) \Pi_\lambda^{(d)}\right] \left[1 - \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)}\right], \tag{86}$$

$\mathrm{hook}(\mu)$ *is defined by Eq. (52), and F_{est} is the entanglement fidelity of the covariant unitary estimation.*

Algorithm 1 Implementation of the quantum instrument $\{\Psi_a\}_a$ utilized in the parallel protocol (83) for isometry adjointation.

```
Input: Quantum state $\rho_{\text{in}} \in \mathcal{L}(\mathbb{C}^D)^{\otimes n+1}$
Output: Quantum state $\rho_{\text{out}} \in \mathcal{L}(\mathbb{C}^d)^{\otimes n+1}$ with a measurement outcome $a \in \{I, O\}$
Apply the quantum Schur transform $V_{\text{Sch}}$ on the input quantum state $\rho_{\text{in}}$.
Measure the Young diagram register to obtain the measurement outcome $\mu$.
Trace out the unitary group register.
Let $\tau_\mu \in \mathcal{L}(\mathcal{S}_\mu)$ be the quantum state in the symmetric group register.
if $\mu \in \mathbb{Y}^d_{n+1}$ then
    $a \leftarrow I$.
    Prepare a quantum state $|\mu\rangle\langle\mu| \otimes \mathbb{1}_{\mathcal{U}^{(d)}_\mu}/m^{(d)}_\mu$.
    Apply the inverse quantum Schur transform $V^\dagger_{\text{Sch}}$ on the joint state $|\mu\rangle\langle\mu| \otimes \mathbb{1}_{\mathcal{U}^{(d)}_\mu}/m^{(d)}_\mu \otimes \tau_\mu$ to obtain the output quantum state $\rho_{\text{out}}$.
else
    $a \leftarrow O$.
    Trace out the quantum state $\tau_\mu \in \mathcal{L}(\mathcal{S}_\mu)$.
    $\rho_{\text{out}} \leftarrow \mathbb{1}_d^{\otimes n+1}/d^{n+1}$.
end if
return $\rho_{\text{out}}, a$
```

Proof. See Appendix A.3 for the proof. □

For $d = 2$, one can utilize the maximum-likelihood qubit-unitary estimation presented in Refs. [55–57] to achieve

$$\epsilon = \frac{6.2287}{n} + O(n^{-2}). \tag{87}$$

For a higher dimension $d > 2$, we can utilize the unitary estimation presented in Ref. [14] to achieve the following scaling:

$$\begin{aligned}\epsilon &= \frac{3\ln 2}{2}\frac{d^2}{n} + O(d^4 n^{-2}, dn^{-1}) &(88)\\ &= 1.0397\frac{d^2}{n} + O(d^4 n^{-2}, dn^{-1}). &(89)\end{aligned}$$

See Appendix B.3 for the details. As shown later (Theorem 14), these protocols achieve the asymptotically optimal worse-case diamond-norm error $\epsilon = \Theta(d^2/n)$.

3.3 Reduction to isometry inversion and universal error detection

By discarding the measurement outcome from the isometry adjointation protocols, we obtain deterministic isometry inversion protocols shown in Figs. 3 (c-1) and 4 (c-1), which are given by replacing $\Gamma_a^{(n+1)}$ and Ψ_a in the original isometry adjointation protocols with $\Gamma^{(n+1)} := \sum_a \Gamma_a^{(n+1)}$ and $\Psi := \sum_a \Psi_a$, respectively. The worst-case channel fidelity of the derived isometry inversion protocol is shown to be the same as the original unitary inversion protocol (see Appendix A.4.1). By replacing the original unitary inversion protocol with the probabilistic exact one, we obtain the probabilistic exact isometry inversion protocols as shown in Figs. 3 (c-2), 4 (c-2). The parallel protocol for probabilistic exact isometry inversion is the same as that shown in Ref. [35]. The derived protocols achieve the same

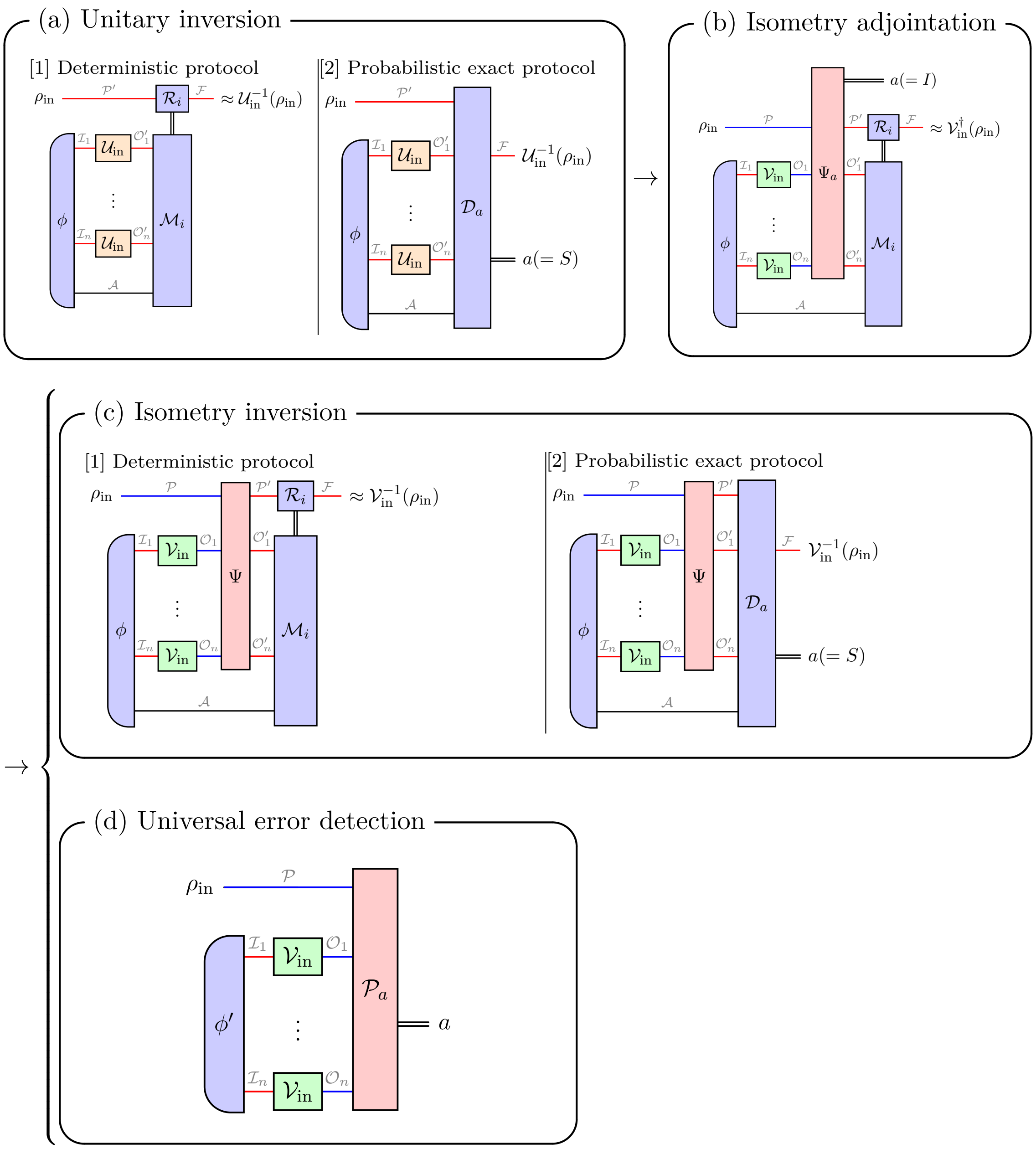

(a) Unitary inversion
[1] Deterministic protocol
ρ_{in}
$\mathcal{P}'$
$\mathcal{R}_i$
$\mathcal{F}$
$\approx \mathcal{U}_{\mathrm{in}}^{-1}(\rho_{\mathrm{in}})$
$\mathcal{I}_1$
$\mathcal{U}_{\mathrm{in}}$
$\mathcal{O}'_1$
ϕ
$\mathcal{M}_i$
$\mathcal{I}_n$
$\mathcal{O}'_n$
$\mathcal{A}$
[2] Probabilistic exact protocol
$\mathcal{D}_a$
$\mathcal{U}_{\mathrm{in}}^{-1}(\rho_{\mathrm{in}})$
$a(= S)$
(b) Isometry adjointation
$a(= I)$
$\mathcal{P}$
Ψ_a
$\approx \mathcal{V}_{\mathrm{in}}^{\dagger}(\rho_{\mathrm{in}})$
$\mathcal{V}_{\mathrm{in}}$
$\mathcal{O}_1$
$\mathcal{O}_n$
(c) Isometry inversion
[1] Deterministic protocol
Ψ
$\approx \mathcal{V}_{\mathrm{in}}^{-1}(\rho_{\mathrm{in}})$
[2] Probabilistic exact protocol
$\mathcal{V}_{\mathrm{in}}^{-1}(\rho_{\mathrm{in}})$
(d) Universal error detection
ϕ'
$\mathcal{P}_a$
a

Figure 4: (a) [1] The estimation-based protocol using covariant unitary estimation achieves the optimal protocol for deterministic unitary inversion among all parallel protocols. [2] The delayed input-state protocol achieves the optimal protocol for probabilistic exact unitary inversion among parallel protocols. (b) A parallel isometry adjointation protocol is constructed by transforming the unitary inversion protocol using the quantum supersupermap. (c, d) Reduction to isometry inversion and universal error detection by discarding the measurement outcome and the output state of the isometry adjointation protocol, respectively.

success probability as the untiary inversion protocol (see Appendix A.4.2). In conclusion, we obtain the following Corollary.

Corollary 7. *Suppose there exists a parallel or sequential protocol for probabilistic exact (deterministic) d-dimensional unitary inversion achieving success probability p_{UI} (average-case channel fidelity F_{UI}) using n calls of $U_{\mathrm{in}} \in \mathbb{U}(d)$. Then, we can construct a parallel protocol for probabilistic exact (deterministic) isometry inversion for $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ achieving success probability $p = p_{\mathrm{UI}}$ (worst-case channel fidelity $F = F_{\mathrm{UI}}$) using n calls of $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$.*

Reference [30] shows a deterministic exact sequential protocol for qubit-unitary inversion using four calls of the input qubit-unitary operation $U_{\mathrm{in}} \in \mathbb{U}(2)$. Combining this protocol with Theorem 7, we can construct a deterministic exact sequential protocol for qubit-encoding isometry inversion using four calls of the input qubit-encoding isometry operation $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(2, D)$ for any $D \geq 2$.

By discarding the output state from the isometry adjointation protocols, we obtain universal error detection protocols shown in Figs. 3 (d) and 4 (d). The sequential protocol shown in Fig. 3 (d) is obtained by discarding $\Lambda''^{(n+1)}$ in the original isometry adjointation protocol and replacing $\Gamma_a^{(n+1)}$ and $\Lambda'^{(n)}$ with the POVM measurement $\mathcal{G}_a := \mathrm{Tr} \circ \Gamma_a^{(n+1)}$ and the quantum channel $\Lambda''^{(n)} := \mathrm{Tr}_{\mathcal{A}_n} \circ \Lambda'^{(n)}$, respectively. The parallel protocol shown in Fig. 4 (d) is obtained by discarding $\mathcal{R}_i$ and M_i in the original isometry adjointation protocol, and replacing ϕ and Ψ_a with the quantum state $\phi' := \mathrm{Tr}_{\mathcal{A}}(\phi)$ and the POVM measurement $\mathcal{P}_a := \mathrm{Tr} \circ \Psi_a$, respectively. The approximation errors of the derived protocols are shown in the following Corollary (see Appendix A.4.3).

Corollary 8. *The sequential and parallel protocols shown in Figs. 3 (d) and 4 (d) implement a universal error detection with the approximation errors $\alpha^{(x)}$ for $x = \mathrm{SEQ}$ (sequential protocol) and $x = \mathrm{PAR}$ (parallel protocol) given by*

$$\alpha^{(\mathrm{SEQ})} = \mathrm{Tr}(C''\Sigma'), \tag{90}$$

$$\alpha^{(\mathrm{PAR})} = \sum_{\lambda \in \mathbb{Y}_n^d} \mathrm{Tr}\left(\phi' \Pi_\lambda^{(d)}\right) \sum_{\mu \in \lambda + \square \cap \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} \tag{91}$$

$$= \sum_{\lambda \in \mathbb{Y}_n^d} \mathrm{Tr}\left(\phi' \Pi_\lambda^{(d)}\right) \left[1 - \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)}\right], \tag{92}$$

where C'' is the Choi operator of the quantum comb given by $C'' := J_{\Lambda'(1)} \star J_{\Lambda'(2)} \star \cdots \star J_{\Lambda''(n)}$, Σ' is defined by $\Sigma' := \mathrm{Tr}_{\mathcal{O}_n'} \Sigma$ using Σ defined in Eq. (74), and ϕ' is a quantum state shown in the protocol 4 (d).

3.4 Relationship to programmable projective measurement

Reference [4] considers a task to construct a projective measurement $\{|\psi\rangle\langle\psi|, \mathbb{1} - |\psi\rangle\langle\psi|\}$ from n copies of an unknown quantum state $|\psi\rangle \in \mathbb{C}^D$. The task is to construct a measurement $\{\Pi_I, \Pi_O\}$ such that

$$\mathrm{Tr}(\Pi_I |\psi\rangle\langle\psi|) = 1, \tag{93}$$

$$\mathrm{Tr}\left(\Pi_I \left|\psi^\perp\right\rangle\left\langle\psi^\perp\right|\right) = \alpha \quad (\forall \left|\psi^\perp\right\rangle \perp |\psi\rangle). \tag{94}$$

This task can be considered as a special case ($d = 1$) of universal error detection. Reference [4] shows that the optimal failure probability is given by

$$\alpha = \frac{1}{n+1}. \tag{95}$$

The optimal success probability is achieved by a protocol shown in Fig. 5, where $\mathcal{M} = \{M_I, M_O\}$ is a POVM defined by $M_I = \Pi_{\mathrm{sym}}$ and $M_O = \mathbb{1} - \Pi_{\mathrm{sym}}$, where Π_{sym} is an orthonormal projector onto the totally symmetric subspace of $(\mathbb{C}^D)^{\otimes n+1}$. This protocol corresponds to the universal error detection protocol for $d = 1$. The universal error detection protocol is a generalization of programmable projective measurement for rank-d (destructive) projective measurement given by $\{\Pi_{\mathrm{Im}V_{\mathrm{in}}}, \mathbb{1} - \Pi_{\mathrm{Im}V_{\mathrm{in}}}\}$ using an isometry operator $V_{\mathrm{in}} : \mathbb{C}^d \to \mathbb{C}^D$. In particular, the parallel protocol shown in Fig. 4 (d) can be regarded as an implementation of the rank-d projective measurement using a program state $\mathcal{V}_{\mathrm{in}}^{\otimes n}(\phi')$.

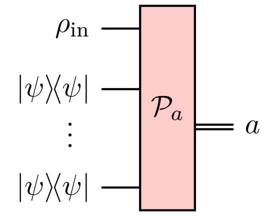


Figure 5: Optimal protocol for programmable projective measurement shown in Ref. [4].

4 Analysis of the optimal protocols

In Section 4.1, we reintroduce the Choi operator of the quantum supermap to describe the general superinstrument that is not implementable by the quantum circuit. We show that the optimal protocols for isometry adjointation, isometry inversion, and universal error detection can be found in the Choi operators satisfying the unitary group symmetry. We utilize the unitary group symmetry to investigate the optimal performances analytically in Section 4.2 and numerically in Section 4.3.

4.1 Choi representation of general superinstruments and $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry of the tasks

Similarly to Eq. (32) for a sequential protocol, a general superchannel $\mathcal{C} : \bigotimes_{i=1}^n [\mathcal{L}(\mathcal{I}_i) \to \mathcal{L}(\mathcal{O}_i)] \to [\mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{F})]$ can be represented in the Choi operator C satisfying

$$J_{\mathcal{C}[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}]} = C \star \bigotimes_{i=1}^{n} J_{\Phi_{\mathrm{in}}^{(i)}}, \tag{96}$$

where J_Φ is the Choi operator of a quantum channel Φ, and $C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ is the Choi operator of $\mathcal{C}$. The set of superchannels implemented by parallel ($x = \mathrm{PAR}$) and sequential ($x = \mathrm{SEQ}$) protocols, and the set of general superchannel ($x = \mathrm{GEN}$) can be characterized by the positivity and linear conditions on C as

$$C \geq 0, \tag{97}$$

$$C \in \mathcal{W}^{(x)}, \tag{98}$$

where $\mathcal{W}^{(x)}$ is a linear subspace of $\mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ [see Appendix E.1 for the definition of $\mathcal{W}^{(x)}$]. The case $x = \mathrm{SEQ}$ corresponds to Theorem 1. A general superinstrument $\mathcal{C}_a : \bigotimes_{i=1}^n [\mathcal{L}(\mathcal{I}_i) \to \mathcal{L}(\mathcal{O}_i)] \to [\mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{F})]$ can also be represented in the Choi operator C_a satisfying

$$J_{\mathcal{C}_a[\Phi_{\mathrm{in}}^{(1)} \otimes \cdots \otimes \Phi_{\mathrm{in}}^{(n)}]} = C_a \star \bigotimes_{i=1}^{n} J_{\Phi_{\mathrm{in}}^{(i)}}. \tag{99}$$

The set of superinstruments implemented by parallel ($x = \mathrm{PAR}$) and sequential ($x = \mathrm{SEQ}$) protocols, and the set of general superinstrument ($x = \mathrm{GEN}$) can be characterized by the positivity and linear conditions on $C := \sum_a C_a$ as

$$C_a \geq 0, \tag{100}$$

$$C := \sum_a C_a \in \mathcal{W}^{(x)}. \tag{101}$$

The case $x = \mathrm{SEQ}$ corresponds to Theorem 2.

The protocols for isometry inversion, universal error detection, and isometry adjointation can be represented by the Choi operators of the corresponding superchannel or superinstrument given by

$$\begin{cases} C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}) & \text{(deterministic isometry inversion)} \\ \{C_S, C_F\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}) & \text{(probabilistic exact isometry inversion)} \\ \{C_I, C_O\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P}) & \text{(universal error detection)} \\ \{C_I, C_O\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}) & \text{(isometry adjointation)} \end{cases}. \tag{102}$$

The optimization of the Choi operators can be done under the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry as shown in the following Theorem.

Theorem 9. *The optimal performances of isometry inversion, universal error detection, and isometry adjointation can be searched within Choi operators satisfying*

$$\begin{cases} [C, U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & & \text{(deterministic isometry inversion)} \\ [C_a, U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & \forall a \in \{S, F\} & \text{(probabilistic exact isometry inversion)} \\ [C_a, U'^{\otimes n}_{\mathcal{I}^n} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & \forall a \in \{I, O\} & \text{(universal error detection)} \\ [C_a, U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & \forall a \in \{I, O\} & \text{(isometry adjointation)} \end{cases} \tag{103}$$

for all $U' \in \mathbb{U}(d)$ and $U'' \in \mathbb{U}(D)$.

Proof. See Appendix B.1 for the proof. □

4.2 Optimal construction of isometry inversion, universal error detection, and isometry adjointation protocols

We show that the construction of parallel or sequential protocols of isometry adjointation, isometry inversion, and universal error detection are the optimal, as shown in the following Theorem.

Theorem 10. *The parallel or sequential protocols for probabilistic exact isometry inversion, deterministic isometry inversion, universal error detection, and isometry adjointation shown in Theorems 5 and 6 and Corollaries 7 and 8 achieve the optimal performances among all parallel or sequential protocols, respectively.*

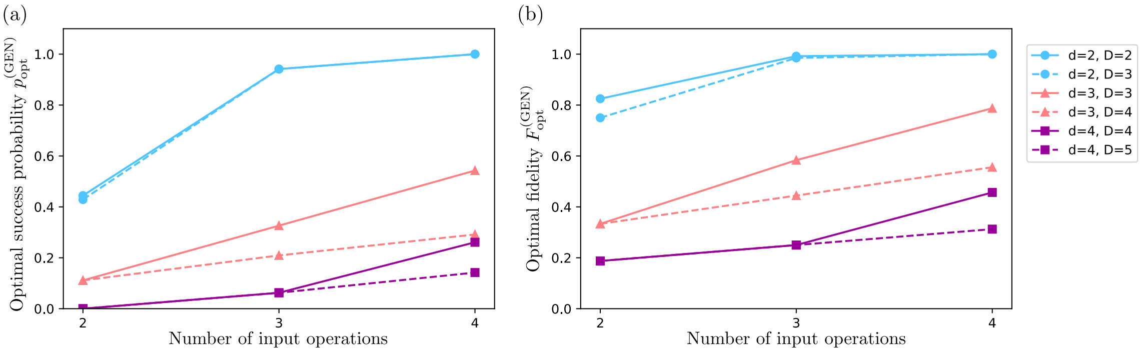


Figure 6: (a) Optimal success probability $p_{\rm opt}^{\rm (GEN)}$ and (b) optimal worst-case channel fidelity $F_{\rm opt}^{\rm (GEN)}$ of isometry inversion among general protocols including indefinite causal order. Solid lines represent the case $D = d$ (unitary inversion), and dashed lines represent the case $D = d+1$ for $d = 2$ (●), $d = 3$ (▲), and $d = 4$ (■). The optimal values shown here are obtained by numerical calculations, and numerical values are shown in Appendix D.

Proof. See Appendix C for the proof. □

Since the figure of merits shown in Theorems 5 and 6 and Corollaries 7 and 8 do not depend on D, we can show that the optimal performances do not depend on D.

Corollary 11. *For $D > d$ and $x \in \{\rm PAR, SEQ\}$, the following relations hold:*

$$\epsilon_{\rm opt}^{(x)}(d, D, n) = \epsilon_{\rm opt}^{(x)}(d, d+1, n), \tag{104}$$

$$F_{\rm opt}^{(x)}(d, D, n) = F_{\rm opt}^{(x)}(d, d, n), \tag{105}$$

$$p_{\rm opt}^{(x)}(d, D, n) = p_{\rm opt}^{(x)}(d, d, n), \tag{106}$$

$$\alpha_{\rm opt}^{(x)}(d, D, n) = \alpha_{\rm opt}^{(x)}(d, d+1, n). \tag{107}$$

Using Theorem 10, we analyze the optimal protocols for isometry inversion, universal error detection, and isometry adjointation in the following subsections.

4.2.1 Isometry inversion

The optimal success probability and fidelity of isometry inversion are given by those of unitary inversion when we use parallel or sequential protocols, as shown in Corollary 11. It is already shown in Ref. [35] for the parallel protocol, but the sequential protocol case is newly shown in this work, which is conjectured in Ref. [35].

To investigate the generalization of Corollary 11 for general protocols including indefinite causal order, we calculate the optimal probability or worst-case channel fidelity numerically (see Section 4.3 for the detail). Numerical results show that a similar equation does not hold for general protocols including indefinite causal order, i.e., $p_{\rm opt}^{\rm (GEN)}(d, D, n) < p_{\rm opt}^{\rm (GEN)}(d, d, n)$ or $F_{\rm opt}^{\rm (GEN)}(d, D, n) < F_{\rm opt}^{\rm (GEN)}(d, d, n)$ hold for some cases (see Fig. 6). This behavior is compatible with the fact that the composition of a general quantum supermap with a quantum comb does not yield a valid quantum supermap in general [58], so the construction of isometry inversion protocols shown in Fig. 3 (c) cannot be applied for general protocols.

4.2.2 Universal error detection

The optimal performance of parallel protocol $\alpha_{\rm opt}^{\rm (PAR)}(d, D, n)$ is given as follows.

Theorem 12.

$$\alpha_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) = \frac{1}{d+k+1}\left(d + \frac{d-l}{d+k-l}\right) = \frac{d^2}{n} + O(d^2 n^{-2}), \tag{108}$$

where k and l are given by $n = kd + l$ ($k \in \mathbb{Z}, 0 \leq l < d$).

Proof. See Appendix B.2 for the proof. □

From Theorem 12 and the result in Ref. [4], we can show the following property on the scaling of $\alpha_{\mathrm{opt}}^{(x)}(d,D,n)$ with respect to n.

Corollary 13.

$$\alpha_{\mathrm{opt}}^{(x)}(d,D,n) = \Theta(n^{-1}) \quad \forall D > d, \forall x \in \{\mathrm{PAR}, \mathrm{SEQ}, \mathrm{GEN}\} \tag{109}$$

holds for an arbitrary fixed value of d.

Proof. From Theorem 12, we obtain

$$\alpha_{\mathrm{opt}}^{(x)}(d,D,n) \leq \alpha_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) = O(n^{-1}). \tag{110}$$

The Hilbert space $\mathbb{C}^D$ can be embedded onto $\mathbb{V}_{\mathrm{iso}}(d,D)$ by identifying $|\psi\rangle \in \mathbb{C}^D$ with $V = |\psi\rangle\langle 0| + \sum_{i=1}^{d-1} |\psi_i\rangle\langle i| \in \mathbb{V}_{\mathrm{iso}}(d,D)$ for a set of orthonormal vectors $\{|\psi_i\rangle\}_{i=1}^{d-1}$ satisfying $\langle\psi_i|\psi\rangle = 0$ for all $i \in \{1,\cdots,d-1\}$. Therefore, a universal error detection protocol for $V \in \mathbb{V}_{\mathrm{iso}}(d,D)$ can simulate a programmable projective measurement for $|\psi\rangle \in \mathbb{C}^D$, which leads to

$$\alpha_{\mathrm{opt}}^{(x)}(d,D,n) \geq \frac{1}{n+1} = \Omega(n^{-1}). \tag{111}$$

Thus, we obtain $\alpha_{\mathrm{opt}}^{(x)}(d,D,n) = \Theta(n^{-1})$. □

4.2.3 Isometry adjointation

The optimal scaling of the approximation error of parallel isometry adjointation is given as follows.

Theorem 14.

$$\epsilon_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) = \Theta(d^2 n^{-1}). \tag{112}$$

Proof. First, $\epsilon_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) \geq \alpha_{\mathrm{opt}}^{(\mathrm{PAR})}$ holds since any isometry adjointation protocol can be transformed to an error detection protocol by discarding the output state of an isometry adjointation protocol. Thus, we obtain $\epsilon_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) = \Omega(d^2 n^{-1})$ from Theorem 12. On the other hand, from the construction shown in Section 3.2.2, we see that $\epsilon_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) = O(d^2 n^{-1})$ (see Appendix B.3). Thus, we obtain $\epsilon_{\mathrm{opt}}^{(\mathrm{PAR})}(d,D,n) = \Theta(d^2 n^{-1})$. □

4.3 Numerical results for the optimal protocols

From numerical calculations, we investigate the optimal protocols for isometry inversion, universal error detection, and isometry adjointation. We represent the protocols implementing isometry inversion, universal error detection, and isometry adjointation by their Choi operators and formulate the optimization of the figure of merits within the possible protocols as SDP. We utilize a $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry of the Choi operator (Theorem 9) to simplify the SDP, which is a similar technique presented in Ref. [30] (see also Ref. [59]). See Appendix E for the details of the derivation of the SDP. We calculate the derived SDP in MATLAB [60] using the interpreter CVX [61, 62] with the solvers SDPT3 [63–65], SeDuMi [66] and MOSEK [67]. Group-theoretic calculations to write down the SDP are done with SageMath [68]. See Appendix D for the numerical results. All codes are available at Ref. [69] under the MIT license [70].

The optimal performances for parallel or sequential protocols are calculated for the case of $D = d + 1$ since they do not depend on D (see Corollary 11), which is shown by the construction of protocols shown in Figs. 3 and 4. Although the same construction is impossible for general protocols including indefinite causal order, we also see that the optimal performances for general protocols do not depend on D as long as $D \geq d + 1$ holds by checking the values for $D = d + 1, \cdots, d + 10$. However, the maximum success probability (channel fidelity) of probabilistic exact (deterministic) isometry inversion for the case of $D = d$ (unitary inversion) is different from those for the case of $D = d + 1$ (isometry inversion), as shown in Tables 5 and 6 (corresponding to Fig. 6 in Section 4.2.1). We also see the advantage of indefinite causal order over sequential protocols in isometry inversion and universal error detection, but the advantage disappears in the case of isometry adjointation.

5 Conclusion

In this work, we investigate the universal transformation of isometry operations to explore the possible transformation in higher-order quantum computation. We define the task called isometry adjointation, which is to transform the isometry operation into its adjoint operation. The isometry adjointation protocol is constructed by transforming the unitary inversion protocol using the probabilistic quantum comb $\{\mathcal{T}_I, \mathcal{T}_O\}$. Using the idea of composition of quantum combs, the problem of designing isometry adjointation protocol reduces to designing a unitary inversion protocol, which is extensively studied in previous works [10, 25–33]. In special cases, the isometry adjointation reduces to unitary inversion (transformation of unitary operations) and programmable projective measurement (transformation of pure states). Due to such reducibility, isometry adjointation is a useful task to understand the difference between higher-order quantum computation and "lower-order" quantum computation (i.e., transformation of states), which are exhibited in several examples such as distinguishability [71] and superreplication [17, 18, 72], under a unified formulation. We also construct isometry inversion and universal error detection protocols by discarding measurement outcome and output quantum state, respectively. We show that our construction gives the optimal performances among all parallel or sequential protocols, which implies that the optimal performances among parallel or sequential protocols do not depend on the output dimension D of the isometry operation. We analyze the optimal performances of isometry adjointation and show that the optimal approximation error ϵ of the parallel isometry adjointation protocol is given by $\epsilon = \Theta(d^2 n^{-1})$, where d is the input dimension of the isometry operation, and n is the number of calls of the input operation.

To investigate the general protocols including indefinite causal order, we also provide the numerical results for the optimal performances of isometry adjointation, isometry inversion, and universal error detection using the semidefinite programming combined with the unitary group symmetry. The optimal performances of probabilistic exact (deterministic) unitary inversion ($D = d$) are different from those of isometry inversion ($D \geq d+1$), which is compatible with the impossibility of the composition of a general supermap with a quantum comb. However, numerical results also show that the optimal performances of isometry adjointation and universal error detection using the general protocol do not depend on D. We also see the advantage of indefinite causal order protocols over sequential protocols in isometry inversion and universal error detection, but the advantage disappears in isometry adjointation.

Acknowledgments

We acknowledge M. Studziński, T. Młynik, M. T. Quintino, M. Ozols, D. Grinko, P. Taranto, and M. Koashi for valuable discussions. We also thank T. J. Volkoff for pointing out a typographical error in the previous manuscript. This work was supported by MEXT Quantum Leap Flagship Program (MEXT QLEAP) JPMXS0118069605, JPMXS0120351339, Japan Society for the Promotion of Science (JSPS) KAKENHI Grants No. 18K13467, 21H03394, 23KJ0734, FoPM, WINGS Program, the University of Tokyo, DAIKIN Fellowship Program, the University of Tokyo, and IBM-UTokyo lab. This work was also supported by JST Moonshot R&D Grant Number JPMJMS226C.

A Construction of isometry adjointation protocols

A.1 Proof of Lemma 4

By definition of $E_{ij}^{\mu,d}$ given in Eq. (54), T_I and T_O can be written as

$$T_I = \sum_{\mu_{n+1}\in\mathbb{Y}_{n+1}^d} \frac{\mathbb{1}_{\mathcal{U}_{\mu_{n+1}}^{(d)}} \otimes \mathbb{1}_{\mathcal{U}_{\mu_{n+1}}^{(D)}} \otimes |\phi_{\mu_{n+1}}\rangle\langle\phi_{\mu_{n+1}}|_{\mathcal{S}_{\mu_{n+1}}\mathcal{S}_{\mu_{n+1}}}}{m_{\mu_{n+1}}^{(d)}}, \tag{113}$$

$$T_O = \sum_{t=d}^{n} \sum_{\substack{\mu_{n+1}\in\cdots\in\mu_t \\ \mu_t\in\mathbb{Y}_t^d, \mu_{t+1}\notin\mathbb{Y}_{t+1}^d}} \frac{\mathbb{1}_{\mathcal{U}_{\mu_t}^{(d)}} \otimes \mathbb{1}_{\mathcal{O}'_t\cdots\mathcal{O}'_n} \otimes \mathbb{1}_{\mathcal{U}_{\mu_{n+1}}^{(D)}} \otimes |\phi_{\mu_{t+1}\cdots\mu_{n+1}}^{\mu_t}\rangle\langle\phi_{\mu_{t+1}\cdots\mu_{n+1}}^{\mu_t}|_{\mathcal{S}_{\mu_t}\mathcal{S}_{\mu_{n+1}}}}{d^{n+1-t} m_{\mu_t}^{(d)}}, \tag{114}$$

where $|\phi_{\mu_{n+1}}\rangle$ and $|\phi_{\mu_{t+1}\cdots\mu_{n+1}}^{\mu_t}\rangle$ are defined by

$$|\phi_{\mu_{n+1}}\rangle := \sum_{m=1}^{d_{\mu_{n+1}}} |\mu_{n+1}, m\rangle_{\mathcal{S}_{\mu_{n+1}}} \otimes |\mu_{n+1}, m\rangle_{\mathcal{S}_{\mu_{n+1}}}, \tag{115}$$

$$\left|\phi_{\mu_{t+1}\cdots\mu_{n+1}}^{\mu_t}\right\rangle := \sum_{a=1}^{d_{\mu_t}} |\mu_t, a\rangle_{\mathcal{S}_{\mu_t}} \otimes \left|\mu_{n+1}, a_{\mu_{t+1}\cdots\mu_{n+1}}^{\mu_t}\right\rangle_{\mathcal{S}_{\mu_{n+1}}}. \tag{116}$$

Therefore, $T_I \geq 0$ and $T_O \geq 0$ hold.

We next show Eq. (64) by redefining operators $T_I^{(i)}, T_O^{(i)} \in \mathcal{L}(\mathcal{P}' \otimes \mathcal{O}'^{i-1} \otimes \mathcal{P} \otimes \mathcal{O}^{i-1})$

for $i \in \{1, \cdots, n+1\}$ by

$$T_I^{(i)} := \sum_{\mu_i \in \mathbb{Y}_i^d} \sum_{m,n=1}^{d_{\mu_i}} \frac{(E_{mn}^{\mu_i,d})_{\mathcal{P}'\mathcal{O}'^{i-1}} \otimes (E_{mn}^{\mu_i,D})_{\mathcal{P}\mathcal{O}^{i-1}}}{m_{\mu_i}^{(d)}}, \tag{117}$$

$$T_O^{(i)} := \sum_{t=d}^{i-1} \sum_{\substack{\mu_i \in \cdots \in \mu_t \\ \mu_t \in \mathbb{Y}_t^d, \mu_{t+1} \notin \mathbb{Y}_{t+1}^d}} \sum_{a,b=1}^{d_{\mu_t}} \frac{(E_{ab}^{\mu_t,d})_{\mathcal{P}'\mathcal{O}'^{t-1}} \otimes \mathbb{1}_{\mathcal{O}'_t \cdots \mathcal{O}'_{i-1}} \otimes (E^{\mu_i,D}_{a^{\mu_t}_{\mu_{t+1}\cdots\mu_i} b^{\mu_t}_{\mu_{t+1}\cdots\mu_i}})_{\mathcal{P}\mathcal{O}^{i-1}}}{d^{i-t} m_{\mu_t}^{(d)}}, \tag{118}$$

which correspond to $T_I = T_O^{(n+1)}$ and $T_O = T_O^{(n+1)}$ for T_I, T_O defined in Eqs. (61) and (62). We show that $T_I^{(i)}, T_O^{(i)}$ defined in Eqs. (117) and (118) satisfy Eq. (64).

When $i = 1$, $T^{(1)}$ is given by

$$T^{(1)} = \frac{\mathbb{1}_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{P}'}}{d}. \tag{119}$$

Thus, $\mathrm{Tr}_{\mathcal{P}'} T^{(1)} = \mathbb{1}_{\mathcal{P}} = T^{(0)} \otimes \mathbb{1}_{\mathcal{P}}$ holds.

When $i > 1$, $T^{(i)}$ decomposes into three parts:

$$T^{(i)} = T_I^{(i)} + T_{t=i-1}^{(i)} + T_{d \leq t < i-1}^{(i)}, \tag{120}$$

where $T_{t=i-1}^{(i)}$ and $T_{d \leq t < i-1}^{(i)}$ are defined by

$$T_{t=i-1}^{(i)} := \sum_{\substack{\mu_i \in \mu_{i-1} \\ \mu_{i-1} \in \mathbb{Y}_{i-1}^d, \mu_i \notin \mathbb{Y}_i^d}} \sum_{a,b=1}^{d_{\mu_{i-1}}} \frac{(E_{ab}^{\mu_{i-1},d})_{\mathcal{P}'\mathcal{O}'^{i-2}} \otimes \mathbb{1}_{\mathcal{O}'_{i-1}} \otimes (E^{\mu_i,D}_{a^{\mu_{i-1}}_{\mu_i} b^{\mu_{i-1}}_{\mu_i}})_{\mathcal{P}\mathcal{O}^{i-2}}}{d m_{\mu_{i-1}}^{(d)}}, \tag{121}$$

$$\begin{aligned} &T_{d \leq t < i-1}^{(i)} \\ &:= \sum_{t=d}^{i-2} \sum_{\substack{\mu_i \in \cdots \in \mu_t \\ \mu_t \in \mathbb{Y}_t^d, \mu_{t+1} \notin \mathbb{Y}_{t+1}^d}} \sum_{a,b=1}^{d_{\mu_t}} \frac{(E_{ab}^{\mu_t,d})_{\mathcal{P}'\mathcal{O}'^{t-1}} \otimes \mathbb{1}_{\mathcal{O}'_t \cdots \mathcal{O}'_{i-1}} \otimes (E^{\mu_i,D}_{a^{\mu_t}_{\mu_{t+1}\cdots\mu_i} b^{\mu_t}_{\mu_{t+1}\cdots\mu_i}})_{\mathcal{P}\mathcal{O}^{i-1}}}{d^{i-t} m_{\mu_t}^{(d)}}. \end{aligned} \tag{122}$$

Partial traces of $T_I^{(i)}$, $T_{t=i-1}^{(i)}$ and $T_{d \leq t < i-1}^{(i)}$ over the subsystem $\mathcal{O}'_{i-1}$ are obtained as follows:

$$\mathrm{Tr}_{\mathcal{O}'_{i-1}} T_I^{(i)} = \sum_{\substack{\mu_i \in \mu_{i-1} \\ \mu_i \in \mathbb{Y}_i^d}} \sum_{a,b=1}^{d_{\mu_{i-1}}} \frac{(E_{ab}^{\mu_{i-1},d})_{\mathcal{P}'\mathcal{O}'^{i-2}} \otimes (E^{\mu_i,D}_{a^{\mu_{i-1}}_{\mu_i} b^{\mu_{i-1}}_{\mu_i}})_{\mathcal{P}\mathcal{O}^{i-1}}}{m_{\mu_{i-1}}^{(d)}}, \tag{123}$$

$$\mathrm{Tr}_{\mathcal{O}'_{i-1}} T_{t=i-1}^{(i)} = \sum_{\substack{\mu_i \in \mu_{i-1} \\ \mu_{i-1} \in \mathbb{Y}_{i-1}^d, \mu_i \notin \mathbb{Y}_i^d}} \sum_{a,b=1}^{d_{\mu_{i-1}}} \frac{(E_{ab}^{\mu_{i-1},d})_{\mathcal{P}'\mathcal{O}'^{i-2}} \otimes (E^{\mu_i,D}_{a^{\mu_{i-1}}_{\mu_i} b^{\mu_{i-1}}_{\mu_i}})_{\mathcal{P}\mathcal{O}^{i-2}}}{m_{\mu_{i-1}}^{(d)}}, \tag{124}$$

$$
\begin{aligned}
&\mathrm{Tr}_{\mathcal{O}'_{i-1}} T^{(i)}_{d\leq t<i-1}\\
&= \sum_{t=d}^{i-2} \sum_{\substack{\mu_{i-1}\in\cdots\in\mu_t\\ \mu_t\in\mathbb{Y}^d_t, \mu_{t+1}\notin\mathbb{Y}^d_{t+1}}} \sum_{a,b=1}^{d_{\mu_t}} \sum_{\mu_i\in\mu_{i-1}+\square} \frac{(E^{\mu_t,d}_{ab})_{\mathcal{P}'\mathcal{O}'^{t-1}} \otimes \mathbb{1}_{\mathcal{O}'_t\cdots\mathcal{O}'_{i-2}} \otimes (E^{\mu_i,D}_{a^{\mu_t}_{\mu_{t+1}\cdots\mu_i} b^{\mu_t}_{\mu_{t+1}\cdots\mu_i}})_{\mathcal{P}\mathcal{O}^{i-1}}}{d^{i-1-t} m^{(d)}_{\mu_t}}
\end{aligned}
\tag{125}
$$

$$
= \sum_{t=d}^{i-2} \sum_{\substack{\mu_{i-1}\in\cdots\in\mu_t\\ \mu_t\in\mathbb{Y}^d_t, \mu_{t+1}\notin\mathbb{Y}^d_{t+1}}} \sum_{a,b=1}^{d_{\mu_t}} \frac{(E^{\mu_t,d}_{ab})_{\mathcal{P}'\mathcal{O}'^{t-1}} \otimes \mathbb{1}_{\mathcal{O}'_t\cdots\mathcal{O}'_{i-2}} \otimes (E^{\mu_{i-1},D}_{a^{\mu_t}_{\mu_{t+1}\cdots\mu_{i-1}} b^{\mu_t}_{\mu_{t+1}\cdots\mu_{i-1}}})_{\mathcal{P}\mathcal{O}^{i-2}} \otimes \mathbb{1}_{\mathcal{O}_{i-1}}}{d^{i-1-t} m^{(d)}_{\mu_t}}
\tag{126}
$$

Therefore, one obtains

$$
\mathrm{Tr}_{\mathcal{O}'_{i-1}}[T^{(i)}_I + T^{(i)}_{t=i-1}] = \sum_{\mu_{i-1}\in\mathbb{Y}^d_{i-1}} \sum_{a,b=1}^{d_{\mu_{i-1}}} \sum_{\mu_i\in\mu_{i-1}+\square} \frac{(E^{\mu_{i-1},d}_{ab})_{\mathcal{P}'\mathcal{O}'^{i-2}} \otimes (E^{\mu_i,D}_{a^{\mu_{i-1}}_{\mu_i} b^{\mu_{i-1}}_{\mu_i}})_{\mathcal{P}\mathcal{O}^{i-1}}}{m^{(d)}_{\mu_{i-1}}}
\tag{127}
$$

$$
\begin{aligned}
&= \sum_{\mu_{i-1}\in\mathbb{Y}^d_{i-1}} \sum_{a,b=1}^{d_{\mu_{i-1}}} \frac{(E^{\mu_{i-1},d}_{ab})_{\mathcal{P}'\mathcal{O}'^{i-2}} \otimes (E^{\mu_{i-1},D}_{ab})_{\mathcal{P}\mathcal{O}^{i-2}} \otimes \mathbb{1}_{\mathcal{O}_{i-1}}}{m^{(d)}_{\mu_{i-1}}} && (128)\\
&= T^{(i-1)}_I \otimes \mathbb{1}_{\mathcal{O}_{i-1}}, && (129)\\
\mathrm{Tr}_{\mathcal{O}'_{i-1}} T^{(i)}_{d\leq t<i-1} &= T^{(i-1)}_O \otimes \mathbb{1}_{\mathcal{O}_{i-1}}. && (130)
\end{aligned}
$$

Thus, we obtain

$$
\begin{aligned}
\mathrm{Tr}_{\mathcal{O}'_{i-1}} T^{(i)} &= \mathrm{Tr}_{\mathcal{O}'_{i-1}}[T^{(i)}_I + T^{(i)}_{t=i-1} + T^{(i)}_{d\leq t<i-1}] && (131)\\
&= [T^{(i-1)}_I + T^{(i-1)}_O] \otimes \mathbb{1}_{\mathcal{O}_{i-1}}, && (132)\\
&= T^{(i-1)} \otimes \mathbb{1}_{\mathcal{O}_{i-1}}. && (133)
\end{aligned}
$$

A.2 Proof of Theorem 5: Construction of a sequential isometry adjointation protocol

First, we show that the probabilistic quantum comb $\{\mathcal{T}_I, \mathcal{T}_O\}$ satisfies

$$
T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = \int_{\mathbb{U}(d)} \mathrm{d}U |UV^\dagger\rangle\!\rangle\langle\!\langle UV^\dagger|_{\mathcal{P}\mathcal{P}'} \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n} + (\mathbb{1}_D - \Pi_{\mathrm{Im}V})^T_{\mathcal{P}} \otimes \Sigma \tag{134}
$$

for all $V \in \mathbb{V}_{\mathrm{iso}}(d, D)$, where $\mathrm{d}U$ is the Haar measure on $\mathbb{U}(d)$ and Σ is defined in Eq. (74). By definition (61) of T_I, it satisfies

$$
[T_I, \mathbb{1}_{\mathcal{P}'\mathcal{O}'^n} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \quad \forall U' \in \mathbb{U}(D). \tag{135}
$$

Therefore,

$$
\begin{aligned}
T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} &= (\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n} \otimes \mathcal{U}'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n})(T_I) \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} && (136)\\
&= (\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n} \otimes \mathcal{U}'_{\mathcal{P}})(T_I \star |U'^T V\rangle\!\rangle\langle\!\langle U'^T V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) && (137)
\end{aligned}
$$

Since $U'^T V = V$ holds for $U'^T = \mathbb{1}_{\mathrm{Im}V} \oplus U''_{(\mathrm{Im}V)^\perp}$ using $U'' \in \mathbb{U}(D-d)$, we obtain

$$
[T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}, \mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n} \otimes (\mathbb{1}_{\mathrm{Im}V} \oplus U''_{(\mathrm{Im}V)^\perp})^T_{\mathcal{P}}] = 0 \quad \forall U'' \in \mathbb{U}(D-d). \tag{138}
$$

Therefore, $T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}$ satisfies

$$\begin{aligned}T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} =& [\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n} \otimes (\Pi^T_{\mathrm{Im}V})_{\mathcal{P}}](T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})[\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n} \otimes (\Pi^T_{\mathrm{Im}V})_{\mathcal{P}}]\\ &+ (\mathbb{1}_D - \Pi_{\mathrm{Im}V})^T_{\mathcal{P}} \otimes \Sigma,\end{aligned} \tag{139}$$

where $\Sigma \in \mathcal{L}(\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n)$ is given by

$$\Sigma = \frac{1}{D-d} T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \star (\mathbb{1}_D - \Pi_{\mathrm{Im}V})_{\mathcal{P}}. \tag{140}$$

Since $\Pi_{\mathrm{Im}V} = VV^\dagger$ holds, the first term in Eq. (137) can be evaluated as

$$\begin{aligned}&[\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n} \otimes (\Pi^T_{\mathrm{Im}V})_{\mathcal{P}}](T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})[\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{I}^n} \otimes (\Pi^T_{\mathrm{Im}V})_{\mathcal{P}}]\\
&= \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{i,j=1}^{d_\mu} \frac{(E^{\mu,d}_{ij})_{\mathcal{P}'\mathcal{O}'^n}}{m^{(d)}_\mu} \otimes (\mathbb{1}_{\mathcal{O}^n} \otimes \mathcal{V}^*_{\mathcal{P}''\to\mathcal{P}} \circ \mathcal{V}^T_{\mathcal{P}\to\mathcal{P}''})(E^{\mu,D}_{ij})_{\mathcal{P}\mathcal{O}^n} \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} &(141)\\
&= \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{i,j=1}^{d_\mu} \frac{(E^{\mu,d}_{ij})_{\mathcal{P}'\mathcal{O}'^n}}{m^{(d)}_\mu} \otimes (\mathbb{1}_{\mathcal{I}^n} \otimes \mathcal{V}^*_{\mathcal{P}''\to\mathcal{P}}) \circ \mathcal{V}^{T\otimes n+1}_{\mathcal{P}\mathcal{O}^n\to\mathcal{P}''\mathcal{I}^n}(E^{\mu,D}_{ij})_{\mathcal{P}\mathcal{O}^n} &(142)\\
&= \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{i,j=1}^{d_\mu} \frac{(E^{\mu,d}_{ij})_{\mathcal{P}'\mathcal{O}'^n}}{m^{(d)}_\mu} \otimes (\mathbb{1}_{\mathcal{I}^n} \otimes \mathcal{V}^*_{\mathcal{P}''\to\mathcal{P}})(E^{\mu,d}_{ij})_{\mathcal{P}''\mathcal{I}^n} &(143)\\
&= \int_{\mathbb{U}(d)} \mathrm{d}U (\mathbb{1}_{\mathcal{P}'} \otimes \mathcal{V}^*_{\mathcal{P}''\to\mathcal{P}})(|U\rangle\!\rangle\langle\!\langle U|_{\mathcal{P}''\mathcal{P}'}) \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n} &(144)\\
&= \int_{\mathbb{U}(d)} \mathrm{d}U |UV^\dagger\rangle\!\rangle\langle\!\langle UV^\dagger|_{\mathcal{P}\mathcal{P}'} \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n}, &(145)\end{aligned}$$

where $\mathcal{P}''$ is a Hilbert spaces given by $\mathcal{P}'' = \mathbb{C}^d$, $\mathrm{d}U$ is the Haar measure on $\mathbb{U}(d)$, and we have utilized the following relations:

$$V^{\dagger\otimes n+1} E^{\mu,D}_{ij} V^{\otimes n+1} = \begin{cases} E^{\mu,d}_{ij} & (\mu \in \mathbb{Y}^d_{n+1}) \\ 0 & (\mu \notin \mathbb{Y}^d_{n+1}) \end{cases}, \tag{146}$$

$$\int_{\mathbb{U}(d)} \mathrm{d}U |U\rangle\!\rangle\langle\!\langle U|^{\otimes n+1}_{\mathcal{P}''\mathcal{I}^n,\mathcal{P}'\mathcal{O}'^n} = \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{i,j=1}^{d_\mu} \frac{(E^{\mu,d}_{ij})_{\mathcal{P}'\mathcal{O}'^n} \otimes (E^{\mu,d}_{ij})_{\mathcal{P}''\mathcal{I}^n}}{m^{(d)}_\mu}, \tag{147}$$

the former of which follows from the decomposition of $V^{\otimes n+1}$ shown in Eq. (53) and the definition (54) of $E^{\mu,d}_{ij}$, and the latter of which is shown in Ref. [29]. The operator Σ defined in Eq. (140) is shown to be the same as Eq. (74) by the following calculation:

$$\begin{aligned}\Sigma &= \frac{1}{D-d} T_I \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \star (\mathbb{1}_D - \Pi_{\mathrm{Im}V})_{\mathcal{P}}\\
&= \frac{1}{D-d}\left[(\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n\mathcal{P}} \otimes \mathcal{V}^{T\otimes n}_{\mathcal{O}^n\to\mathcal{I}^n})(\mathrm{Tr}_{\mathcal{P}}\, T_I) - \mathrm{Tr}_{\mathcal{P}''} \circ (\mathbb{1}_{\mathcal{P}'\mathcal{O}'^n} \otimes \mathcal{V}^{T\otimes n+1}_{\mathcal{P}\mathcal{O}^n\to\mathcal{P}''\mathcal{I}^n})(T_I)\right] &(148)\\
&= \frac{1}{D-d} \sum_{\lambda\in\mathbb{Y}^d_n} \sum_{\mu\in\lambda+\square} \sum_{a,b=1}^{d_\lambda} \left[\frac{m^{(D)}_\mu}{m^{(D)}_\lambda} - \frac{m^{(d)}_\mu}{m^{(d)}_\lambda}\right] (E^{\lambda,d}_{ab})_{\mathcal{I}^n} \otimes \frac{(E^{\mu,d}_{a^\lambda_\mu b^\lambda_\mu})_{\mathcal{O}'^n\mathcal{P}'}}{m^{(d)}_\mu}, &(149)\end{aligned}$$

where we have utilized Lemma 3 and Eq. (146). To calculate it further, we employ the dimension formula of the irreducible representation $\mathcal{U}^{(D)}_\mu$ of $\mathbb{U}(D)$ given by Eq. (51). In particular, for $\mu \in \lambda + \square$, the ratio of $m_\mu^{(d)}$ and $m_\lambda^{(d)}$ is given by

$$\frac{m_\mu^{(d)}}{m_\lambda^{(d)}} = (d + j - i)\frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)}, \tag{150}$$

where (i, j) is a coordinate of the box added to obtain μ from λ, i.e.,

$$\frac{m_\mu^{(D)}}{m_\lambda^{(D)}} - \frac{m_\mu^{(d)}}{m_\lambda^{(d)}} = (D - d)\frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} \tag{151}$$

holds. Thus, we obtain Eq. (134).

We evaluate the Choi operator of $\mathcal{C}_a[\mathcal{V}_{\mathrm{in}}^{\otimes n}]$ given by

$$J_{\mathcal{C}_a[\mathcal{V}_{\mathrm{in}}^{\otimes n}]} = C' \star T_a \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \tag{152}$$

to show Theorem 5. From Eq. (134), it is given by

$$J_{\mathcal{C}_I[\mathcal{V}_{\mathrm{in}}^{\otimes n}]} = C' \star \int_{\mathbb{U}(d)} \mathrm{d}U |UV_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle UV_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{P}'} \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} + (\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})^T_{\mathcal{P}} \otimes C' \star \Sigma. \tag{153}$$

Since C' is the Choi operator of the covariant unitary inversion protocol, we obtain [29]

$$C' \star |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1} |U^{-1}\rangle\!\rangle\langle\!\langle U^{-1}|_{\mathcal{P}'\mathcal{F}} + \frac{d^2(1 - F_{\mathrm{UI}})}{d^2 - 1}\frac{\mathbb{1}_{\mathcal{F}}}{d} \otimes \mathbb{1}_{\mathcal{P}'}. \tag{154}$$

Thus, the first term in Eq. (153) is given by

$$\begin{aligned} &C' \star \int_{\mathbb{U}(d)} \mathrm{d}U |UV_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle UV_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{P}'} \otimes |U\rangle\!\rangle\langle\!\langle U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \\ &= \int_{\mathbb{U}(d)} \mathrm{d}U |UV_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle UV_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{P}'} \star \left[\frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1} |U^{-1}\rangle\!\rangle\langle\!\langle U^{-1}|_{\mathcal{P}'\mathcal{F}} + \frac{d^2(1 - F_{\mathrm{UI}})}{d^2 - 1}\frac{\mathbb{1}_{\mathcal{F}}}{d} \otimes \mathbb{1}_{\mathcal{P}'}\right] \quad (155) \\ &= \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1} |V_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{F}} + \frac{d^2(1 - F_{\mathrm{UI}})}{d^2 - 1}\frac{\mathbb{1}_{\mathcal{F}}}{d} \otimes (\Pi_{\mathrm{Im}V_{\mathrm{in}}}^T)_{\mathcal{P}}. \quad (156) \end{aligned}$$

Since C' and Σ satisfy the $\mathbb{U}(d)$ symmetry, namely,

$$[C', U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathbb{1}_{\mathcal{P}'\mathcal{O}'^n}] = 0, \tag{157}$$

$$[\Sigma, U'^{\otimes n+1}_{\mathcal{I}^n} \otimes \mathbb{1}_{\mathcal{P}'\mathcal{O}'^n}] = 0 \tag{158}$$

for all $U' \in \mathbb{U}(d)$, $C' \star \Sigma$ satisfies

$$[C' \star \Sigma, U'_{\mathcal{F}}] = 0 \tag{159}$$

for all $U' \in \mathbb{U}(d)$, i.e., it is proportional to the identity operator. Thus, the second term in Eq. (153) is given by

$$\begin{aligned} (\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})^T_{\mathcal{P}} \otimes C' \star \Sigma &= (\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})^T_{\mathcal{P}} \otimes \mathrm{Tr}[C' \star \Sigma]\frac{\mathbb{1}_{\mathcal{F}}}{d} \quad (160) \\ &= (\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})^T_{\mathcal{P}} \otimes \mathrm{Tr}[\mathrm{Tr}_{\mathcal{F}}(C')\Sigma]\frac{\mathbb{1}_{\mathcal{F}}}{d}, \quad (161) \end{aligned}$$

where we utilize the fact that $\Sigma = \Sigma^T$. Combining Eqs. (153), (156), and (161), we obtain

$$J_{\mathcal{C}_I[\mathcal{V}_{\mathrm{in}}^{\otimes n}]} = \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1} |V_{\mathrm{in}}^\dagger\rangle\rangle\langle\langle V_{\mathrm{in}}^\dagger|_{\mathcal{PF}} + \frac{\mathbb{1}_{\mathcal{F}}}{d} \otimes \left[\frac{d^2(1-F_{\mathrm{UI}})}{d^2-1} (\Pi^T_{\mathrm{Im} V_{\mathrm{in}}})_{\mathcal{P}} + \alpha_{C'} (\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}})^T_{\mathcal{P}} \right], \tag{162}$$

where $\alpha_{C'}$ is defined by

$$\alpha_{C'} \coloneqq \mathrm{Tr}[\mathrm{Tr}_{\mathcal{F}}(C')\Sigma]. \tag{163}$$

Therefore, we obtain

$$\mathcal{C}_I[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1} \mathcal{V}_{\mathrm{in}}^\dagger(\rho_{\mathrm{in}}) + \frac{\mathbb{1}_d}{d} \mathrm{Tr} \left\{ \left[\frac{d^2(1-F_{\mathrm{UI}})}{d^2-1} \Pi_{\mathrm{Im} V_{\mathrm{in}}} + \alpha_{C'} (\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}}) \right] \rho_{\mathrm{in}} \right\}. \tag{164}$$

Since $\mathcal{C}_I[V_{\mathrm{in}}^{\otimes n}] + \mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}]$ is a CPTP map and

$$\mathrm{Tr}\, \mathcal{C}_I[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = \mathrm{Tr}\left\{ [\Pi_{\mathrm{Im} V_{\mathrm{in}}} + \alpha_{C'}(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}})]\, \rho_{\mathrm{in}} \right\} \tag{165}$$

holds, $\mathrm{Tr}\, \mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = (1 - \alpha_{C'})\, \mathrm{Tr}[(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}})\rho_{\mathrm{in}}]$ holds. Since $\mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}]$ is a CP map, we obtain

$$\mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = \mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\Pi_{(\mathrm{Im} V_{\mathrm{in}})^\perp} \rho_{\mathrm{in}} \Pi_{(\mathrm{Im} V_{\mathrm{in}})^\perp}). \tag{166}$$

Due to the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetries of C' and T_O,

$$[C' \star T_O, U'^{\otimes n+1}_{\mathcal{I}^n \mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \quad \forall U' \in \mathbb{U}(d), U'' \in \mathbb{U}(D) \tag{167}$$

holds. Thus, we obtain

$$\mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = \mathcal{U}' \circ \mathcal{C}_O[(U'' V_{\mathrm{in}} U')^{\otimes n}] \circ \mathcal{U}''(\rho_{\mathrm{in}}) \quad \forall U' \in \mathbb{U}(d), U'' \in \mathbb{U}(D). \tag{168}$$

In particular, for all $U' \in \mathbb{U}(d)$, we take $U'' = U'''_{\mathrm{Im} V_{\mathrm{in}}} \oplus \mathbb{1}_{(\mathrm{Im} V_{\mathrm{in}})^\perp}$ for $U''' \in \mathbb{U}(d)$ such that $U'' V_{\mathrm{in}} U' = V_{\mathrm{in}}$. From Eqs. (166) and (168), we obtain

$$\mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = \mathcal{U}' \circ \mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) \quad \forall U' \in \mathbb{U}(d), \tag{169}$$

thus, $\mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) \propto \frac{\mathbb{1}_d}{d}$. From Eq. (166), we obtain

$$\mathcal{C}_O[V_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}) = \frac{\mathbb{1}_d}{d} (1 - \alpha_{C'})\, \mathrm{Tr}[(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}})\rho_{\mathrm{in}}]. \tag{170}$$

We evaluate the diamond norm $\|\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}] - \mathcal{V}_{\mathrm{adjoint}}\|_\diamond$ to complete the proof, where $\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}]$ and $\mathcal{V}_{\mathrm{adjoint}}$ are defined as

$$\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}](\cdot) \coloneqq \mathcal{C}_I[\mathcal{V}_{\mathrm{in}}^{\otimes n}](\cdot) \otimes |0\rangle\langle 0| + \mathcal{C}_O[\mathcal{V}_{\mathrm{in}}^{\otimes n}](\cdot) \otimes |1\rangle\langle 1|, \tag{171}$$

$$\mathcal{V}_{\mathrm{adjoint}}(\cdot) \coloneqq V_{\mathrm{in}}^\dagger \cdot V_{\mathrm{in}} \otimes |0\rangle\langle 0| + \mathrm{Tr}[(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}}) \cdot] \frac{\mathbb{1}}{d} \otimes |1\rangle\langle 1|. \tag{172}$$

First, $\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}] - \mathcal{V}_{\mathrm{adjoint}}$ decomposes into two completely positive maps Φ_1 and Φ_2 as

$$\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}] - \mathcal{V}_{\mathrm{adjoint}} = \Phi_1 + \Phi_2, \tag{173}$$

$$\Phi_1(\rho_{\mathrm{in}}) \coloneqq -\frac{d^2(1-F_{\mathrm{UI}})}{d^2-1} [\mathcal{V}_{\mathrm{in}}^\dagger(\rho_{\mathrm{in}}) - \mathrm{Tr}(\Pi_{\mathrm{Im} V_{\mathrm{in}}} \rho_{\mathrm{in}})] \otimes |0\rangle\langle 0|, \tag{174}$$

$$\Phi_2(\rho_{\mathrm{in}}) \coloneqq \alpha_{C'}\, \mathrm{Tr}[(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}})\rho_{\mathrm{in}}] \left(\frac{\mathbb{1}_d}{d} \otimes |0\rangle\langle 0| - \frac{\mathbb{1}_d}{d} \otimes |1\rangle\langle 1| \right), \tag{175}$$

whose kernels do not intersect, i.e., $\ker\Phi_1 \cap \ker\Phi_2 = \emptyset$. Since the diamond norm $\|\Phi_1+\Phi_2\|_\diamond$ is defined by

$$\|\Phi_1 + \Phi_2\|_\diamond := \sup_{\psi\in\mathcal{L}(\mathcal{P}\otimes\mathcal{A}), \|\psi\|_1\leq 1} \|(\Phi_1+\Phi_2)\otimes \mathbb{1}_{\mathcal{A}}(\psi)\|_1 \tag{176}$$

using an auxiliary Hilbert space $\mathcal{A}$ and the trace norm $\|\cdot\|_1$, it is given by

$$\begin{aligned}
&\|\Phi_1 + \Phi_2\|_\diamond \\
&= \sup_{\psi_i\in\ker\Phi_i\otimes\mathcal{L}(\mathcal{A}), \|\psi_1+\psi_2\|_1\leq 1} \|(\Phi_1+\Phi_2)\otimes \mathbb{1}_{\mathcal{A}}(\psi_1+\psi_2)\|_1 &(177)\\
&= \max_{0\leq x\leq 1}[x \sup_{\substack{\psi_1\in\ker\Phi_1\otimes\mathcal{L}(\mathcal{A})\\ \|\psi_1\|_1\leq 1}} \|\Phi_1\otimes \mathbb{1}_{\mathcal{A}}(\psi_1)\|_1 + (1-x) \sup_{\substack{\psi_2\in\ker\Phi_2\otimes\mathcal{L}(\mathcal{A})\\ \|\psi_2\|_1\leq 1}} \|\Phi_1\otimes \mathbb{1}_{\mathcal{A}}(\psi_2)\|_1] &(178)\\
&= \max\{\|\Phi_1\|_\diamond, \|\Phi_2\|_\diamond\}. &(179)
\end{aligned}$$

The diamond norm $\|\Phi_1\|_\diamond$ is given by

$$\begin{aligned}
\|\Phi_1\|_\diamond &= \|\Phi_1\circ\mathcal{V}_{\text{in}}\|_\diamond &(180)\\
&= \|\mathbb{1}_d - \mathcal{D}_q\|_\diamond &(181)\\
&= 2(1-F_{\text{UI}}), &(182)
\end{aligned}$$

where $\mathcal{D}_q$ is the depolarizing channel

$$\mathcal{D}_q(\rho) := (1-q)\rho + q\frac{\mathbb{1}_d}{d}\operatorname{Tr}(\rho), \tag{183}$$

q is given by $q := \frac{d^2}{d^2-1}(1-F_{\text{est}})$, and we utilize the fact that [73]

$$\|\mathbb{1}_d - \mathcal{D}_q\|_\diamond = \frac{2(d^2-1)}{d^2}q. \tag{184}$$

The diamond norm $\|\Phi_2\|_\diamond$ is given by

$$\begin{aligned}
&\|\Phi_2\|_\diamond \\
&= \sup_{\psi\in\mathcal{L}(\mathcal{P}\otimes\mathcal{A}), \|\psi\|_1\leq 1} \|\alpha_{C'}\operatorname{Tr}_{\mathcal{P}}[(\mathbb{1}_D - \Pi_{\operatorname{Im}V_{\text{in}}})\psi]\otimes(\frac{\mathbb{1}_d}{d}\otimes|0\rangle\langle 0| - \frac{\mathbb{1}_d}{d}\otimes|1\rangle\langle 1|)\|_1 &(185)\\
&= 2\alpha_\phi. &(186)
\end{aligned}$$

Thus, we obtain

$$\begin{aligned}
\epsilon &:= \frac{1}{2}\sup_{V_{\text{in}}\in\mathbb{V}_{\text{iso}}(d,D)} \|\mathcal{C}[\mathcal{V}_{\text{in}}^{\otimes n}] - \mathcal{V}_{\text{adjoint}}\|_\diamond &(187)\\
&= \max\{\alpha_{C'}, 1-F_{\text{UI}}\}. &(188)
\end{aligned}$$

A.3 Proof of Theorem 6: Construction of a parallel isometry adjointation protocol

The parallel protocol shown in Theorem 6 corresponds to the special case of the sequential protocol such that the Choi operator of the original untiary inversion protocol is given by

$$C' = \phi_{\mathcal{I}^n\mathcal{A}} \star \sum_i (M_i^T)_{\mathcal{O}'^n\mathcal{A}} \otimes (J_{\mathcal{R}_i})_{\mathcal{P}'\mathcal{F}}. \tag{189}$$

Since the Choi operator of a CPTP map $\mathcal{R}_i$ satisfies $\mathrm{Tr}_{\mathcal{F}}(J_{\mathcal{R}_i})_{\mathcal{P}'\mathcal{F}} = \mathbb{1}_{\mathcal{P}'}$, we obtain

$$\begin{aligned}
\mathrm{Tr}_{\mathcal{F}}(C') &= \phi_{\mathcal{I}^n\mathcal{A}} \star \sum_i (M_i^T)_{\mathcal{O}'^n\mathcal{A}} \otimes \mathbb{1}_{\mathcal{P}'} && (190)\\
&= \phi_{\mathcal{I}^n\mathcal{A}} \star \mathbb{1}_{\mathcal{O}'^n\mathcal{A}} \otimes \mathbb{1}_{\mathcal{P}'} && (191)\\
&= \mathrm{Tr}_{\mathcal{A}}(\phi) \otimes \mathbb{1}_{\mathcal{O}'^n\mathcal{P}'}. && (192)
\end{aligned}$$

Then, $\alpha_{C'}$ shown in Eq. (73) reduces to α_ϕ given by

$$\begin{aligned}
\alpha_\phi &:= \mathrm{Tr}[\mathrm{Tr}_{\mathcal{A}}(\phi)\, \mathrm{Tr}_{\mathcal{O}'^n\mathcal{P}'}(\Sigma)] && (193)\\
&= \sum_{\lambda\in\mathbb{Y}_n^d} \mathrm{Tr}\Big[\mathrm{Tr}_{\mathcal{A}}(\phi)\Pi_\lambda^{(d)}\Big] \sum_{\mu\in\lambda\cap\square\cap\mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} && (194)\\
&= \sum_{\lambda\in\mathbb{Y}_n^d} \mathrm{Tr}\Big[\mathrm{Tr}_{\mathcal{A}}(\phi)\Pi_\lambda^{(d)}\Big] \left[1 - \sum_{\mu\in\lambda\backslash\square\cap\mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)}\right], && (195)
\end{aligned}$$

where we have utilized Lemma 3, Eq. (74), and the equality

$$\sum_{\nu\in\lambda+\square} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\nu)} = 1, \tag{196}$$

shown as follows. From Lemma 3,

$$E_{aa}^{\lambda,D} \otimes \mathbb{1}_D = \sum_{\mu\in\lambda+\square} E_{a_\mu^\lambda a_\mu^\lambda}^{\mu,D} \tag{197}$$

holds for $a \in \{1, \cdots, d_\lambda\}$. By taking the trace of the both-hand side, we obtain

$$Dm_\lambda^{(D)} = \sum_{\mu\in\lambda+\square} m_\mu^{(D)}. \tag{198}$$

By using Eqs. (51) and (198), we show Eq. (196) as

$$\begin{aligned}
\sum_{\nu\in\lambda+\square} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\nu)} &= \lim_{D\to\infty} \frac{\sum_{\nu\in\lambda+\square} m_\nu^{(D)}}{Dm_\lambda^{(D)}} && (199)\\
&= 1. && (200)
\end{aligned}$$

Thus, the approximation error of isometry adjointation is given by

$$\epsilon = \max\{\alpha_\phi, 1 - F_{\mathrm{est}}\}. \tag{201}$$

A.4 Reduction to isometry inversion and universal error detection

A.4.1 Deterministic isometry inversion

By discarding the measurement outcome of the isometry adjointation protocol shown in Eqs. (164) and (169), we obtain the following protocol:

$$\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}] = \mathcal{C}_I[\mathcal{V}_{\mathrm{in}}^{\otimes n}] + \mathcal{C}_O[\mathcal{V}_{\mathrm{in}}^{\otimes n}] \tag{202}$$

This protocol satisfies

$$\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}] \circ \mathcal{V}_{\mathrm{in}}(\rho_{\mathrm{in}}) = \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1}\rho_{\mathrm{in}} + \frac{\mathbb{1}_d}{d}\left(1 - \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1}\right)\mathrm{Tr}(\rho_{\mathrm{in}}). \tag{203}$$

Thus, the worst-case channel fidelity of isometry inversion is given by

$$F_{\mathrm{ch}}(\mathcal{C}[\mathcal{V}_{\mathrm{in}}^{\otimes n}] \circ \mathcal{V}_{\mathrm{in}}, \mathbb{1}_d) = F_{\mathrm{UI}}. \tag{204}$$

A.4.2 Probabilistic exact isometry inversion

The construction of deterministic exact unitary inversion protocol can be rewritten in terms of the Choi operator as

$$\begin{aligned}
&C' \star |U_{\mathrm{in}}\rangle\!\rangle\langle\!\langle U_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n} \approx |U_{\mathrm{in}}^{-1}\rangle\!\rangle\langle\!\langle U_{\mathrm{in}}^{-1}|_{\mathcal{P}'\mathcal{F}} \quad \forall U_{\mathrm{in}} \in \mathbb{U}(d)\\
&\Longrightarrow T \star C' \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|_{\mathcal{P}''\mathcal{P}}\\
&\quad = \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1} |\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|_{\mathcal{P}''\mathcal{F}} + \frac{\mathbb{1}_{\mathcal{P}''\mathcal{P}}}{d}\left(1 - \frac{d^2 F_{\mathrm{UI}} - 1}{d^2 - 1}\right) \quad \forall V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D), \qquad (205)
\end{aligned}$$

where $\mathcal{P}''$ is a Hilbert space given by $\mathcal{P}'' = \mathbb{C}^d$. By replacing C' with the probabilistic exact unitary inversion comb $\{C'_S, C'_F\}$ with the success probability p_{UI} satisfying

$$C'_S \star |U_{\mathrm{in}}\rangle\!\rangle\langle\!\langle U_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}'^n} = p_{\mathrm{UI}} |U_{\mathrm{in}}^{-1}\rangle\!\rangle\langle\!\langle U_{\mathrm{in}}^{-1}|_{\mathcal{P}'\mathcal{F}} \quad \forall U_{\mathrm{in}} \in \mathbb{U}(d), \qquad (206)$$

we obtain the probabilistic exact isometry inversion protocol given by

$$\begin{aligned}
T \star C'_S \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|_{\mathcal{P}''\mathcal{P}} = p_{\mathrm{UI}} |\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|_{\mathcal{P}''\mathcal{F}}&\\
\forall V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D).& \qquad (207)
\end{aligned}$$

A.4.3 Universal error detection

By discarding the output state of the isometry adjointation protocol shown in Eqs. (164) and (169), we obtain the following protocol:

$$\mathrm{Tr}(\Pi_a \rho_{\mathrm{in}}) = \mathrm{Tr} \circ \mathcal{C}_a[\mathcal{V}_{\mathrm{in}}^{\otimes n}](\rho_{\mathrm{in}}), \qquad (208)$$

This protocol satisfies

$$\Pi_I = \Pi_{\mathrm{Im} V_{\mathrm{in}}} + \alpha_{C'}(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}}), \qquad (209)$$

$$\Pi_O = (1 - \alpha_{C'})(\mathbb{1}_D - \Pi_{\mathrm{Im} V_{\mathrm{in}}}). \qquad (210)$$

Since C' corresponds to $C' = C'' \otimes \frac{\mathbb{1}_{\mathcal{O}'_n\mathcal{F}}}{d}$ using C'' shown in Corollary 8, $\alpha_{C'}$ is given by

$$\alpha'_C = \mathrm{Tr}(C''\Sigma'). \qquad (211)$$

B Analysis on the optimal protocols

B.1 Proof of Theorem 9: $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry of the tasks

We show Theorem 9 using the idea of a twirling map [74] similarly to Refs. [27, 29]. Assume that the Choi operators (102) achieve the optimal performances in parallel, sequential or general protocols including indefinite causal order. We define the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirled Choi operators by

$$\begin{cases}
C' := \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C) & \text{(deterministic isometry inversion)}\\
C'_a := \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C_a) & \text{(probabilistic exact isometry inversion)}\\
C'_a := \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n}_{\mathcal{I}^n} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C_a) & \text{(universal error detection)}\\
C'_a := \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C_a) & \text{(isometry adjointation)}
\end{cases},$$

$$(212)$$

where $\mathrm{d}U'$ and $\mathrm{d}U''$ are the Haar measures of $\mathbb{U}(d)$ and $\mathbb{U}(D)$, respectively. Then, these operators satisfy $C'_a \geq 0$ and $C' = \sum_a C'_a \in \mathcal{W}^{(x)}$, and the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry given by

$$\begin{cases} [C', U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & \text{(deterministic isometry inversion)} \\ [C'_a, U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \quad \forall a \in \{S, F\} & \text{(probabilistic exact isometry inversion)} \\ [C'_a, U'^{\otimes n}_{\mathcal{I}^n} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \quad \forall a \in \{I, O\} & \text{(universal error detection)} \\ [C'_a, U'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \quad \forall a \in \{I, O\} & \text{(isometry adjointation)} \end{cases} \tag{213}$$

for all $U' \in \mathbb{U}(d)$ and $U'' \in \mathbb{U}(D)$. Then, we can show Theorem 9 by showing that the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirling does not decrease performances of each task. We show this in the following subsections.

B.1.1 Deterministic isometry inversion

The worst-case fidelity F_worst is given using the Choi operator C of the quantum superchannel by

$$F_\text{worst} = \inf_{V_\text{in} \in \mathbb{V}_\text{iso}(d,D)} F_\text{ch}[\mathcal{C}(\mathcal{V}_\text{in}^{\otimes n}) \circ \mathcal{V}_\text{in}, \mathbb{1}_d] \tag{214}$$

$$= \frac{1}{d^2} \inf_{V_\text{in} \in \mathbb{V}_\text{iso}(d,D)} \mathrm{Tr}\Big[C \star (|V_\text{in}\rangle\!\rangle\langle\!\langle V_\text{in}|_{\mathcal{P}''\mathcal{P}} \otimes |V_\text{in}\rangle\!\rangle\langle\!\langle V_\text{in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) |\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|_{\mathcal{P}''\mathcal{F}}\Big] \tag{215}$$

$$= \frac{1}{d^2} \inf_{V_\text{in} \in \mathbb{V}_\text{iso}(d,D)} \mathrm{Tr}\Big[C (|V^*_\text{in}\rangle\!\rangle\langle\!\langle V^*_\text{in}|_{\mathcal{F}\mathcal{P}} \otimes |V^*_\text{in}\rangle\!\rangle\langle\!\langle V^*_\text{in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})\Big]. \tag{216}$$

Then, the worst-case channel fidelity of the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirled Choi operator is given by

$$F'_\text{worst} = \frac{1}{d^2} \inf_{V_\text{in} \in \mathbb{V}_\text{iso}(d,D)} \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U''$$

$$\mathrm{Tr}\Big[\mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C) (|V^*_\text{in}\rangle\!\rangle\langle\!\langle V^*_\text{in}|_{\mathcal{F}\mathcal{P}} \otimes |V^*_\text{in}\rangle\!\rangle\langle\!\langle V^*_\text{in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})\Big] \tag{217}$$

$$\geq \frac{1}{d^2} \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \inf_{V_\text{in} \in \mathbb{V}_\text{iso}(d,D)}$$

$$\mathrm{Tr}\Big[C\mathcal{U}'^{\dagger\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{\dagger\otimes n+1}_{\mathcal{P}\mathcal{O}^n} (|V^*_\text{in}\rangle\!\rangle\langle\!\langle V^*_\text{in}|_{\mathcal{F}\mathcal{P}} \otimes |V^*_\text{in}\rangle\!\rangle\langle\!\langle V^*_\text{in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})\Big] \tag{218}$$

$$= \frac{1}{d^2} \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \inf_{V_\text{in} \in \mathbb{V}_\text{iso}(d,D)}$$

$$\mathrm{Tr}\Big[C (|U''^\dagger V^*_\text{in} U'^*\rangle\!\rangle\langle\!\langle U''^\dagger V^*_\text{in} U'^*|_{\mathcal{F}\mathcal{P}} \otimes |U''^\dagger V^*_\text{in} U'^*\rangle\!\rangle\langle\!\langle U''^\dagger V^*_\text{in} U'^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})\Big] \tag{219}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' F_\text{worst} \tag{220}$$

$$= F_\text{worst}. \tag{221}$$

B.1.2 Probabilistic exact isometry inversion

Suppose a Choi operator C_S satisfies

$$C_S \star (|V_\text{in}\rangle\!\rangle\langle\!\langle V_\text{in}|_{\mathcal{P}''\mathcal{P}} \otimes |V_\text{in}\rangle\!\rangle\langle\!\langle V_\text{in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) = p|\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|_{\mathcal{P}''\mathcal{F}} \quad \forall V_\text{in} \in \mathbb{V}_\text{iso}(d, D). \tag{222}$$

Then, the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirled Choi operator also satisfies

$$C'_S \star (|V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|_{\mathcal{P}''\mathcal{P}} \otimes |V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C_S) \star (|V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|_{\mathcal{P}''\mathcal{P}} \otimes |V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) \tag{223}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' C_S \star \mathcal{U}'^{T\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}''^{T\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(|V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|_{\mathcal{P}''\mathcal{P}} \otimes |V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) \tag{224}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' C_S \star (|U''^T V_{\rm in} U'\rangle\!\rangle\langle\!\langle U''^T V_{\rm in} U'|_{\mathcal{P}''\mathcal{P}} \otimes |U''^T V_{\rm in} U'\rangle\!\rangle\langle\!\langle U''^T V_{\rm in} U'|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) \tag{225}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' p|\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|_{\mathcal{P}''\mathcal{F}} \tag{226}$$

$$= p|\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|_{\mathcal{P}''\mathcal{F}}, \tag{227}$$

i.e., it implements isometry inversion with success probability p.

B.1.3 Universal error detection

Suppose a supermap $\mathcal{C}_I$ satisfies

$$\mathcal{C}_I[\mathcal{V}_{\rm in}^{\otimes n}](\rho) = \mathrm{Tr}[(\Pi_{\mathrm{Im}V_{\rm in}} + \alpha(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\rm in}}))\rho] \tag{228}$$

for all $V_{\rm in} \in \mathbb{V}_{\rm iso}(d, D)$. In terms of the Choi operator, this relation is given by

$$C_I \star |V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = (\Pi^T_{\mathrm{Im}V_{\rm in}})_{\mathcal{P}} + \alpha(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\rm in}})^T_{\mathcal{P}}. \tag{229}$$

Then, the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirlied Choi operator also satisfies

$$C'_I \star |V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n}_{\mathcal{I}^n} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(C_I) \star |V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \tag{230}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}''_{\mathcal{P}}[C_I \star \mathcal{U}'^{T\otimes n}_{\mathcal{I}^n} \otimes \mathcal{U}''^{T\otimes n}_{\mathcal{O}^n}(|V_{\rm in}\rangle\!\rangle\langle\!\langle V_{\rm in}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})] \tag{231}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}''_{\mathcal{P}}(C_I \star |U''^T V_{\rm in} U'\rangle\!\rangle\langle\!\langle U''^T V_{\rm in} U'|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}) \tag{232}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}''_{\mathcal{P}}[(\Pi^T_{\mathrm{Im}U''^T V_{\rm in} U'})_{\mathcal{P}} + \alpha(\mathbb{1}_D - \Pi_{\mathrm{Im}U''^T V_{\rm in} U'})^T_{\mathcal{P}}] \tag{233}$$

$$= \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}''_{\mathcal{P}} \circ \mathcal{U}''^{\dagger}_{\mathcal{P}}[(\Pi^T_{\mathrm{Im}V_{\rm in}})_{\mathcal{P}} + \alpha(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\rm in}})^T_{\mathcal{P}}] \tag{234}$$

$$= (\Pi^T_{\mathrm{Im}V_{\rm in}})_{\mathcal{P}} + \alpha(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\rm in}})^T_{\mathcal{P}}, \tag{235}$$

i.e., it implements a universal error detection with the same performance as C_I.

B.1.4 Isometry adjointation

We introduce the notation to represent the diamond norm of a quantum channel Φ in terms of its Choi operator J_Φ, i.e., we define $\mathfrak{D}[J_\Phi]$ by

$$\mathfrak{D}[J_\Phi] \coloneqq \|\Phi\|_\diamond. \tag{236}$$

Then, $\mathfrak{D}[J_\Phi]$ satisfies the following properties:

$$\mathfrak{D}[(U_\mathcal{I} \otimes U'_\mathcal{O}) J_\Phi (U_\mathcal{I} \otimes U'_\mathcal{O})^\dagger] = \mathfrak{D}[J_\Phi] \quad \forall U \in \mathbb{U}(\dim \mathcal{I}), U' \in \mathbb{U}(\dim \mathcal{O}), \tag{237}$$

$$\mathfrak{D}[aJ_{\Lambda^{(1)}} + bJ_{\Lambda^{(2)}}] \leq a\mathfrak{D}[J_{\Lambda^{(1)}}] + b\mathfrak{D}[J_{\Lambda^{(2)}}] \quad \forall a, b \geq 0, \tag{238}$$

which corresponds to the following properties of the diamond norm:

$$\|\mathcal{U}' \circ \Phi \circ \mathcal{U}\|_\diamond = \|\Phi\|_\diamond \quad \forall U \in \mathbb{U}(\dim \mathcal{I}), U' \in \mathbb{U}(\dim \mathcal{O}), \tag{239}$$

$$\|a\Lambda^{(1)} + b\Lambda^{(2)}\|_\diamond \leq a\|\Lambda^{(1)}\|_\diamond + b\|\Lambda^{(2)}\|_\diamond \quad \forall a, b \geq 0, \tag{240}$$

The worst-case diamond-norm error ϵ is given using the Choi operator C_I by

$$\epsilon = \inf_{V_\mathrm{in} \in \mathbb{V}_\mathrm{iso}(d,D)} \mathfrak{D}[C \star |V_\mathrm{in}\rangle\!\rangle\langle\!\langle V_\mathrm{in}|^{\otimes n}_{\mathcal{I}^n \mathcal{O}^n} \otimes |0\rangle\langle 0| - |V_\mathrm{in}^\dagger\rangle\!\rangle\langle\!\langle V_\mathrm{in}^\dagger|_{\mathcal{P}\mathcal{F}} \otimes |0\rangle\langle 0|_\mathcal{A} - \frac{\mathbb{1}_\mathcal{P} \otimes \mathbb{1}_\mathcal{F}}{d} \otimes |1\rangle\langle 1|_\mathcal{A}], \tag{241}$$

where $C' \coloneqq C_I \otimes |0\rangle\langle 0|_\mathcal{A} + C_O \otimes |1\rangle\langle 1|_\mathcal{A}$ and $\mathcal{A} = \mathbb{C}^2$. Thus, the worst-case diamond-norm error of the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirled Choi operator is given by

$$\begin{aligned}
\epsilon' = & \inf_{V_\mathrm{in} \in \mathbb{V}_\mathrm{iso}(d,D)} \mathfrak{D}[\int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n \mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n} \otimes \mathbb{1}_\mathcal{A}(C) \star |V_\mathrm{in}\rangle\!\rangle\langle\!\langle V_\mathrm{in}|^{\otimes n}_{\mathcal{I}^n \mathcal{O}^n} \\
& \qquad - |V_\mathrm{in}^\dagger\rangle\!\rangle\langle\!\langle V_\mathrm{in}^\dagger|_{\mathcal{P}\mathcal{F}} \otimes |0\rangle\langle 0|_\mathcal{A} - \frac{\mathbb{1}_\mathcal{P} \otimes \mathbb{1}_\mathcal{F}}{d} \otimes |1\rangle\langle 1|_\mathcal{A}] && (242)\\
\leq & \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \inf_{V_\mathrm{in} \in \mathbb{V}_\mathrm{iso}(d,D)} \mathfrak{D}[\mathcal{U}'^{\otimes n+1}_{\mathcal{I}^n \mathcal{F}} \otimes \mathcal{U}''^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n} \otimes \mathbb{1}_\mathcal{A}(C) \star |V_\mathrm{in}\rangle\!\rangle\langle\!\langle V_\mathrm{in}|^{\otimes n}_{\mathcal{I}^n \mathcal{O}^n} \\
& \qquad - |V_\mathrm{in}^\dagger\rangle\!\rangle\langle\!\langle V_\mathrm{in}^\dagger|_{\mathcal{P}\mathcal{F}} \otimes |0\rangle\langle 0|_\mathcal{A} - \frac{\mathbb{1}_\mathcal{P} \otimes \mathbb{1}_\mathcal{F}}{d} \otimes |1\rangle\langle 1|_\mathcal{A}] && (243)\\
= & \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \inf_{V_\mathrm{in} \in \mathbb{V}_\mathrm{iso}(d,D)} \mathfrak{D}[C \star \mathcal{U}'^{T \otimes n}_{\mathcal{I}^n} \otimes \mathcal{U}''^{T \otimes n}_{\mathcal{O}^n} (|V_\mathrm{in}\rangle\!\rangle\langle\!\langle V_\mathrm{in}|^{\otimes n}_{\mathcal{I}^n \mathcal{O}^n}) \\
& \qquad - \mathcal{U}'^\dagger_\mathcal{F} \otimes \mathcal{U}''^\dagger_\mathcal{P} \otimes \mathbb{1}_\mathcal{A} (|V_\mathrm{in}^\dagger\rangle\!\rangle\langle\!\langle V_\mathrm{in}^\dagger|_{\mathcal{P}\mathcal{F}} \otimes |0\rangle\langle 0|_\mathcal{A} + \frac{\mathbb{1}_\mathcal{P} \otimes \mathbb{1}_\mathcal{F}}{d} \otimes |1\rangle\langle 1|_\mathcal{A})] && (244)\\
= & \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \inf_{V_\mathrm{in} \in \mathbb{V}_\mathrm{iso}(d,D)} \mathfrak{D}[C \star (|U''^T V_\mathrm{in} U'\rangle\!\rangle\langle\!\langle U''^T V_\mathrm{in} U'|^{\otimes n}_{\mathcal{I}^n \mathcal{O}^n}) \\
& \qquad - |U'^\dagger V_\mathrm{in}^\dagger U''^*\rangle\!\rangle\langle\!\langle U'^\dagger V_\mathrm{in}^\dagger U''^*|_{\mathcal{P}\mathcal{F}} \otimes |0\rangle\langle 0|_\mathcal{A} - \frac{\mathbb{1}_\mathcal{P} \otimes \mathbb{1}_\mathcal{F}}{d} \otimes |1\rangle\langle 1|_\mathcal{A}] && (245)\\
= & \int_{\mathbb{U}(d)} \mathrm{d}U' \int_{\mathbb{U}(D)} \mathrm{d}U'' \epsilon && (246)\\
= & \epsilon, && (247)
\end{aligned}$$

i.e., it implements isometry adjointation with approximation error $\epsilon' \leq \epsilon$.

B.2 Proof of Theorem 12: Optimal parallel protocol for universal error detection

Due to Theorem 10, the optimal performance α of parallel error detection is given by minimizing α_ϕ shown in Theorem 8:

$$\alpha_\mathrm{opt}^{(\mathrm{PAR})} = \min_{\mathrm{Tr}(\phi)=1, \phi \geq 0} \sum_{\lambda \in \mathbb{Y}_n^d} \mathrm{Tr}(\phi \Pi_\lambda) \left[1 - \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} \right]. \tag{248}$$

The right-hand side has the minimum value

$$\alpha_\mathrm{opt}^{(\mathrm{PAR})} = 1 - \max_{\lambda \in \mathbb{Y}_n^d} \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)} \tag{249}$$

at $\phi = \Pi_\lambda / \operatorname{Tr} \Pi_\lambda$, where λ is given by

$$\lambda = \arg\max_{\lambda \in \mathbb{Y}_n^d} \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\operatorname{hook}(\lambda)}{\operatorname{hook}(\mu)}. \tag{250}$$

We define $f(\lambda)$ for $\lambda \in \mathbb{Y}_n^d$ by

$$f(\lambda) \coloneqq \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\operatorname{hook}(\lambda)}{\operatorname{hook}(\mu)}, \tag{251}$$

and derive the maximum value of $f(\lambda)$. We denote the number of boxes in the i-th row of λ and μ by λ_i and μ_i, respectively. By definition of Young diagrams, λ_i satisfies $\lambda_1 \geq \cdots \lambda_d \geq 0$ and $\sum_i \lambda_i = n$. If $\lambda_d = 0$, any Young diagram in the set $\lambda + \square$ has depth smaller than or equal to d, i.e., $f(\lambda) = 0$. If $\lambda_1 \geq \cdots \lambda_d \geq 1$ holds, the set $\lambda + \square \setminus \mathbb{Y}_{n+1}^d$ is a one-point set whose element μ is given by $\mu_i = \lambda_i$ for $i \in \{1, \cdots, d\}$ and $\mu_{d+1} = 1$. Therefore, $f(\lambda)$ is given by

$$f(\lambda) = \frac{\operatorname{hook}(\lambda)}{\operatorname{hook}(\mu)} = \prod_{i=1}^{d} \frac{\lambda_i + d - i}{\lambda_i + d + 1 - i}. \tag{252}$$

We derive the maximum value of $f(\lambda)$ for $\lambda_1, \cdots, \lambda_d$ such that $\lambda_1 \geq \cdots \geq \lambda_d \geq 1$ and $\sum_i \lambda_i = n$. We show that λ giving the maximum value of $f(\lambda)$ should satisfy $|\lambda_{i_1} - \lambda_{i_2}| \leq 1$ for any $1 \leq i_1 < i_2 \leq d$ by contradiction. If there exists $1 \leq i_1 < i_2 \leq d$ such that $\lambda_{i_1} \geq \lambda_{i_2} + 2$, at least one of the following conditions holds:

1. There exists $i_1' \in \{1, \cdots, d\}$ such that $\lambda_{i_1'} \geq \lambda_{i_1'+1} + 2$
2. There exists $i_1', i_2' \in \{1, \cdots, d\}$ such that $i_1' + 1 \leq i_2' - 1$, $\lambda_{i_1'} \geq \lambda_{i_1'+1} + 1$ and $\lambda_{i_2'-1} \geq \lambda_{i_2'} + 1$

If the first condition holds, we define $i_2' \coloneqq i_1' + 1$. Then, $\kappa_1, \cdots, \kappa_d$ defined by

$$\kappa_i = \begin{cases} \kappa_i & (i \neq i_1', i_2') \\ \kappa_{i_1'} - 1 & (i = i_1') \\ \kappa_{i_2'} + 1 & (i = i_2') \end{cases} \tag{253}$$

satisfies $\kappa_1 \geq \cdots \geq \kappa_d$, $\sum_i \kappa_i = n$, and

$$\frac{f(\kappa)}{f(\lambda)} = \frac{\lambda_{i_1'} + d - i_i' - 1}{\lambda_{i_1'} + d - i_1' + 1} \frac{\lambda_{i_2'} + d - i_2' + 2}{\lambda_{i_2'} + d - i_2'} > 1, \tag{254}$$

i.e., λ cannot give the maximum value of $f(\lambda)$. Therefore, the Young diagram λ giving the maximal value of $f(\lambda)$ should satisfy $|\lambda_{i_1} - \lambda_{i_2}| \leq 1$ for any $1 \leq i_1 < i_2 \leq d$. Such a Young diagram is uniquely determined as

$$\lambda_i = \begin{cases} k + 1 & (i \in \{1, \cdots, l\}) \\ k & (i \in \{l + 1, \cdots, d\}) \end{cases}, \tag{255}$$

where $k \in \mathbb{Z}$ and $l \in \{0, \cdots, d - 1\}$ are defined by $n = kd + l$. Then, we obtain

$$\alpha_{\mathrm{opt}}^{(\mathrm{PAR})} = 1 - \max_{\lambda \in \mathbb{Y}_n^d} f(\lambda) = \frac{1}{d + k + 1} \left(d + \frac{d - l}{d + k - l} \right). \tag{256}$$

B.3 Proof of Theorem 14: Asymptotically optimal parallel protocol for isometry adjointation

For $d=2$, Refs. [55, 57] present the maximum-likelihood qubit-unitary estimation protocol achieving the entanglement fidelity $F_{\mathrm{est}} = 1 - O(n^{-2})$ using n calls of input unitary operation. Although Refs. [55, 57] do not present the explicit form of the probe state, one can utilize the resource state for entanglement-assisted alignment of the reference frames presented in Ref. [56] to achieve the same asymptotic scaling of the entanglement fidelity $F_{\mathrm{est}} = 1 - O(n^{-2})$. The resource state presented in Ref. [56] is given by

$$|\phi\rangle = \frac{2}{\sqrt{n+3}} \sum_{j=0(1/2)}^{n/2} \frac{1}{\sqrt{2j+1}} \sin\frac{(2j+1)\pi}{n+3} \sum_{m=-j}^{j} |jm\rangle_{\mathcal{I}^n} |jm\rangle_{\mathcal{A}}, \tag{257}$$

where j and m represents total angular momentum and z-component of total angular momentum of a n-qubit system. The summation of j starts from 0 if n is even and $1/2$ if n is odd. These values correspond to the Schur basis, where j corresponds to the Young diagram λ whose number of boxes in i-th row, denoted by λ_i ($i = 1, 2$), is determined by $j = (\lambda_1 - \lambda_2)/2$, and m corresponds to an element in $\mathcal{U}_\lambda^{(2)}$. Then, the value α_ϕ shown in Theorem 6 is calculated as

$$\alpha_\phi = \frac{4}{n+3} \sum_{j=0(1/2)}^{n/2} \sin^2\frac{(2j+1)\pi}{n+3} \left[1 - \frac{(\frac{n}{2}+j+1)(\frac{n}{2}-j)}{(\frac{n}{2}+j+2)(\frac{n}{2}-j+1)}\right]. \tag{258}$$

To evaluate α_ϕ in the asymptotic limit $n \to \infty$, we introduce the variable $x = \frac{2j}{n}$ and approximate the sum in Eq. (258) by the integral over x as

$$\begin{aligned} \alpha_\phi &= \frac{4}{n+3} \int_0^1 \mathrm{d}x \frac{n}{2} \sin^2\frac{(x+\frac{1}{n})\pi}{1+\frac{3}{n}} \left[1 - \frac{(1+x+\frac{2}{n})(1-x)}{(1+x+\frac{4}{n})(1-x+\frac{2}{n})}\right] + O(n^{-2}) && (259)\\ &= \frac{8}{n} \int_0^1 \mathrm{d}x \frac{\sin^2(x\pi)}{1-x^2} + O(n^{-2}) && (260)\\ &\approx \frac{6.2287}{n} + O(n^{-2}), && (261) \end{aligned}$$

where the integral is evaluated by Mathematica [75]. Thus, utilizing this estimation method to construct the parallel isometry adjointation protocol, one can achieve

$$\epsilon = \max\{\alpha_\phi, 1 - F_{\mathrm{est}}\} = \frac{6.2287}{n} + O(n^{-2}). \tag{262}$$

For a higher-dimension $d > 2$, Ref. [14] presents an asymptotically optimal unitary estimation protocol achieving the entanglement fidelity $F_{\mathrm{est}} = 1 - O(d^4 n^{-2})$. This protocol utilizes the probe state given by

$$|\phi\rangle = \sum_{\lambda \in \mathrm{S}_{\mathrm{young}}} \sqrt{\frac{q_\lambda}{d_\lambda m_\lambda^{(d)}}} \sum_{i=1}^{d_\lambda} \sum_{u=1}^{m_\lambda^{(d)}} (|\lambda, i\rangle_{\mathcal{S}_\lambda} \otimes |\lambda, u\rangle_{\mathcal{U}_\lambda^{(d)}})_{\mathcal{I}^n} \otimes (|\lambda, i\rangle_{\mathcal{S}_\lambda} \otimes |\lambda, u\rangle_{\mathcal{U}_\lambda^{(d)}})_{\mathcal{A}}, \tag{263}$$

where $\{q_\lambda\}$ is a probability distribution over the set $\mathrm{S}_{\mathrm{young}} \subset \mathbb{Y}_n^d$ defined by

$$\begin{aligned} \mathrm{S}_{\mathrm{young}} := \{\lambda \in \mathbb{Y}_n^d | \lambda_i = \mu_{0,i} + N(2d-3) + 1 - (N+1)(i-1) + \tilde{\lambda}_i \\ \forall i \leq d-1, \exists \tilde{\lambda} \in \{0, \cdots, N-1\}^{d-1}\}. \end{aligned} \tag{264}$$

Here, λ_i represents the number of boxes in the i-th row of λ, N is defined by $N := \lfloor \frac{1}{3d-2}(\frac{2n}{d-1} + d - 2)\rfloor$, $\mu_{0,i}$ is defined by $\mu_{0,i} := \lfloor \frac{n_0}{d} \rfloor + 1$ for $i \in \{1, \cdots, n_0 - \lfloor \frac{n_0}{d} \rfloor d\}$ and $\mu_{0,i} := \lfloor \frac{n_0}{d} \rfloor$ for $i \in \{n_0 - \lfloor \frac{n_0}{d} \rfloor d + 1, \cdots, d\}$, and n_0 is defined by $n_0 := n - \frac{((3d-2)N-d+2)(d-1)}{2}$. Then, the value α_ϕ shown in Theorem 6 is evaluated as

$$\alpha_\phi = \sum_{\lambda \in \mathbb{S}_{\mathrm{young}}} q_\lambda \left[1 - \sum_{\mu \in \lambda + \square \setminus \mathbb{Y}^d_{n+1}} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\mu)}\right] \tag{265}$$

$$= \sum_{\lambda \in \mathbb{S}_{\mathrm{young}}} q_\lambda \left[1 - \prod_{i=1}^{d} \frac{\lambda_i + d - i}{\lambda_i + d - i + 1}\right]. \tag{266}$$

We evaluate α_ϕ in the asymptotic limit $n \to \infty$. In this region, λ_i is given by

$$\lambda_i = \frac{4n}{3d} - \frac{2n}{3d^2}(i-1) + O(d, d^{-2}n). \tag{267}$$

Thus, α_ϕ is evaluated as follows.

$$\alpha_\phi = 1 - \prod_{i=1}^{d} \left[1 - \frac{3d}{2n} \frac{1 + O(d^2 n^{-1}, d^{-1})}{2 - \frac{i-1}{d}}\right] \tag{268}$$

$$= \frac{3d}{2n} \sum_{i=1}^{d} \frac{1}{2 - \frac{i-1}{d}} + O(d^4 n^{-2}, dn^{-1}). \tag{269}$$

$$= \frac{3d^2}{2n} \int_0^1 \frac{\mathrm{d}x}{2-x} + O(d^4 n^{-2}, dn^{-1}) \tag{270}$$

$$= \frac{3 \ln 2}{2} \frac{d^2}{n} + O(d^4 n^{-2}, dn^{-1}). \tag{271}$$

Thus, utilizing this estimation method to construct the parallel isometry adjointation protocol, one can achieve

$$\epsilon = \max\{\alpha_\phi, 1 - F_{\mathrm{est}}\} = \frac{3 \ln 2}{2} \frac{d^2}{n} + O(d^4 n^{-2}, dn^{-1}). \tag{272}$$

C Proof of Theorem 10: Optimal construction of isometry inversion, universal error detection, and isometry adjointation protocols

We show Theorem 10 by constructing the parallel or sequential protocol for isometry inversion, universal error detection, and isometry adjointation in the forms shown in Theorems 5 and 6 and Corollaries 7 and 8 achieving the optimal performances among parallel or sequential protocols. To this end, we utilize Theorem 9 to write down the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetric Choi operators of parallel or sequential protocols achieving the optimal performances. Then we construct the protocols in the forms shown in Theorems 5 and 6 and Corollaries 7 and 8 by constructing the corresponding Choi operators.

Suppose $\mathcal{I}_1 = \cdots = \mathcal{I}_n = \mathcal{F} = \mathbb{C}^d$, $\mathcal{O}_1 = \cdots = \mathcal{O}_n = \mathcal{P} = \mathbb{C}^D$, $\mathcal{O}'_1 = \cdots = \mathcal{O}'_n = \mathcal{P}' = \mathbb{C}^d$, and we define the joint Hilbert spaces $\mathcal{I}^n := \bigotimes_{i=1}^n \mathcal{I}_i$, $\mathcal{O}^n := \bigotimes_{i=1}^n \mathcal{O}_i$, and $\mathcal{O}'^n := \bigotimes_{i=1}^n \mathcal{O}'_i$. We assume that

$$C \in \begin{cases} \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}) & \text{(isometry inversion, isometry adjointation)} \\ \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P}) & \text{(universal error detection)} \end{cases} \tag{273}$$

is the Choi operator satisfying the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry (320), which can be written as Eqs. (321) or (322) using $\{C_{\mu\nu}\}$ or $\{C_{\lambda\nu}\}$. If C is the Choi operator of parallel or sequential protocol, i.e., $C \in \mathcal{W}^{(x)}$ for $x \in \{\mathrm{PAR}, \mathrm{SEQ}\}$, the Choi operator

$$C' \in \begin{cases} \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^n \otimes \mathcal{P}' \otimes \mathcal{F}) & \text{(isometry inversion, isometry adjointation)} \\ \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^n \otimes \mathcal{P}') & \text{(universal error detection)} \end{cases} \tag{274}$$

defined by

$$C' \coloneqq \sum_{\mu \in \mathbb{Y}_{n+1}^d} \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[C_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)} m_\nu^{(D)}} (E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}} \otimes (E_{kl}^{\nu,d})_{\mathcal{P}'\mathcal{O}'^n} \tag{275}$$

for isometry inversion or isometry adjointation, and

$$C' \coloneqq \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} \frac{[C_{\lambda\nu}]_{ak,bl}}{m_\lambda^{(d)} m_\nu^{(D)}} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,d})_{\mathcal{P}'\mathcal{O}'^n} \tag{276}$$

for universal error detection, satisfies $C' \in \mathcal{W}^{(x)}$ [see Eqs. (330) and (331)]. We utilize this fact to show the construction of the protocols in the forms shown in Theorems 5 and 6 and Corollaries 7 and 8.

C.1 Probabilistic exact isometry inversion

Assume that $\{C_S, C_F\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ is the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetric Choi operator of parallel ($x = \mathrm{PAR}$) or sequential ($x = \mathrm{SEQ}$) protocol achieving the optimal success probability $p_{\mathrm{opt}}^{(x)}(d, D, n)$ of isometry inversion, which can be written as Eqs. (403) and (404). Defining $\{C'_S, C'_F\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^n \otimes \mathcal{P}' \otimes \mathcal{F})$ by

$$C'_S = \sum_{\mu \in \mathbb{Y}_{n+1}^d} \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[S_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)} m_\nu^{(D)}} (E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}} \otimes (E_{kl}^{\nu,d})_{\mathcal{P}'\mathcal{O}'^n}, \tag{277}$$

$$C'_F = \sum_{\mu \in \mathbb{Y}_{n+1}^d} \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[F_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)} m_\nu^{(D)}} (E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}} \otimes (E_{kl}^{\nu,d})_{\mathcal{P}'\mathcal{O}'^n}, \tag{278}$$

$C'_S, C'_F \geq 0$ and $C' \coloneqq C'_S + C'_F \in \mathcal{W}^{(x)}$ holds. Thus, the corresponding supermap $\{\mathcal{C}_S, \mathcal{C}_F\}$ can be implemented in a parallel ($x = \mathrm{PAR}$) or sequential ($x = \mathrm{SEQ}$) protocol. In particular for the case $x = \mathrm{PAR}$, since its Choi operator satisfies the $\mathbb{U}(d) \times \mathbb{U}(d)$ symmetry, it can be implemented using a delayed input-state protocol [27, 28]. Since $\{C_S, C_F\}$ achieves the optimal success probability $p_{\mathrm{opt}}^{(x)}(d, D, n)$, it satisfies [see Eq. (402)]

$$\mathrm{Tr}(C_S \Omega) = p_{\mathrm{opt}}^{(x)}(d, D, n), \tag{279}$$

$$\mathrm{Tr}(C_S \Omega) = \mathrm{Tr}[C_S(\Xi \otimes \mathbb{1}_{\mathcal{F}})]. \tag{280}$$

Defining Ω' and Ξ' by replacing $\mathcal{P}\mathcal{O}^n$ and D in Eqs. (394) and (396) with $\mathcal{P}'\mathcal{O}'^n$ and d, respectively, $\{C'_S, C'_F\}$ satisfies

$$\mathrm{Tr}(C'_S \Omega') = p_{\mathrm{opt}}^{(x)}(d, D, n), \tag{281}$$

$$\mathrm{Tr}(C'_S \Omega') = \mathrm{Tr}[C'_S(\Xi' \otimes \mathbb{1}_{\mathcal{F}})], \tag{282}$$

which implies $\{C'_S, C'_F\}$ implements probabilistic exact d-dimensional unitary inversion with success probability $p_{\mathrm{opt}}^{(x)}(d, D, n)$. Therefore, we can construct a parallel or sequential protocol achieving the optimal success probability $p_{\mathrm{opt}}^{(x)}(d, D, n)$ of isometry inversion using the construction shown in Theorem 7.

C.2 Deterministic isometry inversion

Assume that $C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ is the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetric Choi operator of parallel ($x = \text{PAR}$) or sequential ($x = \text{SEQ}$) protocol achieving the optimal worst-case channel fidelity $F_{\text{opt}}^{(x)}(d, D, n)$, which can be written as Eq. (321). Defining $C' \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^n \otimes \mathcal{P}' \otimes \mathcal{F})$ by Eq. (275), $C' \geq 0$ and $C' \in \mathcal{W}^{(x)}$ holds. Thus, the corresponding supermap $\mathcal{C}$ can be implemented in a parallel or sequential protocol. In particular for the case $x = \text{PAR}$, since its Choi operator satisfies the $\mathbb{U}(d) \times \mathbb{U}(d)$ symmetry, it can be implemented using an estimation-based protocol [29]. Since C achieves the optimal worst-case channel fidelity $F_{\text{opt}}^{(x)}(d, D, n)$, it satisfies [see Eq. (410)]

$$\operatorname{Tr}(C\Omega) = F_{\text{opt}}^{(x)}(d, D, n). \tag{283}$$

Defining Ω' by replacing $\mathcal{P}\mathcal{O}^n$ and D in Eq. (394) with $\mathcal{P}'\mathcal{O}'^n$ and d, respectively, C' satisfies

$$\operatorname{Tr}(C'\Omega') = F_{\text{opt}}^{(x)}(d, D, n), \tag{284}$$

which implies C' implements deterministic d-dimensional unitary inversion with worst-case channel fidelity $p_{\text{opt}}^{(x)}(d, D, n)$. Therefore, we can construct a parallel or sequential protocol achieving the optimal worst-case channel fidelity $F_{\text{opt}}^{(x)}(d, D, n)$ of isometry inversion using the construction shown in Theorem 7.

C.3 Universal error detection

Assume that $\{C_I, C_O\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P})$ is the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetric Choi operator of a parallel ($x = \text{PAR}$) or sequential ($x = \text{SEQ}$) protocol achieving the optimal error $\alpha_{\text{opt}}^{(x)}(d, D, n)$, which can be written as Eqs. (413) and (414). Defining $C'' \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^n \otimes \mathcal{P}')$ by Eq. (276) for $C_{\lambda\nu} := I_{\lambda\nu} + O_{\lambda\nu}$ for $\lambda \in \mathbb{Y}_n^d$ and $\nu \in \mathbb{Y}_{n+1}^d$, $C'' \geq 0$ and $C'' \in \mathcal{W}^{(x)}$ hold. Characterization of $\mathcal{W}^{(x)}$ shown in Eqs. (318) and (319) for the case $\mathcal{F} = \mathbb{C}$ (no global future) and the $\mathbb{U}(d) \times \mathbb{U}(d)$ symmetry of C'' implies that C'' can be written as

$$C'' = \begin{cases} \phi_{\mathcal{I}^n} \otimes \mathbb{1}_{\mathcal{P}'\mathcal{O}'^n} & (x = \text{PAR}), \\ C' \otimes \mathbb{1}_{\mathcal{O}_n} & (x = \text{SEQ}), \end{cases} \tag{285}$$

where $\phi \in \mathcal{L}(\mathcal{I}^n)$ is a quantum state and $C' \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^{n-1} \otimes \mathcal{P}')$ is the Choi operator of a $(n-1)$-slot sequential protocol. Since $\{C_I, C_O\}$ achieves the optimal error $\alpha_{\text{opt}}^{(x)}(d, D, n)$, it satisfies [see Eq.(412)]

$$\operatorname{Tr}(C_I\Sigma) = \alpha_{\text{opt}}^{(x)}(d, D, n), \tag{286}$$

$$\operatorname{Tr}(C_I\Xi) = 1. \tag{287}$$

Since Eq. (287) corresponds to the condition

$$\operatorname{Tr}\, \mathcal{C}_I(\mathcal{V}_{\text{in}}^{\otimes n})(\rho_{\text{in}}) = 1 \quad \forall \rho_{\text{in}} \in \mathcal{L}(\operatorname{Im} V_{\text{in}}), \tag{288}$$

it can be replaced with the equivalent condition

$$\operatorname{Tr}\, \mathcal{C}_O(\mathcal{V}_{\text{in}}^{\otimes n})(\rho_{\text{in}}) = 0 \quad \forall \rho_{\text{in}} \in \mathcal{L}(\operatorname{Im} V_{\text{in}}), \tag{289}$$

which can be represented as

$$\mathrm{Tr}(C_O \Xi) = 0. \tag{290}$$

Therefore, we obtain [see Eq. (396)]

$$0 = \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \mathbb{Y}_{n+1}^d} \mathrm{Tr}(O_{\lambda\nu} \Xi_{\lambda\nu}) \tag{291}$$

$$= \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{\lambda \in \nu - \square} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} \frac{m_\nu^{(d)}}{d m_\nu^{(D)} m_\lambda^{(d)}} [\pi_\nu]^*_{a_\nu^\lambda k} [\pi_\nu]_{l b_\nu^\lambda} [O_{\lambda\nu}]_{ba,lk}, \tag{292}$$

which leads to

$$\sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} [\pi_\nu]^*_{a_\nu^\lambda k} [\pi_\nu]_{l b_\nu^\lambda} [O_{\lambda\nu}]_{ba,lk} = 0 \quad \forall \nu \in \mathbb{Y}_{n+1}^d, \lambda \in \nu - \square. \tag{293}$$

Thus, we obtain [see Eq. (401)]

$$\mathrm{Tr}(O_{\lambda\nu} \Sigma_{\lambda\nu}) = 0 \quad \forall \nu \in \mathbb{Y}_{n+1}^d, \lambda \in \nu - \square. \tag{294}$$

Since Eq. (401) reduces to Σ defined in Eq. (74) by replacing $\mathcal{P}\mathcal{O}^n$ and D with $\mathcal{P}'\mathcal{O}'^n$ and d,

$$\mathrm{Tr}(C''\Sigma) = \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{\lambda \in \nu - \square} \mathrm{Tr}(C_{\lambda\nu} \Sigma_{\lambda\nu}) \tag{295}$$

$$= \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{\lambda \in \nu - \square} \mathrm{Tr}(I_{\lambda\nu} \Sigma_{\lambda\nu}) \tag{296}$$

$$\leq \mathrm{Tr}(C_I \Sigma) \tag{297}$$

$$= \alpha_{\mathrm{opt}}^{(x)} \tag{298}$$

holds. Substituting Eq. (285) for $x = \mathrm{PAR}, \mathrm{SEQ}$ to Eq. (298), we obtain

$$\alpha_{\mathrm{opt}}^{(\mathrm{PAR})} \geq \mathrm{Tr}(\phi \, \mathrm{Tr}_{\mathcal{P}'\mathcal{O}'^n}(\Sigma)) \tag{299}$$

$$= \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \lambda + \square \cap \mathbb{Y}_{n+1}^d} \mathrm{Tr}\left(\phi \Pi_\lambda^{(d)}\right) \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\nu)} \tag{300}$$

$$= \alpha_\phi, \tag{301}$$

$$\alpha_{\mathrm{opt}}^{(\mathrm{SEQ})} \geq \mathrm{Tr}(C' \, \mathrm{Tr}_{\mathcal{O}'_n}(\Sigma)) \tag{302}$$

$$= \mathrm{Tr}(C'\Sigma') \tag{303}$$

$$= \alpha_{C'}, \tag{304}$$

where α_ϕ and $\alpha_{C'}$ are defined in Theorem 8, respectively. Thus, the parallel and sequential protocols constructed in Theorem 8 achieves the optimal error $\alpha_{\mathrm{opt}}^{(x)}(d, D, n)$.

C.4 Isometry adjointation

Assume that $\{C_I, C_O\} \subset \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$ is the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetric Choi operator of parallel ($x = \mathrm{PAR}$) or sequential ($x = \mathrm{SEQ}$) protocol achieving the optimal worst-case diamond-norm error $\epsilon_{\mathrm{opt}}^{(x)}(d, D, n)$ of isometry adjointation, which can be written as

Eqs. (419) and (420). Defining $C' \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}'^n \otimes \mathcal{P}' \otimes \mathcal{F})$ by Eq. (275) for $C_{\mu\nu} := I_{\mu\nu} + O_{\mu\nu}$ for $\mu, \nu \in \mathbb{Y}_{n+1}^d$, $C' \geq 0$ and $C' \in \mathcal{W}^{(x)}$ hold. Thus, the corresponding supermap $\mathcal{C}''$ can be implemented by a parallel ($x = \mathrm{PAR}$) or sequential ($x = \mathrm{SEQ}$) protocol. In particular, for the case $x = \mathrm{PAR}$, since its Choi operator satisfies the $\mathbb{U}(d) \times \mathbb{U}(d)$ symmetry, it can be implemented using a covariant-estimation-based protocol as shown in Fig. 4 (a-1) [14, 29]. Since $\{C_I, C_O\}$ achieves the optimal worst-case diamond-norm error $\epsilon_{\mathrm{opt}}^{(x)}(d, D, n)$ of isometry adjointation, it satisfies [see Eq. (418)]

$$1 - \mathrm{Tr}(C_I \Omega) \leq \epsilon_{\mathrm{opt}}^{(x)}(d, D, n), \tag{305}$$

$$\mathrm{Tr}[C_I(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] \leq \epsilon_{\mathrm{opt}}^{(x)}(d, D, n), \tag{306}$$

$$\mathrm{Tr}[C_I(\Xi \otimes \mathbb{1}_{\mathcal{F}})] = 1. \tag{307}$$

Similarly to Sections C.2 and C.3, defining Ω' by replacing $\mathcal{P}\mathcal{O}^n$ and D in Eq. (394) with $\mathcal{P}'\mathcal{O}'^n$ and d, we obtain

$$1 - \mathrm{Tr}(C' \Omega') \leq \epsilon_{\mathrm{opt}}^{(x)}(d, D, n), \tag{308}$$

$$\mathrm{Tr}[C'(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] \leq \epsilon_{\mathrm{opt}}^{(x)}(d, D, n). \tag{309}$$

For the case $x = \mathrm{PAR}$, C' can be implemented by a covariant unitary-estimation protocol achieving the average fidelity $F_{\mathrm{est}} = \mathrm{Tr}(C'\Omega')$ [14, 29]. $\mathrm{Tr}[C'(\Sigma \otimes \mathbb{1}_{\mathcal{F}})]$ can be evaluated by the probe state $\phi \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{A})$ of the unitary estimation protocol as

$$\begin{aligned}
\mathrm{Tr}[C'(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] &= \mathrm{Tr}[\mathrm{Tr}_{\mathcal{F}}(C)\Sigma] && (310)\\
&= \mathrm{Tr}(\mathrm{Tr}_{\mathcal{A}}(\phi)\, \mathrm{Tr}_{\mathcal{P}'\mathcal{O}'^n}(\Sigma)) && (311)\\
&= \sum_{\lambda \in \mathbb{Y}_n^d} \mathrm{Tr}\left[\mathrm{Tr}_{\mathcal{A}}(\phi) \Pi_\lambda^{(d)}\right] \left[1 - \sum_{\nu \in \lambda + \square \setminus \mathbb{Y}_{n+1}^d} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\nu)}\right] && (312)\\
&= \alpha_\phi, && (313)
\end{aligned}$$

where α_ϕ is defined in Theorem 6. Thus, the parallel protocol constructed in Theorem 6 achieves the optimal worst-case diamond-norm error $\epsilon_{\mathrm{opt}}^{(\mathrm{PAR})}(d, D, n)$.

For the case $x = \mathrm{SEQ}$, $\mathrm{Tr}(C'\Omega')$ represents the worst-case channel fidelity of d-dimensional unitary inversion, and $\mathrm{Tr}[C'(\Sigma \otimes \mathbb{1}_{\mathcal{F}})]$ can be evaluated as [see Eq. (319)]

$$\begin{aligned}
\mathrm{Tr}[C'(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] &= \mathrm{Tr}[\mathrm{Tr}_{\mathcal{F}}(C')\Sigma] && (314)\\
&= \alpha_{C'}, && (315)
\end{aligned}$$

where $\alpha_{C'}$ is defined in Theorem 5. Thus, the sequential protocol constructed in Theorem 5 achieves the optimal worst-case diamond-norm error $\epsilon_{\mathrm{opt}}^{(\mathrm{SEQ})}(d, D, n)$.

D Numerical results

We show the numerical results on the optimal performances of probabilistic exact isometry inversion, deterministic isometry inversion, universal error detection, and isometry adjointation using n calls of an input isometry operation $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ with parallel, sequential, or general protocols including indefinite causal order in Tables 1, 2, 3 and 4. The obtained values are compatible with the previous works [27, 29, 30, 35], where Ref. [27] shows the maximum success probability of unitary inversion for the cases of $d = 2, n \leq 3$

and $d = 3, n \leq 2$, Ref. [29] shows the maximum channel fidelity of unitary inversion for the cases of $d = 2, n \leq 3$ and $d = 3, n \leq 2$, Ref. [27] shows the maximum success probability of isometry inversion for the cases of $d = 2, n \leq 3$ and $d = 3, n \leq 2$, and Ref. [30] shows the maximum channel fidelity of unitary inversion for parallel and sequential protocols for the cases of $d \leq 6$ and $n \leq 5$.

$p_{\mathrm{opt}}^{(x)}$	Parallel ($x = \mathrm{PAR}$)			Sequential ($x = \mathrm{SEQ}$)			General ($x = \mathrm{GEN}$)		
	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$
$n = 1$	0.2500	0.0000	0.0000	0.2500	0.0000	0.0000	0.2500	0.0000	0.0000
$n = 2$	0.4000	0.1111	0.0000	0.4286	0.1111	0.0000	0.4286	0.1111	0.0000
$n = 3$	0.5000	0.1385	0.0625	0.7500	0.1861	0.0625	0.9415	0.2093	0.0625
$n = 4$	0.5715	0.2000	0.0708	1.0000	0.2674	0.1064	1.0000	0.2915	0.1419
$n = 5$	0.6250	0.2408	0.0865	1.0000	0.4662	0.1447	-	-	-

Table 1: The maximum success probability of isometry inversion using n calls of an input isometry operation $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ $(D \geq d + 1)$ in parallel, sequential, and general protocols.

$F_{\mathrm{opt}}^{(x)}$	Parallel ($x = \mathrm{PAR}$)			Sequential ($x = \mathrm{SEQ}$)			General ($x = \mathrm{GEN}$)		
	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$
$n = 1$	0.5000	0.2222	0.1250	0.5000	0.2222	0.1250	0.5000	0.2222	0.1250
$n = 2$	0.6545	0.3333	0.1875	0.7500	0.3333	0.1875	0.7500	0.3333	0.1875
$n = 3$	0.7500	0.4310	0.2500	0.9330	0.4444	0.2500	0.9851	0.4444	0.2500
$n = 4$	0.8117	0.5131	0.3105	1.0000	0.5556	0.3125	1.0000	0.5556	0.3125
$n = 5$	0.8536	0.5810	0.3675	1.0000	0.6667	0.3750	-	-	-

Table 2: The maximum worst-case channel fidelity of isometry adjointation using n calls of an input isometry operation $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ $(D \geq d + 1)$ in parallel, sequential, and general protocols.

$\alpha_{\text{opt}}^{(x)}$	Parallel ($x = \text{PAR}$)			Sequential ($x = \text{SEQ}$)			General ($x = \text{GEN}$)		
	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$
$n = 1$	**1**	**1**	**1**	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
$n = 2$	**2/3**	**1**	**1**	0.6667	1.0000	1.0000	0.6667	1.0000	1.0000
$n = 3$	**5/8**	**3/4**	**1**	0.5000	0.7500	1.0000	0.4375	0.7500	1.0000
$n = 4$	**1/2**	**11/15**	**4/5**	0.4000	0.6000	0.8000	0.3600	0.4667	0.8000
$n = 5$	**7/15**	**7/10**	**19/24**	0.3333	0.5000	0.6667	-	-	-

Table 3: The minimum approximation error of universal error detection using n calls of an input isometry operation $V_{\text{in}} \in \mathbb{V}_{\text{iso}}(d, D)$ $(D \geq d + 1)$ in parallel, sequential, and general protocols. Bold values are obtained analytically.

$\epsilon_{\text{opt}}^{(x)}$	Parallel ($x = \text{PAR}$)			Sequential ($x = \text{SEQ}$)			General ($x = \text{GEN}$)		
	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$	$d = 2$	$d = 3$	$d = 4$
$n = 1$	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
$n = 2$	0.6736	1.0000	1.0000	0.6667	1.0000	1.0000	0.6667	1.0000	1.0000
$n = 3$	0.6250	0.7822	1.0000	0.5000	0.7500	1.0000	0.5000	0.7500	1.0000
$n = 4$	0.5169	0.7373	0.8448	0.4444	0.6429	0.8000	0.4444	0.6429	0.8000

Table 4: The minimum approximation error of isometry adjointation using n calls of an input isometry operation $V_{\text{in}} \in \mathbb{V}_{\text{iso}}(d, D)$ $(D \geq d + 1)$ in parallel, sequential, and general protocols.

$p_{\text{opt}}^{(\text{GEN})}$	$d = 2$		$d = 3$		$d = 4$	
	$D = 2$	$D = 3$	$D = 3$	$D = 4$	$D = 4$	$D = 5$
$n = 2$	0.4444	0.4286	0.1111	0.1111	0.0000	0.0000
$n = 3$	0.9415	0.9415	0.3262	0.2093	0.0625	0.0625
$n = 4$	1.0000	1.0000	0.5427	0.2915	0.2609	0.1419

Table 5: Comparison with the maximum success probabilities of unitary inversion $(D = d)$ and isometry inversion $(D = d + 1)$ in general protocols.

$F_{\text{opt}}^{(\text{GEN})}$	$d = 2$		$d = 3$		$d = 4$	
	$D = 2$	$D = 3$	$D = 3$	$D = 4$	$D = 4$	$D = 5$
$n = 2$	0.8249	0.7500	0.3333	0.3333	0.1875	0.1875
$n = 3$	0.9921	0.9851	0.5835	0.4444	0.2500	0.2500
$n = 4$	1.0000	1.0000	0.7874	0.5556	0.4567	0.3125

Table 6: Comparison with the maximum worst-case channel fidelities of unitary inversion $(D = d)$ and isometry inversion $(D = d + 1)$ in general protocols.

E Semidefinite programming to obtain the optimal transformations of isometry operations with the $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry

As shown in Theorem 9, the optimal protocols for isometry inversion, universal error detection and isometry adjointation can be searched within the Choi operators having the $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry. To utilize this symmetry for a numerical search of the optimal protocols, we derive the characterization of the quantum superchannels and the conditions for isometry inversion, universal error detection, and isometry adjointation under the $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry. Then, we derive the SDPs giving the optimal performances of these tasks, which are shown below.

E.1 Choi representation of general superchannels and $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry

As shown in Section 4.1, the Choi operator C of a quantum superchannel $\mathcal{C}:\bigotimes_{i=1}^n[\mathcal{L}(\mathcal{I}_i)\to\mathcal{L}(\mathcal{O}_i)]\to[\mathcal{L}(\mathcal{P})\to\mathcal{L}(\mathcal{F})]$ implemented by parallel ($x=\mathrm{PAR}$) and sequential ($x=\mathrm{SEQ}$) protocols, and general superchannels ($x=\mathrm{GEN}$) can be represented by a Choi operator $C\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P}\otimes\mathcal{F})$ satisfying

$$C\geq 0, \tag{316}$$

$$C\in\mathcal{W}^{(x)}. \tag{317}$$

The set $\mathcal{W}^{(x)}$ for $x\in\{\mathrm{PAR},\mathrm{SEQ}\}$ are given by [27, 44]

$$C\in\mathcal{W}^{(\mathrm{PAR})}\iff\begin{cases}\mathrm{Tr}_{\mathcal{F}}\,C=\mathrm{Tr}_{\mathcal{O}^n}\,C\otimes\mathbb{1}_{\mathcal{O}^n}/\dim\mathcal{O}^n\\ \mathrm{Tr}_{\mathcal{I}^n\mathcal{O}^n}\,C=\dim\mathcal{O}^n\mathbb{1}_{\mathcal{P}}\end{cases}, \tag{318}$$

$$C\in\mathcal{W}^{(\mathrm{SEQ})}\iff\mathrm{Tr}_{\mathcal{I}_i}\,C^{(i)}=C^{(i-1)}\otimes\mathbb{1}_{\mathcal{O}_{i-1}}\quad\forall i\in\{1,\cdots,n+1\}, \tag{319}$$

where $\mathcal{O}_0$ and $\mathcal{I}_{n+1}$ are defined by $\mathcal{O}_0:=\mathcal{P}$ and $\mathcal{I}_{n+1}:=\mathcal{F}$, and $C^{(i)}$ for $i\in\{0,\cdots,n+1\}$ are defined by $C^{(n+1)}:=C$, $C^{(i-1)}:=\mathrm{Tr}_{\mathcal{O}_{i-1}\mathcal{I}_i}\,C^{(i)}/\dim\mathcal{O}_{i-1}$ and $C^{(0)}:=1$. The characterization of the set $\mathcal{W}^{(\mathrm{GEN})}$ is shown in Ref. [76].

We consider the case $\mathcal{I}_1=\cdots=\mathcal{I}_n=\mathcal{F}=\mathbb{C}^d,\mathcal{P}=\mathcal{O}_1=\cdots=\mathcal{O}_n=\mathbb{C}^D$ (isometry inversion, isometry adjointation) and $\mathcal{I}_1=\cdots=\mathcal{I}_n=\mathbb{C}^d,\mathcal{P}=\mathcal{O}_1=\cdots=\mathcal{O}_n=\mathbb{C}^D,\mathcal{F}=\mathbb{C}$ (universal error detection), and characterize the Choi operator $C\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P}\otimes\mathcal{F})$ under the $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry given by

$$\begin{cases}[C,U_{\mathcal{I}^n\mathcal{F}}^{\otimes n+1}\otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}]=0 & \text{(isometry inversion, isometry adjointation)}\\ [C,U_{\mathcal{I}^n}^{\otimes n}\otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}]=0 & \text{(universal error detection)}\end{cases} \tag{320}$$

for all $U\in\mathbb{U}(d)$ and $U'\in\mathbb{U}(D)$ (see Theorem 9). Due to this symmetry, the Choi operator C can be written using the operator $E_{ij}^{\mu,d}$ introduced in Eq. (54) as

$$C=\sum_{\mu\in\mathbb{Y}_{n+1}^d}\sum_{\nu\in\mathbb{Y}_{n+1}^D}\sum_{i,j=1}^{d_\mu}\sum_{k,l=1}^{d_\nu}\frac{[C_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)}m_\nu^{(D)}}(E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}}\otimes(E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n} \tag{321}$$

for isometry inversion or isometry adjointation, and

$$C=\sum_{\lambda\in\mathbb{Y}_n^d}\sum_{\nu\in\mathbb{Y}_{n+1}^D}\sum_{a,b=1}^{d_\lambda}\sum_{k,l=1}^{d_\nu}\frac{[C_{\lambda\nu}]_{ak,bl}}{m_\lambda^{(d)}m_\nu^{(D)}}(E_{ab}^{\lambda,d})_{\mathcal{I}^n}\otimes(E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n} \tag{322}$$

for universal error detection using a $d_\mu d_\nu$ ($d_\lambda d_\nu$)-dimensional square matrix $C_{\mu\nu}$ ($C_{\lambda\nu}$), where ik (ak) and jl (bl) are the indices for row and column numbers, respectively. The characterization of quantum superchannels is rewritten in terms of $C_{\mu\nu}$ or $C_{\lambda\nu}$ as follows. By definition of $E^{\mu,d}_{ij}$ in Eq. (54), the positivity of C is written as

$$\begin{cases} C_{\mu\nu} \geq 0 \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1} & \text{(isometry inversion, isometry adjointation)} \\ C_{\lambda\nu} \geq 0 \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1} & \text{(universal error detection)} \end{cases}. \tag{323}$$

Using Lemma 3, the condition $C \in \mathcal{W}^{(x)}$ for $x \in \{\mathrm{PAR}, \mathrm{SEQ}\}$ is given by

$$C \in \mathcal{W}^{(x)} \iff \begin{cases} \{C_{\mu\nu}\} \in \mathcal{W}^{(x)}_{\mathrm{sym}} & \text{(isometry inversion, isometry adjointation)} \\ \{C_{\lambda\nu}\} \in \mathcal{W}^{(x)}_{\mathrm{sym}} & \text{(universal error detection)} \end{cases}, \tag{324}$$

where $\mathcal{W}^{(x)}_{\mathrm{sym}}$ is given by

$$\{C_{\mu\nu}\} \in \mathcal{W}^{(\mathrm{PAR})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \displaystyle\sum_{\mu \in \lambda + \square} (X^\lambda_\mu \otimes \mathbb{1}_{d_\nu}) \frac{C_{\mu\nu}}{m^{(D)}_\nu} (X^\lambda_\mu \otimes \mathbb{1}_{d_\nu})^\dagger = D_\lambda \otimes \frac{\mathbb{1}_{d_\nu}}{D^{n+1}} \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1} \\ \displaystyle\sum_{\mu \in \mathbb{Y}^d_{n+1}} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \mathrm{Tr}(C_{\mu\nu}) = D^{n+1} \end{cases}, \tag{325}$$

$$\{C_{\mu\nu}\} \in \mathcal{W}^{(\mathrm{SEQ})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \displaystyle\sum_{\lambda \in \gamma + \square} (X^\gamma_\lambda \otimes \mathbb{1}_{d_\kappa}) \frac{C^{(i)}_{\lambda\kappa}}{m^{(D)}_\kappa} (X^\gamma_\lambda \otimes \mathbb{1}_{d_\kappa})^\dagger = \sum_{\delta \in \kappa - \square} (\mathbb{1}_{d_\gamma} \otimes X^\delta_\kappa)^\dagger \frac{C^{(i-1)}_{\gamma\delta}}{m^{(D)}_\delta} (\mathbb{1}_{d_\gamma} \otimes X^\delta_\kappa) \\ \qquad\qquad\qquad\qquad\qquad\qquad \forall i \in \{1, \cdots, n+1\}, \gamma \in \mathbb{Y}^d_{i-1}, \kappa \in \mathbb{Y}^D_i \\ C^{(0)}_{\emptyset\emptyset} = 1 \end{cases} \tag{326}$$

for isometry inversion and isometry adjointation, where D_λ for $\lambda \in \mathbb{Y}^d_n$ are defined by

$$D_\lambda := \sum_{\mu \in \lambda + \square} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \mathrm{Tr}_\nu[(X^\lambda_\mu \otimes \mathbb{1}_{d_\nu}) C_{\mu\nu} (X^\lambda_\mu \otimes \mathbb{1}_{d_\nu})^\dagger] \tag{327}$$

$C^{(i)}_{\lambda\kappa}$ for $\lambda \in \mathbb{Y}^d_i, \kappa \in \mathbb{Y}^D_i$ are defined by

$$C^{(i)}_{\lambda\kappa} := \begin{cases} C_{\lambda\kappa} & (i = n+1) \\ \frac{1}{D} \sum_{\mu \in \lambda + \square, \nu \in \kappa + \square} (X^\lambda_\mu \otimes X^\kappa_\nu) C^{(i+1)}_{\mu\nu} (X^\lambda_\mu \otimes X^\kappa_\nu)^\dagger & (0 \leq i \leq n) \end{cases}, \tag{328}$$

X^γ_λ for $\lambda \in \gamma + \square, \gamma \in \mathbb{Y}^d_{i-1}$ are $d_\gamma \times d_\lambda$ matrices defined by

$$[X^\gamma_\lambda]_{c,a} := \delta_{c^\gamma_\lambda, a}, \tag{329}$$

c^γ_λ is the index of the standard tableau $s^\lambda_{c^\gamma_\lambda}$ obtained by adding a box $\boxed{i}$ to the standard tableau s_c^γ, and $\emptyset$ represents the Young tableau with zero boxes. The set $\mathcal{W}_{\mathrm{sym}}^{(x)}$ is given by

$$\{C_{\lambda\nu}\} \in \mathcal{W}_{\mathrm{sym}}^{(\mathrm{PAR})} \iff$$
$$\begin{cases} \dfrac{C_{\lambda\nu}}{m_\nu^{(D)}} = D_\lambda \otimes \dfrac{\mathbb{1}_{d_\nu}}{D^{n+1}} \quad \forall\lambda \in \mathbb{Y}_n^d, \nu \in \mathbb{Y}_{n+1}^D \\ \displaystyle\sum_{\lambda\in\mathbb{Y}_{n+1}^d} \sum_{\nu\in\mathbb{Y}_{n+1}^D} \mathrm{Tr}(C_{\lambda\nu}) = D^n \end{cases}, \tag{330}$$

$$\{C_{\lambda\nu}\} \in \mathcal{W}_{\mathrm{sym}}^{(\mathrm{SEQ})} \iff$$
$$\begin{cases} \dfrac{C_{\lambda\nu}}{m_\nu^{(D)}} = \displaystyle\sum_{\kappa\in\nu-\square} (\mathbb{1}_{d_\lambda} \otimes X_\nu^\kappa)^\dagger \frac{C_{\lambda\kappa}^{(n)}}{m_\kappa^{(D)}} (\mathbb{1}_{d_\lambda} \otimes X_\nu^\kappa) \quad \forall\lambda \in \mathbb{Y}_n^d, \nu \in \mathbb{Y}_{n+1}^D \\ \displaystyle\sum_{\lambda\in\gamma+\square} (X_\lambda^\gamma \otimes \mathbb{1}_{d_\kappa}) \frac{C_{\lambda\kappa}^{(i)}}{m_\kappa^{(D)}} (X_\lambda^\gamma \otimes \mathbb{1}_{d_\kappa})^\dagger = \sum_{\delta\in\kappa-\square} (\mathbb{1}_{d_\nu} \otimes X_\kappa^\delta)^\dagger \frac{C_{\gamma\delta}^{(i-1)}}{m_\delta^{(D)}} (\mathbb{1}_{d_\nu} \otimes X_\kappa^\delta) \\ \qquad\qquad\qquad\qquad\qquad\qquad \forall i \in \{1, \cdots, n\}, \gamma \in \mathbb{Y}_{i-1}^d, \kappa \in \mathbb{Y}_i^D \\ C_{\emptyset\emptyset}^{(0)} = 1 \end{cases} \tag{331}$$

for universal error detection, where D_λ for $\lambda \in \mathbb{Y}_n^d$ are defined by

$$D_\lambda \coloneqq \sum_{\nu\in\mathbb{Y}_{n+1}^D} \mathrm{Tr}_\nu(C_{\lambda\nu}), \tag{332}$$

$C_{\lambda\kappa}^{(i)}$ for $\lambda \in \mathbb{Y}_i^d, \kappa \in \mathbb{Y}_i^D$ are defined by

$$C_{\lambda\kappa}^{(i)} \coloneqq \begin{cases} \frac{1}{D} \sum_{\nu\in\kappa+\square} (\mathbb{1}_{d_\lambda} \otimes X_\nu^\kappa) C_{\lambda\nu} (\mathbb{1}_{d_\lambda} \otimes X_\nu^\kappa)^\dagger & (i = n) \\ \frac{1}{D} \sum_{\mu\in\lambda+\square, \nu\in\kappa+\square} (X_\mu^\lambda \otimes X_\nu^\kappa) C_{\mu\nu}^{(i+1)} (X_\mu^\lambda \otimes X_\nu^\kappa)^\dagger & (0 \leq i \leq n-1) \end{cases}, \tag{333}$$

and X_λ^γ are defined in Eq. (329).

E.2 Conditions for isometry inversion, universal error detection, and isometry adjointation under the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry

We consider the action of a supermap $\mathcal{C}$ on n calls of an isometry operation $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ when its Choi operator C satisfies the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry (320). Then, $\mathcal{C}(\mathcal{V}_{\mathrm{in}}^{\otimes n})$ is given in the following form.

Lemma 15. *If the Choi operator of a quantum supermap $\mathcal{C}$, denoted by C, satisfies the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry (320), then $\mathcal{C}(\mathcal{V}_{\mathrm{in}}^{\otimes n})$ for $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ is given by*

$$\mathcal{C}(\mathcal{V}_{\mathrm{in}}^{\otimes n})(\rho_{\mathrm{in}}) = \begin{cases} x V_{\mathrm{in}}^\dagger \rho_{\mathrm{in}} V_{\mathrm{in}} + \dfrac{\mathbb{1}_{\mathcal{F}}}{d} \mathrm{Tr}[\rho_{\mathrm{in}}(y \Pi_{\mathrm{Im}V_{\mathrm{in}}} + z(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}}))] \\ \qquad\qquad\qquad\qquad (\text{isometry inversion, isometry adjointation}) \\ \mathrm{Tr}[\rho_{\mathrm{in}}(v \Pi_{\mathrm{Im}V_{\mathrm{in}}} + w(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}}))] \qquad (\text{universal error detection}) \end{cases} \tag{334}$$

for all $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ and $\rho_{\mathrm{in}} \in \mathcal{L}(\mathbb{C}^d)$, where $\Pi_{\mathrm{Im}V_{\mathrm{in}}}$ and $(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})$ are orthogonal projectors onto the image $\mathrm{Im}V_{\mathrm{in}}$ of V_{in} and its complement $(\mathrm{Im}V_{\mathrm{in}})^\perp$, and $x, y, z, v, w \in \mathbb{C}$ are constant numbers given by

$$x \coloneqq \frac{1}{d^2 - 1} \mathrm{Tr}\Big[C(d^2\Omega - \Xi \otimes \mathbb{1}_{\mathcal{F}})\Big], \tag{335}$$

$$y \coloneqq \frac{d^2}{d^2 - 1} \mathrm{Tr}[C(\Xi \otimes \mathbb{1}_{\mathcal{F}} - \Omega)], \tag{336}$$

$$z \coloneqq \mathrm{Tr}[C(\Sigma \otimes \mathbb{1}_{\mathcal{F}})], \tag{337}$$

for isometry inversion and isometry adjointation, and

$$v := \mathrm{Tr}(C\Xi), \tag{338}$$

$$w := \mathrm{Tr}(C\Sigma), \tag{339}$$

for universal error detection, Ω, Ξ, Σ are defined by

$$\Omega := \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{i,j,k,l=1}^{d_\mu} [\Omega_\mu]_{ik,jl} (E^{\mu,d}_{ij})_{\mathcal{I}^n\mathcal{F}} \otimes (E^{\mu,D}_{kl})_{\mathcal{P}\mathcal{O}^n}, \tag{340}$$

$$\Xi := \sum_{\lambda\in\mathbb{Y}^d_n} \sum_{\nu\in\lambda+\square\cap\mathbb{Y}^d_{n+1}} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} [\Xi_{\lambda\nu}]_{ak,bl} (E^{\lambda,d}_{ab})_{\mathcal{I}^n} \otimes (E^{\nu,D}_{kl})_{\mathcal{P}\mathcal{O}^n} \tag{341}$$

$$\Sigma := \sum_{\lambda\in\mathbb{Y}^d_n} \sum_{\nu\in\lambda+\square} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} [\Sigma_{\lambda\nu}]_{ak,bl} (E^{\lambda,d}_{ab})_{\mathcal{I}^n} \otimes (E^{\nu,D}_{kl})_{\mathcal{P}\mathcal{O}^n}, \tag{342}$$

and $\Omega_\mu \in \mathcal{L}(\mathbb{C}^{d_\mu} \otimes \mathbb{C}^{d_\mu})$ and $\Xi_{\lambda\nu}, \Sigma_{\lambda\nu} \in \mathcal{L}(\mathbb{C}^{d_\lambda} \otimes \mathbb{C}^{d_\nu})$ are defined by

$$[\Omega_\mu]_{ik,jl} := \frac{[\pi_\mu]^*_{ik}[\pi_\mu]_{lj}}{d^2 m^{(D)}_\mu}, \tag{343}$$

$$[\Xi_{\lambda\nu}]_{ak,bl} := \frac{m^{(d)}_\nu}{d m^{(D)}_\nu m^{(d)}_\lambda} [\pi_\nu]^*_{a^\lambda_\nu k} [\pi_\nu]_{l b^\lambda_\nu}, \tag{344}$$

$$[\Sigma_{\lambda\nu}]_{ak,bl} := \frac{1}{D-d}\left[\frac{1}{m^{(D)}_\lambda} - \delta_{\nu\in\mathbb{Y}^D_{n+1}} \frac{m^{(d)}_\nu}{m^{(D)}_\nu m^{(d)}_\lambda}\right] [\pi_\nu]^*_{a^\lambda_\nu k} [\pi_\nu]_{l b^\lambda_\nu}, \tag{345}$$

where $[\pi_\mu]_{ij}$ are matrix elements of the irreducible representation π_μ for $\pi := (12\cdots n+1) \in \mathfrak{S}_{n+1}$ shown in Eq. (49) defined by $[\pi_\mu]_{ij} := \langle \mu, i| \pi_\mu |\mu, j\rangle$, $\delta_{\nu\in\mathbb{Y}^D_{n+1}}$ is defined by $\delta_{\nu\in\mathbb{Y}^D_{n+1}} = 1$ for $\nu \in \mathbb{Y}^D_{n+1}$ and $\delta_{\nu\in\mathbb{Y}^D_{n+1}} = 0$ for $\nu \notin \mathbb{Y}^d_{n+1}$, and a^λ_ν is the index of the standard tableau $s^\nu_{a^\lambda_\nu}$ obtained by adding a box $\boxed{n+1}$ to the standard tableau s^λ_a.

Proof. First, we consider the Choi operator C satisfying

$$[C, U^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \tag{346}$$

for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$. Then, $C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}$ for $V_{\mathrm{in}} \in \mathbb{V}_{\mathrm{iso}}(d, D)$ satisfies

$$C \star |U' V_{\mathrm{in}} U\rangle\!\rangle\langle\!\langle U' V_{\mathrm{in}} U|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}$$

$$= C \star (U^{T\otimes n}_{\mathcal{I}^n} \otimes U'^{\otimes n}_{\mathcal{O}^n}) |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} (U^{T\otimes n}_{\mathcal{I}^n} \otimes U'^{\otimes n}_{\mathcal{O}^n})^\dagger \tag{347}$$

$$= (U^{T\otimes n}_{\mathcal{I}^n} \otimes \mathbb{1}_{\mathcal{F}} \otimes \mathbb{1}_{\mathcal{P}} \otimes U'^{\otimes n}_{\mathcal{O}^n})^T C (U^{T\otimes n}_{\mathcal{I}^n} \otimes \mathbb{1}_{\mathcal{F}} \otimes \mathbb{1}_{\mathcal{P}} \otimes U'^{\otimes n}_{\mathcal{O}^n})^* \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \tag{348}$$

$$= (\mathbb{1}_{\mathcal{I}^n} \otimes U^\dagger_{\mathcal{F}} \otimes U'^*_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{O}^n}) C (\mathbb{1}_{\mathcal{I}^n} \otimes U^\dagger_{\mathcal{F}} \otimes U'^*_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{O}^n})^\dagger \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \tag{349}$$

$$= (U'^*_{\mathcal{P}} \otimes U^\dagger_{\mathcal{F}}) [C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}] (U'^*_{\mathcal{P}} \otimes U^\dagger_{\mathcal{F}})^\dagger \tag{350}$$

for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$. For $U \in \mathbb{U}(d)$ and $U'' \in \mathbb{U}[(\mathrm{Im} V_{\mathrm{in}})^\perp]$, $U' := V_{\mathrm{in}} U V^\dagger_{\mathrm{in}} + U''$ is a unitary operator and $U' V_{\mathrm{in}} U = V_{\mathrm{in}}$ holds. By substituting U and $U' = V_{\mathrm{in}} U V^\dagger_{\mathrm{in}} + U''$ to Eq. (350), we obtain

$$[(V_{\mathrm{in}} U V^\dagger_{\mathrm{in}} + U'')^*_{\mathcal{P}} \otimes U^\dagger_{\mathcal{F}}] [C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}] [(V_{\mathrm{in}} U V^\dagger_{\mathrm{in}} + U'')^*_{\mathcal{P}} \otimes U^\dagger_{\mathcal{F}}]^\dagger = C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}. \tag{351}$$

Decomposing $C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}$ as

$$C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = (V_{\mathrm{in}}^* \otimes \mathbb{1}_{\mathcal{F}})P(V_{\mathrm{in}}^* \otimes \mathbb{1}_{\mathcal{F}})^\dagger + (V_{\mathrm{in}}^* \otimes \mathbb{1}_{\mathcal{F}})Q + R(V_{\mathrm{in}}^* \otimes \mathbb{1}_{\mathcal{F}})^\dagger + S \tag{352}$$

using linear operators $P \in \mathcal{L}(\mathbb{C}^d \otimes \mathcal{F})$, $Q : (\mathrm{Im}V_{\mathrm{in}})^\perp \otimes \mathcal{F} \to \mathbb{C}^d \otimes \mathcal{F}$, $R : \mathbb{C}^d \otimes \mathcal{F} \to (\mathrm{Im}V_{\mathrm{in}})^\perp \otimes \mathcal{F}$, and $S \in \mathcal{L}((\mathrm{Im}V_{\mathrm{in}})^\perp \otimes \mathcal{F})$, Eq. (351) is written as

$$(U^* \otimes U)A(U^* \otimes U)^\dagger = A, \tag{353}$$

$$(U^* \otimes U)B(U''^T \otimes U)^\dagger = B, \tag{354}$$

$$(U''^T \otimes U)C(U^* \otimes U)^\dagger = C, \tag{355}$$

$$(U''^T \otimes U)D(U''^T \otimes U)^\dagger = D. \tag{356}$$

Therefore, P is written as a linear combination of $|\mathbb{1}_d\rangle\!\rangle\langle\!\langle\mathbb{1}_d|$ and $\mathbb{1}_d \otimes \mathbb{1}_d$, $Q = 0$, $R = 0$, and S is proportional to $\mathbb{1}_{(\mathrm{Im}V_{\mathrm{in}})^\perp} \otimes \mathbb{1}_{\mathcal{F}}$. Therefore, $C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n}$ can be expressed by three parameters $x_{V_{\mathrm{in}}}$, $y_{V_{\mathrm{in}}}$, and $z_{V_{\mathrm{in}}}$ as

$$C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = x_{V_{\mathrm{in}}}|V_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{F}} + y_{V_{\mathrm{in}}}(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + z_{V_{\mathrm{in}}}(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^\perp})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}. \tag{357}$$

From Eq. (350), we obtain

$$\begin{aligned}
&x_{U'V_{\mathrm{in}}U}|(U'V_{\mathrm{in}}U)^\dagger\rangle\!\rangle\langle\!\langle(U'V_{\mathrm{in}}U)^\dagger|_{\mathcal{P}\mathcal{F}} + y_{U'V_{\mathrm{in}}U}(\Pi^T_{\mathrm{Im}(U'V_{\mathrm{in}}U)})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + z_{U'V_{\mathrm{in}}U}(\Pi^T_{(\mathrm{Im}(U'V_{\mathrm{in}}U))^\perp})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}\\
&= (U'^*_{\mathcal{P}} \otimes U^\dagger_{\mathcal{F}})[x_{V_{\mathrm{in}}}|V_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{F}} + y_{V_{\mathrm{in}}}(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + z_{V_{\mathrm{in}}}(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^\perp})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}](U'^*_{\mathcal{P}} \otimes U^\dagger_{\mathcal{F}})^\dagger \qquad (358)\\
&= x_{V_{\mathrm{in}}}|(U'V_{\mathrm{in}}U)^\dagger\rangle\!\rangle\langle\!\langle(U'V_{\mathrm{in}}U)^\dagger|_{\mathcal{P}\mathcal{F}} + y_{V_{\mathrm{in}}}(\Pi^T_{\mathrm{Im}(U'V_{\mathrm{in}}U)})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + z_{V_{\mathrm{in}}}(\Pi^T_{(\mathrm{Im}(U'V_{\mathrm{in}}U))^\perp})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}, \qquad (359)
\end{aligned}$$

thus, $x_{V_{\mathrm{in}}}$, $y_{V_{\mathrm{in}}}$ and $z_{V_{\mathrm{in}}}$ does not depend on V_{in}. By rewriting $x_{V_{\mathrm{in}}} = x$, $y_{V_{\mathrm{in}}} = y$ and $z_{V_{\mathrm{in}}} = z$, we obtain

$$C \star |V_{\mathrm{in}}\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = x|V_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{F}} + y(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + z(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^\perp})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}. \tag{360}$$

This Choi operator corresponds to the map

$$\mathcal{C}(\mathcal{V}_{\mathrm{in}}^{\otimes n})(\rho_{\mathrm{in}}) = xV_{\mathrm{in}}^\dagger \rho_{\mathrm{in}} V_{\mathrm{in}} + \frac{\mathbb{1}_{\mathcal{F}}}{d}\mathrm{Tr}[\rho_{\mathrm{in}}(y\Pi_{\mathrm{Im}V_{\mathrm{in}}} + z(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}}))]. \tag{361}$$

We calculate x, y and z as follows. Equation (360) is written as

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{I}^n\mathcal{O}^n}[C(\mathbb{1}_{\mathcal{P}\mathcal{F}} \otimes |V_{\mathrm{in}}^*\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})]\\
&= x|V_{\mathrm{in}}^\dagger\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^\dagger|_{\mathcal{P}\mathcal{F}} + y(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + z(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^\perp})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}.
\end{aligned} \tag{362}$$

Taking the Hilbert-Schmidt inner product with $|V_{\mathrm{in}}^*\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^*|_{\mathcal{F}\mathcal{P}}$, $(\Pi_{\mathrm{Im}V_{\mathrm{in}}})^*_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{F}}$ and $((\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}}))^*_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{F}}$, we obtain

$$\mathrm{Tr}\Big[C|V_{\mathrm{in}}^*\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes |V_{\mathrm{in}}^*\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^*|_{\mathcal{F}\mathcal{P}}\Big] = d^2x + y, \tag{363}$$

$$\mathrm{Tr}\Big[C|V_{\mathrm{in}}^*\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes (\Pi_{\mathrm{Im}V_{\mathrm{in}}})^*_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{F}}\Big] = d(x + y), \tag{364}$$

$$\mathrm{Tr}\Big[C|V_{\mathrm{in}}^*\rangle\!\rangle\langle\!\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes ((\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}}))^*_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{F}}\Big] = (D - d)z. \tag{365}$$

Taking the Haar integral $\mathrm{d}V_{\mathrm{in}}$ on $\mathbb{V}_{\mathrm{iso}}(d,D)$, we obtain

$$\mathrm{Tr}(C\Omega) = x + \frac{y}{d^2}, \tag{366}$$

$$\mathrm{Tr}[C(\Xi \otimes \mathbb{1}_{\mathcal{F}})] = x + y, \tag{367}$$

$$\mathrm{Tr}[C(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] = z, \tag{368}$$

where Ω, Ξ and Σ are defined by

$$\Omega := \frac{1}{d^2}\int_{\mathbb{V}_{\mathrm{iso}}(d,D)} \mathrm{d}V |V\rangle\rangle\langle\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes |V\rangle\rangle\langle\langle V|_{\mathcal{F}\mathcal{P}}, \tag{369}$$

$$\Xi := \frac{1}{d}\int_{\mathbb{V}_{\mathrm{iso}}(d,D)} \mathrm{d}V |V\rangle\rangle\langle\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes (\Pi_{\mathrm{Im}V})_{\mathcal{P}}, \tag{370}$$

$$\Sigma := \frac{1}{D-d}\int_{\mathbb{V}_{\mathrm{iso}}(d,D)} \mathrm{d}V |V\rangle\rangle\langle\langle V|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes ((\mathbb{1}_D - \Pi_{\mathrm{Im}V}))_{\mathcal{P}}. \tag{371}$$

Therefore, x, y and z are given by

$$x = \frac{1}{d^2-1}\mathrm{Tr}\Big[C(d^2\Omega - \Xi \otimes \mathbb{1}_{\mathcal{F}})\Big], \tag{372}$$

$$y = \frac{d^2}{d^2-1}\mathrm{Tr}[C(\Xi \otimes \mathbb{1}_{\mathcal{F}} - \Omega)], \tag{373}$$

$$z = \mathrm{Tr}[C(\Sigma \otimes \mathbb{1}_{\mathcal{F}})]. \tag{374}$$

Next, we consider the Choi operator C satisfying

$$[C, U^{\otimes n}_{\mathcal{I}^n} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \tag{375}$$

for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$. Defining $C' := C \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}$, C' satisfies

$$[C', U^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \tag{376}$$

for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$. Therefore, we can show that there exist constant numbers u, v, and w such that

$$\begin{aligned} &C \star |V_{\mathrm{in}}\rangle\rangle\langle\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} \\ &= C' \star |V_{\mathrm{in}}\rangle\rangle\langle\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} && (377) \\ &= u|V_{\mathrm{in}}^{\dagger}\rangle\rangle\langle\langle V_{\mathrm{in}}^{\dagger}|_{\mathcal{P}\mathcal{F}} + v(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d} + w(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^{\perp}})_{\mathcal{P}} \otimes \frac{\mathbb{1}_{\mathcal{F}}}{d}, && (378) \end{aligned}$$

i.e., $u = 0$ and

$$C \star |V_{\mathrm{in}}\rangle\rangle\langle\langle V_{\mathrm{in}}|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} = v(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} + w(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^{\perp}})_{\mathcal{P}} \tag{379}$$

holds. We calculate v and w as follows. Equation (379) is written as

$$\mathrm{Tr}_{\mathcal{I}^n\mathcal{O}^n}[C(\mathbb{1}_{\mathcal{P}} \otimes |V_{\mathrm{in}}^*\rangle\rangle\langle\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n})] = v(\Pi^T_{\mathrm{Im}V_{\mathrm{in}}})_{\mathcal{P}} + w(\Pi^T_{(\mathrm{Im}V_{\mathrm{in}})^{\perp}})_{\mathcal{P}}. \tag{380}$$

Taking the Hilbert-Schmidt inner product with $\Pi^*_{\mathrm{Im}V_{\mathrm{in}}}$ and $(\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}})^*$, we obtain

$$\mathrm{Tr}\Big[C|V_{\mathrm{in}}^*\rangle\rangle\langle\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes (\Pi_{\mathrm{Im}V_{\mathrm{in}}})^*_{\mathcal{P}}\Big] = dv, \tag{381}$$

$$\mathrm{Tr}\Big[C|V_{\mathrm{in}}^*\rangle\rangle\langle\langle V_{\mathrm{in}}^*|^{\otimes n}_{\mathcal{I}^n\mathcal{O}^n} \otimes ((\mathbb{1}_D - \Pi_{\mathrm{Im}V_{\mathrm{in}}}))^*_{\mathcal{P}}\Big] = (D-d)w. \tag{382}$$

Taking the Haar integral $\mathrm{d}V_{\mathrm{in}}$ on $\mathbb{V}_{\mathrm{iso}}(d,D)$, we obtain

$$\mathrm{Tr}(C\Xi) = v, \tag{383}$$

$$\mathrm{Tr}(C\Sigma) = w. \tag{384}$$

We calculate Ω, Ξ and Σ as follows. First, due to the left- and right-invariance of the Haar measure $\mathrm{d}V$ given by $\mathrm{d}V = \mathrm{d}(U'VU)$ for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$, Ω and Ξ satisfies the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry given by

$$[\Omega, U^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \tag{385}$$

for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$. Thus, they can be written as

$$\Omega = \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{\nu\in\mathbb{Y}^D_{n+1}} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \Omega^{\mu\nu}_{ijkl} (E^{\mu,d}_{ij})_{\mathcal{I}^n\mathcal{F}} \otimes (E^{\nu,D}_{kl})_{\mathcal{P}\mathcal{O}^n}, \tag{386}$$

using complex coefficients $\Omega^{\mu\nu}_{ijkl} \in \mathbb{C}$. The coefficients can be calculated as

$$\begin{aligned}
&\Omega^{\mu\nu}_{ijkl}\\
&= \frac{1}{m^{(d)}_\mu m^{(D)}_\nu} \mathrm{Tr}\left[\Omega (E^{\mu,d}_{ji})_{\mathcal{I}^n\mathcal{F}} \otimes (E^{\nu,D}_{lk})_{\mathcal{P}\mathcal{O}^n}\right] && (387)\\
&= \frac{1}{m^{(d)}_\mu m^{(D)}_\nu} \mathrm{Tr}\left[\Omega (E^{\mu,d}_{ji})_{\mathcal{I}^n\mathcal{F}} \otimes (P_\pi^\dagger E^{\nu,D}_{lk} P_\pi)_{\mathcal{O}^n\mathcal{P}}\right] && (388)\\
&= \frac{1}{m^{(d)}_\mu m^{(D)}_\nu} \sum_{k',l'=1}^{d_\nu} \frac{1}{d^2} \int_{\mathbb{V}_{\mathrm{iso}}(d,D)} \mathrm{d}V\, \mathrm{Tr}\left[|V\rangle\!\rangle\langle\!\langle V|^{\otimes n+1}_{\mathcal{I}^n\mathcal{F},\mathcal{O}^n\mathcal{P}} (E^{\mu,d}_{ji})_{\mathcal{I}^n\mathcal{F}} \otimes [\pi_\nu]_{ll'} (E^{\nu,D}_{l'k'})_{\mathcal{O}^n\mathcal{P}} [\pi_\nu]^*_{k'k}\right]\\
& && (389)\\
&= \frac{1}{m^{(d)}_\mu m^{(D)}_\nu} \sum_{k',l'=1}^{d_\nu} \frac{1}{d^2} \int_{\mathbb{V}_{\mathrm{iso}}(d,D)} \mathrm{d}V\, \mathrm{Tr}\left[|\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|^{\otimes n+1} (E^{\mu,d}_{ji}) \otimes [\pi_\nu]_{ll'} V^{\dagger\otimes n+1} (E^{\nu,D}_{l'k'}) V^{\otimes n+1} [\pi_\nu]^*_{k'k}\right],\\
& && (390)
\end{aligned}$$

where P_π is the permutation of Hilbert spaces defined in Eq. (49) for $\pi = (12\cdots n+1) \in \mathfrak{S}_{n+1}$, $[\pi_\mu]_{ij}$ are matrix elements of the irreducible representation π_μ defined by $[\pi_\mu]_{ij} \coloneqq \langle \mu, i|\, \pi_\mu\, |\mu, j\rangle$. As shown in Eq. (146) in Appendix A.2, $V^{\dagger\otimes n+1}(E^{\nu,D}_{l'k'})V^{\otimes n+1}$ is given by $(E^{\nu,d}_{l'k'})\delta_{\nu\in\mathbb{Y}^D_{n+1}}$. We consider the Schur basis introduced in Section 3.1.2. Since the quantum Schur transform is a real matrix, the maximally entangled state in the Schur basis is the same as that in the Schur basis, i.e.,

$$|\mathbb{1}_d\rangle\!\rangle^{\otimes n+1} = \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{u=1}^{m^{(d)}_\mu} \sum_{i=1}^{d_\mu} |\mu, u\rangle_{\mathcal{U}^{(d)}_\mu} \otimes |\mu, i\rangle_{\mathcal{S}_\mu} \otimes |\mu, u\rangle_{\mathcal{U}^{(d)}_\mu} \otimes |\mu, i\rangle_{\mathcal{S}_\mu}. \tag{391}$$

Thus, $\Omega^{\mu\nu}_{ijkl}$ is further calculated as

$$\begin{aligned}
\Omega^{\mu\nu}_{ijkl} &= \frac{\delta_{\nu\in\mathbb{Y}^D_{n+1}}}{m^{(d)}_\mu m^{(D)}_\nu} \sum_{k',l'=1}^{d_\nu} \frac{1}{d^2} \mathrm{Tr}\left[|\mathbb{1}_d\rangle\!\rangle\langle\!\langle \mathbb{1}_d|^{\otimes n+1} (E^{\mu,d}_{ji}) \otimes [\pi_\nu]_{ll'} (E^{\nu,d}_{l'k'}) [\pi_\nu]^*_{k'k}\right] && (392)\\
&= \frac{\delta_{\mu\nu}[\pi_\mu]^*_{ik}[\pi_\mu]_{lj}}{d^2 m^{(D)}_\mu}, && (393)
\end{aligned}$$

Therefore, Ω is given by

$$\Omega = \sum_{\mu \in \mathbb{Y}_{n+1}^d} \sum_{i,j,k,l=1}^{d_\mu} \frac{[\pi_\mu]_{ik}^* [\pi_\mu]_{lj}}{d^2 m_\mu^{(D)}} (E_{ij}^{\mu,d})_{\mathcal{I}^n \mathcal{F}} \otimes (E_{kl}^{\mu,D})_{\mathcal{P}\mathcal{O}^n}. \tag{394}$$

Since $(\Pi_{\mathrm{Im}V})_{\mathcal{P}} = \mathrm{Tr}_{\mathcal{F}} |V\rangle\!\rangle\langle\!\langle V|_{\mathcal{F}\mathcal{P}}$ holds, Ξ is calculated using Lemma 3 as

$$\Xi = d\, \mathrm{Tr}_{\mathcal{F}}\, \Omega \tag{395}$$

$$= \sum_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{\lambda \in \nu - \square} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} \frac{m_\nu^{(d)}}{d m_\nu^{(D)} m_\lambda^{(d)}} [\pi_\nu]_{a_\nu^\lambda k}^* [\pi_\nu]_{l b_\nu^\lambda} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}. \tag{396}$$

Since $((\mathbb{1}_D - \Pi_{\mathrm{Im}V}))_{\mathcal{P}} = \mathbb{1}_{\mathcal{P}} - (\Pi_{\mathrm{Im}V})_{\mathcal{P}}$ holds, Σ is calculated using Lemma 3 as

$$\Sigma = \frac{1}{D-d} \left[\int \mathrm{d}V |V\rangle\!\rangle\langle\!\langle V|_{\mathcal{I}^n \mathcal{O}^n}^{\otimes n} \otimes \mathbb{1}_{\mathcal{P}} - d\Xi \right] \tag{397}$$

$$= \frac{1}{D-d} \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{a,b=1}^{d_\lambda} \left[\frac{(E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{ab}^{\lambda,D})_{\mathcal{O}^n}}{m_\lambda^{(D)}} \otimes \mathbb{1}_{\mathcal{P}} \right.$$

$$\left. - \sum_{\nu \in \lambda + \square \cap \mathbb{Y}_{n+1}^d} \sum_{k,l=1}^{d_\nu} \frac{m_\nu^{(d)}}{m_\nu^{(D)} m_\lambda^{(d)}} [\pi_\mu]_{a_\nu^\lambda k}^* [\pi_\mu]_{l b_\nu^\lambda} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n} \right] \tag{398}$$

$$= \frac{1}{D-d} \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{a,b=1}^{d_\lambda} \sum_{\nu \in \lambda + \square} \left[\frac{(E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (P_\pi^\dagger E_{a_\nu^\lambda b_\nu^\lambda}^{\nu,D} P_\pi)_{\mathcal{P}\mathcal{O}^n}}{m_\lambda^{(D)}} \right.$$

$$\left. - \delta_{\nu \in \mathbb{Y}_{n+1}^d} \sum_{k,l=1}^{d_\nu} \frac{m_\nu^{(d)}}{m_\nu^{(D)} m_\lambda^{(d)}} [\pi_\nu]_{a_\nu^\lambda k}^* [\pi_\nu]_{l b_\nu^\lambda} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n} \right] \tag{399}$$

$$= \frac{1}{D-d} \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \lambda + \square} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} \left[\frac{1}{m_\lambda^{(D)}} - \delta_{\nu \in \mathbb{Y}_{n+1}^d} \frac{m_\nu^{(d)}}{m_\nu^{(D)} m_\lambda^{(d)}} \right] [\pi_\nu]_{a_\nu^\lambda k}^* [\pi_\nu]_{l b_\nu^\lambda} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n} \tag{400}$$

$$= \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \lambda + \square} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} \frac{1}{m_\nu^{(D)}} \frac{\mathrm{hook}(\lambda)}{\mathrm{hook}(\nu)} [\pi_\nu]_{a_\nu^\lambda k}^* [\pi_\nu]_{l b_\nu^\lambda} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}. \tag{401}$$

□

The parameters x, y, z, v, w in Lemma 15 are related to the constraints and the figure of merit of each task considered in this work as follows:

- Probabilistic exact isometry inversion: $x = p$ and $y = 0$.
- Deterministic isometry inversion: $x + y/d^2 = F_{\mathrm{worst}}$.
- Universal error detection: $v = 1$, $w = \alpha$.
- Isometry adjointation: $x + y = 1$, $\max\{1 - x - y/d^2, z\} = \epsilon$.

Using this property, we derive the SDP to obtain the optimal transformations of isometry operations in the next section.

E.3 Derivation of the SDP to obtain optimal transformation of isometry operations

E.3.1 Probabilistic exact isometry inversion

From Theorem 9 and Appendix E.2, the optimization problem of the success probability for isometry inversion is formulated as follows:

$$\begin{aligned}
&\max \operatorname{Tr}(C_S\Omega)\\
\text{s.t. } &0 \leq C_S, C_F \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}),\\
&C := C_S + C_F \in \mathcal{W}^{(x)},\\
&\operatorname{Tr}(C_S\Omega) = \operatorname{Tr}[C_S(\Xi \otimes \mathbb{1}_{\mathcal{F}})],\\
&[C_a, U_{\mathcal{I}^n\mathcal{F}}^{\otimes n+1} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 \quad \forall U \in \mathbb{U}(d), U' \in \mathbb{U}(D), a \in \{S, F\}.
\end{aligned} \tag{402}$$

Using the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry of $\{C_S, C_F\}$, we write $\{C_S, C_F\}$ similarly to Eq. (321) as

$$C_S = \sum_{\mu\in\mathbb{Y}_{n+1}^d} \sum_{\nu\in\mathbb{Y}_{n+1}^D} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[S_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)} m_\nu^{(D)}} (E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}, \tag{403}$$

$$C_F = \sum_{\mu\in\mathbb{Y}_{n+1}^d} \sum_{\nu\in\mathbb{Y}_{n+1}^D} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[F_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)} m_\nu^{(D)}} (E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}. \tag{404}$$

Then, $\operatorname{Tr}(C_S\Omega)$ and $\operatorname{Tr}[C_S(\Xi\otimes\mathbb{1}_{\mathcal{F}})]$ are given by

$$\operatorname{Tr}(C_S\Omega) = \sum_{\mu\in\mathbb{Y}_{n+1}^d} \operatorname{Tr}(S_{\mu\mu}\Omega_\mu), \tag{405}$$

$$\operatorname{Tr}[C_S(\Xi\otimes\mathbb{1}_{\mathcal{F}})] = \operatorname{Tr}[\operatorname{Tr}_{\mathcal{F}}(C_S)\Xi] \tag{406}$$

$$= \sum_{\lambda\in\mathbb{Y}_n^d} \sum_{\mu\in\lambda+\square} \sum_{\nu\in\mathbb{Y}_{n+1}^D} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} \frac{[S_{\mu\nu}]_{a_\mu^\lambda k, b_\mu^\lambda l}}{m_\mu^{(d)} m_\nu^{(D)}} \operatorname{Tr}\Big[(E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}\Xi\Big] \tag{407}$$

$$= \sum_{\lambda\in\mathbb{Y}_n^d} \sum_{\mu\in\lambda+\square} \sum_{\nu\in\mathbb{Y}_{n+1}^d} \operatorname{Tr}\Big[(X_\mu^\lambda \otimes \mathbb{1}_{d_\nu}) S_{\mu\nu} (X_\mu^\lambda \otimes \mathbb{1}_{d_\nu})^\dagger \Xi_{\lambda\nu}\Big], \tag{408}$$

where X_μ^λ is defined in Eq. (329) and a_μ^λ is the index of the standard tableau $s^\mu_{a_\mu^\lambda}$ obtained by adding a box $\boxed{n+1}$ to the standard tableau s_a^λ. Therefore, the SDP (402) is written as

$$\begin{aligned}
&\max \sum_{\mu\in\mathbb{Y}_{n+1}^d} \operatorname{Tr}(S_{\mu\mu}\Omega_\mu)\\
\text{s.t. } &0 \leq S_{\mu\nu}, F_{\mu\nu} \in \mathcal{L}(\mathbb{C}^{d_\mu} \otimes \mathbb{C}^{d_\nu}) \quad \forall \mu \in \mathbb{Y}_{n+1}^d, \nu \in \mathbb{Y}_{n+1}^D,\\
&\{C_{\mu\nu}\} := \{S_{\mu\nu} + F_{\mu\nu}\} \in \mathcal{W}_{\text{sym}}^{(x)},\\
&\sum_{\mu\in\mathbb{Y}_{n+1}^d} \operatorname{Tr}(S_{\mu\mu}\Omega_\mu) = \sum_{\lambda\in\mathbb{Y}_n^d} \sum_{\mu\in\lambda+\square} \sum_{\nu\in\mathbb{Y}_{n+1}^d} \operatorname{Tr}\Big[(X_\mu^\lambda \otimes \mathbb{1}_{d_\nu}) S_{\mu\nu} (X_\mu^\lambda \otimes \mathbb{1}_{d_\nu})^\dagger \Xi_{\lambda\nu}\Big].
\end{aligned} \tag{409}$$

E.3.2 Deterministic isometry inversion

From Theorem 9 and Appendix E.2, the optimization problem of the fidelity of deterministic isometry inversion is formulated as follows:

$$\begin{aligned} &\max \operatorname{Tr}(C\Omega)\\ \text{s.t. } &0 \leq C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}),\\ &C \in \mathcal{W}^{(x)},\\ &[C, U_{\mathcal{I}^n\mathcal{F}}^{\otimes n+1} \otimes U_{\mathcal{P}\mathcal{O}^n}'^{\otimes n+1}] = 0 \quad \forall U \in \mathbb{U}(d), U' \in \mathbb{U}(D). \end{aligned} \tag{410}$$

Similarly to probabilistic isometry inversion, this SDP can be rewritten as follows:

$$\begin{aligned} &\max \sum_{\mu \in \mathbb{Y}_{n+1}^d} \operatorname{Tr}(C_{\mu\mu}\Omega_\mu)\\ \text{s.t. } &0 \leq C_{\mu\nu} \in \mathcal{L}(\mathbb{C}^{d_\mu} \otimes \mathbb{C}^{d_\nu}) \quad \forall \mu \in \mathbb{Y}_{n+1}^d, \nu \in \mathbb{Y}_{n+1}^D,\\ &\{C_{\mu\nu}\} \in \mathcal{W}_{\text{sym}}^{(x)}. \end{aligned} \tag{411}$$

E.3.3 Universal error detection

From Theorem 9 and Appendix E.2, the optimization problem of λ of universal error detection is formulated as follows:

$$\begin{aligned} &\min \operatorname{Tr}(C_I\Sigma)\\ \text{s.t. } &0 \leq C_I, C_O \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P}),\\ &C := C_I + C_O \in \mathcal{W}^{(x)},\\ &\operatorname{Tr}(C_I\Xi) = 1,\\ &[C_a, U_{\mathcal{I}^n}^{\otimes n} \otimes U_{\mathcal{P}\mathcal{O}^n}'^{\otimes n+1}] = 0 \quad \forall U \in \mathbb{U}(d), U' \in \mathbb{U}(D), a \in \{I, O\}. \end{aligned} \tag{412}$$

Using the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry of $\{C_I, C_O\}$, we write $\{C_I, C_O\}$ similarly to Eq. (322) as

$$C_I = \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \mathbb{Y}_{n+1}^D} \sum_{a,b=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[I_{\lambda\nu}]_{ak,bl}}{m_\lambda^{(d)} m_\nu^{(D)}} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}, \tag{413}$$

$$C_O = \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \mathbb{Y}_{n+1}^D} \sum_{a,b=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} \frac{[O_{\lambda\nu}]_{ak,bl}}{m_\lambda^{(d)} m_\nu^{(D)}} (E_{ab}^{\lambda,d})_{\mathcal{I}^n} \otimes (E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}. \tag{414}$$

Then, $\operatorname{Tr}(C_I\Sigma)$ and $\operatorname{Tr}(C_I\Xi)$ are given by

$$\operatorname{Tr}(C_I\Sigma) = \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \mathbb{Y}_{n+1}^D} \operatorname{Tr}(I_{\lambda\nu}\Sigma_{\lambda\nu}), \tag{415}$$

$$\operatorname{Tr}(C_I\Xi) = \sum_{\lambda \in \mathbb{Y}_n^d} \sum_{\nu \in \mathbb{Y}_{n+1}^d} \operatorname{Tr}(I_{\lambda\nu}\Xi_{\lambda\nu}). \tag{416}$$

Therefore, the SDP (412) is written as

$$\begin{aligned}
&\min \sum_{\lambda\in\mathbb{Y}_n^d}\sum_{\nu\in\mathbb{Y}_{n+1}^D} \mathrm{Tr}(I_{\lambda\nu}\Sigma_{\lambda\nu})\\
\text{s.t. } & 0\leq I_{\lambda\nu}, O_{\lambda\nu}\in\mathcal{L}(\mathbb{C}^{d_\lambda}\otimes\mathbb{C}^{d_\nu}) \quad \forall\lambda\in\mathbb{Y}_n^d, \nu\in\mathbb{Y}_{n+1}^D,\\
&\{C_{\lambda\nu}\} := \{I_{\lambda\nu}+O_{\lambda\nu}\}\in\mathcal{W}_{\mathrm{sym}}^{(x)},\\
&\sum_{\lambda\in\mathbb{Y}_n^d}\sum_{\nu\in\mathbb{Y}_{n+1}^d} \mathrm{Tr}(I_{\lambda\nu}\Xi_{\lambda\nu}) = 1.
\end{aligned} \tag{417}$$

E.3.4 Isometry adjointation

From Theorem 9 and Appendix E.2, the optimization problem of ϵ of isometry adjointation is formulated as follows:

$$\begin{aligned}
&\min\max\{1-\mathrm{Tr}(C_I\Omega), \mathrm{Tr}[C_I(\Sigma\otimes\mathbb{1}_{\mathcal{F}})]\}\\
\text{s.t. } & 0\leq C_I, C_O\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P}\otimes\mathcal{F}),\\
&C := C_I + C_O \in \mathcal{W}^{(x)},\\
&\mathrm{Tr}[C_I(\Xi\otimes\mathbb{1}_{\mathcal{F}})] = 1,\\
&[C_a, U_{\mathcal{I}^n\mathcal{F}}^{\otimes n+1}\otimes U_{\mathcal{P}\mathcal{O}^n}^{\prime\otimes n+1}] = 0 \quad \forall U\in\mathbb{U}(d), U'\in\mathbb{U}(D), a\in\{I,O\}.
\end{aligned} \tag{418}$$

Using the $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry of $\{C_I, C_O\}$, we write $\{C_I, C_O\}$ similarly to Eq. (321) as

$$C_I = \sum_{\mu\in\mathbb{Y}_{n+1}^d}\sum_{\nu\in\mathbb{Y}_{n+1}^D}\sum_{i,j=1}^{d_\mu}\sum_{k,l=1}^{d_\nu}\frac{[I_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)}m_\nu^{(D)}}(E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}}\otimes(E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}, \tag{419}$$

$$C_O = \sum_{\mu\in\mathbb{Y}_{n+1}^d}\sum_{\nu\in\mathbb{Y}_{n+1}^D}\sum_{i,j=1}^{d_\mu}\sum_{k,l=1}^{d_\nu}\frac{[O_{\mu\nu}]_{ik,jl}}{m_\mu^{(d)}m_\nu^{(D)}}(E_{ij}^{\mu,d})_{\mathcal{I}^n\mathcal{F}}\otimes(E_{kl}^{\nu,D})_{\mathcal{P}\mathcal{O}^n}. \tag{420}$$

Then, similarly for the case of probabilistic exact isometry inversion, the SDP (418) as follows:

$$\begin{aligned}
&\min\max\left\{1-\sum_{\mu\in\mathbb{Y}_{n+1}^d}\mathrm{Tr}(I_{\mu\mu}\Omega_\mu), \sum_{\lambda\in\mathbb{Y}_n^d}\sum_{\mu\in\lambda+\square}\sum_{\nu\in\mathbb{Y}_{n+1}^D}\mathrm{Tr}\Big[(X_\mu^\lambda\otimes\mathbb{1}_{d_\nu})I_{\mu\nu}(X_\mu^\lambda\otimes\mathbb{1}_{d_\nu})^\dagger\Sigma_{\lambda\nu}\Big]\right\}\\
\text{s.t. } & 0\leq I_{\mu\nu}, O_{\mu\nu}\in\mathcal{L}(\mathbb{C}^{d_\mu}\otimes\mathbb{C}^{d_\nu}) \quad \forall\mu\in\mathbb{Y}_{n+1}^d, \nu\in\mathbb{Y}_{n+1}^D,\\
&\{C_{\mu\nu}\} := \{I_{\mu\nu}+O_{\mu\nu}\}\in\mathcal{W}_{\mathrm{sym}}^{(x)},\\
&\sum_{\lambda\in\mathbb{Y}_n^d}\sum_{\mu\in\lambda+\square}\sum_{\nu\in\mathbb{Y}_{n+1}^d}\mathrm{Tr}\Big[(X_\mu^\lambda\otimes\mathbb{1}_{d_\nu})I_{\mu\nu}(X_\mu^\lambda\otimes\mathbb{1}_{d_\nu})^\dagger\Xi_{\lambda\nu}\Big] = 1.
\end{aligned} \tag{421}$$

E.4 Derivation of the dual problems

We derive the dual problems of the SDPs to obtain the optimal transformations of isometry operations. Due to the strong duality, the dual problems gives the same optimal value as the corresponding primal problems. To this end, we first introduce the dual set of the Choi operators of quantum superchannels. Then, we derive the dual problems using the dual set. Finally, we simplify the derived dual problems using the $\mathbb{U}(d)\times\mathbb{U}(D)$ symmetry.

E.4.1 Characterization of the dual processes

We define the dual set $\overline{\mathcal{W}}^{(x)}$ of $\mathcal{W}^{(x)}$ for $x \in \{\mathrm{PAR}, \mathrm{SEQ}, \mathrm{GEN}\}$ by

$$\overline{C} \in \overline{\mathcal{W}}^{(x)} \iff \mathrm{Tr}\Big(C\overline{C}\Big) = 1 \quad \forall C \in \mathcal{W}^{(x)}. \tag{422}$$

Introducing the basis $\{\overline{C}_j\}$ of $\overline{\mathcal{W}}^{(x)}$, this relation leads to

$$\overline{C} \in \overline{\mathcal{W}}^{(x)} \iff \mathrm{Tr}\Big(C\overline{C}_j\Big) = 1 \quad \forall j. \tag{423}$$

As shown in Ref. [77], $\overline{\mathcal{W}}^{(x)}$ are given by

$$\overline{C} \in \overline{\mathcal{W}}^{(\mathrm{PAR})} \iff \begin{cases} \overline{C} = W \otimes \mathbb{1}_{\mathcal{F}} \\ \mathrm{Tr}_{\mathcal{O}^n} W = \mathrm{Tr}_{\mathcal{I}^n\mathcal{O}^n} W \otimes \mathbb{1}_{\mathcal{I}^n} / \dim \mathcal{I}^n \\ \mathrm{Tr}\, W = \dim \mathcal{I}^n \end{cases}, \tag{424}$$

$$\overline{C} \in \overline{\mathcal{W}}^{(\mathrm{SEQ})} \iff \begin{cases} \overline{C} = W \otimes \mathbb{1}_{\mathcal{F}} \\ \mathrm{Tr}_{\mathcal{O}_i} W^{(i)} = \mathbb{1}_{\mathcal{I}_i} \otimes W^{(i-1)}, \quad \forall i \in \{1, \cdots, n\} \\ \mathrm{Tr}\, W = \dim \mathcal{I}^n \end{cases}, \tag{425}$$

$$\overline{C} \in \overline{\mathcal{W}}^{(\mathrm{GEN})} \iff \begin{cases} \overline{C} = W \otimes \mathbb{1}_{\mathcal{F}} \\ \mathrm{Tr}_{\mathcal{O}_i} W = \mathrm{Tr}_{\mathcal{I}_i\mathcal{O}_i} W \otimes \mathbb{1}_{\mathcal{I}_i} / \dim \mathcal{I}_i \quad \forall i \in \{1, \cdots, n\} \\ \mathrm{Tr}\, W = \dim \mathcal{I}^n \end{cases}, \tag{426}$$

where $W^{(i)}$ are defined by

$$W^{(i)} := \begin{cases} W & (i = n) \\ \mathrm{Tr}_{\mathcal{I}_{i+1}\mathcal{O}_{i+1}} W^{(i+1)} / \dim \mathcal{I}_{i+1} \quad \forall i \in \{0, \cdots, n\} & (i \in \{0, \cdots, n-1\}) \end{cases}. \tag{427}$$

We also introduce the set $\mathrm{Cone}[\overline{\mathcal{W}}^{(x)}]$ of the dual sets $\overline{\mathcal{W}}^{(x)}$ defined by

$$\mathrm{Cone}[\overline{\mathcal{W}}^{(x)}] = \{\lambda \overline{C} | \lambda \in \mathbb{C}, \overline{C} \in \overline{\mathcal{W}}^{(x)}\}. \tag{428}$$

E.4.2 Probabilistic exact isometry inversion

We write down the dual problem of the SDP (402). To this end, we note that the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry does not change the optimal value of the SDP (402), so we can remove it when we consider the dual problem. Then, the SDP (402) corresponds to the following optimization problem:

$$\begin{aligned} &\max \mathrm{Tr}(C_S \Omega) \\ \text{s.t. } &0 \leq C_S, C_F \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}), \\ &\mathrm{Tr}(C_S \Omega) = \mathrm{Tr}[C_S(\Xi \otimes \mathbb{1}_{\mathcal{F}})], \\ &\mathrm{Tr}\Big[(C_S + C_F)\overline{C}_j\Big] = 1, \quad \forall j. \end{aligned} \tag{429}$$

By introducing the Lagrange multipliers $\omega, \lambda_j \in \mathbb{R}$ and $0 \leq \Gamma_S, \Gamma_F \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$, we can write down the corresponding Lagrangian

$$\begin{aligned} L &= \mathrm{Tr}(C_S\Omega) + [\mathrm{Tr}[C_S(\Xi \otimes \mathbb{1}_{\mathcal{F}})] - \mathrm{Tr}(C_S\Omega)]\omega + \mathrm{Tr}(C_S\Gamma_S) + \mathrm{Tr}(C_F\Gamma_F) \\ &\quad + \sum_j [1 - \mathrm{Tr}\left[(C_S + C_F)\overline{C}_j\right]]\lambda_j \qquad (430) \\ &= \sum_j \lambda_j + \mathrm{Tr}\left[C_S(\Omega - \omega\Omega + \omega\Xi \otimes \mathbb{1}_{\mathcal{F}} + \Gamma_S - \sum_j \lambda_j \overline{C}_j)\right] + \mathrm{Tr}\left[F(\Gamma_F - \sum_j \lambda_j \overline{C}_j)\right], \qquad (431) \end{aligned}$$

which gives the SDP (429) as the following optimization:

$$\max_{C_S, C_F \geq 0} \min_{\omega, \lambda_j \in \mathbb{R}, \Gamma_S, \Gamma_F \geq 0} L. \qquad (432)$$

This optimization problem corresponds to the following dual problem:

$$\begin{aligned} &\min \sum_j \lambda_j \\ \text{s.t. } &\omega, \lambda_j \in \mathbb{R}, 0 \leq \Gamma_S, \Gamma_F \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}), \\ &(1-\omega)\Omega + \omega\Xi \otimes \mathbb{1}_{\mathcal{F}} + \Gamma_S - \sum_j \lambda_j \overline{C}_j = 0, \\ &\Gamma_F - \sum_j \lambda_j \overline{C}_j = 0. \end{aligned} \qquad (433)$$

The variables Γ_S, Γ_F can be removed, and the variables λ_j and $\overline{C}_j$ can be replaced with $\overline{C} := \sum_j \lambda_j \overline{C}_j$. Since $\mathrm{Tr}\,\overline{C}_j = d^{n+1}$ holds for $\overline{C}_j \in \overline{\mathcal{W}}^{(x)}$, $\sum_j \lambda_j$ can be replaced with $\mathrm{Tr}\,\overline{C}/d^{n+1}$, which gives the following dual problem:

$$\begin{aligned} &\min \mathrm{Tr}\,\overline{C}/d^{n+1} \\ \text{s.t. } &\omega \in \mathbb{R}, 0 \leq \overline{C} \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}), \\ &\overline{C} \in \mathrm{Cone}[\overline{\mathcal{W}}^{(x)}], \\ &\overline{C} \geq (1-\omega)\Omega + \omega\Xi \otimes \mathbb{1}_{\mathcal{F}}. \end{aligned} \qquad (434)$$

E.4.3 Deterministic isometry inversion

Similarly to the case of probabilistic isometry inversion, the SDP (410) can be rewritten as the following optimization problem:

$$\begin{aligned} &\max \mathrm{Tr}(C\Omega) \\ \text{s.t. } &0 \leq C \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}), \\ &\mathrm{Tr}\left[C\overline{C}_j\right] = 1, \quad \forall j. \end{aligned} \qquad (435)$$

By introducing the Lagrange multipliers $\lambda_j \in \mathbb{R}$ and $0 \leq \Gamma \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$, we can write down the corresponding Lagrangian

$$\begin{aligned} L &= \mathrm{Tr}(C\Omega) + \mathrm{Tr}(C\Gamma) + \sum_j [1 - \mathrm{Tr}\left[C\overline{C}_j\right]]\lambda_j \qquad (436) \\ &= \sum_j \lambda_j + \mathrm{Tr}\left[C(\Omega + \Gamma - \sum_j \lambda_j \overline{C}_j)\right], \qquad (437) \end{aligned}$$

which gives the SDP (410) as the following optimization:

$$\max_{C\geq 0}\min_{\lambda_j\in\mathbb{R},\Gamma\geq 0} L. \tag{438}$$

This optimization problem corresponds to the following dual problem:

$$\begin{aligned}
&\min \sum_j \lambda_j\\
\text{s.t. } &\lambda_j\in\mathbb{R}, 0\leq\Gamma\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P}\otimes\mathcal{F}),\\
&\Omega+\Gamma-\sum_j\lambda_j\overline{C}_j=0.
\end{aligned}\tag{439}$$

The variable Γ can be removed, and the variables λ_j and $\overline{C}_j$ can be replaced with $\overline{C}:=\sum_j\lambda_j\overline{C}_j$ as

$$\begin{aligned}
&\min \operatorname{Tr}\overline{C}/d^{n+1}\\
\text{s.t. } &\overline{C}\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P}\otimes\mathcal{F}),\\
&\overline{C}\in\mathrm{Cone}[\overline{\mathcal{W}}^{(x)}],\\
&\overline{C}\geq\Omega.
\end{aligned}\tag{440}$$

E.4.4 Universal error detection

Similarly to the case of probabilistic isometry inversion, the SDP (412) can be rewritten as the following optimization problem:

$$\begin{aligned}
&\min \operatorname{Tr}(C_I\Sigma)\\
\text{s.t. } &0\leq C_I, C_O\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P}),\\
&\operatorname{Tr}(C_I\Xi)=1,\\
&\operatorname{Tr}\Big[(C_I+C_O)\overline{C}_j\Big]=1\quad\forall j.
\end{aligned}\tag{441}$$

By introducing the Lagrange multipliers $\xi,\lambda_j\in\mathbb{R}$ and $0\leq\Gamma_I,\Gamma_O\in\mathcal{L}(\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{P})$, the corresponding Lagrangian is given by

$$L=\operatorname{Tr}(C_I\Sigma)-\operatorname{Tr}(C_I\Gamma_I)-\operatorname{Tr}(C_O\Gamma_O)+[1-\operatorname{Tr}(C_I\Xi)]\xi+\sum_j[1-\operatorname{Tr}\Big[(C_I+C_O)\overline{C}_j\Big]]\lambda_j \tag{442}$$

$$=\sum_j\lambda_j+\xi+\operatorname{Tr}\left[C_I\Big(\Sigma-\Gamma_I-\xi\Xi-\sum_j\lambda_j\overline{C}_j\Big)\right]+\operatorname{Tr}\left[C_O(-\Gamma_O-\sum_j\lambda_j\overline{C}_j)\right], \tag{443}$$

which gives the SDP (412) as the following optimization:

$$\min_{C_I,C_O\geq 0}\max_{\xi,\lambda_j\in\mathbb{R},\Gamma_I,\Gamma_O\geq 0} L. \tag{444}$$

The corresponding dual problem is given by

$$\begin{aligned}
&\max\sum_j\lambda_j+\xi\\
\text{s.t. } &\Sigma-\Gamma_I-\xi\Xi-\sum_j\lambda_j\overline{C}_j=0,\\
&-\Gamma_O-\sum_j\lambda_j\overline{C}_j=0.
\end{aligned}\tag{445}$$

The variable Γ can be removed, and the variables λ_j and $\overline{C}_j$ can be replaced with $\overline{C} := -\sum_j \lambda_j \overline{C}_j$ as

$$\begin{aligned} &\max \xi - \operatorname{Tr} \overline{C}/d^n \\ \text{s.t. } &\xi \in \mathbb{R}, 0 \leq \overline{C} \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P}), \\ &\overline{C} \in \mathrm{Cone}[\overline{\mathcal{W}}^{(x)}], \\ &\overline{C} \geq \xi \Xi - \Sigma. \end{aligned} \tag{446}$$

E.4.5 Isometry adjointation

Similarly to the case of probabilistic isometry inversion, the SDP (418) can be rewritten as the following optimization problem:

$$\begin{aligned} &\min p \\ \text{s.t. } &0 \leq C_I, C_O \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}), \\ &1 - \operatorname{Tr}(C_I \Omega) \leq p, \\ &\operatorname{Tr}[C_I(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] \leq p \\ &\operatorname{Tr}[C_I(\Xi \otimes \mathbb{1}_{\mathcal{F}})] = 1, \\ &\operatorname{Tr}\Big[(C_I + C_O)\overline{C}_j\Big] = 1 \quad \forall j. \end{aligned} \tag{447}$$

By introducing the Lagrange multipliers $\omega, \sigma \in \mathbb{R}_{\geq 0}$, $\xi, \lambda_j \in \mathbb{R}$ and $0 \leq \Gamma_I, \Gamma_O \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F})$, the corresponding Lagrangian is given by

$$\begin{aligned} L =& p - \operatorname{Tr}(C_I\Gamma_I) - \operatorname{Tr}(C_O\Gamma_O) + [1 - \operatorname{Tr}(C_I\Omega) - p]\omega + [\operatorname{Tr}[C_I(\Sigma \otimes \mathbb{1}_{\mathcal{F}})] - p]\sigma \\ &+ [1 - \operatorname{Tr}[C_I(\Xi \otimes \mathbb{1}_{\mathcal{F}})]]\xi + \sum_j [1 - \operatorname{Tr}\Big[(C_I + C_O)\overline{C}_j\Big]]\lambda_j \end{aligned} \tag{448}$$

$$\begin{aligned} =& \sum_j \lambda_j + \omega + \xi + p(1 - \omega - \sigma) + \operatorname{Tr}\left[C_I(-\Gamma_I - \omega\Omega + \sigma\Sigma \otimes \mathbb{1}_{\mathcal{F}} - \xi\Xi \otimes \mathbb{1}_{\mathcal{F}} - \sum_j \lambda_j \overline{C}_j)\right] \\ &+ \operatorname{Tr}\left[F(-\Gamma_O - \sum_j \lambda_j \overline{C}_j)\right]. \end{aligned} \tag{449}$$

The corresponding dual problem is given by

$$\begin{aligned} &\max \sum_j \lambda_j + \omega + \xi \\ \text{s.t. } &\omega + \sigma = 1, \\ &-\Gamma_I - \omega\Omega + \sigma\Sigma \otimes \mathbb{1}_{\mathcal{F}} - \xi\Xi \otimes \mathbb{1}_{\mathcal{F}} - \sum_j \lambda_j \overline{C}_j = 0, \\ &-\Gamma_O - \sum_j \lambda_j \overline{C}_j = 0. \end{aligned} \tag{450}$$

The variables $\Gamma_I, \Gamma_O, \sigma$ can be removed, and the variables λ_j and $\overline{C}_j$ can be replaced with $\overline{C} := -\sum_j \lambda_j \overline{C}_j$ as

$$\begin{aligned} &\max \omega + \xi - \operatorname{Tr} \overline{C}/d^{n+1} \\ \text{s.t. } &\xi \in \mathbb{R}, 0 \leq \omega \leq 1, 0 \leq \overline{C} \in \mathcal{L}(\mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{P} \otimes \mathcal{F}) \\ &\overline{C} \in \mathrm{Cone}[\overline{\mathcal{W}}^{(x)}], \\ &\overline{C} \geq \omega\Omega + \xi\Xi \otimes \mathbb{1}_{\mathcal{F}} - (1 - \omega)\Sigma \otimes \mathbb{1}_{\mathcal{F}}. \end{aligned} \tag{451}$$

E.4.6 Simplification of the dual problems using $\mathbb{U}(d) \times \mathbb{U}(D)$ and permutation symmetry

In the dual SDPs (434), (440), (446) and (451), we can impose the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry given by

$$\begin{cases} [\overline{C}, U^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & \text{(isometry inversion, universal error detection)} \\ [\overline{C}, U^{\otimes n}_{\mathcal{I}^n} \otimes U'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}] = 0 & \text{(isometry adjointation)} \end{cases} \tag{452}$$

for all $U \in \mathbb{U}(d)$ and $U' \in \mathbb{U}(D)$, since for the optimal $\overline{C}_{\mathrm{opt}}$, the $\mathbb{U}(d) \times \mathbb{U}(D)$-twirled operator $\overline{C}'_{\mathrm{opt}}$ given by

$$\overline{C}'_{\mathrm{opt}} := \begin{cases} \int_{\mathbb{U}(d)} \mathrm{d}U \mathcal{U}^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes \mathcal{U}'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(\overline{C}) & \text{(isometry inversion, universal error detection)} \\ \int_{\mathbb{U}(d)} \mathrm{d}U \mathcal{U}^{\otimes n}_{\mathcal{I}^n} \otimes \mathcal{U}'^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}(\overline{C}) & \text{(isometry adjointation)} \end{cases} \tag{453}$$

also gives the optimal values of the dual SDPs. For the case of $x = \mathrm{GEN}$, we can also impose the permutation symmetry given by

$$\begin{cases} [\overline{C}, (P_\pi)_{\mathcal{I}^n} \otimes (P_\pi)_{\mathcal{O}^n} \otimes \mathbb{1}_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{F}}] = 0 & \text{(isometry inversion, universal error detection)} \\ [\overline{C}, (P_\pi)_{\mathcal{I}^n} \otimes (P_\pi)_{\mathcal{O}^n} \otimes \mathbb{1}_{\mathcal{P}}] = 0 & \text{(isometry adjointation)} \end{cases} \tag{454}$$

for all $\pi \in \mathfrak{S}_n$ and P_π is given in Eq. (49) since the $\mathfrak{S}_n$-twirled operator $\overline{C}''_{\mathrm{opt}}$ given by

$$\overline{C}''_{\mathrm{opt}} := \begin{cases} \sum_{\pi \in \mathfrak{S}_n} (\mathcal{P}_\pi)_{\mathcal{I}^n} \otimes (\mathcal{P}_\pi)_{\mathcal{O}^n} \otimes \mathbb{1}_{\mathcal{P}} \otimes \mathbb{1}_{\mathcal{F}}(\overline{C}) & \text{(isometry inversion, universal error detection)} \\ \sum_{\pi \in \mathfrak{S}_n} (\mathcal{P}_\pi)_{\mathcal{I}^n} \otimes (\mathcal{P}_\pi)_{\mathcal{O}^n} \otimes \mathbb{1}_{\mathcal{P}}(\overline{C}) & \text{(isometry adjointation)} \end{cases} \tag{455}$$

also gives the optimal values of the dual SDPs.

We characterize the set $\overline{\mathcal{W}}^{(x)}$ under the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry (452) [and the permutation symmetry (454) for $x = \mathrm{GEN}$]. Using the $\mathbb{U}(d) \times \mathbb{U}(D)$ symmetry (452), we write $\overline{C}$ using the operator $E^{\mu,d}_{ij}$ introduced in Eq. (54) as

$$\overline{C} = \sum_{\mu \in \mathbb{Y}^d_{n+1}} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \sum_{i,j=1}^{d_\mu} \sum_{k,l=1}^{d_\nu} [\overline{C}_{\mu\nu}]_{ik,jl} (E^{\mu,d}_{ij})_{\mathcal{I}^n\mathcal{F}} \otimes (E^{\nu,D}_{kl})_{\mathcal{P}\mathcal{O}^n} \tag{456}$$

for isometry inversion or isometry adjointation, and

$$\overline{C} = \sum_{\lambda \in \mathbb{Y}^d_n} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} [\overline{C}_{\lambda\nu}]_{ak,bl} (E^{\lambda,d}_{ab})_{\mathcal{I}^n} \otimes (E^{\nu,D}_{kl})_{\mathcal{P}\mathcal{O}^n} \tag{457}$$

for universal error detection using a $d_\mu d_\nu$ $(d_\lambda d_\nu)$-dimensional square matrix $\overline{C}_{\mu\nu}$ $(\overline{C}_{\lambda\nu})$, where ik (ak) and jl (bl) are the indices for row and column numbers, respectively. We also write W and $W^{(i)}$ appearing in the characterization of $\overline{\mathcal{W}}^{(x)}$ as

$$W = \sum_{\lambda \in \mathbb{Y}^d_n} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} [W_{\lambda\nu}]_{ak,bl} (E^{\lambda}_{ab})_{\mathcal{I}^n} \otimes (E^{\nu}_{kl})_{\mathcal{P}\mathcal{O}^n}, \tag{458}$$

$$W^{(i)} = \sum_{\lambda \in \mathbb{Y}^d_i} \sum_{\nu \in \mathbb{Y}^D_{i+1}} \sum_{a,b=1}^{d_\lambda} \sum_{k,l=1}^{d_\nu} [W^{(i)}_{\lambda\nu}]_{ak,bl} (E^{\lambda}_{ab})_{\mathcal{I}^i} \otimes (E^{\nu}_{kl})_{\mathcal{P}\mathcal{O}^i}. \tag{459}$$

Using Lemma 3, the condition $\overline{C} \in \overline{\mathcal{W}}^{(x)}$ for $x \in \{\mathrm{PAR}, \mathrm{SEQ}, \mathrm{GEN}\}$ are given by

$$\overline{C} \in \overline{\mathcal{W}}^{(x)} \iff \begin{cases} \{\overline{C}_{\mu\nu}\} \in \overline{\mathcal{W}}^{(x)}_{\mathrm{sym}} & (\text{isometry inversion, isometry adjointation}) \\ \{\overline{C}_{\lambda\nu}\} \in \overline{\mathcal{W}}^{(x)}_{\mathrm{sym}} & (\text{universal error detection}) \end{cases}, \tag{460}$$

where $\overline{\mathcal{W}}^{(x)}_{\mathrm{sym}}$ is given by

$$\{\overline{C}_{\mu\nu}\} \in \overline{\mathcal{W}}^{(\mathrm{PAR})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \overline{C}_{\mu\nu} = \displaystyle\sum_{\lambda \in \mu - \square} (X^{\mu}_{\lambda} \otimes \mathbb{1}_{d_\nu}) W_{\lambda\nu} (X^{\mu}_{\lambda} \otimes \mathbb{1}_{d_\nu})^\dagger \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1} \\ \displaystyle\sum_{\nu \in \mathbb{Y}^D_{n+1}} m^{(D)}_{\nu} \operatorname{Tr}_\nu (W_{\lambda\nu}) = \mathbb{1}_{d_\lambda} \quad \forall \lambda \in \mathbb{Y}^d_n \end{cases}, \tag{461}$$

$$\{\overline{C}_{\mu\nu}\} \in \overline{\mathcal{W}}^{(\mathrm{SEQ})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \overline{C}_{\mu\nu} = \displaystyle\sum_{\lambda \in \mu - \square} (X^{\mu}_{\lambda} \otimes \mathbb{1}_{d_\nu}) W_{\lambda\nu} (X^{\mu}_{\lambda} \otimes \mathbb{1}_{d_\nu})^\dagger \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1} \\ \displaystyle\sum_{\nu \in \kappa + \square} m^{(D)}_{\nu} (\mathbb{1}_{d_\lambda} \otimes X^{\kappa}_{\nu}) W^{(i)}_{\lambda\nu} (\mathbb{1}_{d_\lambda} \otimes X^{\kappa}_{\nu})^\dagger = \displaystyle\sum_{\gamma \in \lambda - \square} m^{(D)}_{\kappa} (X^{\lambda}_{\gamma} \otimes \mathbb{1}_{d_\kappa}) W^{(i-1)}_{\gamma\kappa} (X^{\lambda}_{\gamma} \otimes \mathbb{1}_{d_\kappa})^\dagger \\ \qquad\qquad \forall i \in \{1, \cdots, n\}, \lambda \in \mathbb{Y}^d_i, \kappa \in \mathbb{Y}^D_i \\ W^{(0)}_{\emptyset\square} = \dfrac{1}{D} \end{cases}, \tag{462}$$

$$\{\overline{C}_{\mu\nu}\} \in \overline{\mathcal{W}}^{(\mathrm{GEN})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \overline{C}_{\mu\nu} = \displaystyle\sum_{\lambda \in \mu - \square} (X^{\mu}_{\lambda} \otimes \mathbb{1}_{d_\nu}) W_{\lambda\nu} (X^{\mu}_{\lambda} \otimes \mathbb{1}_{d_\nu})^\dagger \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1} \\ [W_{\lambda\nu}, \pi_\lambda \otimes \pi'_\nu] = 0 \quad \forall \pi \in \mathfrak{S}_n, \\ \displaystyle\sum_{\nu \in \kappa + \square} m^{(D)}_{\nu} (\mathbb{1}_{d_\lambda} \otimes X^{\kappa}_{\nu}) W_{\lambda\nu} (\mathbb{1}_{d_\lambda} \otimes X^{\kappa}_{\nu})^\dagger = \displaystyle\sum_{\gamma \in \lambda - \square} m^{(D)}_{\kappa} (X^{\lambda}_{\gamma} \otimes \mathbb{1}_{d_\kappa}) W^{(n-1)}_{\gamma\kappa} (X^{\lambda}_{\gamma} \otimes \mathbb{1}_{d_\kappa})^\dagger \\ \qquad\qquad \forall \lambda \in \mathbb{Y}^d_n, \kappa \in \mathbb{Y}^D_n \\ \displaystyle\sum_{\lambda \in \mathbb{Y}^d_n} \sum_{\nu \in \mathbb{Y}^D_{n+1}} m^{(d)}_{\lambda} m^{(D)}_{\nu} \operatorname{Tr}(W_{\lambda\nu}) = d^n \end{cases} \tag{463}$$

for isometry inversion and isometry adjointation, where $W^{(i)}_{\gamma\kappa}$ for $\gamma \in \mathbb{Y}^d_i$ and $\kappa \in \mathbb{Y}^D_{i+1}$ are defined by

$$W^{(i)}_{\gamma\kappa} := \begin{cases} W_{\gamma\kappa} & (i = n) \\ \frac{1}{d} \sum_{\lambda \in \gamma + \square} \sum_{\nu \in \kappa + \square} \frac{m^{(d)}_{\lambda} m^{(D)}_{\nu}}{m^{(d)}_{\gamma} m^{(D)}_{\kappa}} (X^{\gamma}_{\lambda} \otimes X^{\kappa}_{\nu}) W^{(i+1)}_{\lambda\nu} (X^{\gamma}_{\lambda} \otimes X^{\kappa}_{\nu})^\dagger & (i \in \{0, \cdots, n-1\}) \end{cases}, \tag{464}$$

π_λ is the irreducible representation of π given in Eq. (49), and π'_ν is the irreducible representation of π' defined by $\pi'(1) = 1$ and $\pi'(i+1) = \pi(i) + 1$ for $i \in \{1, \cdots, n\}$. The set

$\overline{\mathcal{W}}^{(x)}_{\mathrm{sym}}$ is given by

$$\{\overline{C}_{\lambda\nu}\} \in \overline{\mathcal{W}}^{(\mathrm{PAR})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \overline{C}_{\lambda\nu} = W_{\lambda\nu} \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1} \\ \displaystyle\sum_{\nu\in\mathbb{Y}^D_{n+1}} m^{(D)}_\nu \operatorname{Tr}_\nu(W_{\lambda\nu}) = \mathbb{1}_{d_\lambda} \quad \forall \lambda \in \mathbb{Y}^d_n \end{cases}, \tag{465}$$

$$\{\overline{C}_{\lambda\nu}\} \in \overline{\mathcal{W}}^{(\mathrm{SEQ})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \overline{C}_{\lambda\nu} = W_{\lambda\nu} \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1} \\ \displaystyle\sum_{\nu\in\kappa+\square} m^{(D)}_\nu (\mathbb{1}_{d_\lambda} \otimes X^\kappa_\nu) W^{(i)}_{\lambda\nu} (\mathbb{1}_{d_\lambda} \otimes X^\kappa_\nu)^\dagger = \sum_{\gamma\in\lambda-\square} m^{(D)}_\kappa (X^\lambda_\gamma \otimes \mathbb{1}_{d_\kappa}) W^{(i-1)}_{\gamma\kappa} (X^\lambda_\gamma \otimes \mathbb{1}_{d_\kappa})^\dagger \\ \hfill \forall i \in \{1, \cdots, n\}, \lambda \in \mathbb{Y}^d_i, \kappa \in \mathbb{Y}^D_i \\ W^{(0)}_{\emptyset\square} = \dfrac{1}{D} \end{cases}, \tag{466}$$

$$\{\overline{C}_{\lambda\nu}\} \in \overline{\mathcal{W}}^{(\mathrm{GEN})}_{\mathrm{sym}} \iff$$
$$\begin{cases} \overline{C}_{\lambda\nu} = W_{\lambda\nu} \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1} \\ [W_{\lambda\nu}, \pi_\lambda \otimes \pi'_\nu] = 0 \quad \forall \pi \in \mathfrak{S}_n, \\ \displaystyle\sum_{\nu\in\kappa+\square} m^{(D)}_\nu (\mathbb{1}_{d_\lambda} \otimes X^\kappa_\nu) W_{\lambda\nu} (\mathbb{1}_{d_\lambda} \otimes X^\kappa_\nu)^\dagger = \sum_{\gamma\in\lambda-\square} m^{(D)}_\kappa (X^\lambda_\gamma \otimes \mathbb{1}_{d_\kappa}) W^{(n-1)}_{\gamma\kappa} (X^\lambda_\gamma \otimes \mathbb{1}_{d_\kappa})^\dagger \\ \hfill \forall \lambda \in \mathbb{Y}^d_n, \kappa \in \mathbb{Y}^D_n \\ \displaystyle\sum_{\lambda\in\mathbb{Y}^d_n} \sum_{\nu\in\mathbb{Y}^D_{n+1}} m^{(d)}_\lambda m^{(D)}_\nu \operatorname{Tr}(W_{\lambda\nu}) = d^n \end{cases} \tag{467}$$

for universal error detection. Using this characterization of $\overline{\mathcal{W}}^{(x)}$ with the $\mathbb{U}(d) \times \mathbb{U}(D)$ and permutation symmetry, the dual SDPs (434), (440), (446) and (451) can be simplified as follows:

- Probabilistic exact isometry inversion

$$\begin{aligned} \min \ & \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{\nu\in\mathbb{Y}^D_{n+1}} \operatorname{Tr} \overline{C}_{\mu\nu}/d^{n+1} \\ \text{s.t. } & \omega \in \mathbb{R}, 0 \leq \overline{C}_{\mu\nu} \in \mathcal{L}(\mathbb{C}^{d_\mu} \otimes \mathbb{C}^{d_\nu}) \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1}, \\ & \{\overline{C}_{\mu\nu}\} \in \mathrm{Cone}[\overline{\mathcal{W}}^{(x)}_{\mathrm{sym}}], \\ & \overline{C}_{\mu\nu} \geq \delta_{\mu\nu}(1-\omega)\Omega_\mu + \omega \sum_{\lambda\in\mu-\square} (X^\lambda_\mu \otimes \mathbb{1}_{d_\mu})^\dagger \Xi_{\lambda\nu} (X^\lambda_\mu \otimes \mathbb{1}_{d_\mu}) \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1}. \end{aligned} \tag{468}$$

- Deterministic isometry inversion

$$\begin{aligned} \min \ & \sum_{\mu\in\mathbb{Y}^d_{n+1}} \sum_{\nu\in\mathbb{Y}^D_{n+1}} \operatorname{Tr} \overline{C}_{\mu\nu}/d^{n+1} \\ \text{s.t. } & \omega \in \mathbb{R}, 0 \leq \overline{C}_{\mu\nu} \in \mathcal{L}(\mathbb{C}^{d_\mu} \otimes \mathbb{C}^{d_\nu}) \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1}, \\ & \{\overline{C}_{\mu\nu}\} \in \mathrm{Cone}[\overline{\mathcal{W}}^{(x)}_{\mathrm{sym}}], \\ & \overline{C}_{\mu\mu} \geq \Omega_\mu \quad \forall \mu \in \mathbb{Y}^d_{n+1}. \end{aligned} \tag{469}$$

- Universal error detection

$$\begin{aligned}
&\max \xi - \sum_{\lambda \in \mathbb{Y}^d_n} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \operatorname{Tr} \overline{C}_{\lambda\nu}/d^n \\
\text{s.t. } &\xi \in \mathbb{R}, 0 \leq \overline{C}_{\lambda\nu} \in \mathcal{L}(\mathbb{C}^{d_\lambda} \otimes \mathbb{C}^{d_\nu}) \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1}, \\
&\{\overline{C}_{\lambda\nu}\} \in \operatorname{Cone}[\overline{\mathcal{W}}^{(x)}_{\text{sym}}], \\
&\overline{C}_{\lambda\nu} \geq \xi \Xi_{\lambda\nu} - \Sigma_{\lambda\nu} \quad \forall \lambda \in \mathbb{Y}^d_n, \nu \in \mathbb{Y}^D_{n+1}.
\end{aligned} \tag{470}$$

- Isometry adjointation

$$\begin{aligned}
&\max \omega + \xi - \sum_{\mu \in \mathbb{Y}^d_{n+1}} \sum_{\nu \in \mathbb{Y}^D_{n+1}} \operatorname{Tr} \overline{C}_{\mu\nu}/d^{n+1} \\
\text{s.t. } &\xi \in \mathbb{R}, 0 \leq \omega \leq 1, 0 \leq \overline{C}_{\mu\nu} \in \mathcal{L}(\mathbb{C}^{d_\mu} \otimes \mathbb{C}^{d_\nu}) \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1}, \\
&\{\overline{C}_{\mu\nu}\} \in \operatorname{Cone}[\overline{\mathcal{W}}^{(x)}_{\text{sym}}], \\
&\overline{C}_{\mu\nu} \geq \delta_{\mu\nu} \omega \Omega + \sum_{\lambda \in \mu - \square} (X^\lambda_\mu \otimes \mathbb{1}_{d_\nu})^\dagger [\xi \Xi_{\lambda\nu} - (1-\omega)\Sigma_{\lambda\nu}](X^\lambda_\mu \otimes \mathbb{1}_{d_\nu}) \quad \forall \mu \in \mathbb{Y}^d_{n+1}, \nu \in \mathbb{Y}^D_{n+1}.
\end{aligned} \tag{471}$$

References

[1] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[2] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, R2626 (1999).

[3] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[4] U. Chabaud, E. Diamanti, D. Markham, E. Kashefi, and A. Joux, Phys. Rev. A **98**, 062318 (2018).

[5] A. Bisio and P. Perinotti, Proc. R. Soc. A **475**, 20180706 (2019).

[6] M. Ying, *Foundations of quantum programming* (Morgan Kaufmann, 2016).

[7] E. Chitambar and G. Gour, Rev. Mod. Phys. **91**, 025001 (2019).

[8] F. A. Pollock, C. Rodríguez-Rosario, T. Frauenheim, M. Paternostro, and K. Modi, Phys. Rev. A **97**, 012127 (2018).

[9] O. Oreshkov, F. Costa, and Č. Brukner, Nat. Commun. **3**, 1092 (2012).

[10] G. Chiribella and D. Ebler, New J. Phys. **18**, 093053 (2016).

[11] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180504 (2008).

[12] A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, Phys. Rev. A **81**, 032324 (2010).

[13] M. Sedlák, A. Bisio, and M. Ziman, Phys. Rev. Lett. **122**, 170502 (2019).

[14] Y. Yang, R. Renner, and G. Chiribella, Phys. Rev. Lett. **125**, 210501 (2020).

[15] M. Sedlák and M. Ziman, Phys. Rev. A **102**, 032618 (2020).

[16] A. Bisio, G. M. D'Ariano, P. Perinotti, and M. Sedlák, Phys. Lett. A **378**, 1797 (2014).

[17] W. Dür, P. Sekatski, and M. Skotiniotis, Phys. Rev. Lett. **114**, 120503 (2015).

[18] G. Chiribella, Y. Yang, and C. Huang, Phys. Rev. Lett. **114**, 120504 (2015).

[19] M. Soleimanifar and V. Karimipour, Phys. Rev. A **93**, 012344 (2016).

[20] J. Miyazaki, A. Soeda, and M. Murao, Phys. Rev. Res. **1**, 013007 (2019).

[21] D. Ebler, M. Horodecki, M. Marciniak, T. Młynik, M. T. Quintino, and M. Studziński, IEEE Trans. Inf. Theory **69**, 5069 (2023).

[22] M. Araújo, A. Feix, F. Costa, and Č. Brukner, New J. Phys. **16**, 093026 (2014).

[23] A. Bisio, M. Dall'Arno, and P. Perinotti, Phys. Rev. A **94**, 022340 (2016).

[24] Q. Dong, S. Nakayama, A. Soeda, and M. Murao, arXiv:1911.01645 (2019).
[25] Q. Dong, M. T. Quintino, A. Soeda, and M. Murao, Phys. Rev. Lett. **126**, 150504 (2021).
[26] I. S. Sardharwalla, T. S. Cubitt, A. W. Harrow, and N. Linden, arXiv:1602.07963 (2016).
[27] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Phys. Rev. A **100**, 062339 (2019).
[28] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Phys. Rev. Lett. **123**, 210502 (2019).
[29] M. T. Quintino and D. Ebler, Quantum **6**, 679 (2022).
[30] S. Yoshida, A. Soeda, and M. Murao, Phys. Rev. Lett. **131**, 120602 (2023).
[31] M. Navascués, Phys. Rev. X **8**, 031008 (2018).
[32] D. Trillo, B. Dive, and M. Navascués, Quantum **4**, 374 (2020).
[33] D. Trillo, B. Dive, and M. Navascués, Phys. Rev. Lett. **130**, 110201 (2023).
[34] A. Bisio, G. M. D'Ariano, P. Perinotti, and M. Sedlák, Phys. Rev. A **84**, 042330 (2011).
[35] S. Yoshida, A. Soeda, and M. Murao, Quantum **7**, 957 (2023).
[36] L. Hardy, J. Phys. A **40**, 3081 (2007).
[37] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Phys. Rev. A **88**, 022318 (2013).
[38] M. M. Wilde, *Quantum information theory* (Cambridge university press, 2013).
[39] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Europhys. Lett. **83**, 30004 (2008).
[40] M. Raginsky, Phys. Lett. A **290**, 11 (2001).
[41] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).
[42] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
[43] A. Y. Kitaev, Russ. Math. Surv. **52**, 1191 (1997).
[44] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **80**, 022339 (2009).
[45] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008).
[46] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli, *Representation theory of the symmetric groups: the Okounkov-Vershik approach, character formulas, and partition algebras*, Vol. 121 (Cambridge University Press, 2010).
[47] D. Bacon, I. L. Chuang, and A. W. Harrow, Phys. Rev. Lett. **97**, 170502 (2006).
[48] D. Bacon, I. L. Chuang, and A. W. Harrow, in *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07 (Society for Industrial and Applied Mathematics, USA, 2007) p. 1235–1244.
[49] H. Krovi, Quantum **3**, 122 (2019).
[50] W. M. Kirby and F. W. Strauch, Quantum Inf. Comput. **18**, 0721 (2018).
[51] E. Pearce-Crump, arXiv:2204.10694 (2022).
[52] A. Wills and S. Strelchuk, arXiv:2305.04069 (2023).
[53] M. Mozrzymas, M. Studziński, and M. Horodecki, J. Phys. A **51**, 125202 (2018).
[54] M. Studziński, M. Mozrzymas, P. Kopszak, and M. Horodecki, IEEE Trans. Inf. Theory **68**, 7892 (2022).
[55] G. Chiribella, G. D'Ariano, and M. Sacchi, Phys. Rev. A **72**, 042338 (2005).
[56] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. A **69**, 050303 (2004).
[57] G. Chiribella, G. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. **93**, 180503 (2004).
[58] P. A. Guérin, M. Krumm, C. Budroni, and Č. Brukner, New J. Phys, **21**, 012001 (2019).
[59] D. Grinko and M. Ozols, arXiv:2207.05713 (2022).

[60] MATLAB, *version 9.11.0 (R2021b)* (The MathWorks Inc., Natick, Massachusetts, 2021).

[61] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.2, `http://cvxr.com/cvx` (2020).

[62] M. Grant and S. Boyd, in *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag Limited, 2008) pp. 95–110, `http://stanford.edu/~boyd/graph_dcp.html`.

[63] `http://www.math.nus.edu.sg/.mattohkc/sdpt3.html`.

[64] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, Optim. Methods Softw. **11**, 545 (1999).

[65] R. H. Tütüncü, K.-C. Toh, and M. J. Todd, Math. Program. **95**, 189 (2003).

[66] J. F. Sturm, Optim. Methods Softw. **11**, 625 (1999).

[67] MOSEK ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 10.0.* (2022).

[68] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.7)* (2022), `https://www.sagemath.org`.

[69] `https://github.com/sy3104/isometry_adjointation`.

[70] `https://opensource.org/licenses/MIT`.

[71] A. Acin, Phys. Rev. Lett. **87**, 177901 (2001).

[72] G. Chiribella, Y. Yang, and A. C.-C. Yao, Nat. Commun. **4**, 2915 (2013).

[73] K. Matsumoto, arXiv:1209.2392 (2012).

[74] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[75] Mathematica, Version 13.3 (2023).

[76] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, and Č. Brukner, New J. Phys. **17**, 102001 (2015).

[77] J. Bavaresco, M. Murao, and M. T. Quintino, Phys. Rev. Lett. **127**, 200504 (2021).

Extended abstract: Learning and testing possibly magical fermions

Lennart Bittel[1] * Jens Eisert[1] † Yaroslav Herasymenko[2 3 4] ‡
Lorenzo Leone[1] § Antonio Anna Mele [1] ¶

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[2] *QuSoft and CWI, Science Park 123, 1098 XG Amsterdam, The Netherlands*
[3] *QuTech, TU Delft, P.O. Box 5046, 2600 GA Delft, The Netherlands*
[4]*Delft Institute of Applied Mathematics, TU Delft, 2628 CD Delft, The Netherlands*

Abstract. The experimental realization of increasingly complex quantum states underscores the pressing need for new methods of state testing and learning. We show that any algorithm capable of testing if a state is a possibly mixed free-fermionic states or not would inevitably be inefficient, but we then present an efficient algorithm for testing low-rank free-fermionic states. We also prove improved bounds on the sample complexity for tomography of pure free-fermionic states, and we also generalize the algorithm to the mixed-scenario and to the case of states prepared by free-fermionic evolutions doped with a few fermionic magic gates.

Keywords: Quantum Learning, Tomography, Testing, Magic, Perturbation bounds, Fermions

1 Introduction

Note: This submission is based on this work recently posted on ArXiv [1] and also on another work that we will post shortly [2].

Ubiquitous in various domains of physics, from condensed matter theory to quantum chemistry, free-fermionic states, also known as fermionic Gaussian states or states prepared by matchgates circuits, are unique for quantum computation because they belong to a nontrivial class of efficiently classically simulable states [3, 4]. While these states may be considered ineffective for advantageous quantum computation, they serve as an essential milestone in the ongoing construction of fault-tolerant quantum devices: their efficiency in classical simulation provides a powerful tool for classical benchmarking quantum computation to ensure the correct functionality of quantum chips. However, before implementing any quantum benchmarking protocol based on free-fermionic states, experimentalists must verify that the state prepared on a quantum device is indeed close to a free-fermionic state. Addressing this concern, we formalize the problem as a property testing problem, aiming to distinguish situations where a given state (generally mixed) is close to the set of free-fermionic states from those where it is far. In the same fashion, given access to an unknown free-fermionic state, experimentalists must be able to learn a classical description of the state – a problem formalized as quantum state tomography. Our work comprehensively addresses the problem of testing and tomography of free-fermionic states, providing scenarios with provable efficiency guarantees and ruling out situations in which the aforementioned tasks are hard to perform. We also extend the learning and testing problem to the scenario of states prepared by arbitrary many free-fermionic evolutions and at most t local non-free evolutions, that we call t-doped fermionic Gaussian states (or t-doped free-fermionic/matchgates states). By Jordan-Wigner mapping, this also includes n-qubit states prepared by nearest-neighbour matchgate circuits with at most t SWAP-gates. The workhorse of our results is provided by new insights into free-fermionic states: Specifically, we show lower and upper bound on the minimum trace distance between a state and the set of free-fermionic states, which also serve as efficiently computable measures of 'non-Gaussianity' for the state. We derive useful bounds on the trace distance between two possibly mixed free-fermionic states in terms of the norm difference of their correlation matrices. Furthermore, we show that all the 'magic' in a t-doped free-fermionic state can be compressed via a free-fermionic unitary to a localized region of the system.

2 Fundamental insights

Imagine one aims to prepare a pure free-fermionic state on a quantum processor. In practice, an imperfect, non-Gaussian, yet close version of the state is actually prepared. The task of quantum state certification is to verify the almost correct preparation of the target state based on the operational distance between the two, i.e., the trace distance. However, since the distance between a theoretical quantum state ψ and a quantum state ρ is generally hard to measure, we aim to understand how the trace distance between two "close" quantum states is controlled by their respective correlation matrices, which can be efficiently measured in practical scenarios. Below, we upper bound the trace distance between a perfect pure free-fermionic state ψ and a non-Gaussian (possibly mixed) imperfect realization ρ through their respective covariance matrices.

Proposition 1 *Let ψ be a free fermionic pure state and ρ be a arbitrary quantum state with correlation matrices*

*bittel@fu-berlin.de
†jense@fu-berlin.de
‡yaroslav@cwi.nl
§lorenzo.leone@fu-berlin.de
¶a.mele@fu-berlin.de

$\Gamma(\psi), \Gamma(\rho)$ *respectively. Then:*

$$\|\psi-\rho\|_1 \leq \sqrt{\|\Gamma(\psi)-\Gamma(\rho)\|_1}. \tag{1}$$

Given that the correlation matrix $\Gamma(\psi)$ is known and efficiently classically encoded, Eq. (1) offers an efficient and direct method to verify the accurate preparation of ψ within a marginal error ε, as it is sufficient to measure $\Gamma(\rho)$ up to $O(\varepsilon^2)$ precision that require $\mathrm{poly}(n, 1/\varepsilon)$ resources.

Next, we introduce two perturbation bounds for the trace distance between two free-fermionic states in relation to the distance between their covariance matrices.

Theorem 2 (Trace distance bounds)

- *Let* $|\psi\rangle, |\phi\rangle$ *be two pure free-fermionic states, then:* $\|\psi-\phi\|_1 \leq \frac{1}{2}\|\Gamma(\psi)-\Gamma(\phi)\|_2$,
- *Let* ρ, σ *be two mixed free-fermionic states, then:* $$\|\rho-\sigma\|_1 \leq \sqrt{\|\Gamma(\rho)-\Gamma(\sigma)\|_1 + \tfrac{1}{2}\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2}\,.$$

In our technical manuscript, we also lower bound the quantity $\mathcal{M}(\rho) = \min_{\sigma\in\mathcal{G}} \|\rho-\sigma\|_1$, where $\mathcal{G}$ is the set of free-fermionic states (pure or mixed), in terms of the correlation matrix of the state ρ. This also serve as an efficient to estimate measure of non-Gaussianity for the given state.

We moreover establish a property of states prepared by arbitrary many free-fermionic evolutions (also called matchgates or Gaussian gates) and at most t local non free-fermionic gates (e.g., SWAP gates), that we denote as t-doped free-fermionic states (or, t-doped fermionic Gaussian state).

Theorem 3 (Magic compression) *For any t-doped free-fermionic state $|\psi\rangle$, there exists a Gaussian operation G such that*

$$G|\psi\rangle = |\phi\rangle \otimes |0^{n-\kappa t}\rangle, \tag{2}$$

where $|\phi\rangle$ is a state supported exclusively on κt qubits and κ is a constant.

Besides being fundamental for the efficiency of subsequent testing and tomography algorithms, we expect that these results have extensive applicability in the context of free fermions, in both theoretical and experimental realms. For example, the latter theorem sheds light also on the efficient circuit compilation of this class of states.

3 Testing free-fermionic states

Given copies of an unknown quantum state ρ, how to understand if it close or far from the set of free fermionic states? Our goal is to identify scenarios in which addressing the aforementioned question is feasible in terms of resources, to provide algorithms with provable efficiency guarantees, and to delineate situations in which answering the question is challenging. First of all, let us formulate the problem in a rigorous fashion.

Problem 1 Let $\varepsilon_B > \varepsilon_A \geq 0$. Given N copies of an unknown quantum state ρ with the promise that it falls into one of two distinct situations:

- **Case A:** There exists a free-fermionic state $\sigma \in \mathcal{G}$ such that $\|\rho-\sigma\|_1 \leq \varepsilon_A$.
- **Case B:** ρ is ε_B-far from all free-fermionic states σ, indicating $\min_{\sigma\in\mathcal{G}} \|\rho-\sigma\|_1 > \varepsilon_B$.

Determine whether the state is in Case A or Case B through measurements performed on the provided N state copies. Further specifications regarding the rank of the state ρ and the set of free-fermionic states $\mathcal{G} \equiv \mathcal{G}_{\mathrm{pure}}$, $\mathcal{G}_{\mathrm{mixed}}$, $\mathcal{G}_R$ (being pure, mixed and bounded rank R free-fermionic states respectively) must be provided.

When no prior assumptions on the state ρ and no restrictions on the set of free-fermionic states $\mathcal{G}$ are provided, we establish the general hardness for Problem 1, demonstrating that $N = \Omega(2^n)$ copies of the state ρ are necessary. Below, we present a more refined version of the mentioned no-go result.

Theorem 4 (Hardness of testing) *Let $\varepsilon_B > 0$. Let ρ denote the unknown state and $\mathcal{G}$ the set of free fermionic states considered. To solve Problem 1, with at least a $2/3$ probability of success, $N = \Omega(R/\varepsilon_B^2)$ copies are necessary if either of the following hypotheses is assumed:*

- *ρ is such that* $\mathrm{rank}(\rho) \leq R$,
- $\mathcal{G} \equiv \mathcal{G}_R$.

In particular, for $R = \exp(\Omega(n))$ the sample complexity grows exponentially in the number of modes n.

Given this hardness results, Theorem 4 prompts the natural question of whether an algorithm exists that scales polynomially with the rank R, which solve the property testing problem under the assumption that ρ has a rank at most R or when restricting to the set $\mathcal{G}_R$. In response to this, we present the following theorem.

Theorem 5 (Efficient free-fermionic testing)) *Problem 1 can be solved with $N = \mathrm{poly}(n, R)$ copies of ρ in the following scenarios:*

1. *the given state ρ is such that* $\mathrm{rank}(\rho) \leq R$;
2. *the set of Gaussian states is restricted to $\mathcal{G}_R$.*

We provide algorithms for case (i) and (ii) that use N samples and $\mathrm{poly}(n, R)$ computational resources.

Let us summarize our findings. In its full generality, that is, without rank assumptions on the state ρ and considering $\mathcal{G} \equiv \mathcal{G}_{\mathrm{mixed}}$, Problem 1 requires $N = \Omega(2^n)$ samples of the state to be solved. However, as claimed in Theorem 5, we have established that Problem 1 can be efficiently addressed both sample-wise and computationally under two specific scenarios: (i) when the given state ρ has a rank R that scales polynomially with the number of modes n, or (ii) when the focus is solely on quantifying closeness to the set of Gaussian states with polynomially bounded rank $\mathcal{G}_R$.

4 Learning free-fermionic states

We present a simple algorithm for efficiently learning a unknown n-qubit free-fermionic state either pure or mixed. More rigorously, we are concerned with the following problem: let $\rho \in \mathcal{G}$, with $\mathcal{G} = \mathcal{G}_{\text{mixed}}, \mathcal{G}_{\text{pure}}$, be a unknown (either pure or mixed) free-fermionic state, design a computationally efficient quantum learning algorithm that consumes N copies of ρ and output a classical description $\hat{\rho}$ that is ε-close in trace distance to ρ with failure probability of at most δ. Some earlier works [6, 5, 7] have already tackled this problem, but their analyses have been limited to the specific case of ρ being a pure free fermionic state. We first provide a better sample complexity upper bound limited to the case of pure states that significantly improves upon previous work. What is more, our approach extends to the more realistic mixed state scenario, significantly broadening the scope of such result. This extension, as well as the improved algorithm for pure state case, heavily rely on the toolkit developed and discussed in this paper, in particular Theorem 2.

Theorem 6 (Pure Gaussian states tomography) *Let ψ be a pure free-fermionic quantum state. For $\varepsilon, \delta \in (0, 1)$, there exist a learning algorithm that utilizes $N = O((n^3/\varepsilon^2)\log(n^2/\delta))$ copies of the state and only single-copies measurements to learn an efficient classical representation of the state $\hat{\psi}$ obeying $\|\psi - \hat{\psi}\|_1 \leq \varepsilon$, with a success probability of at least $1 - \delta$.*

Thus, our scaling $O(n^3/\varepsilon^2)$ improves upon the previous best scaling of Ref. [7] that was $O(n^3 m^2/\varepsilon^4)$ (where m represents the fixed number of particles of the fermionic state). We now present the theorem for the mixed case scenario.

Theorem 7 (Mixed Gaussian states tomography) *Let ρ be a mixed free-fermionic quantum state. For $\varepsilon, \delta \in (0, 1)$, there exist a learning algorithm that, utilizing $N = O((n^5/\varepsilon^4)\log(n^2/\delta))$ copies of the state ρ and single-copies measurements, learns a classical representation $\hat{\rho}$ of the state ρ obeying $\|\hat{\rho} - \rho\|_1 \leq \varepsilon$, with a success probability of at least $1 - \delta$.*

5 Learning and testing magical fermions

As in the case of Clifford circuits, for which the introduction of magic gates, such as T-gates, allows to reach universal quantum computation, also for the case of Gaussian (i.e., free-fermionic or matchgates) circuits the inclusion of certain magic gates, for example SWAP gates [8], allows to reach universality. If the number t of T-gates in a Clifford circuit is low, the resulting states can still be efficiently simulated classically [9]; it has also been recently demonstrated that such states, termed as t-doped stabilizer states, are still efficiently learnable [10, 11, 12]. Similarly, in the past year, it has been shown that matchgates circuits with a few magic gates are also classically simulable [13, 14, 15]. However, the learnability of such "t-doped fermionic states" remains unknown and this motivates the question: Can we efficiently learn states prepared by Gaussian operations (e.g. matchgates) and a few magic gates?

We answer it by proposing a sample and time efficient quantum learning algorithm of polynomial time and sample complexity that uses only single-copy measurements and learns a classical description of a t-doped fermionic Gaussian state; the learned state is guaranteed to be close to the true state in trace distance.

Theorem 8 (t-doped tomography) *Let $|\psi\rangle$ be a t-doped Gaussian state, and $\varepsilon, \delta \in (0, 1]$. Utilizing $O(\mathrm{poly}(n, 2^t))$ single-copy measurements and computational time, there exists an algorithm which outputs a classical representation of a state which is guaranteed to be at least ε close in trace distance to $|\psi\rangle$, with probability $\geq 1 - \delta$.*

Our learning algorithm may also be feasible to implement in near-term fermionic analog quantum simulators, like cold atoms in optical lattices, since we only utilize time evolutions of simple few-body fermionic Hamiltonians. The core of our algorithm relies on Theorem 3. Informally, it says that all the magic of such states can be *compressed* to a few qubits via a free-fermionic operation. The proof of this compression theorem is constructive, which has implications for the circuit complexity of $|\psi\rangle$ and for improved preparation of doped fermionic Gaussian states. The high level idea of the learning algorithm is to first learn a Gaussian unitary which *compresses* the magic, apply it to the state, and then perform full state state tomography on the first few qubits alone. Our learning algorithm is efficient for $t = \mathcal{O}(\log(n))$ and no longer efficient if the number of non-Gaussian gates is larger. However, we show that any algorithm to learn such states doped with a *slightly* more than than logarithmic number of non-Gaussian gates, must be necessarily inefficient, based on common cryptographic assumptions [16].

Theorem 9 (Time-complexity lower bound) *Under a common cryptographic assumption, there is no time efficient algorithm to learn a general $\tilde{\omega}(\log(n))$-doped Gaussian state.*

To obtain this result, we exploit the theory of pseudorandom-quantum states [17, 18], so far considered only for qubit-based systems, by bringing it into the fermionic realm.

Furthermore, our algorithm extends to all compressible states, i.e., those which can be written as $|\psi\rangle = G|\phi\rangle \otimes |0^{n-t}\rangle$, where G is a Gaussian unitary and $|\phi\rangle$ an arbitrary state supported solely on t-qubits (or fermionic modes). We also propose an efficient method to *test* if a given state is close or far from the set of compressible states, by showing an efficiently estimatable quantity that lower bounds the distance to this set.

References

[1] A. A. Mele, Y. Herasymenko Efficient learning of quantum states prepared with few fermionic non-Gaussian gates. In ArXiv, 2024.

[2] L. Bittel, A.A. Mele, J. Eisert, L. Leone. Testing free-fermionic quantum states and improved tomography. In *Preparation*, 2024.

[3] E. Knill. Fermionic Linear Optics and Matchgates. In ArXiv, 2001.

[4] B. Terhal, D.P. DiVincenzo. Classical simulation of noninteracting-fermion quantum circuits. In ArXiv, 2002.

[5] B. O'Gorman. Fermionic tomography and learning. In ArXiv, 2022.

[6] M. Gluza, M. Kliesch, J. Eisert, L. Aolita. Fidelity Witnesses for Fermionic Quantum Simulations. In *Phys. Rev. Lett*, 2018.

[7] S. Aaronson, S. Grewal. Efficient Tomography of Non-Interacting Fermion States. In ArXiv, 2018.

[8] D.J. Brod, E.F. Galvão. Extending matchgates into universal quantum computation. In *Physical Review A*, 2011.

[9] D. Gottesman. The Heisenberg Representation of Quantum Computers. In ArXiv, 1998.

[10] S. Grewal, V. Iyer, W. Kretschmer, D. Liang. Efficient Learning of Quantum States Prepared With Few Non-Clifford Gates. In ArXiv, 2023.

[11] L. Leone and S.F.E. Oliviero, A. Hamma. Learning t-doped stabilizer states. In ArXiv, 2023.

[12] D. Hangleiter, M.J. Gullans. Bell sampling from quantum circuits. In ArXiv, 2023.

[13] J. Cudby, S. Strelchuk. Gaussian decomposition of magic states for matchgate computations. In ArXiv, 2023.

[14] B. Dias, R. Koenig. Classical simulation of non-Gaussian fermionic circuits. In ArXiv, 2023.

[15] O. Reardon-Smith, M. Oszmaniec, K. Korzekwa. Improved simulation of quantum circuits dominated by free fermionic operations. In ArXiv, 2023.

[16] S. Arunachalam, A.B. Grilo, A. Sundaram Quantum hardness of learning shallow classical circuits. In Electron. Colloquium Comput. Complex, 2019.

[17] Z. Brakerski and Omri Shmueli. (Pseudo) Random Quantum States with Binary Phase. In ArXiv, 2019.

[18] Z. Ji, Y.K. Liu, F. Song. Pseudorandom Quantum States. In ArXiv, 2018.

APPENDIX

Testing free-fermionic quantum states and improved tomography

Lennart Bittel,[1, *] Antonio Anna Mele,[1, *] Jens Eisert,[1, *] and Lorenzo Leone[1, *]

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

(Dated: May 19, 2024)

Testing whether a quantum state is far from a classically efficiently tractable set of states is a fundamental task in quantum information. A physically relevant instance of such a set of states is given by free-fermionic states, also known as fermionic Gaussian states or states prepared by matchgate circuits. In this study, we analyze property testing of free-fermionic states, specifically the task of determining, through measurements, whether an unknown state is close to or far from the set of free-fermionic states. We first show that any algorithm capable of testing possibly mixed free-fermionic states would inevitably be inefficient. However, we then turn to presenting an efficient algorithm to test low-rank free-fermionic states. We prove improved bounds on the sample complexity for tomography of pure free-fermionic states, and we also generalize the algorithm to the mixed-scenario. The workhorse of our results is provided by new insights into fermionic Gaussian states: Specifically, we show lower and upper bound on the minimum trace distance between a state and the set of free-fermionic states, which also serve as efficiently computable measures of 'non-Gaussianity' for the state. Furthermore, we derive useful bounds on the trace distance between two possibly mixed free-fermionic states in terms of the norm difference of their correlation matrices.

I. Introduction

As the construction of quantum devices such as quantum computers and simulators progresses, there is a growing emphasis on developing efficient learning schemes to extract key diagnostic information from quantum systems. The tasks of quantum certification [1] and benchmarking [2] are crucial in any effort that aims are manipulating or preparing quantum states to utmost precision – and hence to achieve predictive power of a sort. Extracting information from quantum systems is generally a challenging task, marred by obstructions in sample and computational complexity, but real-world scenarios often defy general no-go results. States prepared on current quantum devices commonly feature a lot of structure; they possess specific properties and symmetries, diverging from general states which oftentimes can be seen largely as abstractions. Within the realm of fermionic quantum computation, free-fermionic [3] (or Gaussian) quantum states play a crucial role. Ubiquitous in various domains of physics, ranging from condensed matter theory [4] – then often referred to as arising in "non-interacting" settings – over the study of analog quantum simulators with ultra-cold fermionic atoms [5, 6] to quantum chemistry [7] what makes free-fermionic states unique for quantum computation is that they belong to a non-trivial class of efficiently classically simulable states [8–10]. While these states may be considered ineffective for advantageous quantum computation, they serve as an essential milestone in the ongoing construction of fault-tolerant quantum devices: Their efficiency in classical simulation provides a powerful tool for classical benchmarking quantum computation to ensure the correct functionality of quantum chips. This situation is not dissimilar from that of Clifford circuits and stabilizer states in the quantum computing domain.

However, before implementing any quantum benchmarking protocol based on free-fermionic states, experimentalists must usually verify that the state prepared on a quantum device is indeed close to a free-fermionic state in the first place. Addressing this concern, we formalize the problem as a *property testing problem*, aiming to distinguish situations where a given state (generally mixed) is close to the set of free-fermionic states from those where it is far. We not only provide a meticulous analysis, identifying scenarios for which it can be efficiently executed while ruling out cases in which it is computationally hard, but also provide polynomial-time algorithms to test

- (i) whether a general state is close to or far from the set of free-fermionic low-rank states and
- (ii) whether a low-rank state is close of far to the full set of free-fermionic states. Although seemingly similar, the two approaches differ significantly both conceptually and operationally. Ultimately, the choice between them rests entirely with the user and on the amount of prior knowledge that she has on the state, which we carefully discuss below. Moreover, these algorithms employ single-copy measurements, making them executable on near-term devices in a noise-resilient fashion.
- (iii) Furthermore, we present information-theoretic bounds that hold independent interest from both theoretical and experimental perspectives. In particular, we offer efficiently computable and experimentally measurable lower bounds for the minimum distance between a given state and the set of free-fermionic states. These bounds effectively probe the degree of non-Gaussianity (or magic) of a given state.
- (iv) Moreover, for general mixed free-fermionic states, we demonstrate that the maximal information-theoretic difference (trace distance) between two states is, at most, as large as the distance quantified by their respective correlation matrices, encoding two-body Majorana correlation functions. This relation is rigorously established with a *optimal perturbation bound* between

[*] {l.bittel, a.mele, jense, lorenzo.leone}@fu-berlin.de

the (Uhlmann) fidelity between two free-fermionic states and the operator norm difference between the respective correlation matrices. Beyond contributing to our testing algorithms, this result has significant implications for experimental perspectives, as Majorana correlations are easily measurable with single-copy Pauli measurements.

(v) Confining our analysis to pure states, we enhance this bound by offering an optimal perturbation bound for the overlap between two pure free-fermionic states. This is expressed in terms of the Hilbert-Schmidt norm difference between the correlation matrices of the states. Remarkably, the two bounds for pure and mixed states respectively are optimal in their respective domains, and they differ, making their effective merging unattainable. As an additional consequence of these perturbation bounds result, we develop a straightforward tomography algorithm that extends beyond and significantly improve previous known results [11], which were focused on pure and particle-preserving Gaussian states. In particular, for pure states, we significantly enhance the scaling compared to Ref. [11], and we extend the tomography algorithm for completely general mixed free-fermionic states.

A. Setup, preliminaries and definitions

In this section, we briefly provide the basic definitions necessary for the main results of this work, which are presented later on. We consider systems of n fermionic modes (or qubits, by virtue of the Jordan-Wigner representation). Majorana operators are defined, through standard Pauli single qubit operators $\{X_i, Z_i, Y_i, I\}$, as

$$\gamma_{2k-1} := (\prod_{j=1}^{k-1} Z_j)X_k \,, \qquad \gamma_{2k} := (\prod_{j=1}^{k-1} Z_j)Y_k \tag{1}$$

for $k \in [n]$, where $[n] := \{1, \dots, n\}$. Given a quantum state ρ, its *correlation matrix* (or covariance matrix) $\Gamma(\rho)$ is a $2n \times 2n$ matrix with elements

$$[\Gamma(\rho)]_{j,k} = -\frac{i}{2}\operatorname{Tr}\left([\gamma_j, \gamma_k]\,\rho\right), \tag{2}$$

where $j, k \in [2n]$. Correlation matrices are real and anti-symmetric, with eigenvalues in absolute value contained in the interval $[0, 1]$.

Let $O(2n)$ denote the orthogonal group on a $2n$-dimensional vector space. There is bijection between $O(2n)$ and *free-fermionic unitaries* (or Gaussian) acting a on n qubits system: For any orthogonal matrix $Q \in \mathrm{O}(2n)$, a free-fermionic unitary U_Q is a unitary satisfying

$$U_Q^\dagger \gamma_\mu U_Q = \sum_{\nu=1}^{2n} Q_{\mu,\nu}\gamma_\nu \tag{3}$$

for any $\mu \in [2n]$. This is a mild generalization of the $\mathrm{SO}(2n)$ case, which is associated with physical parity preserving Gaussian unitaries. For the sake of generality, we always present our results in the context of $\mathrm{O}(2n)$. Under free fermionic unitaries U_Q with associated orthogonal matrix $Q \in O(2n)$, correlation matrices transform simply as

$$\Gamma(U_Q \rho U_Q^\dagger) = Q\Gamma(\rho)Q^T. \tag{4}$$

A free fermionic state ρ is a state which can be expressed as

$$\rho = U_Q \bigotimes_{j=1}^{n} \left(\frac{I + \lambda_j Z_j}{2}\right) U_Q^\dagger, \tag{5}$$

for U_Q being the free-fermionic unitary associated with $Q \in \mathrm{O}(2n)$ and $\{\lambda_j\}_{j=1}^n$, dubbed as *normal eigenvalues*, being real numbers with $|\lambda_j| \leq 1$. For more details, refer to Section II. In the remainder of this work, we frequently employ the Schatten p-norms as matrix norms, defined as $\|A\|_p := \mathrm{tr}(|A|^p)^{1/p}$, for $|A| := \sqrt{A^\dagger A}$. From this, the *trace distance* between two quantum states ρ and σ is the distance in the 1-norm and is defined as

$$\|\rho - \sigma\|_1 := \mathrm{tr}\big(\sqrt{\rho - \sigma}\big). \tag{6}$$

The trace distance has a nice operational significance: it is the maximum probability of distinguishing two states via generalized quantum measurements. Related to the trace distance, there is the *fidelity* that quantifies the closeness of two quantum states and is defined as

$$\mathcal{F}(\rho, \sigma) := \operatorname{Tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)^2. \tag{7}$$

Notice that for ρ, σ being pure, it reduces to the square overlap between the state vectors. The trace distance and the fidelity are related by the *Fuchs van de Graaf* inequality [12]

$$1 - \sqrt{\mathcal{F}(\rho, \sigma)} \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{1 - \mathcal{F}(\rho, \sigma)}. \tag{8}$$

Before concluding the section, let us introduce the set of free-fermionic states. In particular, in the rest of this work, two sets of free-fermionic states are considered: $\mathcal{G}_{\mathrm{mixed}}$, comprising all free-fermionic quantum states, and $\mathcal{G}_R$, encompassing free-fermionic states with a rank at most $R = 2^r$, where $r \in [n]$. We denote $\mathcal{G}_{\mathrm{pure}}$ the set $\mathcal{G}_R$ for $R = 1$. As a matter of fact, we have $\mathcal{G}_{\mathrm{pure}} \subset \mathcal{G}_R \subset \mathcal{G}_{\mathrm{mixed}}$ for $1 < r < n$.

B. Overview of the main results

In this section, we present the main results of this work in a relatively informal fashion, omitting their proofs. As mentioned earlier, the primary motivation behind this work is to provide a robust method for testing free-fermionic states. In achieving this goal, we have derived novel and optimal information-theoretic bounds between the trace distance and covariance matrices associated with fermionic states. These bounds are of independent interest and are instrumental for the main algorithms of this work, namely property testing and tomography of Gaussian states. Therefore, we first present the information-theoretic bounds below and briefly comment on their potential usage in other contexts beyond the scope of this work. Later on, we informally discuss the testing algorithm and the tomography algorithm in their simplest version. For a more detailed treatment and formal proofs, the interested reader is then referred to the more technical part of this work in Sections II, III, IV and V for detailed derivations.

A bound for optimal free-fermionic state certification. Imagine one aims to prepare a pure free-fermionic state on a quantum processor. In practice, an imperfect, non-Gaussian, yet close version of the state is actually prepared. The task of quantum state certification [1] is to verify the almost correct preparation of the target state based on the operational distance between the two, i.e., the trace distance. However, since the distance between a theoretical quantum state ψ and a quantum state ρ is generally hard to measure, we aim to understand how the trace distance between two "close" quantum states is controlled by their respective correlation matrices, which can be efficiently measured in practical scenarios. Below, we upper bound the trace distance between a perfect pure free-fermionic state ψ and a non-Gaussian (possibly mixed) imperfect realization ρ through their respective covariance matrices.

Lemma 1 (Closeness of quantum states in terms of correlation matrices). *Let $\psi \in \mathcal{G}_{\text{pure}}$ be a free fermionic pure state and ρ be an arbitrary (possibly non-Gaussian) quantum state. Then*

$$\|\psi - \rho\|_1 \leq \sqrt{\|\Gamma(\psi) - \Gamma(\rho)\|_1}, \tag{9}$$

further discussed and proved in Section III. Therefore, given that the correlation matrix $\Gamma(\psi)$ is known and efficiently classically encoded, Eq. (9) offers an efficient and direct method to verify the accurate preparation of ψ within a marginal error ε, as it is sufficient to measure $\Gamma(\rho)$ up to $O(\epsilon^2)$ precision that require $\text{poly}(n)$ resources.

Optimal perturbation bounds for free-fermionic states. Next, we introduce two perturbation bounds for the fidelity of two close free-fermionic states in relation to the distance between their covariance matrices.

Theorem 1 (Optimal perturbation bounds for free-fermionic states). *Let $|\psi\rangle, |\phi\rangle \in \mathcal{G}_{\text{pure}}$ two pure free-fermionic state vectors, then*

$$1 - |\langle\psi|\phi\rangle|^2 \leq \frac{1}{16}\|\Gamma(\psi) - \Gamma(\phi)\|_2^2, \tag{10}$$

while for $\rho, \sigma \in \mathcal{G}_{\text{mixed}}$ being two mixed free fermionic states, we find

$$1 - \mathcal{F}(\rho,\sigma) \leq \frac{1}{4}\|\Gamma(\rho) - \Gamma(\sigma)\|_1 + \frac{1}{8}\|\Gamma(\rho) - \Gamma(\sigma)\|_2^2. \tag{11}$$

The proof has to be found in Section III. Both inequalities (10) and (11) are optimal, i.e., they are saturated for pure and mixed states respectively. Indeed the pure bound is tight (exact) for all two mode Gaussian states of the the same parity, while the the mixed state bound is tight for general 1 mode Gaussian states.

Besides being fundamental for the efficiency of subsequent testing and tomography algorithms, we anticipate Theorem 1's inequality to have extensive applicability in the context of free fermions, in both theoretical and experimental realms. It operationally quantifies the closeness between two Gaussian states using their correlation matrices, which can be efficiently measured and computed with polynomial efforts.

Distance from the set of free-fermionic states: computable measures of non-Gaussianity. Given a quantum state ρ, the minimal distance from the set of free-fermionic states provides an operational measure of non-Gaussianity for fermionic systems. We recall that the minimal trace distance from a given set of free states constitutes a universally valid measure that respects all the desired properties of resource monotones [13]. However, the problem with such a measure is that it is neither computable, involving a minimization procedure, nor experimentally measurable. Here, we present lower bounds on the trace distance between a quantum state ρ and the set of free-fermionic states, that allow for the efficient estimation of non-Gaussianity in practical and experimental settings.

Lemma 2 (Lower bounds to trace distances). *Let ρ be an arbitrary quantum state and let λ_{r+1} be the $(r+1)$-th smallest normal eigenvalue of its correlation matrix $\Gamma(\rho)$, then*

$$\min_{\sigma \in \mathcal{G}_R} \|\rho - \sigma\|_1 \geq 1 - \lambda_{r+1}, \tag{12}$$

where the extremum is taken over $\mathcal{G}_R$. Conversely, if ρ is a arbitrary quantum state with $\text{rank}(\rho) \leq 2^r$ for $r \in [n]$, then

$$\min_{\sigma \in \mathcal{G}_{\text{mixed}}} \|\rho - \sigma\|_1 \geq \frac{(1-\lambda_{r+1})^{r+1}}{1 + (r+1)(1-\lambda_{r+1})^r}. \tag{13}$$

Note that Eq. (12) requires no assumption on the state ρ, and it lower bounds the distance from the set $\mathcal{G}_R$. Conversely, with the promise that ρ has a rank at most $R := 2^r$ with $r \in [n]$, Eq. (13) establishes a lower bound on the distance from the set of all free-fermionic states $\mathcal{G}_{\text{mixed}}$. The proof for the above results can be found in Section III A.

As discussed in Section II, estimating the normal eigenvalues of the correlation matrix of a quantum state can be done efficiently by employing single-qubit Pauli measurements. Thus, the above inequalities provide an efficient procedure to quantify how far a state is from the set of free-fermionic states in practical scenarios. Additionally, in Section III A, we observe that if we randomly sample a state from certain distributions (e.g., 2-design distributions [14] like states prepared by random quantum circuits of polynomial size or Haar random states), the aforementioned lower bounds are significantly larger than zero with high probability. This implies the detectability of the proposed quantity for most states in such distributions. Also, using such inequalities, we rigorously show that most of pure states are far from being free-fermionic.

Property testing for free-fermionic states. The question that stands behind the main motivation of our work is the following.

Given an unknown quantum state ρ, is it close to or far from the set of free fermionic states?

Specifically, our goal is to identify scenarios in which addressing the aforementioned question is feasible in terms of resources, to provide algorithms with provable efficiency guarantees, and to delineate situations in which answering the question is challenging. First of all, let us formulate the problem in a rigorous fashion.

Problem 1 (Property testing of free-fermionic states)**.** *Let $\varepsilon_B > \varepsilon_A \geq 0$. Given N copies of an unknown quantum state ρ with the promise that it falls into one of two distinct situations:*

- ***Case A:** There exists a free-fermionic state $\sigma \in \mathcal{G}$ such that $\|\rho - \sigma\|_1 \leq \varepsilon_A$.*
- ***Case B:** The state ρ is ε_B-far from all free-fermionic states σ, indicating $\min_{\sigma\in\mathcal{G}} \|\rho - \sigma\|_1 > \varepsilon_B$.*

Determine whether the state is in Case A or Case B through measurements performed on the provided N state copies. Further specifications regarding the rank of the state ρ and the set of free-fermionic states $\mathcal{G} \equiv \mathcal{G}_{\mathrm{pure}}, \mathcal{G}_{\mathrm{mixed}}, \mathcal{G}_R$ must be provided.

While we show that solving Problem 1 in its full generality requires an exponential amount of resources, rendering it unfeasible for practical purposes, we present algorithms capable of efficiently solving it under certain assumptions about the state under examination or by restricting the set of considered Gaussian states.

When no prior assumptions on the state ρ and no restrictions on the set of free-fermionic states $\mathcal{G}$ are provided, we establish the general hardness for Problem 1, demonstrating that $N = \Omega(2^n)$ copies of the state ρ are necessary. Below, we present a more refined version of the mentioned no-go result.

Theorem 2 (Hardness of testing bounded rank free-fermionic states)**.** *Let $\varepsilon_B > 0$ and $r \in [n]$. Let ρ denote the unknown state and $\mathcal{G}$ the set of free fermionic states considered. To solve Problem 1, with at least a $2/3$ probability of success, $N = \Omega(2^r/\varepsilon_B^2)$ copies are necessary if either of the following hypotheses is assumed:*

- *ρ is such that $\mathrm{rank}(\rho) \leq 2^r$ with $r \in [n]$,*
- *$\mathcal{G} \equiv \mathcal{G}_R$ with $R \leq 2^r$.*

In particular, for $r = \Omega(n)$ the sample complexity grows exponentially in the number of modes n.

While the formal proof has to be found Section IV B, the general idea at core of this complexity arises from recognizing that the maximally mixed state is free-fermionic. This fact allows us to leverage the hardness of distinguishing whether the underlying state is the maximally mixed state or far from it in trace distance, which is a notoriously hard problem [15]. The above theorem establishes necessary conditions on the samples N to be spent to solve Problem 1 given assumptions either on ρ or on $\mathcal{G}$. Given these results, Theorem 2 prompts the natural question of whether an algorithm exists that scales exponentially with r (polynomially with the rank), which solve the property testing problem under the assumption that ρ has a rank at most $R = 2^r$ or when restricting to the set $\mathcal{G}_R$. In response to this, we propose two learning algorithms that scale as $O(\mathrm{poly}(n, 2^r))$, and summarize our findings in the following informal theorem.

Theorem 3 (Efficient free-fermionic testing - Informal version of Theorems 16 and 17)**.** *Problem 1 can be solved with $N = \mathrm{poly}(n, 2^r)$ copies of ρ in the following scenarios:*

(i) The given state ρ is such that $\mathrm{rank}(\rho) \leq 2^r$.

(ii) The set of Gaussian states is restricted to $\mathcal{G}_R$ with $R \leq 2^r$.

We provide algorithms for case (i) and (ii) that use N samples and $\mathrm{poly}(n, 2^r)$ computational resources.

The core idea behind the efficiency of low-rank free-fermionic states lies in the fact that any free-fermionic state, up to a free-fermionic unitary, is equivalent to a product state. Thus, the algorithm first identifies this free-fermionic unitary to factorize the state. This reduction allows the problem to be simplified to testing whether the underlying state is a (free-fermionic) product state or not. This can be solved with a complexity that scales polynomially with the rank of the state 2^r. For instance, this can be achieved by employing full state tomography on only $r + 1$ qubits. Additional details, including assumptions on ε_A and ε_B, the algorithms presented in a pseudocode fashion, as well as the sample and computational analyses have to be found in Section IV.

Let us summarize our findings. In its full generality, that is, without rank assumptions on the state ρ and considering $\mathcal{G} \equiv \mathcal{G}_{\mathrm{mixed}}$, Problem 1 requires $N = \Omega(2^n)$ samples of the state to be solved. However, as claimed in Theorem 3, we have established that Problem 1 can be efficiently addressed both sample-wise and computationally under two specific scenarios: (i) when the given state ρ has a rank that scales polynomially with the number of modes n, or (ii) when the focus is solely on quantifying closeness to the set of Gaussian states with polynomially bounded rank.

Although these two approaches share similarities in principle, they differ significantly both conceptually and operationally. Ultimately, the choice between them rests entirely with the user. Specifically, if they possesses guarantees that the prepared state predominantly occupies a relatively small subspace of the Hilbert space, then we provided provable guarantees in probing the distance concerning all Gaussian states $\mathcal{G}_{\mathrm{mixed}}$. Conversely, if an experimentalist lacks a clear understanding of the nature of the state due to imprecisions or noise, they only have reliable assurances in determining whether the state is close to or far from the set of Gaussian states with polynomially bounded rank. Although seemingly less satisfactory, the latter approach is more general and applicable in completely agnostic situations.

Efficient tomography of free-fermionic states. We conclude this work by presenting a simple algorithm for efficiently learning a unknown n-qubit free-fermionic state either pure or mixed. More rigorously, we are concerned with the following problem: let $\rho \in \mathcal{G}$, with $\mathcal{G} = \mathcal{G}_{\mathrm{mixed}}, \mathcal{G}_{\mathrm{pure}}$, be a unknown free-fermionic state, design a computationally efficient quantum learning algorithm that consumes N copies of ρ and output a classical description $\hat{\rho}$ that is ε-close in trace distance to ρ with failure probability of at most δ. Some earlier works [11, 16, 17] have already tackled this problem, but their analysis has been limited to the specific case of ρ being a pure free fermionic state. We first provide an algorithm limited to the case of pure states that significantly improves upon previous work. What's more, our approach extends to the more realistic mixed state scenario, significantly broadening the scope of such result. This extension, as well as the improved algorithm for pure state case, heavily rely on the toolkit developed and discussed in the first part of this work, in particular Theorem 1.

Proposition 1 (Tomography of pure free-fermionic states). *Let ψ be a pure free-fermionic quantum state. For $\varepsilon \in (0,1)$ and $\delta \in (0,1]$ there exist a learning algorithm that utilize $N = 32(n^3/\varepsilon^2)\log\big(4n^2/\delta\big)$ copies of the state and only single-copies measurements to learn an efficient classical representation of the state $\hat{\psi}$ obeying $\|\psi - \hat{\psi}\|_1 \leq \varepsilon$.*

Therefore the overall scaling can be enhanced from $O(n^3m^2/\varepsilon^4)$ (where m represents the fixed number of particles) to $O(n^3/\varepsilon^2)$ significantly improving over the results of Ref. [11]. A more detailed analysis is conducted in Section V. The following theorem is a direct consequence of Theorem 1.

Theorem 4 (Tomography of mixed free-fermionic states). *Let $\varepsilon \in (0,1)$ and $\delta \in (0,1]$ and $\rho \in \mathcal{G}_{\mathrm{mixed}}$. There exists a computationally efficient quantum algorithm that, employing $N = O\left((n^5/\varepsilon^4)\log\big(n^2/\delta\big)\right)$ copies of the state ρ and single-copies Gaussian measurements, learns a classical representation $\hat{\rho}$ of the state ρ obeying $\|\hat{\rho} - \rho\|_1 \leq \varepsilon$, with a success probability of at least $1 - \delta$.*

In fact, we can even strengthen this result under specific assumptions on the input state ρ. Under the assumption that the underlying state is an n-modes fermionic state with a *fixed number of particles* m, the sample complexity of the protocol can be similarly demonstrated to be $O(n^3m^2)$.

C. Related work

The main motivation behind this work is to provide practical and efficient quantum algorithms for free-fermionic state testing. However, we also consider the task of quantum state tomography for free-fermionic states. In this section, we discuss previous work and position our algorithms in the current literature. Addressing the testing of specific properties in quantum states spans various contexts. A property tester for a quantum state class C involves taking copies of a state ρ as input and determining either A) whether ρ belongs to C or B) if ρ is ϵ-far in trace distance from all states in C, provided that one of these scenarios is true. The property testing problem is particularly intriguing due to its potential experimental applicability. Indeed, under relatively weak assumptions, it provides a direct means to experimentally verify if a given property holds.

In Ref. [15], the identity testing problem was explored with the goal of distinguishing whether the underlying state belongs to the class C of states close to maximally mixed states or is far from it. The problem, in its full generality, was shown to require a sample complexity scaling exponentially with the number of qubits, i.e., $\Omega(2^n)$. Simultaneously, an algorithm performing identity testing using $O(2^n)$ samples was demonstrated, thus showing optimality. Building on this hardness, product state testing has been examined in Ref. [18], focusing on the class C being the one of product states. Given the significance of testing genuine multipartite entanglement in quantum states, it is crucial to determine whether the underlying state is a product state or not. In Ref. [18], the authors have established a lower bound on the sample complexity of $\Omega(2^n)$, as well as an algorithm achieving the task using $O(2^n)$ copies by using entangled measurements over many specimens or "copies" and $O(4^n)$ unentangled (single-copy) measurements.

In a similar spirit to our work, there exists another relevant class of non-trivial classically simulatable states known as stabilizer states [19]. Stabilizer states are eigenstates of n independent and mutually commuting Pauli operators. In Ref. [20], considering the class C as the set of pure stabilizer states, a property testing algorithm was demonstrated that requires only $O(1)$ samples of the state. This remarkable efficiency is ultimately attributed to the use of entangling (Bell) measurements and techniques known as *Bell difference sampling*. In a slightly more general and practically applicable problem considered in Ref. [21], where the class C consists of states ε-close in trace distance to pure stabilizer states, it was shown that $O(1)$ copies of the state are sufficient for the testing algorithm to succeed. Similar settings in the free-bosonic realm have also been considered [22].

Quantum state tomography is the other learning problem addressed in this work. Given N copies of an unknown quantum state ρ, the aim of quantum state tomography is, through arbitrary measurements, to produce a classical description $\hat{\rho}$ of the state that is ε-close in trace distance to ρ with a failure probability of at most δ. In Ref. [23], a sample-optimal quantum state tomography algorithm has been introduced. Specifically, it has been shown that $\Omega(4^n)$ copies of the state are necessary for any quantum tomography algorithm to succeed. They have presented a sample-optimal algorithm scaling as $O(n4^n)$, thereby matching the lower bound up to a linear scaling factor in the number of qubits (modes) n.

Given the intrinsic inefficiency of quantum state tomography algorithm for general states, a natural question is whether if one restricts the class of input quantum states, whether quantum state tomography can be conducted both sample and computationally efficiently. In this regard, a number of insightful work has been produced that demonstrates sample and computational efficiency for specific class of states, which include: Pure stabilizer states [24], t-doped stabilizer states [25? , 26] (states obtained by at most t non-Clifford gates), matrix product states [27–31], quantum phase states [?] and more. Relevant for the current work is the recent efficient learning algorithm for n free-fermionic states with fixed particle number m presented in Ref. [11], which we significantly improve in scope and efficiency. The algorithm presented in Ref. [11] focuses only on learning *pure* free-fermionic states with fixed particle number m, with a scaling $O(n^3m^2\varepsilon^{-4})$. In this work, we not only improve the scaling from $O(n^3m^2\varepsilon^{-4})$ to $O(n^3\varepsilon^{-2})$, but we broaden the scope of the tomography algorithm to more practical scenarios and consider the case of mixed free-fermionic states. Notably, the analogous problem of learning mixed Gaussian states was previously unresolved also in the bosonic context. However, in a parallel work [32], together with other coauthors, we fill this gap in the bosonic literature.

D. Discussion and open questions

In this work, we have demonstrated an efficient method for discerning whether a quantum state is free-fermionic or not, utilizing experimentally feasible measurements. Additionally, we have introduced lower bounds, that can be efficiently estimated, on the distance of a state from the set of free-fermionic states. These bounds offer valuable insights into quantifying the extent of non-free fermionic features present in a quantum system. Furthermore, we have formally extended a series of algorithms algorithms previously proposed for learning free-fermionic pure states to the more complex mixed-state scenario. We posit that the findings presented in this work can serve as a valuable resource for designing and conducting quantum simulation experiments.

Furthermore, while our analysis comprehensively addresses the literature on testing and tomography of free-fermionic states, providing scenarios with provable efficiency guarantees and ruling out situations in which the aforementioned tasks are hard to perform, there remain several open questions related to the topics discussed in this paper.

- As discussed above, one particularly relevant class of classically simulatable states is the class of stabilizer states. While testing whether a given pure state is close or far in trace distance to the set of *pure* stabilizer states has been addressed, provable efficiency guarantees, as well as sample complexity lower bounds, are still missing for the more general and practical case of mixed states. Exploring this avenue would be interesting, especially in light of the algorithms discussed and developed in the manuscript.

- Within the class of classically simulatable states, there are subclasses representing "small" deviations from the sets of free-fermionic states or stabilizer states. Typically, such "small" deviations can be characterized by various notions related to the non-Gaussianity or non-stabilizerness of the given states, such as Gaussian rank (resp. stabilizer rank), doping the states with non-Gaussian (resp. non-Clifford) operations, or Gaussian extent (resp. stabilizer extent). Exploring these more general scenarios is therefore essential for both testing problems and quantum state tomography problems.

- The technical aspect of our work heavily relies on novel matrix inequalities proven here. In particular, Theorem 1 presents two optimal bounds relating the fidelity and the norm distance between the correlation matrices of pure and mixed Gaussian states, respectively. However, as also noted below Theorem 1, the two bounds cannot be merged. However, if we transfer the perturbation bound through the Fuchs-van de Graaf inequality to the trace distance, from Eq.(11) we obtain different results for the pure and mixed cases, respectively,

  $$\|\psi-\phi\|_1 \leq 4^{-1}\|\Gamma(\psi)-\Gamma(\phi)\|_2, \quad \text{pure states,}$$
  $$\|\rho-\sigma\|_1 \lesssim 2^{-1}\sqrt{\|\Gamma(\rho)-\Gamma(\sigma)\|_1}, \quad \text{mixed states.}$$

  Moreover, for the restrictive case in which $[\rho,\sigma]=0$, in Theorem 15, we can tighten Eq. (11) to

  $$\|\rho-\sigma\|_1 \leq 2^{-1}\|\Gamma(\rho)-\Gamma(\sigma)\|_1. \tag{14}$$

  Therefore, we conclude that it should be plausible that, for the trace-distance bound, there should be a universal bound for the pure and mixed cases that goes as

  $$|\rho-\sigma| \lesssim \alpha\|\Gamma(\rho)-\Gamma(\sigma)\|_1, \quad \text{(universal bound?)}$$

  with $\alpha=\Theta(1)$. Finding such a bound would guarantee optimal perturbation bounds for the trace norm difference as well and will be a matter of exciting future investigation.

Acknowledgments We thank Frederik Von Ende, Francesco Anna Mele, Ludovico Lami, Alexander Nietner for useful discussions. This work has been supported by the BMBF (FermiQP, MuniQCAtoms), the ERC (DebuQC) and the DFG (CRC 183).

[1] M. Kliesch and I. Roth, Theory of quantum system certification, PRX Quantum **2**, 010201 (2021).

[2] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham,

R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, Nature Rev. Phys. **2**, 382–390 (2020).

[3] J. Surace and L. Tagliacozzo, Fermionic Gaussian states: an introduction to numerical approaches, SciPost Physics Lecture Notes , 54 (2022).

[4] L. Onsager, Crystal statistics. i. a two-dimensional model with an order-disorder transition, Phys. Rev. **65**, 117 (1944).

[5] R. Jördens, N. Strohmaier, K. Günter, H. Moritz, and T. Esslinger, A Mott insulator of fermionic atoms in an optical lattice, Nature **455**, 204 (2008).

[6] J. Vijayan, P. Sompet, G. Salomon, J. Koepsell, S. Hirthe, A. Bohrdt, F. Grusdt, I. Bloch, and C. Gross, Time-resolved observation of spin-charge deconfinement in fermionic Hubbard chains, Science **367**, 186 (2020).

[7] P. Echenique and J. L. Alonso, A mathematical and computational review of Hartree–Fock SCF methods in quantum chemistry, Mol. Phys. **105**, 3057 (2007).

[8] E. Knill, Fermionic linear optics and matchgates (2001), arXiv:quant-ph/0108033, arXiv:quant-ph/0108033 [quant-ph].

[9] B. M. Terhal and D. P. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits, Phys. Rev. A **65**, 032325 (2002).

[10] R. Jozsa and A. Miyake, Matchgates and classical simulation of quantum circuits, Proc. Roy. Soc. A **464**, 3089–3106 (2008).

[11] S. Aaronson and S. Grewal, Efficient tomography of non-interacting fermion states (2023), arXiv:2102.10458 [quant-ph].

[12] C. A. Fuchs and J. van de Graaf, Cryptographic distinguishability measures for quantum-mechanical states, IEEE Trans. Inf. Th. **45**, 1216 (1999).

[13] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[14] D. Gross, K. M. R. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, J. Math. Phys. **48**, 052104 (2007).

[15] R. O'Donnell and J. Wright, Quantum spectrum testing (2015), arXiv:1501.05028 [quant-ph].

[16] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, Fidelity witnesses for fermionic quantum simulations, Phys. Rev. Lett. **120**, 190501 (2018).

[17] B. O'Gorman, Fermionic tomography and learning (2022), arXiv:2207.14787, arXiv:2207.14787.

[18] N. Yu, Sample efficient identity testing and independence testing of quantum states, in *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 185, edited by J. R. Lee (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021) pp. 11:1–11:20.

[19] D. Gottesman, The Heisenberg representation of quantum computers (1998), arXiv:quant-ph/9807006 [quant-ph].

[20] D. Gross, S. Nezami, and M. Walter, Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations, Commun. Math. Phys. **385**, 1325 (2021).

[21] S. Grewal, V. Iyer, W. Kretschmer, and D. Liang, Improved stabilizer estimation via Bell difference sampling (2023), arXiv:2304.13915, arXiv:2304.13915 [quant-ph].

[22] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Reliable quantum certification for photonic quantum technologies, Nature Comm. **6**, 8498 (2015).

[23] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, Sample-optimal tomography of quantum states, IEEE Trans. Inf. Th. , 1–1 (2017).

[24] A. Montanaro, Learning stabilizer states by Bell sampling (2017), arXiv:1707.04012 [quant-ph].

[25] L. Leone, S. F. E. Oliviero, and A. Hamma, Learning t-doped stabilizer states (2024), arXiv:2305.15398 [quant-ph].

[26] D. Hangleiter and M. J. Gullans, Bell sampling from quantum circuits (2023), arXiv:2306.00083, arXiv:2306.00083 [quant-ph].

[27] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Efficient quantum state tomography, Nature Comm. **1**, 149 (2010).

[28] R. Hübener, A. Mari, and J. Eisert, Wick's theorem for matrix product states, Phys. Rev. Lett. **110**, 040401 (2013).

[29] B. P. Lanyon, C. Maier, T. B. Milan Holzäpfel, C. Hempel, P. Jurcevic, I. Dhand, A. S. Buyskikh, A. J. Daley, M. Cramer, M. B. Plenio, R. Blatt, and C. F. Roos, Efficient tomography of a quantum many-body system, Nature Physics **13**, 1158 (2017).

[30] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, Direct certification of a class of quantum simulations, Quantum Sci. Technol. **2**, 015004 (2017).

[31] T. Baumgratz, D. Gross, M. Cramer, and M. B. Plenio, Scalable reconstruction of density matrices, Phys. Rev. Lett. **111**, 020401 (2013).

[32] F. A. Mele, A. A. Mele, L. Bittel, J. Eisert, V. Giovannetti, L. Lami, L. Leone, and S. F. E. Oliviero, Learning quantum states of continuous variable systems (2024), arXiv:2405.01431 [quant-ph].

[33] Z. Jiang, K. J. Sung, K. Kechedzhi, V. N. Smelyanskiy, and S. Boixo, Quantum algorithms to simulate many-body physics of correlated fermions, Phys. Rev. Applied **9**, 044036 (2018).

[34] B. Dias and R. Koenig, Classical simulation of non-Gaussian fermionic circuits (2023), arXiv:2307.12912.

[35] A. Chapman and A. Miyake, Classical simulation of quantum circuits by dynamical localization: Analytic results for pauli-observable scrambling in time-dependent disorder, Phys. Rev. A **98**, 012309 (2018).

[36] S. Bravyi and D. Gosset, Complexity of quantum impurity problems, Commun. Math. Phys. **356**, 451–500 (2017).

[37] T.-Y. Tam and M. C. Thompson, Determinant and Pfaffian of sum of skew symmetric matrices, Lin. Alg. Appl. **433**, 412 (2010).

[38] B. Windt, A. Jahn, J. Eisert, and L. Hackl, Local optimization on pure Gaussian state manifolds, SciPost Physics **10**, 066 (2021).

[39] J. Gao, Quantum union bounds for sequential projective measurements, Phys. Rev. A **92**, 052331 (2015).

[40] R. Bhatia, *Matrix analysis*, Graduate Texts in Mathematics (Springer New York, 1996).

[41] K. M. R. Audenaert, A generalisation of Mirsky's singular value inequalities (2014), arXiv:1410.4941 [math.FA].

[42] X. Bonet-Monroig, R. Babbush, and T. E. O'Brien, Nearly optimal measurement scheduling for partial tomography of quantum states, Phys. Rev. X **10**, 031064 (2020).

[43] D. S. França, F. G. L. Brandão, and R. Kueng, Fast and robust quantum state tomography from few basis measurements, in *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 197, edited by M.-H. Hsieh (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021) pp. 7:1–7:13.

Supplemental material

Contents

II. Preliminaries

A. Notation and basic definitions

We use the following notation throughout our work. We denote with $\mathbb{C}^{d\times d}$ the set of $d \times d$ complex matrices, with $d \in \mathbb{N}$. The notation $[d]$ denotes the set of integers from 1 to d, i.e., $[d] := \{1, \dots, d\}$. We denote as I the identity operator, with a subscript specifying the dimension when necessary for clarity. The *Schatten p-norm* of a matrix $A \in \mathbb{C}^{d\times d}$, with $p \in [1, \infty]$, is given by

$$\|A\|_p := \mathrm{Tr}((\sqrt{A^\dagger A})^p)^{1/p}, \tag{S15}$$

which corresponds to the p-norm of the vector of singular values of A. The *operator norm* of a matrix $A \in \mathbb{C}^d$ is equal to its largest singular value. We denote the *Hilbert-Schmidt scalar product* as $\langle A, B\rangle_{HS} := \mathrm{Tr}\left(A^\dagger B\right)$. We denote as $\mathrm{O}(2n)$ the group of real orthogonal $2n \times 2n$ matrices. We denote the n-qubits Pauli operators as the elements of the set $\{I, X, Y, Z\}^{\otimes n}$, where I, X, Y, Z represent the standard single qubits Pauli. Pauli operators are traceless, Hermitian, square to the identity and form an orthogonal basis with respect the Hilbert-Schmidt scalar product for the space of linear operators. We define the set of quantum states as $\mathcal{S}\left(\mathbb{C}^d\right) := \{\rho \in \mathbb{C}^{d\times d} \,:\, \rho \geq 0,\ \mathrm{Tr}(\rho) = 1\}$. A state ρ is pure if and only if $\rho^2 = \rho$.

B. Free-fermionic states

In this subsection we provide definitions and Lemmas on free-fermionic states, which are useful for deriving our results. While we define these concepts in terms of qubits, it is worth noting that they can also be directly expressed in terms of fermions via the Jordan-Wigner mapping. In the following we consider an n-qubits system (or equivalently, n fermionic modes). Throughout this discussion, we focus on an n-qubit system. To begin, we introduce the definition of Majorana operators in relation to Pauli matrices.

Definition 1 (Majorana operators). *For each $k \in [n]$, Majorana operators can be defined as*

$$\gamma_{2k-1} := \left(\prod_{j=1}^{k-1} Z_j\right) X_k, \quad \gamma_{2k} := \left(\prod_{j=1}^{k-1} Z_k\right) Y_k. \tag{S16}$$

As can be readily verified, Majorana operators are Hermitian, traceless, and they square to the identity

$$\gamma_\mu = \gamma_\mu^\dagger, \quad \mathrm{Tr}(\gamma_\mu) = 0, \quad \gamma_\mu^2 = I \tag{S17}$$

for all $\mu \in [2n]$. Moreover, they anti-commute and are orthogonal with respect to the Hilbert-Schmidt inner product

$$\{\gamma_\mu, \gamma_\nu\} = 2\delta_{\mu,\nu} I, \quad \langle \gamma_\mu, \gamma_\nu \rangle_{HS} = 0 \tag{S18}$$

for all $\mu, \nu \in [2n]$. As such, operators defined by Jordan-Wigner transformation conforms with the Majorana anti-commutation relations. A useful and easy to verify identity is $iZ_j = \gamma_{2j-1}\gamma_{2j}$.

Definition 2 (Majorana products). *Let S be the set $S := \{\mu_1, \ldots, \mu_{|S|}\} \subseteq [2n]$ with $1 \leq \mu_1 < \cdots < \mu_{|S|} \leq 2n$. We define*

$$\gamma_S := \gamma_{\mu_1} \cdots \gamma_{\mu_{|S|}}$$

if $S \neq \emptyset$ and $\gamma_\emptyset = I$ otherwise.

It is worth noting that the number of different sets $S \in [2n]$ and hence Majorana products is 4^n. For any set $S, S' \subseteq [2n]$, Majorana products are orthogonal

$$\langle \gamma_S, \gamma_{S'} \rangle_{HS} = 2^n \delta_{S,S'}.$$

Hence, they form a basis for $\mathbb{C}^{d \times d}$.

Definition 3 (Free-fermionic unitary). *For any orthogonal matrix $Q \in \mathrm{O}(2n)$, a free-fermionic unitary U_Q (also known as Gaussian unitary) is a unitary which satisfies*

$$U_Q^\dagger \gamma_\mu U_Q = \sum_{\nu=1}^{2n} Q_{\mu,\nu} \gamma_\nu \tag{S19}$$

for any $\mu \in [2n]$.

From this definition, it follows that $U_Q^\dagger = U_{Q^T}$. Since product of Majorana operators γ_μ with $\mu \in [2n]$ form a basis for the linear operators $\mathbb{C}^{d \times d}$, it suffices to specify how a unitary acts on the $2n$ Majorana operators γ_μ with $\mu \in [2n]$ to uniquely specify the unitary up to a phase. Specifically, for a given orthogonal matrix, there exists a known exact implementation of the associated free-fermionic unitary, which can be achieved using either $O(n^2)$ local 2-qubit gates [33] or $O(n^2)$ local 2-modes free-fermionic unitary Majorana evolutions [34]. From the previous definition, it follows the following.

Lemma 3 (Adjoint action of Gaussian unitary on a Majorana product). *For any $S \subseteq [2n]$ and U_Q free-fermionic unitary with $Q \in \mathrm{O}(2n)$, we have*

$$U_Q^\dagger \gamma_S U_Q = \sum_{S' \subseteq \binom{[2n]}{|S|}} \det(Q|_{S,S'}) \gamma_{S'} \tag{S20}$$

where $\binom{[2n]}{|S|}$ is defined as the set of subsets of $[2n]$ of cardinality $|S|$, while $Q|_{S,S'}$ is the restriction of the matrix Q to rows and columns indexed by S and S' respectively.

Proof. See Ref. [35] for a proof. □

We now give the definition of free-fermionic states (also known as fermionic Gaussian states).

Definition 4 (Free-fermionic states). *A free-fermionic state (also known as Gaussian state) in the Jordan-Wigner mapping can be defined as*

$$\rho = U_Q \rho_0 U_Q^\dagger, \quad \textit{with} \quad \rho_0 := \bigotimes_{j=1}^{n} \left(\frac{I + \lambda_j Z_j}{2}\right) \tag{S21}$$

where $\lambda_j \in [0,1]$ for each $j \in [n]$ and U_Q is the free-fermionic unitary associated to the orthogonal matrix $Q \in \mathrm{O}(2n)$.

This definition is slightly more general than defining a free-fermionic state like a state of the form $\exp(-\beta H)/\operatorname{Tr}(\exp(-\beta H)))$, where $\beta \in \mathbb{R}$ and H is a quadratic Hamiltonian in the Majorana operators. From the previous definition, it follows that ρ is pure if and only if $\lambda_j \in \{-1, 1\}$ for each $j \in [n]$. In such pure case, the state will be $U_Q |x\rangle$, where $|x\rangle := \bigotimes_{i=1}^{n} |x_i\rangle$ is a computational basis state with $x_i := (1 - \lambda_i)/2$. Since X_1 and $\{X_j X_{j+1}\}_{j=1}^{n} = \{-i\gamma_{2j}\gamma_{2j+1}\}_{j=1}^{n}$ are fermionic Gaussian unitaries, and the product of Gaussian unitaries is Gaussian, it follows that $\{X_j\}_{j=1}^{n}$ are Gaussian unitaries. Thus, without loss of generality, any pure fermionic Gaussian state can be written as $U_Q |0^n\rangle$, which is uniquely specified by an orthogonal matrix $Q \in \mathrm{O}(2n)$.

We can define now the correlation matrix of any (possibly non-free-fermionic) state.

Definition 5 (Correlation matrix)**.** *Given a (general) state ρ, we define its correlation matrix $\Gamma(\rho)$ as:*

$$[\Gamma(\rho)]_{j,k} := -\frac{i}{2} \operatorname{Tr}\left([\gamma_j, \gamma_k]\, \rho\right), \tag{S22}$$

where $j, k \in [2n]$.

The correlation matrix of any state is real and anti-symmetric, thus it has eigenvalues in pairs of the form $\pm i\lambda_j$ for $j \in [2n]$, where λ_j are real numbers such that $|\lambda_j| \leq 1$. Under free-fermionic unitaries, the correlation matrix of any quantum state changes by the adjoint action with the associated orthogonal matrix, as expressed in the following proposition.

Lemma 4 (Transformation of the correlation matrix under free-fermionic unitary)**.** *For any state ρ, we have*

$$\Gamma(U_Q \rho U_Q^\dagger) = Q\Gamma(\rho)Q^T, \tag{S23}$$

for any free-fermionic unitary U_Q associated to an orthogonal matrix $Q \in \mathrm{O}(2n)$.

This is easily verified by the definition of correlation matrix and free-fermionic unitary. We denote as Λ the correlation matrix of the $|0^n\rangle$ state vector, namely

$$\Lambda := \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \bigoplus_{j=1}^{n} (iY). \tag{S24}$$

The correlation matrix of a computational basis state $|x\rangle$ with $x \in \{0,1\}^n$ is $\Gamma(|x\rangle) = \bigoplus_{j=1}^{n} (-1)^{x_i} (iY)$. It turns out that any real anti-symmetric matrix can be diagonalized with an orthogonal matrix, in particular we have the following result.

Lemma 5 (Normal decomposition of real anti-symmetric matrices [3])**.** *Any real anti-symmetric matrix Γ can be decomposed in the so-called* normal *form*

$$\Gamma = Q \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} Q^T, \tag{S25}$$

for an orthogonal matrix $Q \in \mathrm{O}(2n)$ and $\{\lambda_j\}_{j=1}^{n} \in \mathbb{R}$ real numbers ordered in increasing order. Thus, the eigenvalues of Γ are $\pm i\lambda_j$ for any $j \in [n]$. We denote $\{\lambda_j\}_{j=1}^{n}$ as normal eigenvalues.

The decomposition in Lemma 5 can be always performed in such a way that the orthogonal matrix $Q \in \mathrm{SO}(2n)$ (i.e., its determinant is one). In fact, if that is not the case, then we can write $Q = Q'\operatorname{diag}(-1, 1, \ldots, 1)$, for a matrix $Q' \in \mathrm{SO}(2n)$ (note that this matrix Q' exists because the product of two orthogonal matrix is an orthogonal matrix and because of the Cauchy–Binet formula of the determinant).

Using Lemma 5, we can show that the correlation matrix of any state ρ has normal eigenvalues less than one (and thus also the absolute values of its eigenvalues). In fact, let $\Gamma(\rho) = Q(\bigoplus_{j=1}^{n} i\lambda_j Y)Q^T$ be the correlation matrix expressed in its normal form. Then, we have

$$\lambda_j = (Q^T \Gamma(\rho) Q)_{2j-1,2j} = (\Gamma(U_Q^\dagger \rho U_Q))_{2j-1,2j} = \operatorname{Tr}\Big(U_Q^\dagger \rho U_Q Z_j\Big). \tag{S26}$$

Thus, because of Holder inequality we have $|\lambda_j| \leq \|U_Q^\dagger \rho U_Q\|_1 \|Z_j\|_\infty = 1$

Furthermore, by using Lemma 5, we establish a bijection between the set of free-fermionic states and the set of real-anti-symmetric matrices with eigenvalues smaller than one in absolute value.

Lemma 6 (Bijection between free-fermionic states and correlation matrices). *Given a free-fermionic state of the form*

$$\rho = U_Q \rho_0 U_Q^\dagger, \qquad \textit{with} \quad \rho_0 := \bigotimes_{j=1}^{n} \left(\frac{I + \lambda_j Z_j}{2} \right) \tag{S27}$$

where $\lambda_j \in [-1,1]$ for each $j \in [n]$ and U_Q is the free-fermionic unitary associated to the orthogonal matrix $Q \in \mathrm{O}(2n)$, then its correlation matrix is

$$\Gamma = Q \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} Q^T, \tag{S28}$$

which is a real and anti-symmetric matrix, with eigenvalues $\pm i\lambda_j$ in pairs such that $\lambda_j \in [-1,1]$ for any $j \in [n]$. Conversely, given a real, anti-symmetric matrix Γ, it can be decomposed as in Eq. (S28), in particular, its eigenvalues are of the form $\pm i\lambda_j$ in pairs. If $\lambda_j \in [-1,1]$, then Γ uniquely defines a state ρ of the form of Eq. (S27).

The previous theorem ensures that by specifying a valid correlation matrix (i.e., real, anti-symmetric, with eigenvalues smaller than one), we uniquely specify a free-fermionic state. Vice versa, having a free-fermionic state, it uniquely defines a correlation matrix. In particular, any pure free-fermionic state $|\psi\rangle = U_Q |0^n\rangle$ is specified by an orthogonal matrix $Q \in \mathrm{O}(2n)$, and its correlation matrix will be $\Gamma(\psi) = Q\Lambda Q^T$, where Λ is defined in Eq. (S24). From this, it follows:

Remark 1. *The correlation matrix $\Gamma(\psi)$ of a pure free-fermionic state ψ satisfies $\det(\Gamma(\psi)) = 1$, is an orthogonal matrix and its normal eigenvalues are all equal to one in absolute value.*

Moreover, we also have that the rank of a mixed free-fermionic state is related to the number of normal eigenvalues strictly smaller than one in absolute value, as it follows by Lemma 6.

Remark 2 (Relation between rank and normal eigenvalues of a free-fermionic state). *Let ρ be a free-fermionic state, expressed as $\rho = U_Q \left(\bigotimes_{j=1}^{n} (I + \lambda_j Z_j)/2 \right) U_Q^\dagger$, where $\{\lambda_j\}_{j=1}^{n} \subseteq [-1,1]$ and U_Q is a free-fermionic unitary. Let m be the number of elements in $\{\lambda_1, \ldots, \lambda_n\}$ that are in absolute value smaller than one. We then have $\mathrm{rank}(\rho) = 2^m$.*

In our analysis the notion of *Pfaffian* will be useful.

Definition 6 (Pfaffian of a matrix). *Let C be a $2n \times 2n$ anti-symmetric matrix. Its Pfaffian is defined as*

$$\mathrm{Pf}(C) = \frac{1}{2^n n!} \sum_{\sigma \in S_{2n}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} C_{\sigma(2i-1),\sigma(2i)}, \tag{S29}$$

where S_{2n} is the symmetric group of order $(2n)!$ and $\mathrm{sgn}(\sigma)$ is the signature of σ. The Pfaffian of an $m \times m$ antisymmetric matrix with m odd is defined to be zero.

Well-known properties are the following. For any matrix B, we have $\mathrm{Pf}(BCB^T) = \det(B)\,\mathrm{Pf}(C)$ and $\mathrm{Pf}(\lambda C) = \lambda^n\,\mathrm{Pf}(C)$, where C is a $2n \times 2n$ anti-symmetric matrix and $\lambda \in \mathbb{C}$. Moreover, it holds that $\mathrm{Pf}(C)^2 = \det(C)$ (note that this is consistent with the fact that the Pfaffian of an odd anti-symmetric matrix is defined to be zero, since the determinant of an odd anti-symmetric matrix is zero). Another useful identity is

$$\mathrm{Pf}\left(\bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} \right) = \prod_{j=1}^{n} \lambda_j. \tag{S30}$$

Now we recall the well-known Wick's theorem, which states that the any Majorana product expectation value over a free-fermionic state can be computed efficiently given access to its correlation matrix.

Lemma 7 (Wick's Theorem [3, 36]). *Let ρ be a free-fermionic state with the associated correlation matrix $\Gamma(\rho)$. Then, we have*

$$\mathrm{Tr}(\gamma_S \rho) = i^{|S|/2}\,\mathrm{Pf}(\Gamma(\rho)|_S), \tag{S31}$$

where $\gamma_S = \gamma_{\mu_1} \cdots \gamma_{\mu_{|S|}}$, and $S = \{\mu_1, \ldots, \mu_{|S|}\} \subseteq [2n]$ with $1 \le \mu_1 < \cdots < \mu_{|S|} \le 2n$, while $\Gamma(\rho)|_S$ is the restriction of the matrix $\Gamma(\rho)$ to the rows and columns corresponding to elements in S.

Note that, since, for any $S \subseteq [2n]$ the restriction of the correlation matrix $\Gamma|_S$ is still anti-symmetric, its Pfaffian is well-defined. The Pfaffian of $\Gamma|_S$ can be computed efficiently in time $\Theta(|S|^3)$.

Definition 7 (Parity). *The parity operator is defined as the operator:*

$$Z^{\otimes n} = (-1)^n \gamma_1 \gamma_2 \cdots \gamma_{2n-1}\gamma_{2n}. \tag{S32}$$

The parity of a quantum state ρ is defined as the expectation values of the parity operator, i.e.,

$$\mathrm{Parity}(\rho) := \mathrm{Tr}\big(Z^{\otimes n}\rho\big).$$

Lemma 8 (Gaussian states are eigenstates of the parity operator). *Any Gaussian pure state $|\psi_Q\rangle := U_Q|0^n\rangle$ associated with the orthogonal matrix $Q \in \mathrm{O}(2n)$ satisfies:*

$$Z^{\otimes n}|\psi_Q\rangle = \det(Q)\,|\psi_Q\rangle\,. \tag{S33}$$

Thus, we also have $\mathrm{Parity}(\psi_Q) = \det(Q)$.

Proof. We have

$$Z^{\otimes n}|\psi_Q\rangle = (-i)^n\gamma_{[2n]}|\psi_Q\rangle = (-i)^n U_Q U_Q^\dagger \gamma_{[2n]} U_Q|0^n\rangle = (-i)^n \det(Q) U_Q \gamma_{[2n]}|0^n\rangle \tag{S34}$$

$$= \det(Q) U_Q Z^{\otimes n}|0^n\rangle = \det(Q)\,|\psi_Q\rangle\,, \tag{S35}$$

where the first step follows from Jordan-Wigner, and we defined $\gamma_{[2n]} := \prod_{j=1}^{n}\gamma_j$. The third step follows from Eq. S20. □

From this lemma, it follows that if two pure fermionic Gaussian states have different parity, then they have also zero overlap (however, the viceversa is not true: two pure Gaussian states with the same parity can have zero overlap, e.g., $|00\rangle$ and $|11\rangle$). This result can also be derived using Wick's Theorem (Lemma 7). In fact, for a possibly mixed free-fermionic state ρ, we have

$$\mathrm{Parity}(\rho) = \mathrm{Tr}\big(Z^{\otimes n}\rho\big) = \mathrm{Pf}(\Gamma(\rho)). \tag{S36}$$

Furthermore, according to the properties of the Pfaffian, we obtain:

$$\mathrm{Pf}(\Gamma(\rho)) = \Big(\prod_{j=1}^{n}\lambda_j\Big)\det(Q), \tag{S37}$$

where $Q \in \mathrm{O}(2n)$ and $\{\lambda_j\}_{j=1}^{n}$ are respectively the orthogonal matrix and the normal eigenvalues associated with the normal form of $\Gamma(\rho)$. If the Gaussian state ρ is pure, then all the normal eigenvalues are equal to one, hence the parity is equal to $\det(Q)$.

We now mention an important formula that relates the overlap of two pure fermionic Gaussian states to their correlation matrices [36].

Lemma 9 (Overlap between two pure Gaussian states [36]). *The overlap between two pure Gaussian states $|\psi_1\rangle, |\psi_2\rangle$ is:*

$$|\langle\psi_1|\psi_2\rangle|^2 = \left|\mathrm{Pf}\left(\frac{1}{2}(\Gamma(\psi_1)+\Gamma(\psi_2))\right)\right|. \tag{S38}$$

It can be shown that the preceding formula is consistent with the fact that two Gaussian states with opposite parity have zero overlap: in fact, the Pfaffian of the sum of the correlation matrices associated to the two pure Gaussian states with opposite parity must be zero, as follows from Corollary 2.4.(b) of Ref. [37].

In our discussion, we leverage the following lemma, which is available in the literature in various forms (for instance, see Ref. [38]).

Lemma 10 (Purification of a mixed free-fermionic state.). *Any n-qubits mixed free-fermionic state ρ can be purified into a pure free-fermionic state $|\psi_\rho\rangle$ of $2n$-qubits. Specifically, the purified state vector $|\psi_\rho\rangle$ corresponds to the free-fermionic state associated with the correlation matrix*

$$\Gamma(\psi_\rho) = \begin{pmatrix} \Gamma(\rho) & \sqrt{I_{2n}+\Gamma^2(\rho)} \\ -\sqrt{I_{2n}+\Gamma^2(\rho)} & -\Gamma(\rho) \end{pmatrix}. \tag{S39}$$

Proof. Since any free-fermionic state is fully specified by its correlation matrix, we only need to demonstrate that $\Gamma(|\psi\rangle\langle\psi|)$ is a valid correlation matrix corresponding to a pure state, and that the partial trace of this pure state corresponds to ρ. This latter assertion is trivial, as taking the partial trace with respect to qubits indexed by $E := \{n+1,\dots,2n\}$ of $|\psi\rangle\langle\psi|$ involves considering only the restriction of $\Gamma(|\psi\rangle\langle\psi|)$ to the first diagonal block, corresponding to $\Gamma(\rho)$, and thus yielding the state ρ [3]. Therefore, we are left to demonstrate that $\Gamma(|\psi\rangle\langle\psi|)$ is a valid correlation matrix corresponding to a pure state. In particular, we need to show that it is real-anti-symmetric with eigenvalues $\{\pm i\}_{j=1}^{2n}$. The fact that it is anti-symmetric follows from the fact that $\sqrt{I_{2n}+\Gamma^2(\rho)}$ is Hermitian. Since it is anti-symmetric and real, its eigenvalues are purely imaginary. We are left to show that the eigenvalues are all one in absolute value. This follows from the fact that $\Gamma(|\psi\rangle\langle\psi|)$ is unitary, as can be verified by inspection. □

Particle-number preserving fermionic states

In this section, we introduce standard notions related to particle-number preserving fermionic states, which form a common subset of fermionic states often considered in condensed matter physics. This concept will be useful for deriving a particle-number preserving version of the inequality we establish for general free-fermionic states in the subsequent section.

Definition 8 (Creation and annihilation operators)**.** *The annihilation operators* $\{a_j\}_{j=1}^n$ *and creation operators* $\{a_j^\dagger\}_{j=1}^n$ *are defined as:*

$$a_j := \frac{\gamma_{2j-1} + i\gamma_{2j}}{2}, \quad a_j^\dagger := \frac{\gamma_{2j-1} - i\gamma_{2j}}{2}. \tag{S40}$$

for all $j \in [n]$.

They satisfy the commutation relations $\{a_k, a_l\} = 0$, $\{a_k, a_l^\dagger\} = \delta_{k,l}$ for each $k, l \in [n]$. Moreover, they satisfy $a_k^\dagger a_k = \frac{1}{2}(I - Z_j) = |1\rangle\!\langle 1|_k$ for each $k \in [n]$. Majorana operators can be then written as $\gamma_{2k-1} = a_j + a_j^\dagger$ and $\gamma_{2j} = -i(a_j - a_j^\dagger)$ for each $k \in [n]$.

Definition 9 (Particle number operator)**.** *The operator* $\hat{N} := \sum_{i=1}^n a_i^\dagger a_i$ *is denoted as the particle number operator.*

The computational basis forms a set of eigenstates for the particle number operator:

$$\hat{N} |x_1, \dots, x_n\rangle = (x_1 + \cdots + x_n) |x_1, \dots, x_n\rangle , \tag{S41}$$

where $x_1, \dots, x_n \in \{0, 1\}$. The eigenvalue $|x| := x_1 + \cdots + x_n$ of the particle-number operator is the Hamming weight of the bitstring $x := (x_1, \dots, x_n)$.

Definition 10 (Particle number preserving states)**.** *A state* ρ *is is said to be particle number preserving if and only if it commutes with the particle number operator, i.e.,* $[\hat{N}, \rho] = 0$.

From this definition, it follows that any particle-number preserving pure state is an eigenstate of the particle-number operator $\hat{N}$, and, more generally, any particle-number preserving mixed state can be written as a convex combination of eigenstates of the particle-number operator.
We now define the particle-number preserving correlation matrix of a quantum state ρ.

Definition 11 (Particle-number preserving correlation matrix)**.** *Given a state* ρ*, we define its particle number-preserving correlation matrix* $C(\rho)$ *as the* $n \times n$ *matrix such that, for each* $j, k \in [n]$*, we have:*

$$[C(\rho)]_{j,k} := \mathrm{Tr}\left(a_j^\dagger a_k \rho\right), \tag{S42}$$

It is easy to see that the particle-number preserving correlation matrix is an Hermitian matrix. In fact, for each $j, k \in [n]$, we have

$$[C(\rho)]_{j,k}^* = \mathrm{Tr}\left((a_j^\dagger a_k \rho)^*\right) = \mathrm{Tr}\left((a_j^\dagger a_k \rho)^\dagger\right) = \mathrm{Tr}\left(\rho a_k^\dagger a_j\right) = [C(\rho)]_{k,j}, \tag{S43}$$

Thus, it can be unitarily diagonalized.

Lemma 11 (Relation between the correlation matrix and the particle-number preserving one of a particle-number preserving state)**.** *Let* ρ *be a particle-number preserving quantum state. The correlation matrix* $\Gamma(\rho)$ *can be written in terms of the particle-number preserving correlation matrix* $C(\rho)$ *as follows:*

$$\Gamma(\rho) = (I - 2\,\mathrm{Re}(C(\rho)) \otimes iY + (2\,\mathrm{Im}(C(\rho))) \otimes I, \tag{S44}$$

where $\mathrm{Re}(\cdot)$ *and* $\mathrm{Im}(\cdot)$ *are the entry-wise real and immaginary part.*

Proof. Since ρ is a particle-number preserving quantum state, then it commutes with the particle-number operator $[\hat{N}, \rho] = 0$, which implies that ρ can be diagonalized as $\rho = \sum_{j=1}^{2^n} p_j |\psi_j\rangle\!\langle\psi_j|$, where $\{p_j\}_{j=1}^{2^n}$ are non-negative numbers which add up to one and $\{|\psi_j\rangle\}_{j=1}^{2^n}$ are eigenstates of the particle number operators. Hence, for all $j, k \in [n]$, we have that:

$$\mathrm{Tr}\left(\rho a_i^\dagger a_j^\dagger\right) = \sum_{m=1}^{2^n} p_m \langle\psi_m| a_i^\dagger a_j^\dagger |\psi_m\rangle = 0, \tag{S45}$$

where the last equality follows from the fact that $|\psi_m\rangle$ and $a_i^\dagger a_j^\dagger|\psi_m\rangle$ are two vectors which are in the span of two different orthogonal eigenspaces of the particle number operator (i.e., associated with two different Hamming weight). Similarly, we have $\mathrm{Tr}\Big(\rho a_i^\dagger a_j^\dagger\Big) = 0$.

For all $j, k \in [n]$, we have:

$$\begin{aligned}
[\Gamma(\rho)]_{2j-1,2k} &= -i\,\mathrm{Tr}(\gamma_{2j-1}\gamma_{2k}\rho) = \mathrm{Tr}\Big((a_j + a_j^\dagger)(a_k^\dagger - a_k)\rho\Big) = \mathrm{Tr}\Big(a_j a_k^\dagger \rho\Big) - \mathrm{Tr}\Big(a_j^\dagger a_k \rho\Big) && \text{(S46)}\\
&= \delta_{j,k} - \mathrm{Tr}\Big(a_k^\dagger a_j \rho\Big) - \mathrm{Tr}\Big(a_j^\dagger a_k \rho\Big) = \delta_{j,k} - [C(\rho)]^*_{j,k} - [C(\rho)]_{j,k} && \text{(S47)}\\
&= [I - 2\,\mathrm{Re}(C(\rho)]_{j,k}, && \text{(S48)}
\end{aligned}$$

where in the third step we have used Eq. (S45), in the fourth step we have used the commutation relation of annihilation and creation operators, in the fifth step we have used the definition of $C(\rho)$ and the fact that it is Hermitian. For all $j, k \in [n]$, we also have:

$$[\Gamma(\rho)]_{2j,2k-1} = -[\Gamma(\rho)]_{2k-1,2j} = -[I - 2\,\mathrm{Re}(C(\rho)]_{k,j} = -[I - 2\,\mathrm{Re}(C(\rho)]_{j,k}, \tag{S49}$$

where in the first step we use the fact that $\Gamma(\rho)$ is anti-symmetric, in the second step we used Eq.(S48), and in the last step the fact that $I - 2\,\mathrm{Re}(C(\rho)$ is a symmetric matrix. Moreover, for all $j \neq k \in [n]$, it follows that:

$$\begin{aligned}
[\Gamma(\rho)]_{2j-1,2k-1} &= -i\,\mathrm{Tr}(\gamma_{2j-1}\gamma_{2k-1}\rho) = -i\,\mathrm{Tr}\Big((a_j + a_j^\dagger)(a_k + a_k^\dagger)\rho\Big) = -i\,\mathrm{Tr}\Big(a_j a_k^\dagger \rho\Big) - i\,\mathrm{Tr}\Big(a_j^\dagger a_k \rho\Big) && \text{(S50)}\\
&= i[C(\rho)]^*_{j,k} - i[C(\rho)]_{j,k} = [2\,\mathrm{Im}(C(\rho)]_{j,k}, && \text{(S51)}
\end{aligned}$$

Similarly, we also have, for all $j \neq k \in [n]$:

$$[\Gamma(\rho)]_{2j,2k} = -i\,\mathrm{Tr}(\gamma_{2j}\gamma_{2k}\rho) = i\,\mathrm{Tr}\Big((a_j - a_j^\dagger)(a_k - a_k^\dagger)\rho\Big) = -i\,\mathrm{Tr}\Big(a_j a_k^\dagger \rho\Big) - i\,\mathrm{Tr}\Big(a_j^\dagger a_k \rho\Big) = [2\,\mathrm{Im}(C(\rho)]_{j,k}, \tag{S52}$$

Thus, Eq.(S44) follows.

□

From the previous Lemma, it follows that for two particle-number preserving state ρ and σ and any p-norms with $p \in [1, \infty]$, we have:

$$\begin{aligned}
\|\Gamma(\rho) - \Gamma(\sigma)\|_p &= 2\|\mathrm{Re}(C(\rho) - C(\sigma)) \otimes iY + \mathrm{Im}(C(\rho) - C(\sigma)) \otimes I\|_p && \text{(S53)}\\
&\leq 2\,2^{1/p}\|\mathrm{Re}(C(\rho) - C(\sigma))\|_p + 2\,2^{1/p}\|\mathrm{Im}(C(\rho) - C(\sigma))\|_p, && \text{(S54)}\\
&\leq 4\,2^{1/p}\|C(\rho) - C(\sigma)\|_p, && \text{(S55)}
\end{aligned}$$

where in the second step we have used the triangle inequality and the fact that $\|A \otimes B\|_p = \|A\|_p\|A\|_p$, and in the last step the fact that $\mathrm{Re}(A) = (A + A^*)/2$ and $\mathrm{Im}(A) = -i(A - A^*)/2$.

Lemma 12 (Relation between eigenvalues of the correlation matrices)**.** *Let ρ be a particle-number preserving quantum state. Let $\{D_j\}_{j=1}^n$ be the eigenvalues of the particle-number preserving correlation matrix $C(\rho)$. There exists an orthogonal matrix which puts the correlation matrix $\Gamma(\rho)$ in the normal form (as in Lemma 5) with normal eigenvalues*

$$\lambda_j = 1 - 2D_j,$$

for each $j \in [n]$.

Proof. Since $C(\rho)$ is Hermitian, for the spectral theorem, there exists $u \in \mathrm{U}(n)$, such that $C(\rho) = uDu^\dagger$, where D is a diagonal (real) matrix. We now define the matrix O

$$O = \mathrm{Re}(u) \otimes I + \mathrm{Im}(u) \otimes iY. \tag{S56}$$

This matrix O is orthogonal (and symplectic), as it can be verified by using that

$$\mathrm{Re}(u)\,\mathrm{Re}(u)^t + \mathrm{Im}(u)\,\mathrm{Im}(u)^t = I, \qquad \mathrm{Re}(u)\,\mathrm{Im}(u)^t - \mathrm{Im}(u)\,\mathrm{Re}(u)^t = 0, \tag{S57}$$

which follow from the unitarity of u. Now, using Eq.(S56), Eq.(S57) and the fact that for particle-preserving states, $\Gamma(\rho)$ can be written in terms of $C(\rho)$ as in Eq.(S44), it can be verified by inspection that

$$O^T\Gamma(\rho)O = \mathrm{diag}(1 - 2D_1, \dots, 1 - 2D_n) \otimes iY. \tag{S58}$$

Thus, the normal eigenvalues of $\Gamma(\rho)$ are $\{1 - 2D_j\}_{j=1}^n$, where D_j are the eigenvalues of $C(\rho)$. □

Using the upper bound in Eq.(S55) and the eigenvalues relation in Lemma 12, we can directly transfer many of the inequalities that we show in the following section to the particle-preserving case.

III. Norm inequalities for free and non-free fermionic states

In this section, we derive key relations concerning free-fermionic states, laying the groundwork for our subsequent analysis of property testing and tomography. We start by introducing a key lemma which will be pivotal in our proofs.

Lemma 13 (Gentle measurement lemma (or quantum union bound) [39]). *Let $\varepsilon_1, \dots, \varepsilon_M > 0$, where $M \in \mathbb{N}$. Consider the projectors $\{P_i\}_{i=1}^M$. Let ρ be a quantum state. If $\operatorname{Tr}(P_i\rho) \geq 1 - \varepsilon_i$ holds for all $i \in [n]$, then*

$$\left\| \rho - \frac{P_n \dots P_1 \rho P_1 \dots P_M}{\operatorname{Tr}(P_n \dots P_1 \rho P_1 \dots P_M)} \right\|_1 \leq 2\sqrt{\sum_{i\in[M]} \varepsilon_i}\,. \tag{S59}$$

We leverage the *gentle measurement lemma* to establish the following result.

Lemma 14 (Trace distance between a pure free-fermionic state and an arbitrary state). *For a pure free-fermionic state $|\psi\rangle$ and an arbitrary (possibly non-free-fermionic) state ρ, it holds that*

$$\| \rho - |\psi\rangle\!\langle\psi| \,\|_1 \leq \sqrt{\|\Gamma(\rho) - \Gamma(|\psi\rangle\!\langle\psi|)\|_1}\,. \tag{S60}$$

Proof. Since $|\psi\rangle$ is a free-fermionic state, it can be expressed as $|\psi\rangle = U_Q |0^n\rangle$ for a free-fermionic unitary associated with $Q \in \mathrm{O}(2n)$. Define $\rho' := U_Q^\dagger \rho U_Q$. For any $j \in [n]$, we have

$$\operatorname{Tr}\Big(|0\rangle\!\langle 0|_j\, \rho'\Big) = \frac{1}{2} + \frac{1}{2}\left[\Gamma(\rho')\right]_{2j-1,2j} =: 1 - \varepsilon_j, \tag{S61}$$

where we have used $|0\rangle\!\langle 0|_j = (I + Z_j)/2 = (I - i\gamma_{2j-1}\gamma_{2j})/2$ and $\varepsilon_j := (1 - [\Gamma(\rho')]_{2j-1,2j})/2$. Now, we have

$$\| \rho - |\psi\rangle\!\langle\psi| \,\|_1 = \| \rho' - |0^n\rangle\!\langle 0^n| \,\|_1 \leq 2\sqrt{\sum_{j=1}^n \varepsilon_j} = 2\sqrt{\sum_{j=1}^n \frac{1 - [\Gamma(\rho')]_{2j-1,2j}}{2}}, \tag{S62}$$

where we used the unitary invariance of the one-norm and the gentle measurement Lemma 13. Let Λ be the matrix $\Lambda := \bigoplus_{j=1}^n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \Gamma(|0^n\rangle\!\langle 0^n|)$. Observe that $\sum_{j=1}^n [\Gamma(\rho')]_{2j-1,2j} = \frac{1}{2}\operatorname{Tr}\big(\Lambda^\dagger \Gamma(\rho')\big)$. Using this and Eq.(S62), we have

$$\begin{aligned}
\| \rho - |\psi\rangle\!\langle\psi| \,\|_1 &\leq \sqrt{\operatorname{Tr}\left(I_{2n} - \Lambda^\dagger \Gamma(\rho')\right)} \\
&\leq \sqrt{\|I_{2n} - \Lambda^\dagger \Gamma(\rho')\|_1} \\
&= \sqrt{\|\Lambda - \Gamma(U_Q^\dagger \rho U_Q)\|_1} \\
&= \sqrt{\|\Lambda - Q^T \Gamma(\rho) Q\|_1} \\
&= \sqrt{\|\Gamma(|\psi\rangle\!\langle\psi|) - \Gamma(\rho)\|_1},
\end{aligned} \tag{S63}$$

where in the second step we used Hölder inequality, in the third step the definition of one-norm, in the third step the unitary invariance of the one-norm and the definition of ρ', in the fourth step the fact that $\Gamma(U_Q^\dagger \rho U_Q) = Q^T \Gamma(\rho) Q$, and in the last step the unitary invariance of the one-norm and the fact that $\Gamma(|\psi\rangle\!\langle\psi|) = Q\Gamma(|0^n\rangle\!\langle 0^n|)Q^T$. □

Lemma 15 (Trace distance between a free-fermionic state and the maximally mixed state). *Let σ be an n-qubits free-fermionic state, and $d := 2^n$. Then we have*

$$\left\| \sigma - \frac{I_d}{d} \right\|_1 \leq \frac{1}{2}\|\Gamma(\sigma)\|_1\,. \tag{S64}$$

Proof. Since σ is a free-fermionic state, it can be expressed as $\sigma = U_Q \bigotimes_{j=1}^n \left(\frac{I + \lambda_j Z_j}{2}\right) U_Q^\dagger$, where U_Q is a free-fermionic unitary with $Q \in O(2n)$, and $\{\lambda_j\}_{j=1}^n \in [-1,1]$. Therefore, we have

$$\begin{aligned} \left\| \sigma - \frac{I_d}{d} \right\|_1 &= \left\| \bigotimes_{j=1}^n \left(\frac{I + \lambda_j Z_j}{2} \right) - \frac{I_d}{d} \right\|_1 \\ &= \left\| \bigotimes_{j=1}^n \left(\frac{I + \lambda_j Z_j}{2} \right) - \bigotimes_{j=1}^n \frac{I}{2} \right\|_1 \\ &\le \sum_{j=1}^n \left\| \frac{I + \lambda_j Z_j}{2} - \frac{I}{2} \right\|_1 \\ &= \sum_{j=1}^n |\lambda_j| \,, \end{aligned} \tag{S65}$$

where the first step utilizes the unitary invariance of the one-norm, and the second step applies the triangle inequality. We conclude by observing that

$$\|\Gamma(\sigma)\|_1 = \left\| \bigoplus_{j=1}^n \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} \right\|_1 = 2 \sum_{j=1}^n |\lambda_j| \,. \tag{S66}$$

□

Lemma 16 (Lower bound on trace distance in terms of correlation matrices). *Given two quantum states ρ and σ, their trace distance is lower bounded by the operator norm difference*

$$\|\rho - \sigma\|_1 \ge \|\Gamma(\rho) - \Gamma(\sigma)\|_\infty \tag{S67}$$

of their correlation matrices $\Gamma(\rho)$ and $\Gamma(\sigma)$.

Proof. Due to Hölder's inequality, we have

$$\|\rho - \sigma\|_1 \ge \sup_{\|W\|_\infty = 1} |\operatorname{Tr}(W(\rho - \sigma))|. \tag{S68}$$

Now, let us restrict the operators W to the form $W = U_Q^\dagger i\gamma_j\gamma_k U_Q$, where $j,k \in [2n]$ and U_Q is a free-fermionic unitary associated with an orthogonal matrix $Q \in \mathrm{O}(2n)$. Indeed, note that $\|U_Q^\dagger i\gamma_j\gamma_k U_Q\|_\infty = \|i\gamma_j\gamma_k\|_\infty = 1$. It holds that

$$\|\rho - \sigma\|_1 \ge \sup_{\|W\|_\infty = 1} |\operatorname{Tr}(W(\rho - \sigma))| = \sup_{\substack{j,k \in [2n] \\ Q \in \mathrm{O}(2n)}} \left|\operatorname{Tr}\left(U_Q^\dagger i\gamma_j\gamma_k U_Q(\rho - \sigma)\right)\right|. \tag{S69}$$

We then have

$$\begin{aligned} \sup_{\substack{j,k \in [2n] \\ Q \in \mathrm{O}(2n)}} \left|\operatorname{Tr}\left(U_Q^\dagger i\gamma_j\gamma_k U_Q(\rho - \sigma)\right)\right| &= \sup_{\substack{j,k \in [2n] \\ Q \in \mathrm{O}(2n)}} \left|\operatorname{Tr}\left(i\gamma_j\gamma_k U_Q(\rho - \sigma)U_Q^\dagger\right)\right| \\ &= \sup_{\substack{j,k \in [2n] \\ Q \in \mathrm{O}(2n)}} |(Q(\Gamma(\rho) - \Gamma(\sigma))Q^T)_{j,k}|, \end{aligned} \tag{S70}$$

where in the last step we used that $\Gamma(U_Q\rho U_Q^\dagger) = Q\Gamma(\rho)Q^T$. Since $\Gamma(\rho) - \Gamma(\sigma)$ is real and anti-symmetric, it can be brought into a normal form $\Gamma(\rho) - \Gamma(\sigma) = O'\Lambda' O'^T$, where $\Lambda' = \bigoplus_{i=1}^n \begin{pmatrix} 0 & \lambda_i' \\ -\lambda_i' & 0 \end{pmatrix}$ and $\{\pm i\lambda_i'\}_{i=1}^n$ are the purely imaginary eigenvalues of $\Gamma(\rho) - \Gamma(\sigma)$. By choosing $Q = O'^T$, we have

$$\sup_{\substack{j,k \in [2n] \\ Q \in \mathrm{O}(2n)}} |(Q'(\Gamma(\rho) - \Gamma(\sigma))Q'^T)_{j,k}| \ge \sup_{j,k \in [2n]} |\Lambda'_{j,k}| = \sup_{i \in [n]} |\lambda_i'| = \|\Gamma(\rho) - \Gamma(\sigma)\|_\infty \tag{S71}$$

that concludes the proof. □

Lemma 17. *Let A and B be two $2n \times 2n$ anti-symmetric real matrices with eigenvalues $\{\pm i\lambda_k(A)\}_{k=1}^n$ and $\{\pm i\lambda_k(B)\}_{k=1}^n$ respectively, where $\lambda(A)_1 \leq \cdots \leq \lambda_n(A)$ and $\lambda(B)_1 \leq \cdots \leq \lambda_n(B)$. We then have*

$$\|A - B\|_\infty \geq |\lambda_k(A) - \lambda_k(B)|, \tag{S72}$$

for any $k \in [n]$.

Proof. This follows from the fact that $C := iA$ and $D := iB$ are Hermitian matrices. Applying *Weyl's perturbation theorem* (see Ref. [40], section VI), which states that given two $2n \times 2n$ Hermitian matrices C and D with eigenvalues $c_1 \leq \cdots \leq c_{2n}$ and $d_1 \leq \cdots \leq d_{2n}$, we have

$$\|C - D\|_\infty \geq |c_j - d_j|, \tag{S73}$$

for any $j \in [2n]$. This implies that

$$\|A - B\|_\infty = \|C - D\|_\infty \geq \max_{j \in [2n]} |c_j - d_j| = \max_{k \in [n]} |\lambda_k(A) - \lambda_k(B)|. \tag{S74}$$

□

Theorem 5 (Trace distance upper bound between two pure free-fermionic states)**.** *Let ψ_1, ψ_2 be two pure free-fermionic states with correlation matrices $\Gamma(\psi_1), \Gamma(\psi_2)$. Assuming that $\|\Gamma(\psi_1) - \Gamma(\psi_2)\|_\infty < 2$, it holds that*

$$\|\psi_1 - \psi_2\|_1 \leq \frac{1}{2}\|\Gamma(\psi_1) - \Gamma(\psi_2)\|_2. \tag{S75}$$

Otherwise, if the quantity $\|\Gamma(\psi_1) - \Gamma(\psi_2)\|_\infty$ (which is always ≤ 2) is equal to 2, then we simply have $\|\psi_1 - \psi_2\|_1 = 2$.

Proof. First of all, we have

$$\|\psi_1 - \psi_2\|_1 = 2\sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}. \tag{S76}$$

This can be seen by considering $Q := \psi_1 - \psi_2$. The Hermitian matrix Q has a rank of at most 2, which means it can have at most two non-zero eigenvalues denoted as λ_1 and λ_2. Since the trace of Q is zero, we have $\lambda_2 = -\lambda_1$. Additionally, we know that $\mathrm{Tr}(Q^2) = \lambda_1^2 + \lambda_2^2 = 2\lambda_1^2$, and $\mathrm{Tr}(Q^2) = 2(1 - |\langle u|v\rangle|^2)$. Therefore, we can conclude that $\lambda_1 = \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}$. The 1-norm of Q is given by $\|Q\|_1 = |\lambda_1| + |\lambda_2|$, which simplifies to $\|Q\|_1 = 2\sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}$. From Lemma 9, it follows that:

$$|\langle\psi_1|\psi_2\rangle|^2 = \sqrt{\det\left(\frac{\Gamma(\psi_1) + \Gamma(\psi_2)}{2}\right)}, \tag{S77}$$

where we used that $(\mathrm{Pf}(A))^2 = \det(A)$ (note that the determinant of an antisymmetric matrix is positive). Thus, we have

$$|\langle\psi_1|\psi_2\rangle|^2 = \sqrt{\det(\Gamma(\psi_1)^T)\det\left(\frac{\Gamma(\psi_1) + \Gamma(\psi_2)}{2}\right)} = \sqrt{\det\left(\frac{\mathbb{1} + \Gamma(\psi_1)^T\Gamma(\psi_2)}{2}\right)} = \sqrt{\det\left(\frac{\mathbb{1} + X}{2}\right)} \tag{S78}$$

where the first step follows because $\det(\Gamma(\psi_1)^T) = \det(\Gamma(\psi_1)) = 1$ (see Remark 1), the second step follows from $\det(A)\det(B) = \det(AB)$ and the fact that $\Gamma(\psi_1)$ is an orthogonal matrix (see Remark 1). In the last step, we defined $X := \Gamma(\psi_1)^T\Gamma(\psi_2)$, which is also an orthogonal matrix (being product of two orthogonal matrices). Since X is an normal matrix, also $2^{-1}(\mathbb{1} + X)$ is normal, thus its determinant is equal to the product of its eigenvalues. Thus:

$$|\langle\psi_1|\psi_2\rangle|^2 = \sqrt{\det\left(\frac{\mathbb{1} + X}{2}\right)} = \sqrt{\prod_{j=1}^{2n}\left(\frac{\mathbb{1} + \lambda_j(X)}{2}\right)}, \tag{S79}$$

where we denoted as $\{\lambda_j(X)\}_{j=1}^{2n}$ the eigenvalues of X. Since X is orthogonal, we also have that for each $j \in [2n]$, there exists $\phi_j \in \mathbb{R}$ such that $\lambda_j(X) = e^{i\phi_j}$.

We are now going to show that all eigenvalues of X have multiplicity two. Let $|v\rangle$ be an eigenstate of X corresponding to the eigeinvalue λ:

$$X|v\rangle = \lambda|v\rangle. \tag{S80}$$

We also have that:

$$X(\Gamma(\psi_2)\,|v\rangle^*) = \Gamma(\psi_1)^T\Gamma(\psi_2)^2\,|v\rangle^* = -\Gamma(\psi_1)^T\,|v\rangle^* = -\Gamma(\psi_1)^T\frac{1}{\lambda^*}(X\,|v\rangle)^* = \lambda(\Gamma(\psi_2)\,|v\rangle^*), \tag{S81}$$

where the third step follows from the fact that $\Gamma(\psi_2)$ is anti-symmetric and orthogonal and the fifth step from the fact that $\lambda^{-1} = \lambda^*$. Thus, $\Gamma(\psi_2)\,|v\rangle^*$ and $|v\rangle$ are both eigenstates of X with eigenvalue λ. Note that they must be different vectors. In fact, if it holds that $\Gamma(\psi_2)\,|v\rangle^* = e^{i\theta}\,|v\rangle$ for $\theta \in [0, 2\pi]$, then multiplying by $\Gamma(\psi_2)$ we also have

$$-\,|v\rangle^* = e^{i\theta}\Gamma(\psi_2)\,|v\rangle = e^{i\theta}(\Gamma(\psi_2)\,|v\rangle^*)^* = e^{i\theta}(e^{i\theta}\,|v\rangle)^* = |v\rangle^*\,, \tag{S82}$$

Thus, we have $|v\rangle^* = -\,|v\rangle^*$, which is an absurd. Thus we have shown that all eigenvalues of X have multiplicity two. Thus, without loss of generality, we can assume that $\lambda_{n+k}(X) = \lambda_k(X)$ for $k \in [n]$. Hence, from Eq. S79, we have

$$|\langle\psi_1|\psi_2\rangle|^2 = \prod_{j=1}^{n}\left(\frac{\mathbb{1} + \lambda_j(X)}{2}\right), \tag{S83}$$

If an eigenvalue $\lambda_j(X) = e^{i\phi_j}$ is not real (which implies that its associated eigenstate is not a real vector), then also $\lambda_j^*(X) = e^{-i\phi_j}$ will be a distinct eigenvalue of X (as follows by simply taking the complex conjugate of Eq. (S80)). The remaining eigenvalues will be $+1$ or -1. Let us denote with $2n_c$ the number of not-real eigenvalues (they are even, as they come in pairs), with n_+ the number of $+1$ eigenvalues, and with n_- the number of -1 eigenvalues. So that we have

$$n_+ + n_- + 2n_c = n. \tag{S84}$$

Thus, the X's eigenvalues will be

$$\{\lambda_1(X), \dots, \lambda_n(X)\} = \{\underbrace{e^{i\phi_1}, e^{-i\phi_1}, \dots, e^{i\phi_{n_c}}, e^{-i\phi_{n_c}}}_{2n_c}, \underbrace{+1, \dots, +1}_{n_+}, \underbrace{-1, \dots, -1}_{n_-}\}, \tag{S85}$$

where $\{e^{i\phi_j}\}_{j=1}^{n_c}$ are not real (without loss of generality). Hence, we find

$$\begin{aligned}|\langle\psi_1|\psi_2\rangle|^2 &= \delta_{n_-,0}\prod_{j=1}^{n_c}\frac{1}{4}\left(1 + e^{i\phi_j}\right)\left(1 + e^{-i\phi_j}\right)\\ &= \delta_{n_-,0}\prod_{j=1}^{n_c}\frac{1}{2}\left(1 + \cos(\phi_j)\right)\\ &= \delta_{n_-,0}\prod_{j=1}^{n_c}\left(1 - \sin^2(\phi_j)\right)\\ &\geq \delta_{n_-,0}\left(1 - \sum_{j=1}^{n_c}\sin^2(\phi_j)\right),\end{aligned} \tag{S86}$$

where in the last step we used Weierstrass product inequality. Next, we can rewrite

$$\begin{aligned}\|\Gamma(\psi_1) - \Gamma(\psi_2)\|_2^2 &= \|1 - \Gamma(\psi_1)^T\Gamma(\psi_2)\|_2^2\\ &= \|1 - X\|_2^2\\ &= \sum_{j=1}^{2n}|1 - \lambda_j(X)|^2\\ &= 2\sum_{j=1}^{n}|1 - \lambda_j(X)|^2\\ &= 2\left(\sum_{j=1}^{n_c}\left(|1 - e^{i\phi_j}|^2 + |1 - e^{-i\phi_j}|^2\right) + \sum_{j=1}^{n_+}0 + \sum_{j=1}^{n_-}2\right)\\ &= 16\sum_{j=1}^{n_c}\sin^2(\phi_j/2) + 4n_-,\end{aligned} \tag{S87}$$

where in the last step we used that $|1-e^{i\phi_j}|=2|\sin(\phi_j/2)|$. If $n_->0$, Eq.(S86) implies that $|\langle\psi_1|\psi_2\rangle|^2=0$. Thus, using Eq.(S76), we have

$$\|\psi_1-\psi_2\|_1=2,\quad \text{if } n_->0. \tag{S88}$$

If $n_-=0$, Eqs. (S86),(S87) imply that:

$$|\langle\psi_1|\psi_2\rangle|^2\geq 1-\frac{1}{16}\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_2^2, \tag{S89}$$

Thus, by Eq.(S76), we arrive at

$$\|\psi_1-\psi_2\|_1\leq\frac{1}{2}\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_2,\quad \text{if } n_-=0. \tag{S90}$$

We are now only left to show that the condition $n_-=0$ is satisfied if and only if it holds that $\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_\infty<2$. This is indeed the case, since the quantity (which is always ≤ 2)

$$\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_\infty=\|1-X\|_\infty \tag{S91}$$

can be equal to 2 if and only if X has at least a -1 eigenvalues if and only if $n_->0$. □

Remark 3 (Saturation of the inequality). *We note that the above upper bound is saturated for all pure free-fermionic state ψ_1,ψ_2 with number of modes/qubits $n\leq 3$. Thus, we get*

$$\|\psi_1-\psi_2\|_1=\begin{cases}\frac{1}{2}\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_2, & \textit{if } \|\Gamma(\psi_1)-\Gamma(\psi_2)\|_\infty<2,\\ 2, & \textit{if } \|\Gamma(\psi_1)-\Gamma(\psi_2)\|_\infty=2.\end{cases} \tag{S92}$$

Proof. The case $\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_\infty=2$ is analogous to the previous proof, so let us focus on $\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_\infty<2$. Using the same notation of the previous proof, we have that $n_-=0$, i.e., the number of -1 eigenvalues of $X:=\Gamma(\psi_1)^T\Gamma(\psi_2)$ is zero. Hence, because of Eq. (S86), we have

$$|\langle\psi_1|\psi_2\rangle|^2=\prod_{j=1}^{n_c}\left(1-\sin^2(\phi_j)\right). \tag{S93}$$

From Eq.(S84) and using that $n\leq 3$, we get

$$2n_c+n_+\leq 3, \tag{S94}$$

which implies that $n_c=0$ or $n_c=1$.
If $n_c=0$, we have $|\langle\psi_1|\psi_2\rangle|^2=1$, which implies $\|\psi_1-\psi_2\|_1=0$. Furthermore, because of Eq. (S87), we also have $\frac{1}{2}\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_2=0$.
If $n_c=1$, we then have

$$|\langle\psi_1|\psi_2\rangle|^2=1-\sin^2(\phi_1)=1-\frac{1}{16}\|\Gamma(\psi_1)-\Gamma(\psi_2)\|_2^2, \tag{S95}$$

where in the first step we have used Eq. (S93), and in the second step we have used Eq. (S87). Thus, we reach the conclusion by using that $\|\psi_1-\psi_2\|_1=2\sqrt{1-|\langle\psi_1|\psi_2\rangle|^2}$. □

Next, we present an upper bound on the trace distance between two (possibly mixed) Gaussian states in terms of the norm difference of their respective correlation matrices.

Theorem 6 (Trace distance upper bound between two mixed free-fermionic states). *Let ρ,σ be two (possibly mixed) free-fermionic states. Then it holds*

$$\|\rho-\sigma\|_1\leq\sqrt{\|\Gamma(\rho)-\Gamma(\sigma)\|_1+\frac{1}{2}\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2}. \tag{S96}$$

Moreover, we also have

$$\mathcal{F}(\sigma,\rho)\geq 1-\frac{1}{8}\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2-\frac{1}{4}\|\Gamma(\rho)-\Gamma(\sigma)\|_1, \tag{S97}$$

where $\mathcal{F}(\rho,\sigma):=\mathrm{Tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)^2$ is the fidelity between ρ and σ.

Proof. By using Lemma 10, we can purify ρ and σ to two pure free-fermionic states ψ_ρ and ψ_σ with correlation matrix

$$\Gamma(\psi_\rho) = \begin{pmatrix} \Gamma(\rho) & \sqrt{I+\Gamma(\rho)^2} \\ -\sqrt{I+\Gamma(\rho)^2} & -\Gamma(\rho) \end{pmatrix}. \tag{S98}$$

This means

$$\begin{aligned} \|\Gamma(\psi_\rho)-\Gamma(\psi_\sigma)\|_2^2 &= 2\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2 + 2\|\sqrt{I+\Gamma(\rho)^2}-\sqrt{I+\Gamma(\sigma)^2}\|_2^2 \\ &\leq 2\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2 + 2\|\Gamma(\rho)^2-\Gamma(\sigma)^2\|_1 \\ &\leq 2\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2 + 2\|\Gamma(\rho)(\Gamma(\rho)-\Gamma(\sigma))\|_1 + 2\|(\Gamma(\rho)-\Gamma(\sigma))\Gamma(\sigma)\|_1 \\ &\leq 2\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2 + 4\|\Gamma(\rho)-\Gamma(\sigma)\|_1, \end{aligned} \tag{S99}$$

where in the first step we have used that the square of the 2-norm of the entire matrix is given by the sum of the square of the 2-norm of each sub-block (as follows by the fact that, if A_1 and A_2 are orthogonal with respect the Hilbert-Schmidt scalar product, then $\|A_1\otimes B_1 + A_2\otimes B_2\|_2^2 = \|A_1\otimes B_1\|_2^2 + \|A_2\otimes B_2\|_2^2$). In the second step we have used the inequality (Ref. [40], Eq. X.23)

$$\|A^{1/t}-B^{1/t}\|_p \leq \|A-B\|_{p/t}^{1/t}, \tag{S100}$$

which is valid for each $t\in[1,\infty), p\in[1,\infty]$ and positive matrix A and B. In particular, for our case we use $p=t=2$. In the third step we have used triangle inequality, and in the fourth step the Holder inequality for the one-norm

$$\|AB\|_1 \leq \min(\|A\|_\infty\|B\|_1, \|B\|_\infty\|A\|_1), \tag{S101}$$

and the fact that the infinity norm of any correlation matrix is upper bounded by 1. From the fact that the fidelity of two mixed state is the maximum over all the possible purifications, we conclude that

$$\mathcal{F}(\sigma,\rho) \geq |\langle\psi_\rho|\psi_\sigma\rangle|^2 = 1-\frac{1}{4}\|\psi_\rho-\psi_\sigma\|_1^2, \tag{S102}$$

where we used Eq.(S76). By using Theorem 5, we have that, if $\|\Gamma(\psi_\rho)-\Gamma(\psi_\sigma)\|_\infty < 1$, then

$$\|\psi_\rho-\psi_\sigma\|_1 \leq \frac{1}{2}\|\Gamma(\psi_\rho)-\Gamma(\psi_\sigma)\|_2. \tag{S103}$$

The condition $\|\Gamma(\psi_\rho)-\Gamma(\psi_\sigma)\|_\infty < 1$ is satisfied if and only if the number of -1 eigenvalues of $X := \Gamma(\psi_\rho)^\dagger\Gamma(\psi_\sigma)$ is zero (as discussed also in the proof of Theorem 5). However, in this case, we can assume that X has always zero -1 eigenvalues Thus, by Eq.(S102) and Eq.(S103), we have:

$$\mathcal{F}(\sigma,\rho) \geq 1-\frac{1}{16}\|\Gamma(\psi_\rho)-\Gamma(\psi_\sigma)\|_2^2 \tag{S104}$$

$$\geq 1-\frac{1}{8}\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2 - \frac{1}{4}\|\Gamma(\rho)-\Gamma(\sigma)\|_1, \tag{S105}$$

where in the last step we used Eq.(S99). Thus, by using Fuchs van de Graaf inequality (Eq.(8)), we have

$$\|\rho-\sigma\|_1 \leq \sqrt{\|\Gamma(\rho)-\Gamma(\sigma)\|_1 + \frac{1}{2}\|\Gamma(\rho)-\Gamma(\sigma)\|_2^2} \leq \sqrt{\frac{3}{2}\|\Gamma(\rho)-\Gamma(\sigma)\|_1}, \tag{S106}$$

□

If in the previous Theorem we have the additional assumption that $\|\Gamma(\rho)-\Gamma(\sigma)\|_1 < 1$, then it follows that

$$\|\rho-\sigma\|_1 \leq \sqrt{\frac{3}{2}}\|\Gamma(\rho)-\Gamma(\sigma)\|_1. \tag{S107}$$

A. Quantifying non-Gaussianity: Distance from the set of free-fermionic states

In this section, our objective is to establish lower bounds on the minimum trace distance between a state ρ and the set of free-fermionic states. This distance serves as a metric for the inherent "magic" in a given state, providing a precise quantification of its "non-free-fermionic" or "non-Gaussianity" degree. The presented lower bounds on the proposed measure of non-free-fermionic degree are carefully designed to enable time and sample-efficient estimation up to a constant precision in an experimental setting. This capability is crucial for quantifying the extent to which a state exhibits non-free-fermionic behavior in experimental scenarios.

We will derive bounds in different scenarios: one without prior assumptions on the state ρ and another assuming that ρ is pure or, more generally, has a rank at most R. Moreover, we consider two distinct sets of free-fermionic states: $\mathcal{G}_{\text{mixed}}$ and $\mathcal{G}_R$. Here, $\mathcal{G}_{\text{mixed}}$ represents the set of all free-fermionic states, while $\mathcal{G}_R$ represents the set of free-fermionic states constrained to those with a rank at most R. We begin with a simple result, addressing the case where ρ is an arbitrary state and we consider its distance from the set $\mathcal{G}_R$.

Theorem 7 (Lower bound on the distance of an arbitrary state from the set of free-fermionic states with rank at most R)**.** *Let ρ be an arbitrary quantum state. Denote with $\mathcal{G}_R$ the set of free-fermionic states restricted to those states with rank at most R. Let $\lambda_\kappa(\Gamma(\rho))$ with $\kappa := \lceil \log_2(R) \rceil + 1$ denote the (possibly negative) κ-th smallest normal eigenvalue of the correlation matrix of ρ. We then have*

$$\min_{\sigma \in \mathcal{G}_R} \|\rho - \sigma\|_1 \geq 1 - \lambda_\kappa(\Gamma(\rho)). \tag{S108}$$

Proof. By virtue of Lemma 16, we further establish

$$\|\rho - \sigma\|_1 \geq \|\Gamma(\rho) - \Gamma(\sigma)\|_\infty. \tag{S109}$$

Furthermore, according to Lemma 17, the infinity norm difference serves as a lower bound for the difference in eigenvalues

$$\|\Gamma(\rho) - \Gamma(\sigma)\|_\infty \geq |\lambda_j(\Gamma(\rho)) - \lambda_j(\Gamma(\sigma))|, \tag{S110}$$

where $\{\lambda_j(\Gamma(\rho))\}_{j=1}^n$ and $\{\lambda_j(\Gamma(\sigma))\}_{j=1}^n$ are the normal eigenvalues of the two correlation matrices ordered in increasing order. We then have

$$\|\Gamma(\rho) - \Gamma(\sigma)\|_\infty \geq |\lambda_\kappa(\Gamma(\rho)) - 1| = 1 - \lambda_\kappa(\Gamma(\rho)), \tag{S111}$$

where we used that because of Lemma 2 $\lambda_j(\Gamma(\sigma)) = 1$ for all $j \in \{\kappa, \dots, n\}$ and for all $\sigma \in \mathcal{G}_R$. The result thus follows. □

From this, it follows the results when restricting to the set of pure free-fermionic states $\mathcal{G}_{\text{pure}} \equiv \mathcal{G}_{R=1}$.

Corollary 1 (Lower bound on the distance of an arbitrary state from the set of pure free-fermionic states)**.** *Let ρ be a quantum state. Let $\lambda_{\min}$ denote the smallest normal eigenvalue of the correlation matrix of ρ. We then have*

$$\min_{\sigma \in \mathcal{G}_{\text{pure}}} \|\rho - \sigma\|_1 \geq 1 - \lambda_{\min}. \tag{S112}$$

Next, we establish a lower bound on the distance between a quantum state ρ and the set of all free-fermionic states $\mathcal{G}_{\text{mixed}}$. It is crucial to mention that in our previous discussion, we focused on the set of free-fermionic states with a rank no greater than R. For pedagogical reasons, we begin by assuming that ρ is pure. Later, we will extend our analysis to ρ having a rank at most R.

Theorem 8 (Lower bound on the distance of a pure state from the set of all free-fermionic states)**.** *Let ρ be a pure state. Let $\lambda_{\min}$ denote the (possibly negative) smallest normal eigenvalue of the correlation matrix of ρ. Then, we have*

$$\min_{\sigma \in \mathcal{G}_{\text{mixed}}} \|\rho - \sigma\|_1 \geq \frac{1}{2}\left(1 - \lambda_{\min}\right). \tag{S113}$$

Here, $\mathcal{G}_{\text{mixed}}$ is the set of all free-fermionic states.

Proof. Because of Lemma 16, we can write for any $\sigma \in \mathcal{G}_{\text{mixed}}$ the lower bound

$$\|\rho - \sigma\|_1 \geq \|\Gamma(\rho) - \Gamma(\sigma)\|_\infty \tag{S114}$$

to the 1-norm. Let us denote as $\{\lambda_i^\rho\}_{i=1}^n$ the eigenvalues of $\Gamma(\rho)$ and $\{\lambda_i^\sigma\}_{i=1}^n$ the eigenvalues of $\Gamma(\sigma)$ for an arbitrary free-fermionic state σ. The bound in Eq. (S114) translates to $\|\rho-\sigma\|_1 \geq \max_i |\lambda_i^\rho - \lambda_i^\sigma|$ using the fact that the infinity norm difference serves as a lower bound for the difference in eigenvalues [41]. Contrasting this, we also have that [41]

$$\|\rho-\sigma\|_1 \geq \|\mathrm{diag}(1,0,\ldots,0)-\mathrm{diag}(z_{\max},\ldots,z_d)\|_1 = |1-z_{\max}| + \sum_{i=2}^{d} z_i = 2(1-z_{\max}), \tag{S115}$$

where $\{z_i\}_{i=1}^n$ are the ordered eigenvalues of the (in general) mixed free-fermionic state σ. We know that the eigenvalues z_i of σ are related to the (positive) normal eigenvalues $\{\lambda_i^\sigma\}_{i=1}^n$ of the correlation matrix $\Gamma(\sigma)$ because the diagonal form of σ reads $\bigotimes_{i=1}^n \frac{I+\lambda_i^\sigma Z_i}{2}$. Therefore,

$$z_{\max} = \prod_{i=1}^{n} \frac{1}{2}(1+\lambda_i^\sigma) \leq \frac{1+\min_{i\in[n]}\lambda_i^\sigma}{2}. \tag{S116}$$

Plugging this upper bound on $z_{\max}$ into Eq. (S115), we get, for any $\sigma \in \mathcal{G}_{\mathrm{mixed}}$, the lower bound

$$\|\rho-\sigma\|_1 \geq (1-\min_{i\in[n]}\lambda_i^\sigma) \tag{S117}$$

to the 1-norm distance. Therefore, we have two lower bounds to the 1-norm distance $\|\rho-\sigma\|_1$, and we can consider the extremum over σ and lower bound it with the maximum between these two universal lower bounds (valid for any σ). We thus write

$$\begin{aligned}\min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}} \|\rho-\sigma\|_1 &\geq \min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}} \max\{\max_{i\in[n]}|\lambda_i^\rho-\lambda_i^\sigma|, \max_{i\in[n]}(1-\lambda_i^\sigma)\} \\ &= \min_{\vec{\lambda}^\sigma\in[-1,1]^n} \max_{i\in[n]} \max\{|\lambda_i^\rho-\lambda_i^\sigma|,(1-\lambda_i^\sigma)\} \\ &= \max_{i\in[n]} \min_{\lambda^\sigma\in[-1,1]} \max\{|\lambda_i^\rho-\lambda^\sigma|,(1-\lambda^\sigma)\} \\ &= \max_{i\in[n]} \frac{1-\lambda_i^\rho}{2}.\end{aligned} \tag{S118}$$

We can exchange the minimum and maximum because they act independently, and the last step follows because the function is maximized for $\lambda^\sigma = \frac{1+\lambda_i^\rho}{2}$. Therefore, we obtain the lower bound

$$\min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}} \|\rho-\sigma\|_1 \geq \frac{1-\min_i\lambda_i^\rho}{2} \equiv \frac{1}{2}(1-\lambda_{\min}) \tag{S119}$$

on the minimal trace norm. This proves our claim. □

Theorem 9 (Lower bound on the distance of a bounded rank state from the set of all free-fermionic states)**.** *Let ρ be a quantum state with rank $\mathrm{rank}(\rho) \leq R$. Let $\sigma \in \mathcal{G}_{\mathrm{mixed}}$. Let $\Gamma(\rho)$ be the correlation matrix associated to ρ and let $\lambda_1^\rho, \lambda_2^\rho, \ldots, \lambda_n^\rho$ be its normal eigenvalues in decreasing order. Assume that $R \leq 2^r$ for some $r \in [0,n]$ and denote $\bar{\lambda} = \lambda_{r+1}^\rho$. Then the trace distance is lower bounded by*

$$\min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}} \|\rho-\sigma\|_1 \geq \frac{(1-\bar{\lambda})^{r+1}}{1+(r+1)(1-\bar{\lambda})^r}. \tag{S120}$$

In particular, this implies for $\bar{\lambda} \geq \frac{1}{2}$,

$$\min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}} \|\rho-\sigma\|_1 \geq \frac{(1-\bar{\lambda})^{r+1}}{2}. \tag{S121}$$

For $R = 1$ it reduces to the bound in Theorem 8 valid for pure states ρ.

Proof. First of all, let us make use of Lemma 16 to bound $\|\rho-\sigma\|_1 \geq \|\Gamma(\rho)-\Gamma(\sigma)\|_\infty \geq |\bar{\lambda} - \lambda_{\log_2 R+1}^\sigma|$ for a arbitrary free-fermionic state $\sigma \in \mathcal{G}_{\mathrm{mixed}}$. Then, similar to Eq. (S115), we can lower bound [41]

$$\begin{aligned}\|\rho-\sigma\|_1 &\geq \left\|\mathrm{diag}(z_1^\rho,\ldots,z_R^\rho,0,\ldots,0)-\mathrm{diag}(z_1^\sigma,\ldots,z_R^\sigma,z_{R+1}^\sigma,\ldots,z_d^\sigma)\right\|_1 \\ &= \sum_{i=1}^{R}|z_i^\rho - z_i^\sigma| + \sum_{i=R+1}^{d} z_i^\sigma \geq 1 - \sum_{i=1}^{R} z_i^\sigma + \sum_{i=R+1}^{d} z_i^\sigma = 2 - 2\sum_{i=1}^{R} z_i^\sigma\,,\end{aligned} \tag{S122}$$

where z_i^σ are the non-increasingly ordered eigenvalues of σ. We also have that

$$\sum_{i=1}^{R} z_i =: \|\sigma\|_{\mathrm{KF},R} \tag{S123}$$

is a Ky Fan norm of σ. In the eigenbasis of σ, we can define

$$\sigma = \bigotimes_{i=1}^{r+1} \frac{1-\lambda_i Z_i}{2} \otimes \bigotimes_{i=r+2}^{n} \frac{1-\lambda_i Z_i}{2} =: \sigma_1 \otimes \sigma_2. \tag{S124}$$

It follows that

$$\begin{aligned}\|\sigma\|_{\mathrm{KF},R} = \|\sigma_1 \otimes \sigma_2\|_{\mathrm{KF},R} = \left\|\sigma_1 \otimes \sum_{k=1}^{2^{n-r-1}} \alpha_k \left|\Psi_k\right\rangle \left\langle\Psi_k\right|\right\|_{\mathrm{KF},R} &\leq \sum_{k=1}^{2^{n-r-1}} \alpha_k \left\|\sigma_1 \otimes \left|\Psi_k\right\rangle \left\langle\Psi_k\right|\right\|_{\mathrm{KF},R} \\ \leq \sum_{k=1}^{2^{n-r-1}} \alpha_k \|\sigma_1\|_{\mathrm{KF},R} \leq \|\sigma_1\|_{\mathrm{KF},R}\end{aligned} \tag{S125}$$

where $\sigma_2 = \sum_{k=1}^{2^{n-r-1}} \alpha_k \left|\Psi_k\right\rangle \left\langle\Psi_k\right|$ is the spectral decomposition of σ_2 and we have used that $\|\rho \otimes |\Psi\rangle\langle\Psi|\|_{\mathrm{KF},R} = \|\rho\|_{\mathrm{KF},R}$ as well as the norm inequality. As such, $\|\sigma\|_{\mathrm{KF},R}$ is maximal, if σ_2 is pure, i.e., $\lambda_k = 1$ for $k > r+1$. In general, we have for any state σ'

$$\begin{aligned}\left\|\sigma' \otimes \left(\alpha \frac{\mathbb{1}+\bar{\lambda}Z}{2} + (1-\alpha)\frac{\mathbb{1}}{2}\right)\right\|_{\mathrm{KF},R} &\leq \alpha \left\|\sigma' \otimes \frac{\mathbb{1}+\bar{\lambda}Z}{2}\right\|_{\mathrm{KF},R} + (1-\alpha) \left\|\sigma' \otimes \frac{\mathbb{1}}{2}\right\|_{\mathrm{KF},R} \\ &= \alpha \left\|\sigma' \otimes \frac{\mathbb{1}+\bar{\lambda}Z}{2}\right\|_{\mathrm{KF},R} + (1-\alpha) \|\sigma'\|_{\mathrm{KF},R/2} \\ &\leq \left\|\sigma' \otimes \frac{\mathbb{1}+\bar{\lambda}Z}{2}\right\|_{\mathrm{KF},R}\end{aligned} \tag{S126}$$

where we have used that $\|\sigma' \otimes \mathbb{1}/2\|_{\mathrm{KF},R} = \|\sigma'\|_{\mathrm{KF},R/2}$ since appending the maximally mixed state doubles multiplicity of the singular values, while halving their respective value. In the last line we used that for any 2 level state ρ_2, $\|\rho_1 \otimes \rho_2\|_{\mathrm{KF},R} \geq \|\rho\|_{\mathrm{KF},R/2}$. Since $\lambda_i \leq \lambda$, we can use this procedure to upper-bound the norm of σ_1 by $\tilde{\sigma} = \bigotimes_{i=1}^{r+1} \frac{1+\bar{\lambda}Z}{2}$.

$$\begin{aligned}\|\sigma_1\|_{\mathrm{KF},R} \leq \|\tilde{\sigma}\|_{\mathrm{KF},R} &= \max_{\bar{S}\subset\{0,1\}^{r+1}, |S|=R} \sum_{s\in\bar{S}} \prod_{i=1}^{r+1} \left(\frac{1+(-1)^{s_i}\bar{\lambda}}{2}\right) \\ &= 1 - \min_{\bar{S}_c\subset\{0,1\}^{r+1}, |S_c|=2^{r+1}-R} \sum_{s\in\bar{S}} \prod_{i=1}^{r+1} \left(\frac{1+(-1)^{s_i}\bar{\lambda}}{2}\right) \\ &\leq 1 - (2^{r+1}-R) \left(\frac{1-\bar{\lambda}}{2}\right)^{r+1} \\ &\leq 1 - \frac{\left(1-\bar{\lambda}\right)^{r+1}}{2}\end{aligned} \tag{S127}$$

where we have bounded the sum by its smallest term. Therefore, we can write the following two bounds we need to optimize over for $\|\rho - \sigma\|_1$ and $\sigma \in \mathcal{G}_{\mathrm{mixed}}$

$$\begin{aligned}\|\rho - \sigma\|_1 &\geq \max_{\lambda\in[0,1]} \min\left((1-\lambda)^{r+1}, |\lambda - \bar{\lambda}|\right) \\ &= \min_{\lambda\in[0,1]} \max\left((1-\lambda)^{r+1}, |\lambda - \bar{\lambda}|\right).\end{aligned} \tag{S128}$$

We can find a lower bound for this expression by inserting a particular λ. For this we use the difference function of the two expressions $f(\lambda) = (1-\lambda)^{r+1} - (x+\bar{\lambda})$ which holds for $\lambda \in [\bar{\lambda}, 1]$ which is the area of interest. By applying Newtons method once starting with $\lambda_0 = \bar{\lambda}$, we obtain

$$\lambda_1 = \bar{\lambda} + \frac{(1-\bar{\lambda})^{r+1}}{1+(r+1)(1-\bar{\lambda})^{r}}. \tag{S129}$$

Since $f(\lambda)$ monotonously decreases and is convex on the interval, we can be sure that $\lambda_1 \leq \lambda^*$, the root of f. This means that $(1-\lambda_1)^{r+1} \geq |\lambda_1 - \bar{\lambda}|$, which allows us to conclude that

$$\|\rho - \sigma\|_1 \geq \frac{(1-\bar{\lambda})^{r+1}}{1+(r+1)(1-\bar{\lambda})^r}\,. \tag{S130}$$

In particular, we have for $\bar{\lambda} \geq 1/2$

$$1+(r+1)(1-\bar{\lambda})^r \leq 1 + \frac{r+1}{2^r} \leq 2 \tag{S131}$$

which concludes the proof. □

IV. Property testing of free-fermionic states

In this section, we address the problem of property testing free-fermionic states. Our goal is to determine whether a given quantum state ρ is close to or far from the set of all free-fermionic states $\mathcal{G}_{\text{mixed}}$. To enable an efficient testing algorithm, we must make certain assumptions about the rank of the state ρ, as we show. Assuming that ρ is pure (i.e., rank one), we present an efficient learning algorithm that relies solely on single-qubit measurements (as detailed in Subsection IV A). However, when no assumptions are made about the rank of the state ρ, we establish the general hardness of the problem. Information-theoretically, it requires $\Omega(\text{rank}(\rho))$ copies to be solved (as discussed in Subsection IV B). Moreover, we provide a matching upper bound by introducing a single-copy algorithm. This algorithm utilizes only single-copy or free-fermionic measurements and is efficient as long as $\text{rank}(\rho) = O(\text{poly}(n))$ (explored in Subsection IV C).
Similarly, we show that there is an efficient property-testing algorithm in the case when ρ is an arbitrary quantum state and the goal is to determine whether a given quantum state ρ is close to or far from the set of pure free-fermionic states $\mathcal{G}_{\text{pure}}$. We also show an information theoretic lower bound to solve the property testing problem when ρ is arbitrary and consider $\mathcal{G}_R$, that is, the set of all free-fermionic states with rank at most R. This section concludes by providing a matching upper bound for the above scenario. We formalize the property testing problem as follows

Problem 2 (Property testing of free-fermionic states)**.** *Given N copies of an unknown quantum state ρ, with the promise that it falls into one of two distinct scenarios $\varepsilon_B > \varepsilon_A \geq 0$.*

- ***Case A:*** *There exists a free-fermionic state $\sigma \in \mathcal{G}$ such that $\|\rho - \sigma\|_1 \leq \varepsilon_A$.*
- ***Case B:*** *The state ρ is ε_B-far from all free-fermionic states σ, i.e., $\min_{\sigma \in \mathcal{G}} \|\rho - \sigma\|_1 > \varepsilon_B$.*

Determine whether we are in Case A or Case B by performing arbitrary measurements on the queried copies of the state ρ.

Further restrictions on the state ρ and precise specifications regarding the set of free-fermionic states $\mathcal{G}$ considered (e.g., $\mathcal{G} = \mathcal{G}_{\text{pure}}$, $\mathcal{G} = \mathcal{G}_{\text{mixed}}$, $\mathcal{G} = \mathcal{G}_R$) must be provided as input to the problem. Before delving into more details, we establish a preliminary lemma that will be instrumental later.

Lemma 18 (Sample complexity for infinity norm approximation of the correlation matrix via Pauli measurements)**.** *Let $N \geq 16(n^4/\varepsilon_{\text{stat}}^2)\log(n^2/\delta)$ be the number of copies of an n-qubit state ρ. Through single-qubit Pauli-basis measurements, we can find a real and anti-symmetric matrix $\hat{\Gamma}$ such that, with probability at least $1-\delta$, it holds that*

$$\left\|\hat{\Gamma} - \Gamma(\rho)\right\|_\infty < \varepsilon_{\text{stat}}. \tag{S132}$$

Proof. For $j < k \in [2n]$, we estimate $[\Gamma(\rho)]_{j,k} = -\text{Tr}(i\gamma_j\gamma_k\rho)$. For each $i\gamma_j\gamma_k$, which are $M := n(2n-1)$ in total, we measure

$$N' \geq \frac{2}{\varepsilon^2}\log\left(\frac{2M}{\delta}\right) \tag{S133}$$

many copies of ρ in the Pauli basis, obtaining outcomes $\{\hat{X}_m\}_{m=1}^{N'}$, where $\hat{X}_m \in \{-1,+1\}$. Define $\hat{\Gamma}_{j,k} := \frac{1}{N'}\sum_{m=1}^{N'}\hat{X}_m$. By Hoeffding's inequality, we have

$$\Pr\left(|\hat{\Gamma}_{j,k} - [\Gamma(\rho)]_{j,k}| \geq \varepsilon\right) \leq 2\exp\left(-\frac{2N'\varepsilon^2}{(b-a)^2}\right) \tag{S134}$$

where $a := -1$ and $b := 1$. By the union bound, we have

$$\Pr\left(\forall j < k : |\hat{\Gamma}_{j,k} - [\Gamma(\rho)]_{j,k}| < \varepsilon\right) = 1 - \sum_{i<j} \Pr\left(|\hat{\Gamma}_{j,k} - [\Gamma(\rho)]_{j,k}| \geq \varepsilon\right) \geq 1 - 2M \exp\left(-\frac{N'\varepsilon^2}{2}\right). \tag{S135}$$

By using that $N' \geq \frac{2}{\varepsilon^2}\log\left(\frac{2M}{\delta}\right)$, we have that this probability is greater than $1-\delta$. The total number of measurements is $N = N'M$. Finally, employing the Gershgorin circle theorem, we have

$$\left\|\hat{\Gamma} - \Gamma(\rho)\right\|_\infty \leq 2n\varepsilon. \tag{S136}$$

By choosing $\varepsilon = \varepsilon_{\mathrm{stat}}/2n$, we can draw our conclusions. Moreover, note that by construction $\hat{\Gamma}$ is real and anti-symmetric. □

While sequentially estimating correlation matrix entries in the Pauli basis may not be the most sample-efficient, it proves convenient for experiments due to its easy implementation. Alternatively, measuring commuting observables simultaneously [42] reduces sample complexity by n but requires a slightly more intricate setup. For completeness, we present a Lemma establishing a sample complexity upper bound for estimating the correlation matrix using this refined measurement scheme. The idea is to partition observables $O^{(j,k)} := -i\gamma_j\gamma_k$ into $2n-1$ sets of commuting observables. Commuting Pauli observables can be measured simultaneously via a Clifford Gaussian measurements [42]. Notably, different Pauli observables $-i\gamma_j\gamma_k$ commute only if associated with different Majorana operators. This allows us to partition $M = (2n-1)n$ observables into $2n-1$ sets, each containing n commuting Pauli observables. We refer to Ref. [42], Appendix C, for partition details, omitted here for brevity.

Lemma 19 (Sample complexity for infinity norm approximation of the correlation matrix via commuting observables)**.** *Let $\varepsilon_{\mathrm{stat}}, \delta > 0$. Assume access to $N \geq \lceil (8n^3/\varepsilon^2_{\mathrm{stat}})\log(4n^2/\delta) \rceil$ copies of an n-qubit state ρ. Using N single-copy measurements, with probability $\geq 1-\delta$, we can construct an anti-symmetric real matrix $\hat{\Gamma}$ such that*

$$\left\|\hat{\Gamma} - \Gamma(\rho)\right\|_\infty \leq \varepsilon_{\mathrm{stat}}. \tag{S137}$$

Proof. For each of the $2n-1$ sets of commuting Pauli, find the Clifford C allowing simultaneous measurement of such observables, and measure N' copies of $C\rho C^\dagger$ in the computational basis. Note that we can choose such Clifford to be also Gaussian. This because such Clifford diagonalizes the free fermionic Hamiltonian given by the sum of the commuting Pauli, hence it can be chosen to be Gaussian. For each $A^{(j,k)}$, obtain outcomes $\{A^{(j,k)}_m\}^{N'}_{m=1}$, where $A^{(j,k)}_m \in \{-1,+1\}$. The unbiased estimators are

$$\hat{\Gamma}_{j,k} := \frac{1}{N'}\sum_{m=1}^{N'} A^{(j,k)}_m. \tag{S138}$$

Hoeffding's inequality and union bound imply

$$N' \geq \frac{2}{\varepsilon^2_{\mathrm{stat}}}\log\left(\frac{4n}{\delta}\right) \tag{S139}$$

suffices to ensure $|\hat{\Gamma}_{j,k} - \mathrm{Tr}(A^{(j,k)}\rho)| < \varepsilon_{\mathrm{stat}}$ for each $j < k \in [2n]$ with probability at least $1-\delta$. The total number of measurements needed is $N = N'(2n-1)$, concluding as in the previous lemma. □

Analogously, we get also the following by just using that $\|B\|_2 \leq 2n\max_{i,j\in[2n]}|B_{i,j}|$ for any matrix $B \in \mathbb{C}^{2n\times 2n}$.

Lemma 20 (Sample complexity for 2-norm approximation of the correlation matrix via commuting observables)**.** *Let $\varepsilon_{\mathrm{stat}}, \delta > 0$. Assume access to $N \geq \lceil (8n^3/\varepsilon^2_{\mathrm{stat}})\log(4n^2/\delta) \rceil$ copies of an n-qubit state ρ. Using N single-copy measurements, with probability $\geq 1-\delta$, we can construct an anti-symmetric real matrix $\hat{\Gamma}$ such that*

$$\left\|\hat{\Gamma} - \Gamma(\rho)\right\|_2 \leq \varepsilon_{\mathrm{stat}}. \tag{S140}$$

Algorithm 1: Property testing algorithm for pure free-fermionic states

```
Input: Error thresholds $\varepsilon_A, \varepsilon_B$, failure probability $\delta$. $N := \lceil 8(n^3/\varepsilon_{\text{stat}}^2)\log\big(4n^2/\delta\big)\rceil$ copies of the pure state $\rho$, where
    $\varepsilon_{\text{stat}} < \frac{1}{2}(\frac{\varepsilon_B^2}{2n} - 2\varepsilon_A)$. Let $\varepsilon_{\text{T}} := \frac{1}{2}\left(\frac{\varepsilon_B^2}{2n} + 2\varepsilon_A\right)$.
Output: Output either Case A or Case B.
Step 1: Estimate the entries of the correlation matrix using $N$ single-copy measurements, resulting in the estimated $2n \times 2n$ matrix $\hat{\Gamma}$;
Step 2: Find $\hat{\lambda}_{\text{min}}$, which corresponds to the smallest singular value of $\hat{\Gamma}$;
Step 3: if $\hat{\lambda}_{\text{min}} \geq 1 - \varepsilon_{\text{T}}$ then
    Output: Case A
else
    Output: Case B
```

A. Efficient testing of pure free-fermionic states

We will now show an efficient quantum learning algorithm to solve Problem 2 when ρ is a assumed to be pure, having as assumption that $\varepsilon_B, \varepsilon_A \in (0,1)$ are such that $\varepsilon_B > 2\sqrt{n\varepsilon_A}$. The proposed algorithm uses only single copies of the state ρ. The set of free-fermionic state $\mathcal{G}$ that will be considered can be either the set of all free-fermionic states $\mathcal{G}_{\text{mixed}}$ or the set of free-fermionic states restricted to the pure ones $\mathcal{G}_{\text{pure}}$. The high-level idea of the algorithm is to output A (the state is close to the free-fermionic set) if the eigenvalues of the estimated correlation matrix are all close to 1, while outputting B otherwise. We present now the following Theorem which show the correctness of the algorithm presented in Table 1.

Theorem 10 (Efficient pure free-fermionic testing)**.** *Let ρ be an n-qubit pure state. Assume $\varepsilon_B, \varepsilon_A \in (0,1)$ such that $\varepsilon_B > 2\sqrt{n\varepsilon_A}$, $\delta \in (0,1]$, and $\varepsilon_{\text{stat}} < \frac{1}{2}(\frac{\varepsilon_B^2}{2n} - 2\varepsilon_A)$. Assume that ρ is one of the two cases detailed in Problem 2, i.e., there exists a free-fermionic state $\sigma \in \mathcal{G}$ such that $\|\rho - \sigma\|_1 \leq \varepsilon_A$ or $\min_{\sigma\in\mathcal{G}} \|\rho - \sigma\|_1 > \varepsilon_B$. The set $\mathcal{G}$ considered here can be either the set of all free-fermionic states $\mathcal{G}_{\text{mixed}}$ or the set of pure free-fermionic states $\mathcal{G}_{\text{pure}}$. Then there exists a quantum learning algorithm (1) which can solve Problem 2 using $N = 8(n^3/\varepsilon_{\text{stat}}^2)\log\big(4n^2/\delta\big)$ single-copies measurements of the state ρ with a probability of success at least $1-\delta$.*

Proof. Let $\varepsilon_{\text{stat}} > 0$ be an accuracy parameter to be fixed later. By Lemma 18, with $N \geq 8(n^3/\varepsilon_{\text{stat}}^2)\log\big(4n^2/\delta\big)$, single-qubit Pauli-basis measurements we can find a matrix $\hat{\Gamma}$ such that, with probability at least $1-\delta$, it holds that $\left\|\hat{\Gamma} - \Gamma(\rho)\right\|_\infty < \varepsilon_{\text{stat}}$. This implies that for all $k \in [n]$ [41]

$$|\hat{\lambda}_k - \lambda_k| < \varepsilon_{\text{stat}}, \tag{S141}$$

where $\{\hat{\lambda}_k\}_{k=1}^n, \{\lambda_k\}_{k=1}^n$ are the normal eigenvalues of $\hat{\Gamma}$ and $\Gamma(\rho)$, respectively. We can put $\hat{\Gamma}$ in its normal form

$$\hat{\Gamma} = \hat{O}\hat{\Lambda}\hat{O}^T, \tag{S142}$$

where

$$\hat{\Lambda} = \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & \hat{\lambda}_i \\ -\hat{\lambda}_i & 0 \end{pmatrix} \tag{S143}$$

and find its eigenvalues. Our algorithm now works as follows. Let ε_{T} be a parameter to fix later. If for all $k \in [n]$, we have $\hat{\lambda}_k \geq 1 - \varepsilon_{\text{T}}$, then we output A, otherwise B. In case we output A, we need to proof that there exists a free-fermionic state σ such that $\|\rho - \sigma\|_1 \leq \varepsilon_B$. From Eq.(S141), we have that for all $k \in [2n]$

$$\lambda_k \geq \hat{\lambda}_k - \varepsilon_{\text{stat}} \geq 1 - \varepsilon_{\text{T}} - \varepsilon_{\text{stat}}. \tag{S144}$$

The anti-symmetry of the correlation matrix $\Gamma(\rho)$ implies the existence of an orthogonal matrix O such that $\Gamma(\rho) = O\Lambda O^T$, where $\Lambda = \bigoplus_{i=1}^n \begin{pmatrix} 0 & \lambda_i \\ -\lambda_i & 0 \end{pmatrix}$. Moreover, we have $\Gamma(U_O^\dagger \rho U_O) = \Lambda$, where U_O is the free-fermionic unitary associated with O. This leads to

$$\mathrm{Tr}\Big(Z_k U_O^\dagger \rho U_O\Big) = \Gamma(U_O^\dagger \rho U_O)_{2k-1,2k} = \Lambda_{2k-1,2k} = \lambda_k. \tag{S145}$$

Consequently, we obtain

$$\mathrm{Tr}\Big(|0\rangle\!\langle 0|_k\, U_O^\dagger \rho U_O\Big) \geq \frac{1+\lambda_k}{2} \geq 1 - \frac{\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}}}{2}, \tag{S146}$$

where we used that $|0\rangle\!\langle 0|_k = (I + Z_k)/2$. Applying the quantum union bound (Lemma 13), we deduce

$$\Big\| U_O^\dagger \rho U_O - |0^n\rangle\!\langle 0^n| \Big\|_1 \leq 2\sqrt{n\left(\frac{\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}}}{2}\right)}. \tag{S147}$$

Taking $\sigma := U_O\, |0^n\rangle\!\langle 0^n|\, U_O^\dagger$, we have successfully demonstrated the existence of a free-fermionic state σ that closely approximates ρ in terms of the one-norm distance, i.e., $\|\rho - \sigma\|_1 \leq \sqrt{2n\,(\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}})}$. To ensure the validity of this approximation, we must impose the condition

$$\sqrt{2n(\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}})} \leq \varepsilon_B, \tag{S148}$$

which constitutes the initial requirement for determining the values of ε_{T} and $\varepsilon_{\mathrm{stat}}$, which we will fix at a later stage. Let us analyze the case in which we output case B, i.e., we observe there exists $k \in [2n]$ such that $\hat{\lambda}_k < 1 - \varepsilon_{\mathrm{T}}$. In this case, from Eq. (S141), we have

$$\lambda_k \leq \hat{\lambda}_k + \varepsilon_{\mathrm{stat}} < 1 - \varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}}. \tag{S149}$$

Using Theorem 7 and Theorem 8, we establish the following inequality

$$\min_{\sigma \in \mathcal{G}} \|\rho - \sigma\|_1 \geq \frac{1 - \min\limits_{k \in [n]}(\lambda_k)}{2}, \tag{S150}$$

where $\mathcal{G}$ can represent either the set of all free-fermionic states, denoted as $\mathcal{G}_{\mathrm{mixed}}$, or the set of all pure free-fermionic states, denoted as $\mathcal{G}_{\mathrm{pure}}$. If we had considered only the set of pure free-fermionic states, the lower bound would be $1 - \min\limits_{k\in[n]} \lambda_k$, without the factor of one-half, as indicated by Lemma 7. However, Eq. (S150) holds true for both $\mathcal{G}_{\mathrm{mixed}}$ and $\mathcal{G}_{\mathrm{pure}}$. From this and Eq. (S149) we have that

$$\min_{\sigma \in \mathcal{G}} \|\rho - \sigma\|_1 \geq \frac{1 - (1 - \varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}})}{2} = \frac{\varepsilon_{\mathrm{T}} - \varepsilon_{\mathrm{stat}}}{2}. \tag{S151}$$

Therefore we impose that

$$\frac{\varepsilon_{\mathrm{T}} - \varepsilon_{\mathrm{stat}}}{2} > \varepsilon_A. \tag{S152}$$

Putting together the two inequalities in Eq. (S148) and Eq.(S152), we have

$$2\varepsilon_A + \varepsilon_{\mathrm{stat}} < \varepsilon_{\mathrm{T}} \leq \frac{\varepsilon_B^2}{2n} - \varepsilon_{\mathrm{stat}}. \tag{S153}$$

Therefore, assuming $\varepsilon_B > \sqrt{4n\varepsilon_A}$, we can choose

$$\varepsilon_{\mathrm{T}} = \frac{1}{2}(\frac{\varepsilon_B^2}{2n} + 2\varepsilon_A) \tag{S154}$$

and

$$\varepsilon_{\mathrm{stat}} < \frac{1}{2}(\frac{\varepsilon_B^2}{2n} - 2\varepsilon_A). \tag{S155}$$

□

The preceding theorem was presented under the assumption that ρ is pure, and the set of free-fermionic states considered can either be the set of all (possibly mixed) free-fermionic states $\mathcal{G}_{\mathrm{mixed}}$ or the more restricted set of all pure free-fermionic states $\mathcal{G}_{\mathrm{pure}}$. However, if we focus solely on the set of all pure free-fermionic states $\mathcal{G}_{\mathrm{pure}}$, we can establish an analogous result without assuming that ρ is pure; i.e., it can be an arbitrary quantum state. The theorem is detailed as follows, and the algorithm is the same as Algorithm 1 with slightly different accuracy parameters, as detailed below.

Theorem 11 (Efficient Pure free-fermionic testing with arbitrary input states). *Let ρ be an arbitrary n-qubit state. Assume $\varepsilon_B, \varepsilon_A \in (0,1)$ such that $\varepsilon_B > \sqrt{2n\varepsilon_A}$, $\delta \in (0,1]$, and $\varepsilon_{\text{stat}} := \frac{1}{4}(\frac{\varepsilon_B^2}{2n} - \varepsilon_A)$. Assume that ρ satisfies one of the two cases detailed in Problem 2, i.e., there exists a free-fermionic state $\sigma \in \mathcal{G}_{\text{pure}}$ such that $\|\rho - \sigma\|_1 \leq \varepsilon_A$ or $\min_{\sigma \in \mathcal{G}_{\text{pure}}} \|\rho - \sigma\|_1 > \varepsilon_B$. Then, there exists a quantum learning algorithm which, utilizing only single-copies measurements, can solve Problem 2 using $N = 8(n^3/\varepsilon_{\text{stat}}^2)\log\left(4n^2/\delta\right)$ copies of the state ρ with a probability of success at least $1 - \delta$.*

Proof. The proof is analogous to the one of the previous theorem, but instead of Eq. (S150), it utilizes Lemma 8, which has no assumptions on the state ρ and provides the inequality

$$\min_{\sigma \in \mathcal{G}_{\text{pure}}} \|\rho - \sigma\|_1 \geq 1 - \min_{k \in [n]} (\lambda_k). \tag{S156}$$

Following the same steps as before, we conclude that, assuming $\varepsilon_B > \sqrt{2n\varepsilon_A}$, we can choose $\varepsilon_{\text{T}} = \frac{1}{2}(\frac{\varepsilon_B^2}{2n} + \varepsilon_A)$ and $\varepsilon_{\text{stat}} = \frac{1}{4}(\frac{\varepsilon_B^2}{2n} - \varepsilon_A)$. Note that, throughout the proof of Theorem 10, there was no need to assume that ρ is a pure state. □

B. Hardness of testing general mixed free-fermionic states

In this section, we establish the general hardness of the free-fermionic property testing problem 2, demonstrating the necessity for $\Omega(2^n)$ copies of the state when no prior assumptions on the state and no restrictions on the set of all free-fermionic states are provided. This is a constraint in sample complexity. The core of this complexity arises from recognizing that the maximally mixed state is free-fermionic. This insight allows us to leverage the hardness of identity testing, that is, to reduce the free-fermionic testing problem to distinguishing whether the underlying state is the maximally mixed state or far from it in trace distance, which is a notoriously hard problem. The following theorem is essential in our reduction:

Theorem 12 (Hardness of identity testing ([15])). *Let $\rho \in \mathcal{S}\left(\mathbb{C}^d\right)$ be a d-dimensional quantum state. Then $0.15\frac{d}{\varepsilon^2}$ copies are necessary to test whether it is the maximally mixed state $\frac{I_d}{d}$ or $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$, with at least a $2/3$ probability of success.*

The subsequent theorem delineates the hardness of testing free-fermionic states, providing a reduction to identity testing as outlined in Algorithm 2.

Algorithm 2: Reduction of testing free-fermionic states to identity testing

```
Input: Error threshold $\varepsilon > 0$. $N := \lceil(8(36n^3/\varepsilon^2)\log\left(400n^2\right) + N_{\text{free testing}})\rceil$ copies of $\rho$, where $N_{\text{free testing}}$ is the number of
       copies sufficient to solve property testing of free-fermionic state (problem 2).
Output: Output either $\frac{I_d}{d}$ or $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$.
Step 1: Estimate the entries of the correlation matrix of $\rho$ using $8(n^3/\varepsilon_{\text{stat}}^2)\log\left(400n^2\right)$ single-copy measurements, resulting in the
    estimated $2n \times 2n$ matrix $\hat{\Gamma}$;
Step 2: if $\left\|\hat{\Gamma}\right\|_\infty > \varepsilon/2$ then
    Output: $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$.
else
    Step 3: Run the free-fermionic property testing algorithm using $N_{\text{free testing}}$ copies of $\rho$, which returns that $\rho$ is "Free-fermions" or
      "Far from free-fermions";
    if "Free-fermions" then
        Output: $\rho = \frac{I_d}{d}$.
    else
        Output: $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$.
```

Theorem 13 (Hardness of testing free-fermionic states (Problem 2)). *At least $N = \Omega(\frac{2^n}{\varepsilon_B^2})$ copies of the state ρ are necessary to solve the free-fermionic property testing problem (Problem 2) with a probability of success at least $\frac{2}{3}$. This holds when no prior assumptions about ρ are provided, and the set $\mathcal{G}$ considered is that of all free-fermionic states.*

Proof. In the following, we establish that the existence of an efficient solver for the free-fermionic testing Problem 2 (requiring $O(\text{poly}(n))$ copies of the state for resolution) implies the existence of an efficient solver for the Identity testing problem, a known hard problem (Theorem 12). Let $\varepsilon > 0$. Let ρ be an n-qubit quantum state with the promise that ρ is either the maximally mixed state $\frac{I_d}{d}$ or $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$. The reduction outlined in Table 2 commences by estimating the correlation matrix $\Gamma(\rho)$ using $8(n^3/\varepsilon_{\text{stat}}^2)\log(400n^2)$ copies of ρ, yielding a real anti-symmetric matrix $\hat{\Gamma}$ guaranteed to satisfy (due to Lemma 18) $\|\hat{\Gamma} - \Gamma(\rho)\|_\infty \leq \varepsilon_{\text{stat}}$ with at least 0.99 probability of success, where $\varepsilon_{\text{stat}}$ is a parameter to be fixed later. Our primary criterion involves assessing $\|\hat{\Gamma}\|_\infty$. If $\|\hat{\Gamma}\|_\infty > \varepsilon_{\text{T}}$ (where ε_{T} is a fixed threshold to be determined later), we output that ρ is far from the maximally mixed state, i.e., $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$; otherwise, we proceed. We aim to prove that if $\|\hat{\Gamma}\|_\infty > \varepsilon_{\text{T}}$, then ρ cannot be the maximally mixed state. This is substantiated by the inequality

$$\|\rho - \frac{I_d}{d}\|_1 \geq \|\Gamma(\rho) - \Gamma(I_d/d)\|_\infty = \|\Gamma(\rho)\|_\infty \geq \|\hat{\Gamma}\|_\infty - \varepsilon_{\text{stat}} > \varepsilon_{\text{T}} - \varepsilon_{\text{stat}}, \tag{S157}$$

where the first step utilizes the inequality in Lemma 16 and the second step the fact that $\Gamma(\frac{I_d}{d}) = 0$. By choosing $\varepsilon_{\text{T}} > \varepsilon_{\text{stat}}$, we can ensure that $\|\rho - \frac{I_d}{d}\|_1 > 0$, implying that we are not in the case where ρ corresponds to the maximally mixed state but in the other case. Subsequently, if $\|\hat{\Gamma}\|_\infty \leq \varepsilon_{\text{T}}$, we proceed to employ a free-fermionic testing solver for Problem 2 with an accuracy parameter $\varepsilon_B = \varepsilon$ and $\varepsilon_A = 0$, consuming $N_{\text{free testing}}$ copies of the state ρ. If the output indicates that the underlying state is a free-fermionic state, we output that ρ is the maximally mixed state; otherwise, if the solver outputs that the state is far from the free-fermionic set, we output that ρ is far from the maximally mixed state. To validate that we cannot be in the case that ρ is the maximally mixed state when outputting that the state is far from free-fermionic, we note that the maximally mixed state is free-fermionic, and therefore it holds that

$$\varepsilon < \min_{\sigma \in \mathcal{G}} \|\rho - \sigma\|_1 \leq \left\|\rho - \frac{I_d}{d}\right\|_1. \tag{S158}$$

Conversely, if the output of the free-fermionic testing solver indicates that the state is free-fermionic, we need to demonstrate that we cannot be in the case that $\left\|\rho - \frac{I_d}{d}\right\|_1 > \varepsilon$. This follows from the inequality

$$\|\rho - \frac{I_d}{d}\|_1 \leq \frac{1}{2}\|\Gamma(\rho)\|_1 \leq n\|\Gamma(\rho)\|_\infty \leq n\left(\left\|\hat{\Gamma} - \Gamma(\rho)\right\|_\infty + \left\|\hat{\Gamma}\right\|_\infty\right) \leq n(\varepsilon_{\text{stat}} + \varepsilon_{\text{T}}), \tag{S159}$$

where the first step uses Lemma 15, and the second step utilizes the fact that $\|\Gamma(\rho)\|_1 \leq 2n\|\Gamma(\rho)\|_\infty$. To satisfy the condition $n(\varepsilon_{\text{T}} + \varepsilon_{\text{stat}}) \leq \varepsilon$, we set $\varepsilon_{\text{stat}} = \varepsilon_{\text{T}}/2$, which implies $\varepsilon_{\text{T}} \leq 2\varepsilon/(3n)$. Consequently, choosing $\varepsilon_{\text{T}} = \varepsilon/(3n)$ is adequate to conclude the reduction. Hence, in accordance with Theorem 12, we infer that $N_{\text{free testing}}$ must satisfy $N_{\text{free testing}} = \Omega(\frac{2^n}{\varepsilon^2})$ for solving the free-fermionic testing problem with at least a $2/3$ probability of success. □

As the reader can appreciate from the proof of the hardness of Problem 2, the difficulty arises from the unknown quantum state being arbitrarily close to the maximally mixed state, which is known to be challenging to test. Therefore, a natural assumption to facilitate Problem 2 is to assume the state ρ to have at most a fixed rank. In this context, we establish a fundamental lower bound on the number of copies required to solve the free-fermionic testing problem, which depends on the rank of the quantum state.

Theorem 14 (Lower bound for free-fermionic testing of states with bounded rank). *Let $\varepsilon_B > 0$. Let ρ be a quantum state such that $\operatorname{rank}(\rho) \leq 2^r$ with $r \in [n]$. To solve the free-fermionic testing property testing (Problem 2) with at least a $2/3$ probability of success, $N = \Omega(2^r/\varepsilon_B^2)$ copies are necessary. This holds when considering the set $\mathcal{G}$ in Problem 2 corresponding to the set of all free-fermionic states $\mathcal{G}_{\text{mixed}}$.*

Proof. Choose ρ of the form $\rho = \rho_r \otimes |\chi\rangle\langle\chi|$, where $|\chi\rangle$ is a pure free-fermionic state on $(n-r)$-qubits. Moreover, impose the promise that ρ_r is either the maximally mixed state on the first r-qubits, i.e., $\rho_r = 2^{-r}I_{2^r}$, or ρ_r satisfies $\|\rho_r - 2^{-r}I_{2^r}\|_1 > \varepsilon_B$. In both cases, it is clear that ρ has at most rank 2^r. By Theorem 12, to solve this problem with at least a $2/3$ probability of success, $N = \Omega(2^r/\varepsilon_B^2)$ copies of the state ρ_r are necessary. The proof now follows the same lines as the proof of Theorem 13, but on an effective space of r qubits. □

The same lower bound applies when considering the state ρ to be an arbitrary state, while restricting the set $\mathcal{G}$ in Problem 2 to be the set of all free-fermionic states with rank at most R, denoted by $\mathcal{G}_R$.

Theorem 15 (Lower bound for free-fermionic testing with respect to the set of bounded rank free-fermionic states $\mathcal{G}_R$). *Let $\varepsilon_B > 0$. For an arbitrary quantum state ρ, if we consider $\mathcal{G}$ in Problem 2 to correspond to the set $\mathcal{G}_R$ of all free-fermionic states with rank at most $R := 2^r$, where $r \in [n]$, then to solve the free-fermionic testing property testing (Problem 2) with at least a $2/3$ probability of success, $N = \Omega(2^r/\varepsilon_B^2)$ copies are necessary.*

Proof. The proof follows the same lines as the previous theorem, and everything holds analogously, even with the assumption that the set to be considered is $\mathcal{G}_R$ instead of $\mathcal{G}_{\text{mixed}}$. □

C. Efficient testing of low-rank free-fermionic states

In the preceding subsection, we established information-theoretic lower bounds for solving the free-fermionic property testing problem. Specifically, we demonstrated that when the input n-qubit state ρ has a rank less than or equal to 2^r, where $r \in [n]$, a minimum of $\Omega(2^r)$ copies is required. Similarly, when no assumptions are made about ρ, but $\mathcal{G}$ in Problem 2 corresponds to the set $\mathcal{G}_R$ of all free-fermionic states with rank at most $R := 2^r$, then $N = \Omega(2^r)$ copies are necessary.
Now, we address the question of whether an algorithm can match these information-theoretic lower bounds. We notice that if $r = O(\log(n))$, i.e., $R = O(\mathrm{poly}(n))$, then such an algorithm would be efficient. The following theorem provides an affirmative answer to this question.

Theorem 16 (Upper bound for free-fermionic testing with respect to the set of bounded rank free-fermionic states $\mathcal{G}_R$). *Let ρ be any n-qubit state. Assume error thresholds $\varepsilon_B, \varepsilon_A \in (0,1)$ such that*

$$\varepsilon_B > \sqrt{2^5(n-r)\varepsilon_A}, \tag{S160}$$

and consider a failure probability $\delta \in (0,1]$. Suppose ρ falls into one of two cases in Problem 2: either there exists a free-fermionic state $\sigma \in \mathcal{G}_R$ with $\|\rho - \sigma\|_1 \le \varepsilon_A$ (Case A), or $\min_{\sigma\in\mathcal{G}_R} \|\rho-\sigma\|_1 > \varepsilon_B$ (Case B), where $R := 2^r$ with $r \in [n]$.
Then, a quantum learning algorithm (Algorithm 3) can solve Problem 2 using

$$N := \lceil 8(n^3/\varepsilon_{\mathrm{stat}}^2)\log\left(8n^2/\delta\right) + N_{\mathrm{tom}}(\varepsilon_{\mathrm{tom}}, \delta/2, r)\rceil \tag{S161}$$

copies of the state ρ with a success probability at least $1-\delta$. Here, $N_{\mathrm{tom}}(\varepsilon_{\mathrm{tom}}, \delta/2, r)$ is the number of copies sufficient for a full state tomography algorithm (e.g., [43]) of an r-qubit state with accuracy $\varepsilon_{\mathrm{tom}}$ and failure probability at most $\delta/2$. Here, $\varepsilon_{\mathrm{stat}} < \frac{1}{2}\left(\frac{\varepsilon_B^2}{2^5(n-r)} - \varepsilon_A\right)$ and $\varepsilon_{\mathrm{tom}} := \frac{1}{2}(\frac{\varepsilon_B}{2} - \varepsilon_A)$.

Algorithm 3: Property testing algorithm for bounded rank free-fermionic states

```
Input: Let $R = 2^r$, with $r \in [n]$. Error thresholds $\varepsilon_A, \varepsilon_B$ such that $\varepsilon_B > \sqrt{2^5(n-r)\varepsilon_A}$, failure probability $\delta$.
    $N := \lceil 8(n^3/\varepsilon_{\mathrm{stat}}^2)\log(8n^2/\delta) + N_{\mathrm{tom}}(\varepsilon_{\mathrm{tom}}, \delta/2, r)\rceil$ copies of $\rho$. Here, $N_{\mathrm{tom}}(\varepsilon_{\mathrm{tom}}, \delta/2, r)$ is the number of copies sufficient
    for full state tomography of an $r$-qubit state with accuracy $\varepsilon_{\mathrm{tom}}$ and failure probability at most $\delta/2$. Let
    $\varepsilon_{\mathrm{stat}} < \frac{1}{2}\left(\frac{\varepsilon_B^2}{2^5(n-r)} - \varepsilon_A\right)$, $\varepsilon_{\mathrm{T}} > (\varepsilon_{\mathrm{stat}} + \varepsilon_A)$, $\varepsilon_{\mathrm{tom}} := \frac{1}{2}(\frac{\varepsilon_B}{2} - \varepsilon_A)$ and $\varepsilon_{\mathrm{T},2} \le \frac{1}{2}(\frac{\varepsilon_B}{2} + \varepsilon_A)$.
Output: Output either Case A or Case B.
Step 1: Estimate the entries of the correlation matrix of $\rho$ using $\lceil 8(n^3/\varepsilon_{\mathrm{stat}}^2)\log(8n^2/\delta)\rceil$ single-qubit measurements, resulting in the
  matrix $\hat{\Gamma}$ ;
Step 2: Find $\hat{\lambda}_{r+1}$, the $(r+1)$-th smallest singular value of $\hat{\Gamma}$ ;
Step 3: if $\hat{\lambda}_{r+1} \le 1 - \varepsilon_{\mathrm{T}}$ then
    Output: Case B
else
    Step 4: Evolve $\rho$ with the free-fermionic unitary $U_{\hat{O}}$, where $\hat{O}$ is the orthogonal matrix that puts $\hat{\Gamma}$ in its normal form. ;
    Step 5: Full state tomography on the first $r$ qubits of $U_{\hat{O}}\rho U_{\hat{O}}^{\dagger}$, which returns the state $\hat{\rho}_r'$ with correlation matrix $\Gamma_r$;
    Output: Case B if $\|\hat{\rho}_r' - \sigma(\hat{\Gamma}_r)\| > \varepsilon_{\mathrm{T},2}$, else Case A. Here, $\sigma(\hat{\Gamma}_r)$ is the free-fermionic state associated with the correlation
      matrix $\hat{\Gamma}_r$ of $\hat{\rho}_r'$.
```

Proof. Let $\varepsilon_{\mathrm{stat}}$ be an accuracy parameter, yet to be determined. According to Lemma 18, with $N \ge 8(n^3\varepsilon_{\mathrm{stat}}^2)\log\left(8n^2/\delta\right)$ single-qubit measurements, we can construct a matrix $\hat{\Gamma}$ such that, with a probability of at least $1-\delta/2$, it satisfies $\|\hat{\Gamma} - \Gamma(\rho)\|_\infty < \varepsilon_{\mathrm{stat}}$. Consequently, for each sorted (normal) eigenvalue λ_k of the correlation matrix, it holds that $|\hat{\lambda}_k - \lambda_k| < \varepsilon_{\mathrm{stat}}$, where $\hat{\lambda}_k$ is the k-th eigenvalue of $\hat{\Gamma}$. Now, consider that if ρ were a free-fermionic state with rank bounded by R, the first r eigenvalues could potentially be less than one, while the remaining $n-r$ should be one (as per Lemma 2). We proceed to perform our first check. If $\hat{\lambda}_{r+1} \ge 1 - \varepsilon_{\mathrm{T}}$, we continue; otherwise, we output B, where $\varepsilon_{\mathrm{T}} > 0$ is an error threshold to be fixed later. In case we output B, let us demonstrate that we cannot be in case A. We need to show that $\min_{\sigma\in\mathcal{G}_R}\|\rho-\sigma\|_1 > \varepsilon_A$. We have

$$\min_{\sigma\in\mathcal{G}_R}\|\rho-\sigma\|_1 \ge 1 - \lambda_{r+1} \ge 1 - \hat{\lambda}_{r+1} - \varepsilon_{\mathrm{stat}} > \varepsilon_{\mathrm{T}} - \varepsilon_{\mathrm{stat}}, \tag{S162}$$

where the first inequality follows from Theorem 7. Therefore, by choosing

$$\varepsilon_{\mathrm{T}} - \varepsilon_{\mathrm{stat}} > \varepsilon_A, \tag{S163}$$

we successfully ensure that ρ cannot be in case A. This condition forms the first criterion for determining the accuracy parameter $\varepsilon_{\mathrm{stat}}$ and the threshold ε_{T}. To proceed, we define $\hat{O}$ as the orthogonal matrix such that $\hat{O}\hat{\Gamma}\hat{O}^T = \hat{\Lambda}$, where

$$\hat{\Lambda} := \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & \hat{\lambda}_k \\ -\hat{\lambda}_k & 0 \end{pmatrix} \tag{S164}$$

and define $U_{\hat{O}}$ as the associated free-fermionic unitary. Consider the state $\rho' := U_{\hat{O}}\rho U_{\hat{O}}^{\dagger}$. We observe that

$$|\Gamma(\rho')_{j,k} - (\hat{\Lambda})_{j,k}| \leq \|\Gamma(\rho') - \hat{\Lambda}\|_\infty \leq \|\Gamma(\rho) - \hat{\Gamma}\|_\infty \leq \varepsilon_{\mathrm{stat}}, \tag{S165}$$

leveraging the relationships $\Gamma(\rho') = \hat{O}\Gamma(\rho)\hat{O}^T$ and $\hat{\Lambda} = \hat{O}\hat{\Gamma}\hat{O}^T$, Cauchy-Schwartz, and the definition of the infinity norm. Consequently, we establish $\Gamma(\rho')_{j,k} \geq (\hat{\Lambda})_{j,k} - \varepsilon_{\mathrm{stat}}$. Specifically, for $k \geq r+1$, we find:

$$\mathrm{Tr}(Z_k\rho') = \Gamma(\rho')_{2k-1,k} \geq (\hat{\Lambda})_{2k-1,2k} - \varepsilon_{\mathrm{stat}} = \hat{\lambda}_k - \varepsilon_{\mathrm{stat}} \geq 1 - \varepsilon_{\mathrm{T}} - \varepsilon_{\mathrm{stat}}, \tag{S166}$$

where $Z_k = -i\gamma_{2k-1}\gamma_{2k}$ represents the Z-Pauli operator acting on the k-th qubit. Consequently, we also find $\mathrm{Tr}(|0\rangle\langle 0|_k\, \rho') \geq 1 - (\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}})/2$. Employing Lemma 13, we derive:

$$\left\|\rho' - \phi \otimes |0^{n-r}\rangle\langle 0^{n-r}|\right\|_1 \leq 2\sqrt{(n-r)(\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}})/2}, \tag{S167}$$

where $\phi\otimes|0^{n-r}\rangle\langle 0^{n-r}|$ represents the post-measurement state obtained after measuring the outcomes corresponding to $|0^{n-r}\rangle$ in the last $n-r$ qubits. Define the subsystem E with sites $E = [r+1, \ldots, n]$ and define

$$\rho'_r := \mathrm{tr}_E[\rho'] = \mathrm{tr}_E[U_{\hat{O}}\rho U_{\hat{O}}^{\dagger}]. \tag{S168}$$

We also have

$$\begin{aligned} \left\|\rho' - \rho'_r \otimes |0^{n-r}\rangle\langle 0^{n-r}|\right\|_1 &\leq \left\|\rho' - \phi \otimes |0^{n-r}\rangle\langle 0^{n-r}|\right\|_1 + \|\phi - \rho'_r\|_1 \\ &\leq \left\|\rho' - \phi \otimes |0^{n-r}\rangle\langle 0^{n-r}|\right\|_1 + \left\|\phi \otimes |0^{n-r}\rangle\langle 0^{n-r}| - \rho'\right\|_1 \\ &\leq 4\sqrt{(n-r)(\varepsilon_{\mathrm{T}} + \varepsilon_{\mathrm{stat}})/2}, \end{aligned} \tag{S169}$$

where in the first step, we used the triangle inequality, in the second step, the data-processing inequality ($\|\,\mathrm{tr}_E(\rho - \sigma)\|_1 \leq \|\rho - \sigma\|_1$ for any quantum states ρ, σ), and in the last step, we used Eq.(S167). We now perform full-state tomography on the first r qubits of ρ'. More precisely, using copies of ρ'_r, we can output a state $\hat{\rho}'_r$ such that, with a probability of at least $1 - \delta/2$, we find that

$$\|\hat{\rho}'_r - \rho'_r\|_1 \leq \varepsilon_{\mathrm{tom}}. \tag{S170}$$

There are various algorithms for full-state tomography that utilize single-copy measurements (see, e.g., Ref. [43]), all having sample complexity that scales exponentially with the number of qubits constituting the quantum state, in our case, r. Furthermore, through the computation of the correlation matrix of $\hat{\rho}'_r$, we can compute its correlation matrix $\hat{\Gamma}_r$, which satisfies

$$\left\|\hat{\Gamma}_r - \Gamma(\rho'_r)\right\|_\infty \leq \|\hat{\rho}'_r - \rho'_r\|_1 \leq \varepsilon_{\mathrm{tom}}, \tag{S171}$$

where we have invoked Lemma 16. Now, let us consider the free-fermionic state $\sigma(\hat{\Gamma}_r)$ associated with the correlation matrix $\hat{\Gamma}_r$. Our second discrimination test hinges on the quantity $\left\|\hat{\rho}'_r - \sigma(\hat{\Gamma}_r)\right\|_1$, which can be computed with a time complexity scaling as $O(\exp(r))$, which is efficient as long as the rank of ρ is $O(\mathrm{poly}(n))$. If $\left\|\hat{\rho}'_r - \sigma(\hat{\Gamma}_r)\right\|_1 \leq \varepsilon_{\mathrm{T},2}$, we output A; otherwise, we output B. In the case of outputting A, our goal is to demonstrate that we cannot be in case B. Specifically, we show that there exist a free-fermionic state closer, in trace distance, than ε_B to ρ. Consider the free-fermionic state

$U_{\hat{O}}^{\dagger}\left(\sigma(\hat{\Gamma}_r)\otimes|0^{n-r}\rangle\langle 0^{n-r}|\right)U_{\hat{O}}$, which is readily free-fermionic. We have

$$\begin{aligned}&\left\|\rho-U_{\hat{O}}^{\dagger}\left(\sigma(\hat{\Gamma}_r)\otimes|0^{n-r}\rangle\langle 0^{n-r}|\right)U_{\hat{O}}\right\|_1\\&=\left\|\rho'-\sigma(\hat{\Gamma}_r)\otimes|0^{n-r}\rangle\langle 0^{n-r}|\right\|_1\\&\le\|\rho'-\rho'_r\otimes|0^{n-r}\rangle\langle 0^{n-r}|\|_1+\left\|\rho'_r-\sigma(\hat{\Gamma}_r)\right\|_1\\&\le\|\rho'-\rho'_r\otimes|0^{n-r}\rangle\langle 0^{n-r}|\|_1+\|\rho'_r-\hat{\rho}'_r\|_1+\left\|\hat{\rho}'_r-\sigma(\hat{\Gamma}_r)\right\|_1\\&\le 4\sqrt{(n-r)(\epsilon_{\mathrm{T}}+\epsilon_{\mathrm{stat}})/2}+\epsilon_{\mathrm{tom}}+\varepsilon_{\mathrm{T},2},\end{aligned}\tag{S172}$$

where in the first inequality, we used the unitary invariance of the trace norm; in the second and third steps, we applied the triangle inequality; and in the last step, we used the previously derived bound. Now, we must ensure

$$4\sqrt{(n-r)(\epsilon_{\mathrm{T}}+\epsilon_{\mathrm{stat}})/2}+\epsilon_{\mathrm{tom}}+\varepsilon_{\mathrm{T},2}\le\varepsilon_B.\tag{S173}$$

Now, let us explore the scenario where we output case B. Considering that the application of a free-fermionic unitary $U_{\hat{O}}$ and the partial trace map a free-fermionic state into another free-fermionic state [3], we employ the data processing inequality, leading to the inequality

$$\min_{\sigma\in\mathcal{G}_R}\|\rho-\sigma\|_1=\min_{\sigma\in\mathcal{G}_R}\|\rho'-\sigma\|\ge\min_{\sigma_R\in\mathcal{G}_R}\|\rho_R-\sigma_R\|.\tag{S174}$$

Now, let us demonstrate that if $\|\hat{\rho}'_R-\sigma(\hat{\Gamma}_R)\|>\varepsilon_{\mathrm{T},2}$, we cannot be in case A. To establish this, let us first express the lower bounds

$$\|\rho'_R-\sigma_R\|_1\ge\begin{cases}\left\|\hat{\Gamma}_R-\Gamma(\sigma_R)\right\|_\infty-\varepsilon_{\mathrm{tom}}\\\left\|\hat{\rho}'_R-\sigma(\hat{\Gamma}_R)\right\|_1-\varepsilon_{\mathrm{tom}}-\alpha\left\|\hat{\Gamma}_R-\Gamma(\sigma_R)\right\|_\infty^{1/2}\end{cases},\tag{S175}$$

where, for the first bound, we utilize Lemma 16 and the triangle inequality, namely

$$\|\rho'_R-\sigma_R\|_1\ge\|\Gamma(\rho'_R)-\Gamma(\sigma_R)\|_\infty\ge\left\|\hat{\Gamma}_R-\Gamma(\sigma_R)\right\|_\infty-\varepsilon_{\mathrm{tom}},\tag{S176}$$

and for the second bound, by utilizing Theorem 6 and triangle inequality, we have

$$\begin{aligned}\|\rho'_R-\sigma_R\|_1&\ge\|\rho'_r-\sigma(\hat{\Gamma}_R)\|_1-\|\sigma(\hat{\Gamma}_R)-\sigma_R\|_1\\&\ge\|\rho'_R-\sigma(\hat{\Gamma}_R)\|_1-\alpha\|\hat{\Gamma}_R-\Gamma(\sigma_R)\|_\infty^{1/2},\end{aligned}\tag{S177}$$

with $\alpha:=2\sqrt{n}$. Our objective is to optimize and find the threshold corresponding to a universal lower bound. To achieve this, we solve the equation

$$\left\|\hat{\rho}'_R-\sigma(\hat{\Gamma}_R)\right\|_1-\varepsilon_{\mathrm{tom}}-\alpha\left\|\hat{\Gamma}_R-\Gamma(\sigma_R)\right\|_\infty^{1/2}=\left\|\hat{\Gamma}_R-\Gamma(\sigma_R)\right\|_\infty-\varepsilon_{\mathrm{tom}},\tag{S178}$$

for $\|\hat{\Gamma}_R-\Gamma(\sigma_R)\|_\infty$. Let $y:=\|\hat{\Gamma}_R-\Gamma(\sigma_R)\|_\infty^{1/2}$ and $b:=\|\hat{\rho}'_R-\sigma(\hat{\Gamma}_R)\|_1$. Solving such equation reduces to solving $y^2+\alpha y-b=0$. Substituting the solution in the previous inequality, we obtain

$$\begin{aligned}\min_{\sigma_R\in\mathcal{G}_R}\|\rho'_R-\sigma_R\|_1&\ge\|\rho'_R-\sigma(\hat{\Gamma}_R)\|_1-2\sqrt{n}(\sqrt{n+\|\rho'_R-\sigma(\hat{\Gamma}_R)\|_1}-\sqrt{n})-\varepsilon_{\mathrm{tom}}\\&\ge\|\rho'_R-\sigma(\hat{\Gamma}_R)\|_1-\frac{1}{6n}\|\rho'_R-\sigma(\hat{\Gamma}_R)\|_1^2-\varepsilon_{\mathrm{tom}}\end{aligned}\tag{S179}$$

where we have used the inequality $\sqrt{1+x}\le 1+\frac{x}{2}-\frac{x^2}{32}$ valid for $x\in[0,8]$. Now, we only need to impose that, given $\left\|\hat{\rho}'_R-\sigma(\hat{\Gamma}_R)\right\|_1>\varepsilon_{\mathrm{T},2}$, we cannot be in case A and, therefore, impose

$$\varepsilon_{T,2}-\frac{\varepsilon_{T,2}^2}{6n}-\varepsilon_{\mathrm{tom}}>\varepsilon_A.\tag{S180}$$

To satisfy the constraints in Eq. (S163), (S173), and (S180), we need to choose the constants $\varepsilon_{\mathrm{stat}}$, ε_{T}, $\varepsilon_{\mathrm{tom}}$, and $\varepsilon_{\mathrm{T},2}$. We start by imposing the two inequalities (which implies Eq. (S173))

$$4\sqrt{(n-r)(\epsilon_{\mathrm{T}}+\epsilon_{\mathrm{stat}})/2} \leq \frac{\varepsilon_B}{2}, \tag{S181}$$

$$\epsilon_{\mathrm{tom}}+\varepsilon_{\mathrm{T},2} \leq \frac{\varepsilon_B}{2}. \tag{S182}$$

Therefore, we have "disentangled" the three inequalities in Eq. (S163), (S173), and (S180) into two systems of two inequalities, the first containing stat and ϵ_{T} involving Eq. (S163) and (S181), and the other one containing ϵ_{tom} and $\varepsilon_{\mathrm{T},2}$ involving Eq. (S180) and (S182). By solving the one involving Eq. (S163) and (S181), we get

$$\varepsilon_{\mathrm{T}} > (\varepsilon_{\mathrm{stat}}+\varepsilon_A), \tag{S183}$$

$$\varepsilon_{\mathrm{stat}} < \frac{1}{2}\left(\frac{\varepsilon_B^2}{2^5(n-r)}-\varepsilon_A\right). \tag{S184}$$

Moreover, by solving the one involving Eq. (S180) and (S182), we get

$$\epsilon_{\mathrm{tom}} \leq \frac{\varepsilon_B}{2}-\varepsilon_{\mathrm{T},2}, \tag{S185}$$

$$\varepsilon_{\mathrm{T},2} \leq 6n\left(1-\sqrt{1-\frac{\frac{\varepsilon_B}{2}+\varepsilon_A}{6n}}\right). \tag{S186}$$

The latter inequality is satisfied by choosing $\varepsilon_{\mathrm{T},2} \leq \frac{1}{2}(\frac{\varepsilon_B}{2}+\varepsilon_A)$, which implies

$$\epsilon_{\mathrm{tom}} \leq \frac{1}{2}\left(\frac{\varepsilon_B}{2}-\varepsilon_A\right). \tag{S187}$$

By union bound, the total failure probability of the protocol is at most $1-\delta$. □

The previous theorem was presented under the assumption that ρ is an arbitrary n-qubit state, and the set of free-fermionic states considered is $\mathcal{G}_R$, i.e., the set of free-fermionic states with rank at most $R=2^r$, where $r\in[n]$. However, if we assume that ρ has at most rank R, then we can consider the largest set $\mathcal{G}_{\mathrm{mixed}}$, and we can establish an analogous result. The theorem is detailed as follows, and the algorithm is the same as Algorithm 3 with slightly different accuracy parameters, as detailed below.

Theorem 17 (Upper bound for free-fermionic testing for a bounded rank quantum state). *Let ρ be any n-qubit state with rank at most 2^r, where $r\in[n]$. Assume error thresholds $\varepsilon_B,\varepsilon_A\in(0,1)$ such that $\varepsilon_B>\sqrt{2^5(n-r)(2\varepsilon_A)^{1/(r+1)}}$, and consider a failure probability $\delta\in(0,1]$. Suppose ρ falls into one of two cases in Problem 2: either there exists a free-fermionic state $\sigma\in\mathcal{G}_{\mathrm{mixed}}$ with $\|\rho-\sigma\|_1\leq\varepsilon_A$ (Case A), or $\min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}}\|\rho-\sigma\|_1>\varepsilon_B$ (Case B). Then, a quantum learning algorithm (Algorithm 3) can solve Problem 2 using*

$$N := \lceil 8(n^3/\varepsilon_{\mathrm{stat}}^2)\log(8n^2/\delta)+N_{\mathrm{tom}}(\varepsilon_{\mathrm{tom}},\delta/2,r)\rceil$$

copies of the state ρ with a success probability at least $1-\delta$. Here, $N_{\mathrm{tom}}(\varepsilon_{\mathrm{tom}},\delta/2,r)$ is the number of copies sufficient for a full state tomography algorithm (see, e.g., Ref. [43]) of an r-qubit state with accuracy $\varepsilon_{\mathrm{tom}}$ and failure probability at most $\delta/2$. Here, we impose

$$\varepsilon_{\mathrm{T}} > (\varepsilon_{\mathrm{stat}}+(2\varepsilon_A)^{\frac{1}{r+1}}), \tag{S188}$$

$$\varepsilon_{\mathrm{stat}} < \frac{1}{2}\left(\frac{\varepsilon_B^2}{2^5(n-r)}-(2\varepsilon_A)^{\frac{1}{r+1}}\right), \tag{S189}$$

$$\varepsilon_{\mathrm{T},2} \leq \frac{1}{2}(\frac{\varepsilon_B}{2}+\varepsilon_A), \tag{S190}$$

$$\epsilon_{\mathrm{tom}} \leq \frac{1}{2}\left(\frac{\varepsilon_B}{2}-\varepsilon_A\right) \tag{S191}$$

Proof. The proof is the same as the one of the previous theorem, but this time we have utilized instead of Eq.(S162) the expression

$$\min_{\sigma\in\mathcal{G}_{\mathrm{mixed}}}\|\rho-\sigma\|_1 \geq \frac{1}{2}(1-\lambda_{r+1})^{r+1}, \tag{S192}$$

which follows from Lemma 9. From this, it follows that (using the same notation as in the previous proof)

$$\min_{\sigma\in\mathcal{G}_{\text{mixed}}} \|\rho-\sigma\|_1 > \frac{1}{2}(\varepsilon_{\text{stat}}-\varepsilon_{\text{T}})^{r+1}. \tag{S193}$$

Hence, we have the condition

$$(\varepsilon_{\text{T}}-\varepsilon_{\text{stat}})^{r+1} > 2\varepsilon_A. \tag{S194}$$

This is the only condition that is different from the ones in the previous Theorem. We impose

$$\begin{aligned}
\varepsilon_{\text{T}} &> (\varepsilon_{\text{stat}} + (2\varepsilon_A)^{\frac{1}{r+1}}), && \text{(S195)}\\
\varepsilon_{\text{stat}} &< \frac{1}{2}\left(\frac{\varepsilon_B^2}{2^5(n-r)} - (2\varepsilon_A)^{\frac{1}{r+1}}\right), && \text{(S196)}\\
\varepsilon_{\text{T},2} &\le \frac{1}{2}(\frac{\varepsilon_B}{2} + \varepsilon_A), && \text{(S197)}\\
\epsilon_{\text{tom}} &\le \frac{1}{2}\left(\frac{\varepsilon_B}{2} - \varepsilon_A\right) && \text{(S198)}
\end{aligned}$$

and this suffices to satisfy all the constraints. □

V. Efficient tomography of mixed free-fermionic states and improved pure states tomography

In this section, we present an algorithm for learning n-qubit mixed free-fermionic states in trace distance. The algorithm is efficient in terms of samples, time, and memory, and is a straightforward consequence of Lemma 6, which establishes a relationship between the trace distance of mixed free-fermionic states and the one-norm difference of their correlation matrices. It is worth noting that previous works have provided sample complexity bounds to learn free-fermionic states [11, 16, 17] (in parts by the same authors), but they are limited to the pure case scenario. Moreover, we improve over their sample complexity for the pure case scenario as well.

Algorithm 4: Learning mixed free-fermionic states

```
Input: Error threshold $\varepsilon > 0$, failure probability $\delta > 0$. $N = \lceil 128(n^5/\varepsilon^4)\log(4n^2/\delta)\rceil$ copies of the mixed free-fermionic state $\rho$.
Output: A classical description of a state $\hat{\rho}$, such that $\|\hat{\rho}-\rho\|_1 \le \varepsilon$ with at least $1-\delta$ success probability.
Step 1: Estimate the entries of the correlation matrix of $\rho$ using $N$ single-copy measurements, resulting in the estimated $2n \times 2n$ matrix $\hat{\Gamma}$;
Step 2: Put $\hat{\Gamma}$ in its normal form $\hat{\Gamma} = \hat{O}\hat{\Lambda}\hat{O}^T$, where $\hat{O} \in \mathrm{O}(2n)$, and $\hat{\Lambda}$ is the matrix determined by the normal eigenvalues $\{\hat{\lambda}_j\}_{j=1}^n$. ;
return $\hat{O}$ and $\{\hat{\lambda}_i\}_{i=1}^n$, so that $\hat{\rho} := G_{\hat{O}}\left(\bigotimes_{j=1}^n \frac{I+\hat{\lambda}_j Z_j}{2}\right)G_{\hat{O}}^\dagger$, where $G_{\hat{O}}$ is the free-fermionic unitary associated with $\hat{O}$.
```

Theorem 18 (Tomography of free-fermionic mixed states). *Let ρ be a free-fermionic state. For $\varepsilon \in (0,1)$ and $\delta \in (0,1]$, there exists a quantum learning algorithm (outlined in table 4) that, utilizing $N = \lceil 128(n^5/\varepsilon^4)\log(4n^2/\delta)\rceil$ single-copies of the state ρ learns an efficient representation of a state $\hat{\rho}$ such that:*

$$\|\hat{\rho}-\rho\|_1 \le \varepsilon, \tag{S199}$$

with a probability of success at least $1-\delta$.

Proof. Let $\varepsilon_{\text{stat}} > 0$ be an accuracy parameter to be fixed later. By Lemma 19, with $N \ge 8(n^3/\varepsilon_{\text{stat}}^2)\log(4n^2/\delta)$ copies of the state, we can find a matrix $\hat{\Gamma}$ such that, with probability at least $1-\delta$, it holds that $\left\|\hat{\Gamma}-\Gamma(\rho)\right\|_\infty < \varepsilon_{\text{stat}}$. Since $\hat{\Gamma}$ is a valid correlation matrix, i.e., it is real-anti-symmetric and has normal eigenvalues in absolute value less than or equal to one, it corresponds to a free-fermionic state $\hat{\rho}$ (due to Lemma 6). Therefore, the matrix $\Gamma(\hat{\rho}) := \hat{\Gamma}$ fully identifies the free-fermionic state $\hat{\rho}$. In particular, $\hat{\Gamma}$ can be expressed in its normal form $\hat{\Gamma} = \hat{O}\hat{\Lambda}\hat{O}^T$, where $\hat{O} \in \mathrm{O}(2n)$, and $\hat{\Lambda} = \bigoplus_{k=1}^n \begin{pmatrix} 0 & \hat{\lambda}_k \\ -\hat{\lambda}_k & 0 \end{pmatrix}$, and $\hat{\rho}$ assumes the form

$$\hat{\rho} := G_{\hat{O}}\left(\bigotimes_{j=1}^n \frac{I+\hat{\lambda}_j Z_j}{2}\right)G_{\hat{O}}^\dagger, \tag{S200}$$

where $G_{\hat{O}}$ is the free-fermionic unitary associated with $\hat{O}$. By Theorem 6, we have

$$\|\hat{\rho}-\rho\|_1 \leq 2\sqrt{n\|\Gamma(\hat{\rho})-\Gamma(\rho)\|_\infty}. \tag{S201}$$

By choosing $\varepsilon_{\text{stat}} = \varepsilon^2/(4n)$, we can conclude. □

Corollary 2 (Tomography of free-fermionic states via single Pauli measurements). *Let ρ be a free-fermionic quantum state. For $\varepsilon \in (0,1)$ and $\delta \in (0,1]$ there exist a learning algorithm that utilize $N = 256(n^6/\varepsilon^4)\log\left(4n^2/\delta\right)$ copies of the state and only single-qubit Pauli measurements to learn an efficient classical representation $\hat{\rho}$ of the state ρ obeying $\|\rho-\hat{\rho}\|_1 \leq \varepsilon$.*

Proof. The proof follows identically to that of Theorem 18. The only difference lies in the estimation of the correlation matrix $\hat{\Gamma}$, which, if estimated through single-qubit Pauli measurements, requires $N = 16(n^4/\varepsilon^2_{\text{stat}})\log\left(4n^2/\delta\right)$ copies of the state ρ, as detailed in Lemma 18. □

We now show also the following improved learning algorithm for pure free-fermionic states, which is a direct implication of Lemma 20 and our novel inequality valid for pure Gaussian states (Theorem 5):

Proposition 2 (Tomography of pure free-fermionic states). *Let ψ be a free-fermionic quantum state. For $\varepsilon \in (0,1)$ and $\delta \in (0,1]$ there exist a learning algorithm that utilize $N = 32(n^3/\varepsilon^2)\log\left(4n^2/\delta\right)$ copies of the state and only single-copies measurements to learn an efficient classical representation of the state $\hat{\psi}$ obeying $\|\psi-\hat{\psi}\|_1 \leq \varepsilon$.*

Efficient learning of quantum states prepared with few fermionic non-Gaussian gates

Antonio Anna Mele[1, *] and Yaroslav Herasymenko[2, 3, 4, †]

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[2] *QuSoft and CWI, Science Park 123, 1098 XG Amsterdam, The Netherlands*
[3] *QuTech, TU Delft, P.O. Box 5046, 2600 GA Delft, The Netherlands*
[4] *Delft Institute of Applied Mathematics, TU Delft, 2628 CD Delft, The Netherlands*

(Dated: March 1, 2024)

The experimental realization of increasingly complex quantum states underscores the pressing need for new methods of state learning and verification. In one such framework, quantum state tomography, the aim is to learn the full quantum state from data obtained by measurements. Without prior assumptions on the state, this task is prohibitively hard. Here, we present an efficient algorithm for learning states on n fermion modes prepared by any number of Gaussian and at most t non-Gaussian gates. By Jordan-Wigner mapping, this also includes n-qubit states prepared by nearest-neighbour matchgate circuits with at most t SWAP-gates. Our algorithm is based exclusively on single-copy measurements and produces a classical representation of a state, guaranteed to be close in trace distance to the target state. The sample and time complexity of our algorithm is $\mathrm{poly}(n, 2^t)$; thus if $t = \mathcal{O}(\log(n))$, it is efficient. We also show that, if t scales *slightly* more than logarithmically, any learning algorithm to solve the same task must be inefficient, under common cryptographic assumptions. We also provide an efficient property testing algorithm that, given access to copies of a state, determines whether such state is far or close to the set of states for which our learning algorithm works. Beyond tomography, our work sheds light on the structure of states prepared with few non-Gaussian gates and offers an improved upper bound on their circuit complexity.

Introduction

Quantum state tomography is the task of reconstructing a classical description of a quantum state from experimental data [1, 2]. Beyond its foundational significance in quantum information theory, it stands as the gold standard for verification and benchmarking of quantum devices [2]. However, in the absence of any prior assumptions on the state to be learned, one encounters necessarily the *curse of dimensionality* of the Hilbert space: learning the classical description of a generic quantum state demands resources that grow exponentially with the number of qubits [1, 3]. Simply storing and outputting the density matrix of a state already results in an exponential cost in time. This raises the crucial question of identifying classes of quantum states that can be efficiently learned using a number of state copies and time scaling at most *polynomially* with the system size. Only a few classes of states are currently known to be efficiently learnable — in particular, matrix product states [2, 4], finitely-correlated states [5], high-temperature Gibbs states [6], states prepared by shallow quantum circuits [7], stabilizer states [8], quantum phase states [9], and fermionic Gaussian states [10, 11]. The latter class of states comprises those prepared by fermionic Gaussian circuits [12], also referred to as free fermionic evolutions or fermionic linear-optics circuits [13, 14]. Via Jordan-Wigner mapping, such states on n fermionic modes can also be viewed as n-qubit states, prepared by generalized matchgate circuits [14–16]. Fermionic Gaussian states states play a key role in condensed matter physics and quantum chemistry, via the Hartree-Fock method and in the context of Fermi Liquid and Bardeen-Cooper-Schrieffer theories [17–20]. These states are also essential in understanding many exactly solvable spin models [21–23]. In quantum computing, fermionic Gaussian states are primarily recognized for their efficient classical simulability [13, 15, 16]. As in the case of Clifford circuits, for which the introduction of magic gates, such as T-gates, allows to reach universal quantum computation [24], also for the case of Gaussian circuits the inclusion of certain magic gates [25–27], for example SWAP gates [26], allows to reach universality. If the number t of T-gates in a Clifford circuit is low, the resulting states can still be efficiently simulated classically [28–30]; it has also been recently demonstrated that such states, termed as t-doped stabilizer states [31, 32], are still efficiently learnable [33–35]. Similarly, in the past year, it has been shown that Gaussian circuits with a few magic gates are also classically simulable [36–38]. However, the learnability of such "t-doped fermionic Gaussian states" remains unknown and this motivates the core-question of our work:

Can we efficiently learn states prepared by Gaussian operations (e.g. matchgates) and a few magic gates?

We answer it by proposing a quantum algorithm of polynomial time and sample complexity that uses only single-copy measurements and learns a classical description of a t-doped fermionic Gaussian state; the learned state is guaranteed to be close to the true state in trace distance. Our presentation is framed in the language of qubits, but the results seamlessly translate into the fermionic formalism. Our learning algorithm may also be feasible to implement in near-term fermionic analog quantum simulators [39, 40], like cold atoms in optical lattices [41], since we only utilize time evolutions of simple few-body fermionic Hamiltonians [42]. The core of our algorithm relies on a result of independent interest, elucidating the structure of states in question. In particular, for any t-doped fermionic Gaussian state $|\psi\rangle$ we show that there exists a Gaussian operation G such that

$G^\dagger |\psi\rangle = |\phi\rangle \otimes |0^{n-\kappa t}\rangle$, where $|\phi\rangle$ is supported on κt qubits and κ is a small constant. Informally, this says that all the magic of such states can be *compressed* to a few qubits via a Gaussian operation. The proof of our compression theorem is constructive, which has implications for the circuit complexity of $|\psi\rangle$ and for improved preparation of doped fermionic Gaussian states.

The high level idea of the learning algorithm is to first learn a Gaussian unitary G which *compresses* the magic, apply it to the state, and then perform full state state tomography on the first few qubits alone. Our learning algorithm has a time complexity $\mathcal{O}(\mathrm{poly}(n, 2^t))$, i.e. it scales polynomially in the system size n and exponentially in the number of non-Gaussian gates t. Thus it is efficient as long as the number of non-Gaussian gates is $t = \mathcal{O}(\log(n))$. Furthermore, we establish that the task of learning such states is computationally intractable when the number of non-Gaussian gates scales *slightly* more than logarithmically, under a common cryptography assumption [43–46]. We show the latter result using the theory of pseudorandom quantum states [47, 48] and qubit-to-fermion mappings [23]. In doing that, we bring pseudorandom quantum states, so far explored only for qubit-based systems, to the fermionic realm. Our learning algorithm generalizes the one presented by Aaronson et al. [33], which is tailored to learn only those states prepared by *particle-number conserving* Gaussian gates and $t = 0$ (in our work we relax both of these assumptions). Furthermore, our algorithm extends to all compressible states, i.e., those which can be written as $|\psi\rangle = G\,|\phi\rangle \otimes |0^{n-\kappa t}\rangle$. We also propose an efficient method to *test* if a given state is close or far from the set of compressible states, by showing an efficiently estimatable quantity that lower bounds the distance to this set.

It should be noted that the concept of magic compression was first introduced in the context of Clifford+T circuits by Leone, Oliviero et al. [49, 50] and later exploited for learning t-doped stabilizer states [33, 34]. Our strategy of proving non-Gaussianity compression and applying it to quantum state tomography was inspired by these earlier works. It is an intriguing fact that a similar compression theorem holds in our context, even though the mathematical structures of stabilizer states and fermionic Gaussian states appear quite different.

In the next sections we summarize our findings, stating more precisely our results and the essential ideas that underlie them. In the Supplementary Material, we provide the technical details.

Preliminaries

Our work can be applied to two distinct and naively separate settings: a system of n qubits with 1D matchgates circuits and their magic gates (e.g., SWAP gates), or a native fermionic system of n modes with states prepared by fermionic Gaussian evolutions and local non-Gaussian evolutions. These two perspectives are mathematically related through the Jordan-Wigner mapping. We will use it now as a *definition* of Majorana operators, thus directly aligning our discussion with the qubit language. Majorana operators, denoted as γ_{2k-1} and γ_{2k} for $k \in [n] := \{1, \dots, n\}$, are defined in terms of standard Pauli operators as $\gamma_{2k-1} := (\prod_{j=1}^{k-1} Z_j)X_k$ and $\gamma_{2k} := (\prod_{j=1}^{k-1} Z_j)Y_k$. Alternatively, they can be defined in the fermionic language through their anticommutation relations [13, 51]. A fermionic Gaussian unitary G is a unitary that satisfies $G^\dagger \gamma_\mu G = \sum_{\nu=1}^{2n} O_{\mu,\nu}\gamma_\nu$ for any $\mu \in [2n]$, where $O \in \mathrm{O}(2n)$ is an orthogonal matrix. The product of two Gaussian unitaries is Gaussian. Notably, a one-to-one correspondence exists between Gaussian unitaries up to a global phase and $\mathrm{O}(2n)$ orthogonal matrices. Given an orthogonal matrix, it is known how to exactly implement the associated Gaussian unitary using $\mathcal{O}(n^2)$ 2-local qubits or 2-local fermionic Gaussian operations [36, 52]. A pure fermionic Gaussian state can be defined as $|\psi\rangle = G\,|0^n\rangle$, where G is a Gaussian unitary and $|0^n\rangle$ denotes the zero computational basis state. Given a quantum state ρ, its correlation matrix $C(\rho)$ is defined as the real anti-symmetric $2n \times 2n$ matrix with elements $[C(\rho)]_{j,k} := -\frac{i}{2}\,\mathrm{Tr}\,(\gamma_j\gamma_k\rho)$, for any $j < k \in [2n]$. We have that $C(G\rho G^\dagger) = OC(\rho)O^T$, for any Gaussian unitary G associated with $O \in \mathrm{O}(2n)$. A well-known result in linear algebra [53] asserts that any real anti-symmetric matrix C can be decomposed in the so-called 'normal form':

$$C = O \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} O^T, \tag{1}$$

where O is an orthogonal matrix in $\mathrm{O}(2n)$ and $\lambda_j \geq 0$, for any $j \in [n]$, are dubbed as 'normal' eigenvalues, ordered in increasing order. We denote the trace distance between two quantum states $|\psi\rangle$ and $|\phi\rangle$ as $d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle) := \frac{1}{2}\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_1$. Given a matrix A, its operator norm $\|A\|_\infty$ is defined as its largest singular value. We refer to the Supplementary Material (SM) for more preliminaries.

Structure of t-doped Gaussian states

States prepared by Gaussian circuits applied to a computational basis state are efficiently simulable classically. However, by incorporating 'non-Gaussian', or 'magic' operations, such as SWAP-gates [15, 26], one can render Gaussian circuits universal for quantum computation. The term 'magic gate' comes from a loose parallel to Clifford circuits, which are efficiently simulable per se but become universal upon introduction of 'magic' non-Clifford T-gates.

Here we consider non-Gaussian operations generated by κ Majorana operators $\{\gamma_{\mu(r)}\}_{r=1}^{\kappa}$, where $\mu(1),\ldots,\mu(\kappa) \in [2n]$. Examples of such non-Gaussian operations for $\kappa = 4$ are the SWAP-gate or a unitary $\exp(i\theta\gamma_1\gamma_5\gamma_6\gamma_8)$ for $\theta \in \mathbb{R}$; for $\kappa = 3$, an example is $\exp(\theta\gamma_2\gamma_6\gamma_7)$. We refer to κ as the maximum Majorana locality of the employed non-Gaussian gates.

Definition 1 (t-doped fermionic Gaussian state)**.** *A state $|\psi\rangle$ is a (t,κ)-doped Gaussian state if it can be prepared by Gaussian unitaries $\{G_i\}_{i=0}^{t}$ and t non-Gaussian κ-local gates $\{W_i\}_{i=1}^{t}$, specifically*

$$|\psi\rangle = G_t W_t \cdots G_1 W_1 G_0 |0^n\rangle \,, \tag{2}$$

where κ-local means that each non-Gaussian gate involves at most κ Majorana operators. Informally, a state is t-doped Gaussian if it is (t,κ)-doped Gaussian for some fixed constant κ.

Similarly, we denote the unitary $U_t := G_t W_t \cdots G_1 W_1 G_0$ as a t-doped Gaussian unitary. We now present our main result concerning the structure of t-doped Gaussian states: it is possible to compress all the 'non-Gaussianity' of the state into a localized region of the system via a Gaussian operation. This motivates the following definition.

Definition 2 (t-compressible Gaussian state)**.** *Let $t \in [n]$. A state $|\psi\rangle$ is (Gaussian) t-compressible if and only if*

$$|\psi\rangle = G(|\phi\rangle \otimes |0^{n-t}\rangle), \tag{3}$$

where G is a Gaussian operation, and $|\phi\rangle$ is a state supported solely on the first t qubits.

In the following, we assume $\kappa t \leq n$.

Theorem 3 (Magic compression in t-doped Gaussian states)**.** *Any (t,κ)-doped Gaussian state is κt-compressible.*

Proof sketch. Let $U_t |0^n\rangle$ be the t-doped state, where $U_t = (\prod_{t'=1}^{t} G_{t'} W_{t'}) G_0$ is the t-doped unitary. We rearrange U_t as $U_t = \tilde{G}_t G_{\text{aux}} \prod_{t'=1}^{t} (G_{\text{aux}}^{\dagger} \tilde{W}_{t'} G_{\text{aux}}) G_{\text{aux}}^{\dagger}$, introducing a Gaussian operation G_{aux} to be fixed and defining $\tilde{W}_{t'} := \tilde{G}_{t'-1}^{\dagger} W_{t'} \tilde{G}_{t'-1}$ and $\tilde{G}_{t'} := G_{t'}..G_0$. We require that G_{aux} satisfies $G_{\text{aux}}^{\dagger} |0^n\rangle = |0^n\rangle$, and that each $G_{\text{aux}}^{\dagger} \tilde{W}_{t'} G_{\text{aux}}$ is supported non-trivially only on the first κt qubits. The latter is enforced by demanding that the Heisenberg evolution, via $\tilde{G}_{t'-1} G_{\text{aux}}$, of each Majorana operator involved in the Hamiltonian generating $W_{t'}$, has non-trivial support exclusively on the first κt qubits. The existence of G_{aux} is shown by demonstrating the existence of its associated orthogonal matrix O_{aux}. The requirements on G_{aux} translate into the demand that O_{aux} must be symplectic and such that it sends κt fixed vectors to the span of the first $2\kappa t$ canonical basis vectors. The existence of such O_{aux} can be proven via the isomorphism between real $2n \times 2n$ symplectic orthogonal matrices and $n \times n$ unitaries [54]. Additional details are provided in the Supplementary Material (see Theorem 27). □

Note that while a (t,κ)-doped Gaussian state is a κt-compressible Gaussian state, the reverse implication does not hold due to circuit complexity arguments. Similarly to Theorem 3, we show that any t-doped Gaussian unitary can be represented as:

$$U_t = G_A(u_t \otimes I) G_B, \tag{4}$$

where G_A and G_B denote Gaussian operations, and u_t is a unitary operator supported on $\lceil \kappa t/2 \rceil$ qubits (with $\lceil \cdot \rceil$ denoting rounding to the next integer), as elaborated in the Supplementary Material (Theorem 26). Notably, if U_t is a particle number conserving unitary [13], then G_A, u_t and G_B can also be chosen as such.

Our proof of Theorem 3 is constructive, i.e., given a classical description of the circuit that prepares $|\psi\rangle$, it provides an efficient procedure for finding the compressing Gaussian circuit G and the state $|\phi\rangle$. The decomposition of t-doped Gaussian states (unitaries) reveals also that they have a circuit complexity, i.e., number of local gates needed for implementing the state (unitary), upper bounded by $\mathcal{O}(n^2 + t^3)$ (Proposition 30 in SM). This provides a better circuit complexity upper bound compared to the naive $\mathcal{O}(n^2 t)$ implied by definition 1 for $\kappa = \mathcal{O}(1)$. Hence, our construction reveals also a method to compress the circuit depth (and not only the magic). Remarkably, analogous results hold for the Clifford+T gates circuits [50].

In the Clifford case [33], the notion of *stabilizer dimension* was introduced for quantifying the degree of "stabilizerness". Here, in analogy to this, we define the *Gaussian dimension* of a state as the number of normal eigenvalues of its correlation matrix that are equal to one. By using Eq.(1), it can be shown that a state has a Gaussian dimension of $n - t$ if and only if it is t-compressible. Therefore, (t,κ)-doped Gaussian states have a Gaussian dimension of $n - \kappa t$.

Learning Algorithm

We present an algorithm for learning t-compressible Gaussian states, or, equivalently, quantum states with $n-t$ Gaussian dimension. Note that this is a broader class than t-doped Gaussian states; as an example unrelated to t-doped states, ground states of quantum impurity models are approximately of this form (as shown in [55]). By definition, any t-compressible Gaussian state $|\psi\rangle$ can be factorized as $G^\dagger|\psi\rangle = |\phi\rangle \otimes |0^{n-t}\rangle$, where $G^\dagger$ is Gaussian and $|\phi\rangle$ is a state on t qubits. At a high level, our strategy is to learn the Gaussian unitary $G^\dagger$, apply it to $|\psi\rangle$, and then perform full state tomography solely on the first t qubits to learn $|\phi\rangle$. Since full state tomography algorithms scale exponentially with the number of qubits [56], for $t = \mathcal{O}(\log(n))$ our algorithm will be efficient.

Algorithm 1: Learning Algorithm

```
Input: $\mathcal{O}(\mathrm{poly}(2^t, n))$ copies of $|\psi\rangle$, accuracy $\varepsilon$, failure probability $\delta$.
Output: A classical description of $|\hat{\psi}\rangle$, such that $d_{\mathrm{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq \varepsilon$ with probability at least $1-\delta$.
Estimate the correlation matrix of $|\psi\rangle$ using $\lceil 256\frac{n^5}{\varepsilon^4}\log\left(12\frac{n^2}{\delta}\right)\rceil$ copies, yielding $\hat{C}$;
Expressing $\hat{C}$ in its normal form (Eq.(1)), find the Gaussian unitary $\hat{G}$ associated with $\hat{O} \in \mathrm{O}(2n)$;
Set $N_t := \lceil 2N_{\mathrm{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3}) + 24\log\left(\frac{3}{\delta}\right)\rceil$ (where $N_{\mathrm{tom}}$ is the number of copies for $t$-qubit state tomography);
for $i \leftarrow 1$ to $N_t$ do
    Apply $\hat{G}^\dagger$ to $|\psi\rangle$;
    Measure the last $n-t$ qubits in the computational basis;
    If the outcome is $|0^{n-t}\rangle$, proceed; otherwise, discard and move to the next iteration;
    Perform a step of state tomography [56, 57] on the remaining $t$ qubits;
Consider the $t$-qubit state $|\hat{\phi}\rangle$ obtained from tomography;
return $\hat{G}$ and $|\hat{\phi}\rangle$, which identify $|\hat{\psi}\rangle := \hat{G}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle)$;
```

To delve deeper, the initial phase of our learning algorithm entails estimating the correlation matrix entries through single-copy measurements. This can be achieved using different methods outlined in the Supplementary Material, such as measurements in the Pauli basis, global Clifford Gaussian measurements [58], or fermionic classical shadows [52, 59, 60]. The estimated correlation matrix $\hat{C}$ is subsequently transformed into its normal form in Eq.(1) to yield the corresponding orthogonal matrix $\hat{O}$ associated with the Gaussian operation $\hat{G}$. (We use the hat symbol to denote the objects estimated from the measurements.) Applying the inverse operation $\hat{G}^\dagger$ to $|\psi\rangle$ results in a state that exhibits high fidelity with a state, which is tensor product of an arbitrary state on the first t qubits and the zero computational basis state on the remaining $n-t$ qubits. Consequently, the learning algorithm queries multiple copies of $|\psi\rangle$ (one at a time), applies $\hat{G}^\dagger$ to them and measures the last $n-t$ qubits. If the outcome of such measurements correspond to $|0^{n-t}\rangle$, then the algorithm proceeds with a step of pure state tomography [56, 57] on the t-qubits state. The state tomography routine performed in the compressed space yields the state $|\hat{\phi}\rangle$. The final output of the learning algorithm is $|\hat{\psi}\rangle := \hat{G}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle)$, and an efficient classical representation can be provided if $t = \mathcal{O}(\log(n))$. Namely, to specify $|\hat{\psi}\rangle$, it is sufficient to provide the complete description of the t-qubit state $|\hat{\phi}\rangle$ and the orthogonal matrix $\hat{O} \in \mathrm{O}(2n)$ associated with $\hat{G}$.

We now present a theorem which formalizes and proves the efficiency of the discussed procedure, outlined in Algorithm 1, to learn doped Gaussian states or, more generally, t-compressible Gaussian states.

Theorem 4 (Learning algorithm guarantees)**.** *Let $|\psi\rangle$ be a t-compressible Gaussian state, and $\varepsilon, \delta \in (0,1]$. Utilizing $\mathcal{O}(\mathrm{poly}(n, 2^t))$ single-copy measurements and computational time, Algorithm 1 outputs a classical representation of a state $|\hat{\psi}\rangle$, such that $d_{\mathrm{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq \varepsilon$ with probability $\geq 1-\delta$.*

Proof sketch. Using $\mathcal{O}(\mathrm{poly}(n))$ copies of $|\psi\rangle$, we estimate its correlation matrix C, yielding $\hat{C}$ such that $\|\hat{C} - C\|_\infty \leq \varepsilon_c$ with a failure probability $\leq \frac{\delta}{3}$, where $\varepsilon_c := \varepsilon^2/(4(n-t))$. Expressing $\hat{C}$ in its normal form (Eq.(1)), we find the Gaussian unitary $\hat{G}$ associated to $\hat{O} \in \mathrm{O}(2n)$. Let $|\psi'\rangle := \hat{G}^\dagger|\psi\rangle$. As detailed in the Supplementary Material, we derive $\langle\psi'| Z_k |\psi'\rangle \geq 1 - 2\varepsilon_c$ for each $k \in \{t+1, \dots, n\}$ and, by Quantum Union Bound [61] we get $d_{\mathrm{tr}}(|\phi\rangle \otimes |0^{n-t}\rangle, |\psi'\rangle) \leq \frac{\varepsilon}{2}$, where $|\phi\rangle \otimes |0^{n-t}\rangle$ corresponds to the state obtained by measuring the last $n-t$ qubits of $\hat{G}^\dagger|\psi\rangle$ in the computational basis and obtaining the outcome corresponding to $|0^{n-t}\rangle$, an event which occurs with probability $\geq 1 - \varepsilon^2/4$. By querying $\lceil 2N_{\mathrm{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3}) + 24\log\left(\frac{3}{\delta}\right)\rceil$ copies of $|\psi\rangle$, and, for each copy, applying $\hat{G}^\dagger$ and measuring the last $n-t$ qubits, we get the outcome $|0^{n-t}\rangle$ at least $N_{\mathrm{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3})$ times, with failure probability $\leq \frac{\delta}{3}$ due to Chernoff bound. Here, $N_{\mathrm{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3})$ is the number of copies sufficient for full state tomography [56] of a t-qubit state with an $\frac{\varepsilon}{2}$ accuracy and a failure probability $\leq \frac{\delta}{3}$. Performing the t-qubit tomography on all the copies where the outcome $|0^{n-t}\rangle$ occurred yields $|\hat{\phi}\rangle$ such that $d_{\mathrm{tr}}(|\hat{\phi}\rangle, |\phi\rangle) \leq \frac{\varepsilon}{2}$, with a failure probability $\leq \frac{\delta}{3}$. Defining $|\hat{\psi}\rangle := \hat{G}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle)$, we have $d_{\mathrm{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq d_{\mathrm{tr}}(|\hat{\phi}\rangle, |\phi\rangle) + d_{\mathrm{tr}}(|\phi\rangle \otimes |0^{n-t}\rangle, \hat{G}^{\dagger}|\psi\rangle)$. This is $\leq \varepsilon$ if the algorithm does not fail, an event occurring with probability $\geq 1-\delta$ due to the union bound. □

Theorem 4 is re-stated and rigorously proven in the Supplemental Material as Theorem 44. The sample, time and memory complexity of our algorithm for learning t-compressible states exhibits a polynomial dependence on n and an exponential dependence on t: specifically, the $\mathrm{poly}(n)$ contribution (specifically an $\mathcal{O}(n^5)$ scaling) arises solely from estimating and post-processing the correlation matrix, while the $\exp(t)$ contribution arises from full state tomography on t-qubits. It is easy to see that the dependence on t is optimal, because learning t-compressible states is at least as hard as learning an arbitrary pure state on t qubits and thus requires at least $\Omega(\exp(t))$ copies of the state [3].

However, if we focus on the subclass of t-doped Gaussian states, a classical shadow tomography based algorithm presented in [62, 63] achieves $\mathcal{O}(\mathrm{poly}(n,t))$ sample complexity. Specifically, this algorithm requires a number of copies that scales polynomially with the circuit complexity of the state, and t-doped states have a circuit complexity $\mathcal{O}(\mathrm{poly}(n,t))$. However, the time complexity of the algorithm in [62, 63] scales exponentially with the number of qubits n, while our algorithm's time complexity scales only polynomially (although always exponentially in t). This observation also applies to t-doped stabilizer states learning analyzed in recent works [33, 34].

Time complexity lower bound

It is natural to wonder whether there exist algorithms for learning t-doped Gaussian states with time complexity scaling in t as $\mathcal{O}(\mathrm{poly}(t))$. We establish that the answer is no (see Proposition 50 in SM), relying on a widely-believed cryptography assumption. Specifically, we show that certain families of pseudorandom quantum states [47, 48] can be generated using a polynomial number of local non-Gaussian gates. This implies that if there were an algorithm with polynomial time complexity in t for learning t-doped Gaussian states, quantum computers could solve RingLWE [64] in polynomial time, which is considered unlikely [43–45, 64–66]. While this rules out the existence of efficient algorithms if t scales polynomially with the number of qubits n, it does not yet preclude the existence of efficient algorithms if t grows *slightly* more than logarithmically, for example $t = \mathcal{O}((\log n)^2)$. However, we can rule out this possibility by making the stronger assumption that quantum computers cannot solve RingLWE in sub-exponential time [43–46]. This implies that the time complexity of any algorithm to learn $\tilde{\mathcal{O}}(t)$-doped Gaussian states (where $\tilde{\mathcal{O}}(\cdot)$ hides polylogarithmic factors) would necessarily be $\exp(\Omega(t))$. In other words, the following holds.

Theorem 5 (Time-complexity lower bound, informal)**.** *Assuming that quantum computers cannot solve* RingLWE *in sub-exponential time, then there is no time efficient algorithm to learn $\tilde{\omega}(\log(n))$-doped Gaussian state which outputs a description of an efficiently preparable quantum state. Here, $\tilde{\omega}(\log(n)) := \omega(\log(n)\mathrm{polyloglog}(n))$.*

This would prove that the time complexity in t of our algorithm is essentially optimal, because our algorithm is efficient as long as $t = \mathcal{O}(\log(n))$. We show Theorem 5 by efficiently encoding the pseudorandom quantum states constructions [63] via a specific qubits-to-fermions mapping [23] into other states produced by the same number of gates, all of which are now local non-Gaussian. Crucially for our construction, this mapping sends local qubit operations to local fermionic operations with only a constant overhead in the number of qubits. Please refer to the Supplementary Material (Proposition 52) for more details.

Testing Gaussian dimension

We have introduced an algorithm for efficiently learning states with a high Gaussian dimension, specifically those promised to be t-compressible with a small t. A natural question arises: How can we test the Gaussian dimension of a state? In other words, how can we determine if the underlying state is close or far from the set of t-compressible states? In our Supplementary Material, using ideas developed in [67] for the case of Gaussian states ($t=0$), we establish that the minimum trace distance between a state $|\psi\rangle$ and the set of t-compressible Gaussian states, denoted by $\mathcal{G}_t$, satisfies:

$$\frac{1-\lambda_{t+1}}{2} \leq \min_{|\phi_t\rangle \in \mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \leq \sqrt{\sum_{k=t+1}^{n} \frac{1-\lambda_k}{2}}, \tag{5}$$

where $\{\lambda_k\}_{k=1}^n$ represents the normal eigenvalues of the correlation matrix of $|\psi\rangle$ ordered in increasing order. These inequalities imply that $|\psi\rangle$ is close in trace distance to the set $\mathcal{G}_t$ if and only if λ_{t+1} is close to one. In particular, assuming that $|\psi\rangle$ is either a state in $\mathcal{G}_t$ or $\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \geq \varepsilon$, we can determine with at least $1-\delta$ probability which of the two cases is true by accurately estimating λ_{t+1}. Specifically, $\mathcal{O}((n^5/\varepsilon^4)\log(n^2/\delta))$ copies of the state suffice for this purpose. Notably, this complexity scaling for testing is independent from t, in contrast to learning.

Conclusions

In this work, we have presented an algorithm for efficiently learning t-doped fermionic Gaussian states, with sample and time complexity scaling as $\mathcal{O}(\mathrm{poly}(n, 2^t))$. Additionally, we have established, under standard cryptography assumptions, that there is no learning algorithm for such class of states with a polynomial dependence on t in the time complexity. Crucially, our algorithm utilizes solely experimentally feasible single-copy measurements. Its working idea is based on a theorem that we prove, which says that all the non-Gaussianity in a t-doped fermionic Gaussian state can be efficiently compressed onto $\mathcal{O}(t)$ qubits through a Gaussian operation. This observation carries potential significance beyond the scope of learning, particularly within the context of quantum many-body theory or within circuit compilation. Thus, the results presented in this work, besides being directly relevant to device verification and benchmarking, among other tasks, hold fundamental significance for quantum information theory, as they reveal more about the structure of Gaussian states with fermionic magic gates. Additionally, we introduce a variety of useful analytical techniques, such as new ways to leverage the Quantum Union Bound [61] in the context of fermionic states, which are likely to find applications in future research.

Our work offers new directions for further research. For instance, an open question arising from this work is to study the noise-robustness of our protocol, and whether t-doped Gaussian unitaries can be efficiently learned in the scenario where the input states to the unitary and measurements at the end can be chosen: the particular case of $t = 0$ has already been solved in Ref. [68] and it would be interesting to generalize it. Additionally, a promising future direction is the one of extending the results presented in this work to the domain of continuous variable systems and bosonic Gaussian states. Finally, an intriguing question to explore is whether the classical simulability of a class of states, under precise notions of classical simulability, generally implies learnability in trace distance.

Acknowledgments

We thank Mauro Moralez, Lorenzo Leone, Lennart Bittel, Janek Denzler, Tommaso Guaita, Ansgar Burchards, Julio Magdalena de la Fuente, Daniel Liang, Matthias Caro, Alexander Nietner, Marten Folkertsma, Francisco Escudero Gutiérrez, Simona Etinski, Jonas Helsen, Barbara Terhal and Jens Eisert for insightful discussions. We acknowledge the PCMI 2023 program for providing a collaborative space where the authors brainstormed this project. AAM acknowledges fundings from BMBF (FermiQP).

* a.mele@fu-berlin.de
† yaroslav@cwi.nl

[1] A. Anshu and S. Arunachalam, A survey on the complexity of learning quantum states (2023), arXiv:2305.20069 [quant-ph].

[2] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nature Communications **1**, 10.1038/ncomms1147 (2010).

[3] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, IEEE Transactions on Information Theory , 1 (2017).

[4] B. P. Lanyon, C. Maier, M. Holzäpfel, T. Baumgratz, C. Hempel, P. Jurcevic, I. Dhand, A. S. Buyskikh, A. J. Daley, M. Cramer, M. B. Plenio, R. Blatt, and C. F. Roos, Nature Physics **13**, 1158–1162 (2017).

[5] M. Fanizza, N. Galke, J. Lumbreras, C. Rouzé, and A. Winter, Learning finitely correlated states: stability of the spectral reconstruction (2023), arXiv:2312.07516 [quant-ph].

[6] C. Rouzé and D. S. França, Learning quantum many-body systems from a few copies (2023), arXiv:2107.03333 [quant-ph].

[7] H.-Y. Huang, Y. Liu, M. Broughton, I. Kim, A. Anshu, Z. Landau, and J. R. McClean, Learning shallow quantum circuits (2024), arXiv:2401.10095 [quant-ph].

[8] A. Montanaro, Learning stabilizer states by bell sampling (2017), arXiv:1707.04012 [quant-ph].

[9] S. Arunachalam, S. Bravyi, A. Dutt, and T. J. Yoder, Optimal algorithms for learning quantum phase states (2023), arXiv:2208.07851 [quant-ph].

[10] S. Aaronson and S. Grewal, Efficient tomography of non-interacting fermion states (2023), arXiv:2102.10458 [quant-ph].

[11] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, Physical Review Letters **120**, 10.1103/physrevlett.120.190501 (2018).

[12] J. Surace and L. Tagliacozzo, SciPost Physics Lecture Notes 10.21468/scipostphyslectnotes.54 (2022).

[13] B. M. Terhal and D. P. DiVincenzo, Physical Review A **65**, 10.1103/physreva.65.032325 (2002).

[14] E. Knill, Fermionic linear optics and matchgates (2001), arXiv:quant-ph/0108033 [quant-ph].

[15] R. Jozsa and A. Miyake, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **464**, 3089 (2008).

[16] L. G. Valiant, SIAM Journal on Computing **31**, 1229 (2002), https://doi.org/10.1137/S0097539700377025.

[17] P. Echenique and J. L. Alonso, Molecular Physics **105**, 3057–3098 (2007).

[18] R. M. Martin, *Electronic Structure: Basic Theory and Practical Methods* (Cambridge University Press, 2004).

[19] G. Giuliani and G. Vignale, *Quantum theory of the electron liquid* (Cambridge university press, 2008).

[20] J. R. Schrieffer, *Theory of superconductivity* (CRC press, 2018).
[21] R. J. Baxter, *Exactly solved models in statistical mechanics* (1982).
[22] L. Fidkowski and A. Kitaev, Phys. Rev. B **83**, 075103 (2011).
[23] A. Kitaev, Annals of Physics **321**, 2–111 (2006).
[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
[25] M. Hebenstreit, R. Jozsa, B. Kraus, S. Strelchuk, and M. Yoganathan, Physical Review Letters **123**, 10.1103/physrevlett.123.080503 (2019).
[26] D. J. Brod and E. F. Galvão, Physical Review A **84**, 10.1103/physreva.84.022310 (2011).
[27] D. J. Brod, The computational power of non-interacting particles (2014), arXiv:1412.7637 [quant-ph].
[28] D. Gottesman, The heisenberg representation of quantum computers (1998), arXiv:quant-ph/9807006 [quant-ph].
[29] S. Bravyi and D. Gosset, Physical Review Letters **116**, 10.1103/physrevlett.116.250501 (2016).
[30] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[31] S. F. Oliviero, L. Leone, and A. Hamma, Physics Letters A **418**, 127721 (2021).
[32] L. Leone, S. F. E. Oliviero, Y. Zhou, and A. Hamma, Quantum **5**, 453 (2021).
[33] S. Grewal, V. Iyer, W. Kretschmer, and D. Liang, Efficient learning of quantum states prepared with few non-clifford gates (2023), arXiv:2305.13409 [quant-ph].
[34] L. Leone, S. F. E. Oliviero, and A. Hamma, Learning t-doped stabilizer states (2023), arXiv:2305.15398 [quant-ph].
[35] D. Hangleiter and M. J. Gullans, Bell sampling from quantum circuits (2024), arXiv:2306.00083 [quant-ph].
[36] B. Dias and R. Koenig, Classical simulation of non-gaussian fermionic circuits (2023), arXiv:2307.12912 [quant-ph].
[37] O. Reardon-Smith, M. Oszmaniec, and K. Korzekwa, Improved simulation of quantum circuits dominated by free fermionic operations (2023), arXiv:2307.12702 [quant-ph].
[38] J. Cudby and S. Strelchuk, Gaussian decomposition of magic states for matchgate computations (2023), arXiv:2307.12654 [quant-ph].
[39] J. Vijayan, P. Sompet, G. Salomon, J. Koepsell, S. Hirthe, A. Bohrdt, F. Grusdt, I. Bloch, and C. Gross, Science **367**, 186–189 (2020).
[40] A. Mazurenko, C. S. Chiu, G. Ji, M. F. Parsons, M. Kanász-Nagy, R. Schmidt, F. Grusdt, E. Demler, D. Greif, and M. Greiner, Nature **545**, 462 (2017).
[41] T. Esslinger, Annual Review of Condensed Matter Physics **1**, 129 (2010), https://doi.org/10.1146/annurev-conmatphys-070909-104059.
[42] P. Naldesi, A. Elben, A. Minguzzi, D. Clément, P. Zoller, and B. Vermersch, Physical Review Letters **131**, 10.1103/physrevlett.131.060601 (2023).
[43] S. Arunachalam, A. B. Grilo, and A. Sundaram, Electron. Colloquium Comput. Complex. **TR19-041** (2019), TR19-041.
[44] I. Diakonikolas, D. M. Kane, P. Manurangsi, and L. Ren, Cryptographic hardness of learning halfspaces with massart noise (2022), arXiv:2207.14266 [cs.LG].
[45] P. Ananth, A. Poremba, and V. Vaikuntanathan, Revocable cryptography from learning with errors (2023), arXiv:2302.14860 [quant-ph].
[46] A. Gupte, N. Vafa, and V. Vaikuntanathan, Continuous lwe is as hard as lwe and applications to learning gaussian mixtures (2022), arXiv:2204.02550 [cs.CR].
[47] Z. Ji, Y.-K. Liu, and F. Song, Pseudorandom quantum states, in *Advances in Cryptology – CRYPTO 2018* (Springer International Publishing, 2018) p. 126–152.
[48] Z. Brakerski and O. Shmueli, (pseudo) random quantum states with binary phase (2019), arXiv:1906.10611 [quant-ph].
[49] S. F. E. Oliviero, L. Leone, S. Lloyd, and A. Hamma, Phys. Rev. Lett. **132**, 080402 (2024).
[50] L. Leone, S. F. E. Oliviero, S. Lloyd, and A. Hamma, Phys. Rev. A **109**, 022429 (2024).
[51] S. B. Bravyi and A. Y. Kitaev, Annals of Physics **298**, 210–226 (2002).
[52] A. Zhao, Learning, optimizing, and simulating fermions with quantum computers (2023), arXiv:2312.10399 [quant-ph].
[53] B. Zumino, Journal of Mathematical Physics **3**, 1055 (2004), https://pubs.aip.org/aip/jmp/article-pdf/3/5/1055/11115137/1055_1_online.pdf.
[54] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, 2017).
[55] S. Bravyi and D. Gosset, Communications in Mathematical Physics **356**, 451–500 (2017).
[56] D. S. França, F. G. L. Brandão, and R. Kueng, in *16th Conference on the Theory of Quantum Computation, Communication and Cryptography* (Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021).
[57] M. Guta, J. Kahn, R. Kueng, and J. A. Tropp, Fast state tomography with optimal error bounds (2018), arXiv:1809.11162 [quant-ph].
[58] X. Bonet-Monroig, R. Babbush, and T. E. O'Brien, Phys. Rev. X **10**, 031064 (2020).
[59] A. Zhao, N. C. Rubin, and A. Miyake, Physical Review Letters **127**, 10.1103/physrevlett.127.110504 (2021).
[60] K. Wan, W. J. Huggins, J. Lee, and R. Babbush, Matchgate shadows for fermionic quantum simulation (2023), arXiv:2207.13723 [quant-ph].
[61] J. Gao, Physical Review A **92**, 10.1103/physreva.92.052331 (2015).
[62] A. Abbas, R. King, H.-Y. Huang, W. J. Huggins, R. Movassagh, D. Gilboa, and J. R. McClean, On quantum backpropagation, information reuse, and cheating measurement collapse (2023), arXiv:2305.13362 [quant-ph].
[63] H. Zhao, L. Lewis, I. Kannan, Y. Quek, H.-Y. Huang, and M. C. Caro, Learning quantum states and unitaries of bounded gate complexity (2023), arXiv:2310.19882 [quant-ph].
[64] V. Lyubashevsky, C. Peikert, and O. Regev, in *Advances in Cryptology – EUROCRYPT 2010*, edited by H. Gilbert (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010) pp. 1–23.
[65] O. Regev, On lattices, learning with errors, random linear codes, and cryptography (2024), arXiv:2401.03703 [cs.CR].
[66] D. Aggarwal, H. Bennett, Z. Brakerski, A. Golovnev, R. Kumar, Z. Li, S. Peters, N. Stephens-Davidowitz, and V. Vaikuntanathan, Lattice problems beyond polynomial time (2022), arXiv:2211.11693 [cs.CC].
[67] L. Bittel, A. A. Mele, J. Eisert, and L. Leone, Testing and tomography of free-fermionic quantum states (2024, in preparation).

[68] M. Oszmaniec, N. Dangniam, M. E. Morales, and Z. Zimborás, PRX Quantum **3**, 020328 (2022).

[69] Z. Jiang, K. J. Sung, K. Kechedzhi, V. N. Smelyanskiy, and S. Boixo, Physical Review Applied **9**, 10.1103/physrevapplied.9.044036 (2018).

[70] D. Miller, L. E. Fischer, I. O. Sokolov, P. K. Barkoutsos, and I. Tavernelli, Hardware-tailored diagonalization circuits (2022), arXiv:2203.03646 [quant-ph].

[71] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics (Springer New York, 1996).

[72] R. O'Donnell and R. Venkateswaran, The quantum union bound made easy (2021), arXiv:2103.07827 [quant-ph].

[73] S. Aaronson, Qma/qpoly is contained in pspace/poly: De-merlinizing quantum protocols (2006), arXiv:quant-ph/0510230 [quant-ph].

[74] R. O'Donnell and J. Wright, Efficient quantum tomography (2015), arXiv:1508.01907 [quant-ph].

[75] J. Roffe, Contemporary Physics **60**, 226–245 (2019).

[76] J. Dehaene and B. De Moor, Physical Review A **68**, 10.1103/physreva.68.042318 (2003).

[77] M. M. Wilde, Preface to the second edition, in *Quantum Information Theory* (Cambridge University Press, 2017) p. xi–xii.

Supplementary Material

In this supplementary material, we provide a more comprehensive level of detail and explanation for certain aspects covered in the main text.

Contents

Supplementary Material I: Preliminaries

A. Notation and basics

In this work, we employ the following notation. $\mathcal{L}(\mathbb{C}^d)$ denotes the set of linear operators acting on the d-dimensional complex vector space $\mathbb{C}^d$. Additionally, we use $[d]$ to represent the set of integers from 1 to d, i.e., $[d] := \{1, \dots, d\}$. We denote with $\mathrm{Mat}(d, \mathbb{F})$ the set of $d \times d$ matrices over the field $\mathbb{F}$. Let $v \in \mathbb{C}^d$ be a vector, and let $p \in [1, \infty]$. The p-norm of v is denoted by $\|v\|_p$, defined as $\|v\|_p := (\sum_{i=1}^d |v_i|^p)^{1/p}$. The Schatten p-norm of a matrix $A \in \mathbb{C}^d$, with $p \in [1, \infty]$, is given by $\|A\|_p := \mathrm{Tr}\Big((\sqrt{A^\dagger A})^p\Big)^{1/p}$, corresponding to the p-norm of the vector of singular values of A. The trace norm and the Hilbert-Schmidt norm are important instances of Schatten p-norms, denoted as $\|\cdot\|_1$ and $\|\cdot\|_2$ respectively. The Hilbert-Schmidt norm is induced by the Hilbert-Schmidt scalar product $\langle A,B\rangle_{HS} := \mathrm{Tr}\big(A^\dagger B\big)$ for $A,B\in\mathcal{L}(\mathbb{C}^d)$. The infinity norm, $\|\cdot\|_\infty$, of a matrix is defined as its largest singular value. This norm can be interpreted as the limit of the Schatten p-norm of the matrix as p approaches infinity. For any unitaries U and V, and a matrix A, we have the unitary invariance property $\|UAV\|_p = \|A\|_p$. Also, $\|A\otimes B\|_p = \|A\|_p\|B\|_p$ for $A,B\in\mathcal{L}(\mathbb{C}^d)$. We denote with $\mathrm{U}(n)$ the group of $n\times n$ unitary matrices. We denote $\mathrm{O}(2n)$ as the group of real orthogonal $2n\times 2n$ matrices. $\mathrm{Sp}(2n,\mathbb{R})$ denotes the group of symplectic matrices over the real field, defined as

$$\mathrm{Sp}(2n,\mathbb{R}) := \{S\in\mathrm{Mat}(2n,\mathbb{R})\,:\, S\Omega S^T = \Omega\}, \tag{S1}$$

where $\Omega := \bigoplus_{i=1}^n \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}$. The n-qubits Pauli operators are represented as elements of the set $\{I,X,Y,Z\}^{\otimes n}$, where I,X,Y,Z represent the standard single qubit Pauli. Pauli operators are traceless, Hermitian, they square to the identity, and form an orthogonal basis with respect to the Hilbert-Schmidt scalar product for the space of linear operators. We define the set of quantum states as $\mathcal{S}(\mathbb{C}^d) := \{\rho\in\mathcal{L}(\mathbb{C}^d)\,:\,\rho\geq 0,\ \mathrm{Tr}(\rho)=1\}$. The trace distance between two pure quantum states $|\psi\rangle, |\phi\rangle\in\mathbb{C}^d$ is defined as $d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle) := \frac{1}{2}\||\psi\rangle\!\langle\psi| - |\phi\rangle\!\langle\phi|\|_1$.

For a function $f(n)$, if there exists a constant c and a specific input size n_0 such that $f(n)\leq c\cdot g(n)$ for all $n\geq n_0$, where $g(n)$ is a well-defined function, then we express it as $f(n) = \mathcal{O}(g(n))$. This notation signifies the upper limit of how fast a function grows in relation to $g(n)$.

For a function $f(n)$, if there exists a constant c and a specific input size n_0 such that $f(n)\geq c\cdot g(n)$ for all $n\geq n_0$, where $g(n)$ is a well-defined function, then we express it as $f(n) = \Omega(g(n))$. This notation signifies the lower limit of how fast a function grows in relation to $g(n)$.

For a function $f(n)$, if for any constant c, there exists an input size n_0 such that $f(n) > c\cdot g(n)$ for all $n\geq n_0$, where $g(n)$ is a well-defined function, then then we express it as $f(n) = \omega(g(n))$. This notation implies that the function grows strictly faster than the provided lower bound.

B. Basics of probability theory

In this section, we present fundamental results from probability theory useful in our work.

Lemma 6 (Union Bound)**.** *Let $A_1, A_2,\dots, A_M$ be events in a probability space. The probability of the union of these events is bounded by the sum of their individual probabilities:*

$$\Pr\left(\bigcup_{i=1}^M A_i\right) \leq \sum_{i=1}^M \Pr(A_i).$$

Lemma 7 (Chernoff Bound)**.** *Consider a set of independent and identically distributed random variables $\{X_i\}_{i=1}^N$ with binary outcomes, taking values in $\{0,1\}$. Define $X := \sum_{i=1}^N X_i$ and $\mu := \mathbb{E}[X]$. For any $\alpha\in(0,1)$, the probability of X being less than $(1-\alpha)$ times its expected value is exponentially bounded as follows:*

$$\Pr\left[X\leq (1-\alpha)\mu\right] \leq \exp\left(-\frac{\alpha^2\mu}{2}\right).$$

Lemma 8 (Hoeffding's Inequality)**.** *Let $\{X_i\}_{i=1}^N$ be independent and identically distributed (i.i.d) random variables with values in $[a,b]\subseteq\mathbb{R}$. For any $\varepsilon > 0$, the probability of the deviation of $\hat{X} := (\sum_{i=1}^N X_i)/N$ from its expected value is exponentially bounded as follows:*

$$\Pr\left(\left|\frac{1}{N}\sum_{i=1}^N X_i - \mathbb{E}[\hat{X}]\right| \geq \varepsilon\right) \leq 2\exp\left(-\frac{2N\varepsilon^2}{(b-a)^2}\right).$$

Corollary 9. *For any $\varepsilon > 0$ and $\delta > 0$, let $\{X_i\}_{i=1}^N$ be i.i.d. random variables with values in $[a,b]\subseteq\mathbb{R}$ and $\hat{X} := (\sum_{i=1}^N X_i)/N$. According to Hoeffding's inequality, a sample size N satisfying*

$$N \geq \frac{(b-a)^2}{2\varepsilon^2}\log\left(\frac{2}{\delta}\right)$$

suffices to guarantee that $|\frac{1}{N}\sum_{i=1}^N X_i - \mathbb{E}[\hat{X}]| < \varepsilon$ with a probability of at least $1-\delta$.

C. Fermionic Gaussian states

In this section, we explore the definitions and essential properties of fermionic Gaussian states. We focus on a system consisting of n qubits or n fermionic modes, resulting in a Hilbert space dimension of 2^n. More precisely, our work is approached from two perspectives: examining a system of n qubits with 1D matchgates circuits and their magic gates (e.g., SWAP gates), or an equivalent native fermionic system of n modes with states prepared by fermionic Gaussian evolutions and local non-Gaussian evolutions. These perspectives are mathematically connected through the Jordan-Wigner mapping, which we use now for defining Majorana operators in terms of Pauli operators.

Definition 10 (Majorana Operators)**.** *For each $k \in [n]$, Majorana operators are defined as:*

$$\gamma_{2k-1} := \left(\prod_{j=1}^{k-1} Z_j\right) X_k, \quad \gamma_{2k} := \left(\prod_{j=1}^{k-1} Z_j\right) Y_k. \tag{S2}$$

Majorana operators can also be defined directly in the fermionic language through their anticommutation relations [13, 51]. Majorana operators are Hermitian, traceless, and their squares yield the identity, as deducible from their definitions. Moreover, distinct Majorana operators exhibit anticommutativity and orthogonality with respect to the Hilbert-Schmidt inner product.

Definition 11 (Majorana Ordered Products)**.** *Given a set $S := \{\mu_1, \ldots, \mu_{|S|}\} \subseteq [2n]$ with $1 \leq \mu_1 < \cdots < \mu_{|S|} \leq 2n$, we define the Majorana product operator as $\gamma_S = \gamma_{\mu_1} \cdots \gamma_{\mu_{|S|}}$ if $S \neq \emptyset$, and $\gamma_\emptyset = I$ otherwise.*

The 4^n distinct ordered Majorana products are orthogonal to each other with respect the Hilbert-Schmidt inner product, therefore they form a basis for the linear operators $\mathcal{L}\big(\mathbb{C}^{2^n}\big)$.

Definition 12 (Fermionic Gaussian Unitary (FGU))**.** *A fermionic Gaussian unitary G_O is a unitary operator satisfying:*

$$G_O^\dagger \gamma_\mu G_O = \sum_{\nu=1}^{2n} O_{\mu,\nu} \gamma_\nu \tag{S3}$$

for any $\mu \in [2n]$, where $O \in \mathrm{O}(2n)$ is an orthogonal matrix.

Since the ordered products of Majorana operators γ_μ with $\mu \in [2n]$ form a basis for the linear operators, it is sufficient to specify how a unitary acts under conjugation on the $2n$ Majorana operators γ_μ, where $\mu \in [2n]$, to uniquely determine the unitary up to a phase. Thus, there is a one-to-one mapping between n-qubit fermionic Gaussian unitaries (up to a global phase) and orthogonal matrices $\mathrm{O}(2n)$. In particular, given $O \in \mathrm{O}(2n)$, it is possible to build the associated unitary using at most $\mathcal{O}(n(n-1)/2)$ 2-qubit FGU operations. For a more detailed explanation on how to map an $\mathrm{O}(2n)$ matrix to a fermionic Gaussian unitary, refer to [36, 52, 69]. From the previous definition, it readily follows that $G_O^\dagger = G_{O^T}$. Moreover we have that the product of two Gaussian unitaries is Gaussian, namely $(G_{O_1}G_{O_2})^\dagger \gamma_\mu G_{O_1}G_{O_2} = \sum_{\nu=1}^{2n}(O_1O_2)_{\mu,\nu}\gamma_\nu$. To streamline notation, we will frequently refer to fermionic Gaussian unitaries G_O simply as G when there is no need to specify the associated orthogonal matrix. Now, we define a fermionic Gaussian state.

Definition 13 (Fermionic Gaussian State)**.** *An n-qubit state $|\psi\rangle$ is a (pure) fermionic Gaussian state if it can be expressed as $|\psi\rangle = G\,|0^n\rangle$, where G is a fermionic Gaussian unitary.*

It is noteworthy that any computational basis state $|x\rangle$ is a Gaussian state. This stems from the observation that each Pauli X_i gate acting on the i-th qubit, where $i \in [n]$, is a fermionic Gaussian unitary. An additional useful identity is $Z_j = -i\gamma_{2j-1}\gamma_{2j}$. Thus, the density matrix of a pure fermionic Gaussian state associated to an orthogonal matrix $O \in \mathrm{O}(2n)$ can be written as:

$$G_O\,|0^n\rangle\!\langle 0^n|\,G_O^\dagger = G_O\left(\prod_{j=1}^{n}\frac{I - i\gamma_{2j-1}\gamma_{2j}}{2}\right)G_O^\dagger = \prod_{j=1}^{n}\left(\frac{I - i\tilde{\gamma}_{2j-1}\tilde{\gamma}_{2j}}{2}\right), \tag{S4}$$

where $\tilde{\gamma}_\mu := G_O\gamma_\mu G_O^\dagger = \sum_{\nu=1}^{2n} O^T_{\mu,\nu}\gamma_\nu$ for each $\mu \in [2n]$.

We now proceed to define the correlation matrix for any (possibly non-Gaussian) state.

Definition 14 (Correlation Matrix)**.** *For any n-qubit quantum state ρ, its correlation matrix $C(\rho)$ is defined as:*

$$[C(\rho)]_{j,k} := -\frac{i}{2}\operatorname{Tr}\left([\gamma_j, \gamma_k]\,\rho\right), \tag{S5}$$

where $j, k \in [2n]$.

The correlation matrix of any state is real and anti-symmetric, possessing eigenvalues in pairs $\pm i\lambda_j$ for $j \in [2n]$, where λ_j are real numbers such that $|\lambda_j| \leq 1$. The correlation matrix of a quantum state, when evolved using fermionic Gaussian unitaries, undergoes a transformation through conjugation with the corresponding orthogonal matrix, as articulated in the following lemma.

Lemma 15 (Transformation of the Correlation Matrix under FGU)**.** *For a given n-qubit state ρ, we have:*

$$C(G_O \rho G_O^\dagger) = OC(\rho)O^T, \tag{S6}$$

for any orthogonal matrix $O \in \mathrm{O}(2n)$ and associated fermionic Gaussian unitary G_O.

This result is readily verified through the definitions of the correlation matrix and fermionic Gaussian unitary. The state $|x\rangle$ is characterized by a correlation matrix of the form:

$$C(|x\rangle\langle x|) = \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & (-1)^{x_i} \\ -(-1)^{x_i} & 0 \end{pmatrix}. \tag{S7}$$

Hence, for a fermionic Gaussian state $|\psi\rangle := G_O |0^n\rangle$, the correlation matrix takes the form:

$$C(|\psi\rangle\langle\psi|) = O \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} O^T. \tag{S8}$$

In the subsequent discussion, we will use $C(|\psi\rangle)$ to denote the correlation matrix of a pure state $|\psi\rangle$. If the state $|\psi\rangle$ is a pure Gaussian state, then each of the eigenvalues of $C(|\psi\rangle)$ is one in absolute value. Moreover, it is worth noting that every real anti-symmetric matrix can be decomposed in the following form:

Lemma 16 (Normal form of Real Anti-Symmetric Matrices [53])**.** *Any real anti-symmetric matrix C can be decomposed in the so-called 'normal-form':*

$$C = O \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} O^T, \tag{S9}$$

where O is an orthogonal matrix in $\mathrm{O}(2n)$ and $\lambda_j \geq 0 \in \mathbb{R}$, for any $j \in [n]$, are ordered in increasing order. The eigenvalues of C are $\pm i\lambda_j$ where $\lambda_j \in \mathbb{R}$ for any $j \in [n]$.

Definition 17 (Normal eigenvalues)**.** *Given a real-antisymmetric matrix decomposed as in the previous Lemma 16, $\{\lambda_j\}_{j=1}^n$ are dubbed as the 'normal eigenvalues' of the matrix.*

D. Particle-number preserving unitaries

In this section, we introduce the concept of particle-number preserving fermionic unitaries and establish definitions and facts useful for subsequent discussions. We begin by defining creation and annihilation operators.

Definition 18 (Creation and Annihilation Operators)**.** *The annihilation operators are defined as:*

$$a_j := \frac{\gamma_{2j-1} + i\gamma_{2j}}{2}, \tag{S10}$$

for any $j \in [n]$. The creation operators $\{a_j^\dagger\}_{j=1}^n$ are defined as the adjoints of the annihilation operators.

Definition 19 (Particle Number Operator)**.** *The operator $\hat{N} := \sum_{i=1}^n a_i^\dagger a_i$ is denoted as the particle number operator.*

The computational basis forms a set of eigenstates for the particle number operator:

$$\hat{N} |x_1, \dots, x_n\rangle = (x_1 + \dots + x_n) |x_1, \dots, x_n\rangle, \tag{S11}$$

where $x_1, \dots, x_n \in \{0, 1\}$.

Definition 20 (Particle Number Preserving Unitaries)**.** *A unitary U is said to be particle number preserving if and only if*

$$U^\dagger \hat{N} U = \hat{N}, \tag{S12}$$

where $\hat{N} := \sum_{i=1}^n a_i^\dagger a_i$ is the particle number operator.

Definition 21 (Symplectic Group)**.** *The group of real symplectic matrices, denoted as* $\mathrm{Sp}(2n,\mathbb{R})$*, is defined as*

$$\mathrm{Sp}(2n,\mathbb{R}) := \{S \in \mathrm{Mat}(2n,\mathbb{R}) \,:\, S\Omega S^T = \Omega\}, \tag{S13}$$

where $\Omega := \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \bigoplus_{i=1}^{n} iY$*.*

It is often convenient to express Ω as $\Omega = I_n \otimes iY$, where I_n denotes the $n \times n$ identity matrix. Note that Ω in the literature is sometimes defined (see, e.g., [54]) as $iY \otimes I_n = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}$, but the two definitions are equivalent up to orthogonal transformation.

Now, we state an important proposition that will be useful in the subsequent section.

Proposition 22 ($\mathrm{U}(n)$ is Isomorphic to $\mathrm{O}(2n)\cap\mathrm{Sp}(2n,\mathbb{R})$)**.** *The set of unitaries* $\mathrm{U}(n)$ *is isomorphic to the set of real symplectic orthogonal matrices* $\mathrm{O}(2n) \cap \mathrm{Sp}(2n,\mathbb{R})$*.*

In particular, any orthogonal symplectic matrix $O \in \mathrm{O}(2n) \cap \mathrm{Sp}(2n,\mathbb{R})$ *can be written as follows:*

$$O = \mathrm{Re}(u) \otimes I + \mathrm{Im}(u) \otimes iY, \tag{S14}$$

where $u \in \mathrm{U}(n)$ *is an* $n \times n$ *unitary.*

Proof. We refer the reader to Appendix B.1. of the book [54]. □

We now present a Lemma, which shows (some) equivalent definitions of a particle-number preserving fermionic Gaussian unitary.

Lemma 23 (Particle Number Preserving Gaussian Unitary)**.** *Let* G *be a fermionic Gaussian unitary associated with the orthogonal matrix* $O \in \mathrm{O}(2n)$*. The following points are equivalents:*

1. *G is particle number-preserving,*
2. $G\,|0^n\rangle\!\langle 0^n|\,G^\dagger = |0^n\rangle\!\langle 0^n|$*,*
3. *O is symplectic orthogonal, i.e.,* $O \in \mathrm{O}(2n) \cap \mathrm{Sp}(2n,\mathbb{R})$*.*

Proof. If G is particle number-preserving, then

$$G^\dagger \hat{N} G\,|0^n\rangle = \hat{N}\,|0^n\rangle = 0, \tag{S15}$$

where the first equality uses Definition 20. This implies $\hat{N}G\,|0^n\rangle = 0$. Since the ground space corresponding to the zero eigenvalue of the particle number operator $\hat{N}$ is one-dimensional and spanned by $|0^n\rangle$, it follows that $G\,|0^n\rangle$ is equal to $|0^n\rangle$, up to a phase. Thus, 1. implies 2.

Noting that $|0^n\rangle\!\langle 0^n|$ is a Gaussian state with a correlation matrix $\Omega = \bigoplus_{j=1}^{n} iY$, we deduce that the correlation matrix of $G\,|0^n\rangle\!\langle 0^n|\,G^\dagger$ is $O\Omega O^T$. Therefore the condition $G\,|0^n\rangle\!\langle 0^n|\,G^\dagger = |0^n\rangle\!\langle 0^n|$ is equivalent to $O\Omega O^T = \Omega$, i.e., O is a real symplectic orthogonal matrix. This proves that 2. is equivalent to 3.

Now, let us assume that $O \in \mathrm{O}(2n) \cap \mathrm{Sp}(2n,\mathbb{R})$. Then, we have for $l \in [n]$:

$$G^\dagger a_l G = G^\dagger \left(\frac{\gamma_{2l-1} + i\gamma_{2l}}{2}\right) G = \sum_{j=1}^{2n} (O_{2l-1,j} + iO_{2l,j})\,\frac{\gamma_j}{2} \tag{S16}$$

$$= \sum_{j=1}^{n} (O_{2l-1,2j-1} + iO_{2l,2j-1})\,\frac{\gamma_{2j-1}}{2} + \sum_{j=1}^{n} (O_{2l-1,2j} + iO_{2l,2j})\,\frac{\gamma_{2j}}{2}, \tag{S17}$$

$$= \sum_{j=1}^{n} (\mathrm{Re}(u)_{l,j} + i\,\mathrm{Im}(u)_{l,j})\,\frac{\gamma_{2j-1}}{2} + \sum_{j=1}^{n} (-\,\mathrm{Im}(u)_{l,j} + i\,\mathrm{Re}(u)_{l,j})\,\frac{\gamma_{2j}}{2}, \tag{S18}$$

$$= \sum_{j=1}^{n} u_{l,j}\,\frac{(\gamma_{2j-1} + i\gamma_{2j})}{2} = \sum_{j=1}^{n} u_{l,j} a_j. \tag{S19}$$

where in the fourth equality we used that $O \in \mathrm{O}(2n) \cap \mathrm{Sp}(2n,\mathbb{R})$, and so, because of Proposition 22, it can be written as $O = \mathrm{Re}(u) \otimes I + \mathrm{Im}(u) \otimes iY$ where $u \in \mathrm{U}(n)$ is a $n \times n$ unitary. Similarly, we have $G^\dagger a_l G = \sum_{j=1}^{n} u^*_{l,j} a^\dagger_j$. This implies

$$G^\dagger \hat{N} G = \sum_{l=1}^{n} G^\dagger a_l^\dagger a_l G = \sum_{l,j,k=1}^{n} u^*_{l,j} u_{l,k} a_j^\dagger a_k = \sum_{j=1}^{n} a_j^\dagger a_j = \hat{N}, \tag{S20}$$

where we used the unitarity of u in the last step. This proves that 3. implies 1. □

Supplementary Material II: Structure of t-doped Gaussian unitaries and states

In this section, we analyze the concept of t-doped fermionic Gaussian unitaries and states.

Definition 24 (t-Doped Fermionic Gaussian Unitary)**.** *A unitary U_t is a (t,κ)-doped fermionic Gaussian unitary if it can be decomposed in terms of Gaussian unitaries $\{G_i\}_{i=0}^t$ and at most t non-Gaussian κ-local gates $\{W_i\}_{i=1}^t$, specifically*

$$U_t = G_t W_t \cdots G_1 W_1 G_0. \tag{S21}$$

Here κ-local refers to the number of distinct Majorana operators that generate each non-Gaussian gate. Informally, a unitary is t-doped Gaussian if it is (t,κ)-doped Gaussian for some fixed constant κ.

In our work, we consider non-Gaussian gates $W_{t'}$ for $t' \in [t]$, each generated by $\kappa \leq 2n$ in κ fixed Majorana operators $\{\gamma_{\mu(t',j)}\}_{j=1}^{\kappa}$, where $\mu(t',1),\dots,\mu(t',\kappa) \in [2n]$. For $\kappa = 3$, an example of a non-Gaussian gate is $\exp(\theta\gamma_1\gamma_2\gamma_3) = \exp(-iY_1\theta)$, where $\theta \in \mathbb{R}$, and for $\kappa = 4$, an example is the SWAP-gate.

Definition 25 (t-Doped Fermionic Gaussian State)**.** *An n-qubit state $|\psi\rangle$ is a (t,κ)-doped (informally, t-doped) fermionic Gaussian state if it can be expressed as $|\psi\rangle = U_t |0^n\rangle$, where U_t is a (t,κ)-doped (t-doped) fermionic Gaussian unitary.*

A. Compression of t-doped Gaussian unitaries and states

We start by presenting a Theorem which shows how all non-Gaussianity in a t-doped unitary can be 'compressed' or 'moved' to the first few qubits.

Theorem 26 (Compression of Non-Gaussianity in t-Doped Unitaries)**.** *Any (t,κ)-doped fermionic Gaussian unitary U_t can be expressed as:*

$$U_t = G_A(u_t \otimes I)G_B, \tag{S22}$$

where G_A, G_B are Gaussian unitaries, and u_t is a unitary supported exclusively on $\lceil \frac{\kappa t}{2} \rceil$ qubits.

Proof. Let us denote $M := \kappa t$. We express the t-doped unitary as $U_t = (\prod_{t'=1}^t G_{t'}W_{t'})G_0$. Rearranging it, we have

$$U_t = \tilde{G}_t \prod_{t'=1}^{t} \tilde{W}_{t'}, \tag{S23}$$

where $\tilde{W}_{t'} := \tilde{G}_{t'-1}^\dagger W_{t'} \tilde{G}_{t'-1}$ and $\tilde{G}_{t'} := G_{t'}..G_0$. Informally, the idea behind this rewriting is that Gaussian operations act nicely under conjugation. Next, we rewrite

$$U_t = \tilde{G}_t G_{\text{aux}} \prod_{t'=1}^{t} (G_{\text{aux}}^\dagger \tilde{W}_{t'} G_{\text{aux}}) G_{\text{aux}}^\dagger, \tag{S24}$$

by introducing a Gaussian operation G_{aux} that we fix later and that will be responsible for moving all the non-Gaussian gates to the first qubits. Now, we set:

$$G_A := \tilde{G}_t G_{\text{aux}} \tag{S25}$$

$$u_t := \prod_{t'=1}^{t} (G_{\text{aux}}^\dagger \tilde{W}_{t'} G_{\text{aux}}) \tag{S26}$$

$$G_B := G_{\text{aux}}^\dagger. \tag{S27}$$

Note that G_A so-defined is Gaussian because the product of Gaussian unitaries is Gaussian, and G_B is clearly Gaussian because the adjoint of a Gaussian unitary is Gaussian. We need to show that it is possible to choose G_{aux} such that u_t is supported only on the first $\lceil M/2 \rceil$ qubits.

More precisely, we will require that G_{aux} ensures that each $G_{\text{aux}}^\dagger \tilde{W}_{t'} G_{\text{aux}}$ is generated by the first M Majorana operators alone. We will achieve it by ensuring that the Heisenberg evolution under $\tilde{G}_{t'-1}G_{\text{aux}}$, of each Majorana that generates $W_{t'}$, has non-trivial support exclusively on the first M Majorana operators. To find G_{aux} with the desired property, we will find the associated orthogonal matrix O_{aux}. Let $\{\mu(t',r)\}_{t'\in[t],r\in[\kappa]}$, with $\mu(t',r)\in[2n]$, be the set of indices of Majorana operators generating the t'-th non-Gaussian gate (listed in increasing order). For example, consider $\kappa=4$ and the t'-th non-Gaussian gate $W_{t'}:=\exp(i\gamma_2\gamma_4\gamma_6\gamma_9+i\gamma_4)$. In this case, $\mu(t',3)=6$. For each such Majorana operator $\gamma_{\mu(t',r)}$, where $r\in[2n]$, its Heisenberg evolution yields

$$G_{\text{aux}}^{\dagger}\tilde{G}_{t'-1}^{\dagger}\gamma_{\mu(t',r)}\tilde{G}_{t'-1}G_{\text{aux}}=\sum_{m=1}^{2n}(O_{t'-1}O_{\text{aux}})_{\mu(t',r),m}\gamma_m, \tag{S28}$$

where $O_{t'-1}$ is the orthogonal matrix associated with $\tilde{G}_{t'-1}$. Our demand on the support of Heisenberg-evolved $\gamma_{\mu(t',r)}$ implies

$$(O_{t'-1}O_{\text{aux}})_{\mu(t',r),m}=(O_{\text{aux}}^TO_{t'-1}^T)_{m,\mu(t',r)}=0 \tag{S29}$$

for any $m\in\{M+1,\dots,2n\}$.

Let us denote as $\{\mathbf{e}_i\}_{i=1}^{2n}$ the canonical basis vectors of $\mathbb{R}^{2n}$. For easy notation, we now denote the unit norm vectors $\{O_{t'-1}^T\mathbf{e}_{\mu(t',r)}\}_{t'\in[t],r\in[\kappa]}$ with the set of vectors $\{\mathbf{v}_j\}_{j=1}^{M}$ (remember that $M=\kappa t$). We can prove the existence of such O_{aux} by proving the existence of its transpose $O:=O_{\text{aux}}^T$. In such notation, the condition in Eq.(S29) reads as:

$$\mathbf{e}_m^TO\mathbf{v}_j=0, \tag{S30}$$

for any $j\in[M]$ and $m\in\{M+1,\dots,2n\}$. In other words, we need to prove the existence of an orthogonal matrix O that maps any given real vectors $\mathbf{v}_1,\dots,\mathbf{v}_M\in\mathbb{R}^{2n}$, where $M\le 2n$, to the span of the first M canonical basis vectors of $\mathbb{R}^{2n}$. The existence of such a matrix is readily established by selecting an orthonormal basis for $W:=\text{Span}(\mathbf{v}_1,\dots,\mathbf{v}_M)$ and defining the orthogonal matrix that maps this orthonormal basis to the first $\dim(W)\le M$ canonical basis vectors. This concludes the proof. □

The subsequent Theorem 27 demonstrates the compression of t-doped Gaussian states.

Theorem 27 (Compression of Non-Gaussianity in t-doped Gaussian states). *Any (t,κ)-doped fermionic Gaussian state $|\psi\rangle$ can be represented as:*

$$|\psi\rangle=G(|\phi\rangle\otimes|0^{n-\kappa t}\rangle), \tag{S31}$$

where G is a Gaussian unitary, and $|\phi\rangle$ is a state supported exclusively on κt qubits.

Proof. Let $|\psi\rangle:=U_t|0^n\rangle$, where $U_t=(\prod_{t'=1}^{t}G_{t'}W_{t'})G_0$ is a t-doped fermionic Gaussian unitary. The proof begins analogously to the one of the previous Theorem 26 and it uses the same notation. In particular, we have:

$$U_t=\tilde{G}_tG_{\text{aux}}\prod_{t'=1}^{t}(G_{\text{aux}}^{\dagger}\tilde{W}_{t'}G_{\text{aux}})G_{\text{aux}}^{\dagger}, \tag{S32}$$

where $\tilde{W}_{t'}:=\tilde{G}_{t'-1}^{\dagger}W_{t'}\tilde{G}_{t'-1}$ and $\tilde{G}_{t'}:=G_{t'}..G_0$. We set, as before

$$G_A:=\tilde{G}_tG_{\text{aux}} \tag{S33}$$

$$u_t:=\prod_{t'=1}^{t}(G_{\text{aux}}^{\dagger}\tilde{W}_{t'}G_{\text{aux}}) \tag{S34}$$

$$G_B:=G_{\text{aux}}^{\dagger}. \tag{S35}$$

However, now, we require that u_t has support on the first M qubits, where $M:=\kappa t$ (while in the previous proof of Theorem 26 we requested $\lceil M/2\rceil$), or, equivalently, we request that the generators of $G_{\text{aux}}^{\dagger}\tilde{W}_{t'}G_{\text{aux}}$ for any $t'\in[t]$ involve only the first $2M$ Majorana operators.

This time we also impose that $G_{\text{aux}}^{\dagger}|0^n\rangle=|0^n\rangle$. This implies that $O_{\text{aux}}^T\in\text{Sp}(2n,\mathbb{R})$ (where O_{aux} is the orthogonal matrix associated to G_{aux}), i.e. O_{aux}^T must be a symplectic orthogonal matrix, because of Lemma 23. We now define $O:=O_{\text{aux}}^T$.

Similarly to the previous theorem and using the same notation, we can ensure that u_t is supported only on the first M qubits by demonstrating the existence of an orthogonal, but this time also symplectic, matrix O that satisfies:

$$\mathbf{e}_m^TO\mathbf{v}_j=0, \tag{S36}$$

for any $j\in[M]$ with arbitrary $\mathbf{v}_1,\dots,\mathbf{v}_M$ real vectors, and $m\in\{2M+1,\dots,2n\}$. The existence of such O follows from the subsequent Lemma 28, which crucially uses the isomorphism between $2n\times 2n$ symplectic orthogonal real matrices and $n\times n$ unitaries [54]. □

Lemma 28 (Compression via Symplectic Orthogonal Transformations)**.** *Let $\{\mathbf{e}_i\}_{i=1}^{2n}$ be the canonical basis of $\mathbb{R}^{2n}$. Let $\mathbf{v}_1, \dots, \mathbf{v}_M \in \mathbb{R}^{2n}$ be a set of unit-norm real vectors, where $M \leq n$. There exists an orthogonal symplectic matrix $O \in \mathrm{O}(2n) \cap \mathrm{Sp}(2n, \mathbb{R})$ such that*

$$\mathbf{e}_i^T O \mathbf{v}_j = 0, \tag{S37}$$

for all $i \in \{2M+1, \dots, 2n\}$ and $j \in [M]$, meaning that all $\{O\mathbf{v}_j\}_{j=1}^{M}$ are exclusively supported on the span of the first $2M$ canonical basis vectors.

Proof. Orthogonal symplectic matrices $O \in \mathrm{O}(2n) \cap \mathrm{Sp}(2n, \mathbb{R})$ have a bijective correspondence with unitary matrices $U \in \mathrm{U}(n)$ through a well-defined vector space mapping [54] (see Proposition 22). Specifically, for a $2n$-dimensional real vector $\mathbf{w} := (w_1, \dots, w_{2n})$, there exists a bijective mapping to an n-dimensional complex vector $\mathbf{f}(\mathbf{w}) := (w_1 - iw_2, \dots, w_{2n-1} - iw_{2n})$. A unitary transformation U in this n-dimensional complex space corresponds to an orthogonal symplectic transformation O in the corresponding $2n$-dimensional real space, and vice versa. Thus, finding a unitary U that maps the span of $\mathbf{f}(\mathbf{v}_1), \dots, \mathbf{f}(\mathbf{v}_M)$ to the span of the first M canonical basis vectors of this n-dimensional complex space implies the existence of a symplectic orthogonal matrix O that maps $\mathbf{v}_1, \dots, \mathbf{v}_M$ to the span of the first $2M$ canonical basis vectors of the $2n$-dimensional real space. To establish the existence of such a unitary, consider the complex vector subspace $W := \mathrm{Span}(\mathbf{f}(\mathbf{v}_1), \dots, \mathbf{f}(\mathbf{v}_M))$ of dimension at most M. By selecting an orthonormal basis for this subspace, we can construct a unitary matrix U that maps this basis to the first $\dim(W) \leq M$ canonical basis vectors. Hence, the existence of the required unitary matrix is confirmed, implying the existence of a symplectic orthogonal matrix O that maps $\mathbf{v}_1, \dots, \mathbf{v}_M$ to the span of the first $2M$ canonical basis vectors. This concludes our proof. □

It is noteworthy that the 'compressed size' obtained for t-doped unitaries, which is $\lceil \kappa t/2 \rceil$, is less than κt which we proved for t-doped Gaussian states.

B. Compression of t-doped Gaussian particle-number preserving unitaries

The subsequent Proposition 29 demonstrates that the compression of t-doped Gaussian unitaries can also be achieved in the particle-number preserving case.

Proposition 29 (Particle number preserving t-doped unitaries)**.** *Let U_t be a t-doped fermionic Gaussian unitary, as per Definition 24, where all the unitaries that compose U_t are particle-number preserving. Then U_t can be decomposed as:*

$$U_t := G_A (u_t \otimes I) G_B, \tag{S38}$$

where G_A and G_B are Gaussian unitaries which preserve the number of particles (see Definition 20) and u_t is a particle-number preserving possibly non-Gaussian unitary supported on κt qubits.

Proof. The proof of such proposition follows the same lines as the one of Theorem 27. In fact, by inspecting the proof, it readily follows that the so-defined G_A is particle-number preserving. The fact that G_B and u_t are particle-number preserving follows from the condition $G_{\mathrm{aux}}^{\dagger} |0^n\rangle = |0^n\rangle$, where $G_B := G_{\mathrm{aux}}^{\dagger}$ and by Lemma 23. □

C. Circuit complexity of t-doped Gaussian unitaries and states

The circuit complexity of a unitary (state) is defined as the minimum number of $\mathcal{O}(1)$-local gates needed for implementing the unitary (state). We will consider locality both in the qubit and in the fermionic sense; in the latter case it refers to the number of distinct Majorana operators that generate each non-Gaussian gate. Our subject of interest is the scaling of the complexity of a t-doped unitary. Throughout this section, we assume $\kappa = \mathcal{O}(1)$ and let $t = t(n)$ change in some way with n. By Definition 24, a t-doped Gaussian unitary U_t can be written as $U_t = G_t W_t \cdots G_1 W_1 G_0$, where $\{G_i\}_{i=0}^{t}$ are Gaussian unitaries and $\{W_i\}_{i=1}^{t}$ are, possibly non-Gaussian, κ-local fermionic gates. From this definition and using the fact that any Gaussian unitary can be decomposed as the product of $\leq 2n(2n-1)/2$ (fermionic) 2-local gates [36, 52], the fermionic circuit complexity of t-doped Gaussian unitaries is upper-bounded by $\mathcal{O}(n^2 t)$. The same can be shown for qubit circuit complexity (see below). But more importantly, we have proven earlier that a t-doped Gaussian unitary can be decomposed as $U_t = G_A(u_t \otimes I) G_B$, where G_A, G_B are Gaussians and u_t is a unitary on $\lceil \frac{\kappa t}{2} \rceil$ qubits. In the following, we show that such decomposition reveals an improved upper bound on the circuit complexity of t-doped Gaussian unitaries.

Proposition 30 (Circuit complexity of t-doped Gaussian unitaries)**.** *The circuit complexity $\mathcal{C}(U_t)$ of a t-doped Gaussian unitary U_t is (both in the qubit and fermionic sense):*

$$\mathcal{C}(U_t) = \begin{cases} \mathcal{O}(n^2 + t^3), & \text{if } \kappa t \leq n \\ \mathcal{O}(n^2 t), & \text{otherwise.} \end{cases} \tag{S39}$$

Proof. Let us assume that $\kappa t \leq n$. Then, U_t can be written as $U_t = G_A(u_t \otimes I)G_B$, where G_A, G_B are Gaussians and u_t is a unitary on $\lceil \frac{\kappa t}{2} \rceil$ qubits. In fact, u_t is itself a (t, κ)-doped Gaussian unitary on $\lceil \frac{\kappa t}{2} \rceil$ qubits. It is not directly obvious, but will be shown momentarily; this will imply the desired circuit complexity $\mathcal{O}(t^3)$. We recall our definitions used in the proof of Theorem 26. We have $\tilde{G}_{t'} := G_{t'}..G_0$ for $t' \in [t]$ and a Gaussian unitary G_{aux}, and set

$$u_t := \prod_{t'=1}^{t} (G_{\text{aux}}^\dagger \tilde{G}_{t'-1}^\dagger W_{t'} \tilde{G}_{t'-1} G_{\text{aux}}) = \prod_{t'=1}^{t} w_{t'}, \tag{S40}$$

where we defined the unitaries $w_{t'} := G_{\text{aux}}^\dagger \tilde{G}_{t'-1}^\dagger W_{t'} \tilde{G}_{t'-1} G_{\text{aux}}$ which act only on the first $\lceil \frac{\kappa t}{2} \rceil$ qubits (equivalently, fermionic modes). We note that $w_{t'}$ is generated by κ Majorana operator superpositions of form $\sum_{i=1}^{\kappa t} [\tilde{\mathbf{v}}_j]_i \gamma_i$, $j \in [\kappa(t'-1)+1, \kappa t']$; here $\tilde{\mathbf{v}}_j := O\mathbf{v}_j$ (cf. notation O and $\mathbf{v}_j$ from the proof of Theorem 26). Hence, for each of these (non-local) non-Gaussian unitaries $w_{t'}$, we can find a Gaussian operation $g_{t'}$ on the first $\lceil \frac{\kappa t}{2} \rceil$ qubits whose associated orthogonal matrix rotates vectors $\tilde{\mathbf{v}}_j$ into the span of the first κ basis vectors. As a result, we have $w_{t'} = g_{t'}^\dagger \tilde{w}_{t'} g_{t'}$, where $\tilde{w}_{t'}$ is now a κ-local non-Gaussian unitary generated by the first κ Majorana operators. By implication, it is also a local qubit gate acting on the first $\lceil \frac{\kappa}{2} \rceil$ qubits. From this it follows that the circuit complexity of each $w_{t'}$ scales as that of a Gaussian $g_{t'}$. As $g_{t'}$ acts on the first $O(t)$ qubits/fermionic modes, its circuit complexity is $O(t^2)$ both in the qubit and the fermionic sense. Therefore, the circuit complexity of u_t is $t\mathcal{O}(t^2) = \mathcal{O}(t^3)$. Moreover, the circuit complexity (both qubit and fermionic) to implement G_A and G_B is $\mathcal{O}(n^2)$. Putting the above observations together, it follows that the circuit complexity of U_t is $\mathcal{O}(n^2 + t^3)$. As long as $\kappa t \leq n$, this upper bound is tighter than the one which proof follows from the t-doped definition, namely $\mathcal{O}(n^2 t)$.

The qubit (and not only fermionic) circuit complexity of $\mathcal{O}(n^2 t)$ for $\kappa t > n$ can be found in a similar way as the complexity of $\mathcal{O}(t^3)$ we showed for u_t above. In particular, consider any κ-local non-Gaussian fermionic unitary $W_{t'}$ which participates in U_t. Using auxilliary Gaussian rotations, its generating Majorana operators can be mapped to $\{\gamma_1, .., \gamma_\kappa\}$, resulting in a unitary supported by the first $\lceil \frac{\kappa}{2} \rceil$ qubits alone. The asymptotic qubit complexity of U_t is thus determined by that of remaining t Gaussian layers, yielding $\mathcal{O}(n^2 t)$ as promised. □

This Proposition reveals that t-doped fermion Gaussian unitaries allow not only a 'spatial compression for the magic', but also a compression of the circuit depth.

D. t-compressible Gaussian states

We now introduce the notion of t-compressible fermionic Gaussian state, a class of states that includes the one of t-doped Gaussian states. We now reiterate Definition 2 for convenience. Throughout this section, we assume that $t \in [n]$.

Definition 31 (t-compressible Gaussian state)**.** *A state $|\psi\rangle$ is a t-compressible (Gaussian) state if and only if it can be represented as $|\psi\rangle = G(|\phi\rangle \otimes |0^{n-t}\rangle)$, where G is a Gaussian operation, and $|\phi\rangle$ is a pure state supported solely on the first t qubits.*

A t-doped Gaussian state is also a κt-compressible Gaussian state because of Theorem 27. However, the reverse is not true because of circuit complexity arguments: t-doped Gaussian states exhibit a circuit complexity of at most $\mathcal{O}(n^2 t)$. In contrast, a t-compressible state features a circuit complexity of $\mathcal{O}(n^2 + \exp(t))$, representing the complexity needed for implementing a single Gaussian operation and preparing a generic state supported on t qubits.

In the subsequent Proposition, we elucidate the structure of the correlation matrix of any t-compressible state, such as t-doped states.

Proposition 32 (Correlation Matrix of a t-compressible Gaussian State)**.** *The correlation matrix $C(|\psi\rangle)$ of a t-compressible Gaussian state $|\psi\rangle$ can be expressed as:*

$$C(|\psi\rangle) = O \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} O^T, \tag{S41}$$

where $\lambda_j \leq 1$ for $j \in [t]$ and $\lambda_j = 1$ for $j \in \{t+1, \ldots, n\}$, and $O \in \mathrm{O}(2n)$ is an orthogonal matrix.

Proof. As per Definition 31, we represent $|\psi\rangle$ as $|\psi\rangle = G(|\phi\rangle \otimes |0^{n-t}\rangle)$, where G is a Gaussian operation and $|\phi\rangle$ is a pure state supported solely on the first t qubits. Utilizing Lemma 16, we can express the correlation matrix $C(|\psi\rangle)$ as follows:

$$C(|\psi\rangle) = QC(|\phi\rangle \otimes \left|0^{n-t}\right\rangle)Q^T \tag{S42}$$

$$= Q\left(C(|\phi\rangle) \oplus C(\left|0^{n-t}\right\rangle)\right)Q^T, \tag{S43}$$

where $Q \in \mathrm{O}(2n)$ is the orthogonal matrix associated to the Gaussian unitary G. By Eq.(S7), we have:

$$C(\left|0^{n-t}\right\rangle) = \bigoplus_{j=1}^{n-t} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{S44}$$

Since $C(|\phi\rangle)$ is an antisymmetric real matrix, we can decompose it into its normal form (Lemma 16):

$$C(|\phi\rangle) = O_t \bigoplus_{j=1}^{t} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} O_t^T \tag{S45}$$

The proof concludes by definining $O := Q(O_t \oplus I_{2n-2t})$. □

The previous proposition reveals that t-compressible states exhibit at least $n-t$ normal eigenvalues which are exactly one. This motivates the following definition, in analogy to the stabilizer dimension defined in the stabilizer case [33].

Definition 33 (Gaussian dimension of a state)**.** *The Gaussian dimension of a state is defined as the number of the normal eigenvalues of its correlation matrix which are equal to one.*

In the following, we show that this is also a sufficient condition for a state to be Gaussian t-compressible.

Lemma 34 (Sufficient Condition for t-Compressibility)**.** *Let $|\psi\rangle$ be an n-qubit quantum state. If $|\psi\rangle$ has Gaussian dimension of $n-t$, then $|\psi\rangle$ is a t-compressible Gaussian state.*

Proof. The correlation matrix of $|\psi\rangle$ can be written in its normal form as $C(|\psi\rangle) = O\Lambda O^T$, where $\Lambda := \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix}$, and $O \in \mathrm{O}(2n)$. The $\{\lambda_j\}_{i=1}^{n}$ are the normal eigenvalues such that the last $n-t$ are equal to one. Consider the state $|\psi'\rangle := G_O^\dagger |\psi\rangle$ where G_O is the Gaussian unitary associated with O. Then, $C(\psi') = O^T C(|\psi\rangle)O = \Lambda$. In particular,

$$\mathrm{Tr}(|\psi'\rangle\!\langle\psi'|\, Z_k) = C(\psi')_{2k-1,2k} = \Lambda_{2k-1,2k} = 1, \tag{S46}$$

for each $k \in \{t+1, \dots, n\}$. Therefore, $|\psi'\rangle$ must be of the form $|\psi'\rangle = |\phi\rangle \otimes |0^{n-t}\rangle$, where $|\phi\rangle$ is an arbitrary state on the first t qubits. Therefore, we have $|\psi\rangle = G_O(|\phi\rangle \otimes |0^{n-t}\rangle)$, which is a t-compressible state. □

Hence, Proposition 32 and Lemma 34 prove the following.

Proposition 35 (Equivalence between t-compressibily and $n-t$ Gaussian dimension)**.** *A n-qubit state is t-compressible if and only if its Gaussian dimension is $n-t$.*

Note that Proposition 35 also proves that a quantum state is a pure Gaussian state if and only if its Gaussian dimension is n. Furthermore, as a direct consequence of the proof of Lemma 34, we establish that the Gaussian unitary associated with a t-compressible Gaussian state can be selected as the Gaussian unitary corresponding to any orthogonal matrix placing its correlation matrix in the normal form (Lemma 16). This is summarized as follows:

Lemma 36. *Every t-compressible Gaussian state $|\psi\rangle$ can be written as $|\psi\rangle := G_O(|\phi\rangle \otimes |0^{n-t}\rangle)$, where G_O is chosen as the Gaussian unitary associated with an orthogonal matrix $O \in \mathrm{O}(2n)$ that arranges its correlation matrix in the normal form described in Lemma 16, and $|\phi\rangle$ is a state supported on t qubits.*

Supplementary Material III: Tomography algorithm

In this section, we present a detailed and rigorous analysis of the tomography algorithm for t-compressible states outlined in the main text (Algorithm 1) and reiterated in Algorithm 2 for ease of reference and to include extra details. Throughout this section, we assume that $t \in [n]$.

Algorithm 2: Learning Algorithm for t-compressible fermionic Gaussian states

```
Input: Accuracy $\varepsilon$, failure probability $\delta$, $N := \lceil \frac{256n^5}{\varepsilon^4}\log\left(\frac{12n^2}{\delta}\right) + 2N_{\mathrm{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3}) + 24\log\left(\frac{3}{\delta}\right)\rceil$ copies of the $t$-compressible state
    $|\psi\rangle$, where $N_{\mathrm{tom}}$ is the number of copies needed for $t$-qubit pure state tomography with accuracy $\frac{\varepsilon}{2}$ and failure probability $\frac{\delta}{3}$.
Output: A classical description of $|\hat{\psi}\rangle$, ensuring $d_{\mathrm{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq \varepsilon$ with probability at least $1-\delta$.
Estimate the correlation matrix of $|\psi\rangle$ using $\lceil \frac{256n^5}{\varepsilon^4}\log\left(\frac{12n^2}{\delta}\right)\rceil$ single-copy measurements (see Lemma 38), obtaining $\hat{C}$;
Express $\hat{C}$ in its normal form $\hat{C} = \hat{O}\hat{\Lambda}\hat{O}^T$ (Eq.(1)) and find the Gaussian unitary $G_{\hat{O}}$ associated with $\hat{O} \in \mathrm{O}(2n)$;
for $i \leftarrow 1$ to $\lceil 2N_{\mathrm{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3}) + 24\log\left(\frac{3}{\delta}\right)\rceil$ do
    Apply $G_{\hat{O}}^{\dagger}$ to $|\psi\rangle$;
    Measure the last $n-t$ qubits in the computational basis;
    if the outcome corresponds to $|0^{n-t}\rangle$ then
        Proceed;
    else
        Discard and move to the next iteration;
    Perform a step of pure state tomography [56] on the remaining $t$ qubits;
Obtain the $t$-qubit state $|\hat{\phi}\rangle$ from tomography;
return $\hat{O}$ and $|\hat{\phi}\rangle$, which identify $|\hat{\psi}\rangle := G_{\hat{O}}^{\dagger}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle)$;
```

A. Useful lemmas and subroutines

Let us start with a Lemma, which gives a sample complexity upper bound to estimate the correlation matrix of a state using single-qubit Pauli-basis measurements. We recall that the correlation matrix of a state ρ is a real antisymmetric matrix, defined as:

$$[C(\rho)]_{j,k} = \mathrm{Tr}(O^{(j,k)}\rho), \tag{S47}$$

where $O^{(j,k)} := -i\gamma_j\gamma_k$, for $j < k \in [2n]$ (and the other elements are given by the antisymmetricity of the matrix). Note that $O^{(j,k)}$ are Pauli observables. Thus, we have a total of $M := n(2n-1)$ Pauli expectation values to estimate.

Lemma 37 (Sample Complexity for Estimating the Correlation Matrix by Pauli measurements)**.** *Let $\varepsilon_c, \delta > 0$. Assume to have access to $N \geq N_c(n, \varepsilon_c, \delta)$, with*

$$N_c(n, \varepsilon_c, \delta) := \left\lceil \frac{8n^3(2n-1)}{\varepsilon_c^2}\log\left(\frac{2n(2n-1)}{\delta}\right)\right\rceil, \tag{S48}$$

copies of an n-qubit state ρ. Utilizing only N single-copies measurements in the Pauli basis, with probability $\geq 1-\delta$, we can construct an anti-symmetric real matrix $\hat{C}$ such that it satisfies:

$$\left\|\hat{C} - C(\rho)\right\|_{\infty} \leq \varepsilon_c. \tag{S49}$$

Proof. Let $\varepsilon > 0$ an accuracy parameter to be fixed. For each $j < k \in [2n]$, we measure N' copies of ρ in the Pauli basis corresponding to $O^{(j,k)}$, obtaining outcomes $\{X_m^{(j,k)}\}_{m=1}^{N'}$, where $X_m^{(j,k)} \in \{-1,+1\}$. Let $\hat{C}_{j,k} := \frac{1}{N'}\sum_{m=1}^{N'} X_m^{(j,k)}$. Hoeffding's inequality (specifically Corollary 9) implies that $N' \geq (4/(2\varepsilon^2))\log(2M/\delta)$ suffices to guarantee that, with probability at least $1-\delta/M$, we have $|\hat{C}_{j,k} - \mathrm{Tr}(O^{(j,k)}\rho)| < \varepsilon$. By using the union bound, we conclude that the probability that this holds for any $j < k \in [2n]$ is at least $1-\delta$. More specifically:

$$\Pr\Big(\forall j < k \in [2n] : |\hat{C}_{j,k} - \mathrm{Tr}(O^{(j,k)}\rho)| < \varepsilon\Big) = 1 - \Pr\Big(\exists j < k \in [2n] : |\hat{C}_{j,k} - \mathrm{Tr}(O^{(j,k)}\rho)| \geq \varepsilon\Big) \tag{S50}$$

$$\geq 1 - \sum_{j<k\in[2n]} \Pr\Big(|\hat{C}_{j,k} - \mathrm{Tr}(O^{(j,k)}\rho)| \geq \varepsilon\Big) \tag{S51}$$

$$\geq 1 - \delta. \tag{S52}$$

Therefore, the total number of measurements needed is $N = N'M$. Now, we can conclude by transferring the error to the operator norm. Let $A := \hat{C} - C(\rho)$. For the definition of the operator norm, we have $\|A\|_{\infty} := \sup_{|\psi\rangle}\sqrt{|\langle\psi|\, A^{\dagger}A\, |\psi\rangle|}$. Thus, we have:

$$\left|\langle\psi| A^\dagger A |\psi\rangle\right| \leq \sum_{i,j,k=1}^{2n} \left|\langle\psi| |i\rangle\langle i| A^\dagger |j\rangle\langle j| A |k\rangle\langle k| |\psi\rangle\right| = 2n\varepsilon^2 \sum_{i,k=1}^{2n} |\langle\psi|i\rangle| \, |\langle k|\psi\rangle| \leq 4n^2\varepsilon^2 \tag{S53}$$

where, in the first step, we inserted the resolution of the identity and applied the triangle inequality, in the second step, we applied the upper bound on each matrix element, and, in the last step, we used the Cauchy-Schwartz inequality. Hence, we have $\left\|\hat{C} - C(\rho)\right\|_\infty \leq 2n\varepsilon$. We conclude by choosing $\varepsilon_c := \varepsilon/2n$. □

While the sequential estimation of individual correlation matrix entries by measurements in the Pauli basis, as described above, may not be the most sample-efficient approach, it might be convenient to adopt in an experiment because of its easy implementation scheme. However, instead of independently estimating each correlation matrix entry, one could choose to simultaneously measure mutually commuting observables [58] or utilize the fermionic classical shadow protocol introduced in [52, 59, 60]. This refinement would lead to a reduction in sample complexity by a factor of n, at the cost of implementing a slightly more complicated measurement scheme.

For completeness, we present now a Lemma which gives a sample complexity upper bound for estimating the correlation matrix using a commuting observables measurement scheme. The idea is to partition the observables $O^{(j,k)} := -i\gamma_j\gamma_k$, for $j < k \in [2n]$ into disjoint sets of commuting observables. Subsequently, one employs the fact that commuting Pauli observables can be measured simultaneously via a Clifford measurement [58, 70]. A crucial observation is that two different Pauli observables of the form $-i\gamma_j\gamma_k$ commute if and only if they are associated with different Majorana operators. Using this observation, we can partition these $M = (2n-1)n$ observables into $2n-1$ disjoint sets, each containing n commuting Pauli observables. We refer to [58] Appendix C for details of such a partition, and we omit repeating the construction here. However, we point out that the required Clifford transformations can be chosen to be Gaussian as well.

Lemma 38 (Sample Complexity for Estimating the Correlation Matrix by Grouping Commuting Observables)**.** *Let $\varepsilon_c, \delta > 0$. Assume to have access to $N \geq N_c(n, \varepsilon_c, \delta)$, with*

$$N_c(n, \varepsilon_c, \delta) := \left\lceil \frac{8n^2(2n-1)}{\varepsilon_c^2} \log\left(\frac{2n(2n-1)}{\delta}\right) \right\rceil, \tag{S54}$$

copies of an n-qubit state ρ. Utilizing N single-copy (Gaussian) measurements, with probability $\geq 1-\delta$, we can construct an anti-symmetric real matrix $\hat{C}$ such that it satisfies:

$$\left\|\hat{C} - C(\rho)\right\|_\infty \leq \varepsilon_c. \tag{S55}$$

Proof. For each of the $2n-1$ sets of commuting Pauli, we find the Clifford U that allows us to simultaneously measure such commuting Pauli in the given set, i.e. we map each of the n Pauli to $\{Z_k\}_{k=1}^n$. Now this Clifford can also be chosen to be Gaussian. Indeed, the key constraint on U is that each of the different Paulis of the form $-i\gamma_j\gamma_k$ with $j < k \in [2n]$ (where pairs (j,k) are non-overlapping since these Paulis commute) is mapped to $\{Z_k\}_{k=1}^n$ with $Z_k := -i\gamma_{2k-1}\gamma_{2k}$. This constraint can be satisfied by using a Gaussian operation associated to the orthogonal matrix which is a permutation of the Majorana indices from the commuting Paulis into the Majorana indices from the Z-Paulis. Consequently, we measure N' copies of $U\rho U^\dagger$ in the computational basis. Thus, for each $O^{(j,k)}$, we obtain outcomes $\{X_m^{(j,k)}\}_{m=1}^{N'}$, where $X_m^{(j,k)} \in \{-1,+1\}$. The unbiased estimators are $\hat{C}_{j,k} := \frac{1}{N'}\sum_{m=1}^{N'} X_m^{(j,k)}$. As before, Hoeffding's inequality and union bound imply that $N' \geq (2/\varepsilon^2)\log(2M/\delta)$ suffices to guarantee that the probability of $|\hat{C}_{j,k} - \mathrm{Tr}(O^{(j,k)}\rho)| < \varepsilon$ holding for each $j < k \in [2n]$ is at least $1-\delta$. Therefore, the total number of measurements needed is $N = N'(2n-1)$. We can conclude as in the previous Lemma. □

Lemma 39 (Perturbation bounds on the normal eigenvalues of correlation matrices)**.** *Let A and B be two $2n \times 2n$ anti-symmetric real matrices with normal eigenvalues $\{\lambda_k(A)\}_{k=1}^n$ and $\{\lambda_k(B)\}_{k=1}^n$ respectively ordered in increasing order. Then, we have:*

$$|\lambda_k(A) - \lambda_k(B)| \leq \|A - B\|_\infty, \tag{S56}$$

for any $k \in [n]$.

Proof. This follows from the fact that $C := iA$ and $D := iB$ are Hermitian matrices. Applying Weyl's Perturbation Theorem (see Ref. [71], section VI), which states that two $2n \times 2n$ Hermitian matrices C and D, with eigenvalues $c_1 \leq \cdots \leq c_{2n}$ and $d_1 \leq \cdots \leq d_{2n}$, satisfy:

$$\|C - D\|_\infty \geq \max_{j\in[n]} |c_j - d_j|. \tag{S57}$$

Since A and B are antisymmetric, their eigenvalues are $\{\pm i\lambda_k(A)\}_{k=1}^n$ and $\{\pm i\lambda_k(B)\}_{k=1}^n$ respectively. Hence, the eigenvalues of C and D are $\{\pm\lambda_k(A)\}_{k=1}^n$ and $\{\pm\lambda_k(B)\}_{k=1}^n$ respectively. This implies that:

$$\|A-B\|_\infty = \|C-D\|_\infty \geq \max_{j\in[2n]} |c_j - d_j| = \max_{k\in[n]} |\lambda_k(A)-\lambda_k(B)|. \tag{S58}$$

□

To formalize our learning algorithm, it is useful to invoke the following well-known lemma.

Lemma 40 (Quantum Union Bound (Adapted) [61, 72, 73])**.** *Let $\rho := |\psi\rangle\!\langle\psi|$ be a pure state, and let $\{\varepsilon_i\}_{i=1}^n \in [0,1]$. Consider a subset of qubit indices $\mathcal{Q} \subseteq [n]$. If $\operatorname{tr}\Big(|0\rangle\!\langle 0|_q\,\rho\Big) \geq 1-\varepsilon_i$ for each $q\in\mathcal{Q}$, then, when the qubits in $\mathcal{Q}$ are sequentially measured in the computational basis, all outcomes correspond to $|0\rangle$ with a probability of at least $1-\sum_{i=1}^n \varepsilon_i$. If all measurements correspond to $|0\rangle$, the trace distance between the post-measurement state $|\psi_{\mathrm{post}}\rangle$ and the initial state $|\psi\rangle$ is given by:*

$$d_{\mathrm{tr}}(|\psi\rangle, |\psi_{\mathrm{post}}\rangle) \leq \sqrt{\sum_{i=1}^n \varepsilon_i}, \tag{S59}$$

where $P = \bigotimes_{q\in\mathcal{Q}} |0\rangle\!\langle 0|_q$, and $|\psi_{\mathrm{post}}\rangle := P|\psi\rangle / \|P|\psi\rangle\|_2$.

We now leverage this known lemma to prove the following.

Lemma 41. *Let $|\psi\rangle$ be a t-compressible Gaussian state. Given an estimate $\hat{C}$ for the correlation matrix $C(|\psi\rangle)$, there exists a Gaussian operation $\hat{G}$ such that:*

$$d_{\mathrm{tr}}(|\phi\rangle\otimes|0^{n-t}\rangle, \hat{G}^\dagger|\psi\rangle) \leq \sqrt{(n-t)\left\|\hat{C}-C(|\psi\rangle)\right\|_\infty}, \tag{S60}$$

where $|\phi\rangle\otimes|0^{n-t}\rangle$ corresponds to the post-measurement state obtained by measuring the last $n-t$ qubits of the state $\hat{G}^\dagger|\psi\rangle$ in the computational basis and obtaining the outcome corresponding to $|0^{n-t}\rangle$. This event occurs with a probability of at least $1-(n-t)\left\|\hat{C}-C\right\|_\infty$.

Proof. According to Proposition 32, the correlation matrix $C := C(|\psi\rangle)$ can be put in the form $C = O\Lambda O^{\mathrm{T}}$, where $O\in \mathrm{O}(2n)$ and $\Lambda = i\bigoplus_{j=1}^n \lambda_j(C)Y$. Here, $\lambda_j \leq 1$ for $j\in[t]$ and $\lambda_j = 1$ for $j\in\{t+1,\dots n\}$, and Y represents the Y-Pauli matrix. Let $\varepsilon_c := \left\|\hat{C}-C\right\|_\infty$, then we have (because of Lemma 39) that $|\lambda_j(\hat{C})-\lambda_j(C)| \leq \varepsilon_c$, where $\{\pm\lambda_j(\hat{C})\}_{j=1}^n$ and $\{\pm\lambda_j(C)\}_{j=1}^n$ are the normal eigenvalues of the matrices $\hat{C}$ and C respectively. Thus, we have:

$$\lambda_m(\hat{C}) \geq 1-\varepsilon_c, \tag{S61}$$

for $m\in\{t+1,\dots n\}$. We can now express the real anti-symmetric matrix $\hat{C}$ in its normal form $\hat{C} = \hat{O}\hat{\Lambda}\hat{O}^T$, where $\hat{O}\in\mathrm{O}(2n)$ is an orthogonal matrix and $\hat{\Lambda}$ is a matrix of the form $\hat{\Lambda} = i\bigoplus_{j=1}^n \lambda_j(\hat{C})Y$, with $\lambda_j(\hat{C})\in\mathbb{R}$ for any $j\in[n]$. Next, consider the state $|\psi'\rangle := \hat{G}^\dagger|\psi\rangle$, where $\hat{G}$ is the Gaussian unitary associated to $\hat{O}^T$. It holds that $|C(\psi')_{j,k} - (\hat{\Lambda})_{j,k}| \leq \varepsilon_c$, where we used that $C(\psi') = \hat{O}^T C(|\psi\rangle)\hat{O}$, $\hat{\Lambda} = \hat{O}^T\hat{C}\hat{O}$, Cauchy-Schwarz and the definition of infinity norm. Therefore, we have $C(\psi')_{j,k} \geq (\hat{\Lambda})_{j,k} - \varepsilon_c$. In particular, for $m\in\{t+1,\dots,n\}$, we get:

$$\begin{aligned}
\operatorname{Tr}(Z_m\psi') &= C(\psi')_{2m-1,2m} &\text{(S62)}\\
&\geq (\hat{\Lambda})_{2m-1,2m} - \varepsilon_c &\text{(S63)}\\
&= \lambda_m(\hat{C}) - \varepsilon_c &\text{(S64)}\\
&\geq 1-2\varepsilon_c, &\text{(S65)}
\end{aligned}$$

where $Z_m = -i\gamma_{2m-1}\gamma_{2m}$ is the Z-Pauli operator acting on the m-th qubit and in the last step we used Eq.(S61). Therefore, we also have $\operatorname{Tr}(|0\rangle\!\langle 0|_m\,\psi') \geq 1-\varepsilon_c$. By using the Quantum Union Bound (Lemma 40), we have:

$$d_{\mathrm{tr}}(|\psi'\rangle, |\phi\rangle\otimes|0^{n-t}\rangle) \leq \sqrt{(n-t)\varepsilon_c}, \tag{S66}$$

where $|\phi\rangle\otimes|0^{n-t}\rangle$ is the post-measurement state after having measured the outcomes corresponding to $|0^{n-t}\rangle$ in the last $n-t$ qubits. By Lemma 40, this scenario occurs with probability at least $1-(n-t)\varepsilon_c$. □

In the following, we mention the guarantees of a full pure state tomography algorithm, which demonstrates optimal dependence on the number of qubits and uses only single-copies measurements, albeit with a trade-off in accuracy compared to other algorithms [3, 74]. This is an example of a procedure that we can utilize in our t-qubits full state tomography step of our learning algorithm.

Lemma 42 (Fast State Tomography [56]). *For any unknown n-qubit pure state $|\psi\rangle$, there exists a quantum algorithm that, utilizing $N_{\text{tom}}(n,\varepsilon,\delta) := \mathcal{O}\big(2^n n\log(1/\delta)\varepsilon^{-4}\big)$ copies of $|\psi\rangle$ and $T_{\text{tom}}(n,\varepsilon,\delta) := \mathcal{O}\big(4^n n^3\log(1/\delta)\varepsilon^{-5}\big)$ time, generates a classical representation of a state $|\tilde{\psi}\rangle$ that is ε-close to $|\psi\rangle$ in trace distance with probability at least $1-\delta$. Furthermore, the algorithm requires only single-copy Clifford measurements and classical post-processing.*

Next, we provide a lemma that is useful in the proof of the subsequent Theorem 44.

Lemma 43 (Boosting the probability of success). *Let $\delta > 0$ and $N' \in \mathbb{N}$. Consider an algorithm $\mathcal{A}$ that succeeds with a probability of $p_{\text{succ}} \geq \frac{3}{4}$. If we execute $\mathcal{A}$ a total of $m \geq \lceil 2N' + 24\log(\frac{1}{\delta})\rceil$ times, then $\mathcal{A}$ will succeed at least N' times with a probability of at least $1-\delta$.*

Proof. We will employ a Chernoff bound 7 to establish this result. Define binary random variables $\{X_i\}_{i=1}^m$ as follows:

$$X_i = \begin{cases} 1 & \text{if } \mathcal{A} \text{ succeeds,} \\ 0 & \text{if } \mathcal{A} \text{ fails.} \end{cases} \tag{S67}$$

Define $\hat{X} := \sum_{i=1}^m X_i$. We have $\mathbb{E}[\hat{X}] = mp_{\text{succ}}$. Moreover, we aim to upper bound by δ the probability that $\mathcal{A}$ succeeds fewer than N' times, which is $\Pr\big(\hat{X} \leq N'\big)$. We first write it as $\Pr\big(\hat{X} \leq N'\big) = \Pr\big(\hat{X} \leq (1-\alpha)\,\mathbb{E}[\hat{X}]\big)$, where we defined $\alpha := 1 - \frac{N'}{mp_{\text{succ}}}$. Note that α satisfies $\alpha \geq \frac{1}{3}$, if

$$m \geq 2N', \tag{S68}$$

exploiting the fact that $p_{\text{succ}} \geq \frac{3}{4}$. Applying the Chernoff bound, we obtain:

$$\Pr\Big(\hat{X} \leq (1-\alpha)\mathbb{E}[\hat{X}]\Big) \leq \exp\left(-\frac{\alpha^2\mathbb{E}[\hat{X}]}{2}\right) = \exp\left(-\frac{\alpha^2}{2}p_{\text{succ}}m\right). \tag{S69}$$

This is upper bounded by δ if

$$m \geq \frac{2}{p_{\text{succ}}\alpha^2}\log\left(\frac{1}{\delta}\right). \tag{S70}$$

Therefore, choosing m as follows satisfies Eq. (S68) and Eq. (S70):

$$m \geq 2N' + \frac{2}{\left(\frac{3}{4}\right)\left(\frac{1}{3}\right)^2}\log\left(\frac{1}{\delta}\right) = 2N' + 24\log\left(\frac{1}{\delta}\right), \tag{S71}$$

where we used the fact that $p_{\text{succ}} \geq \frac{3}{4}$ and $\alpha \geq \frac{1}{3}$. □

B. Joining the pieces: proof of correctness

We now present the main theorem which puts together the lemmas we have discussed. It demonstrates that to learn t-doped fermionic Gaussian states, or more generally t-compressible Gaussian states, with $t = \mathcal{O}(\log(n))$, only resources scaling polynomially in the number of qubits are required.

Theorem 44 (Efficient Learning of t-Compressible Gaussian States). *Let $|\psi\rangle$ be a t-compressible Gaussian state, and consider $\varepsilon, \delta \in (0,1]$. By utilizing*

$$N \geq \frac{256n^5}{\varepsilon^4}\log\left(\frac{12n^2}{\delta}\right) + 2N_{\text{tom}}\left(t, \frac{\varepsilon}{2}, \frac{\delta}{3}\right) + 24\log\left(\frac{3}{\delta}\right) \tag{S72}$$

single-copy measurements and

$$T \geq \mathcal{O}(n^3) + T_{\text{tom}}\left(t, \frac{\varepsilon}{2}, \frac{\delta}{3}\right) \tag{S73}$$

computational time, Algorithm 2 yields a classical representation of a state $|\hat{\psi}\rangle$, satisfying $d_{\text{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq \varepsilon$ with probability $\geq 1-\delta$.

Here, $N_{\text{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3})$ and $T_{\text{tom}}(t, \frac{\varepsilon}{2}, \frac{\delta}{3})$ respectively denote the number of copies and computational time sufficient for full state tomography of a t-qubit state with an $\varepsilon/2$ accuracy and a failure probability of at most $\delta/3$ (using the notation of Lemma 42).

Proof. The learning procedure is outlined in Algorithm 2 (or Algorithm 1 in the main text). We now establish its efficiency and correctness. According to Lemma 38, $N_c(n, \varepsilon_c, \delta/3)$ single copies of $|\psi\rangle$ are sufficient to construct an anti-symmetric real matrix $\hat{C}$ such that $\left\|\hat{C} - C\right\|_\infty \leq \varepsilon_c$ with a probability of at least $1 - \delta/3$. Here, we set $\varepsilon_c := \varepsilon^2/(4(n-t))$. Then, we can find the orthogonal matrix $\hat{O} \in \mathrm{O}(2n)$ such that it puts $\hat{C}$ in its normal form Eq.(1), which can be performed in $\mathcal{O}(n^3)$ time. Employing this, we construct the associated Gaussian unitary $\hat{G}$ (a task achievable in time $\mathcal{O}(n^3)$, see [36, 52]). Subsequently, we consider the state $\hat{G}^\dagger |\psi\rangle$. As per Lemma 41, we have

$$d_{\text{tr}}(|\phi\rangle \otimes \left|0^{n-t}\right\rangle, \hat{G}^\dagger |\psi\rangle) \leq \frac{\varepsilon}{2}, \tag{S74}$$

where $|\phi\rangle \otimes |0^{n-t}\rangle$ corresponds to the post-measurement state obtained by measuring the last $n-t$ qubits of the state $\hat{G}^\dagger |\psi\rangle$ in the computational basis and obtaining the outcome corresponding to $|0^{n-t}\rangle$. The probability of such an occurrence, as per Lemma 41, is at least $1 - \varepsilon^2/4 \geq 3/4$. Thus, the algorithm proceeds iteratively by querying a total of m copies of $|\psi\rangle$. In each iteration, it applies the unitary $\hat{G}^\dagger$ to $|\psi\rangle$ and computational basis measurements on the last $n-t$ qubits. By choosing $m := \lceil 2N_{\text{tom}}(t, \varepsilon/2, \delta/3) + 24\log(3/\delta)\rceil$, it is guaranteed that the measurements outcome corresponding to $|0^{n-t}\rangle$ occurred at least $N_{\text{tom}}(t, \varepsilon/2, \delta/3)$ with probability at least $1 - \delta/3$ (this follows by Lemma 43). Applying the tomography algorithm of Lemma 42 to the first t qubits of all the copies where we obtained the outcome corresponding to $|0^{n-t}\rangle$, we obtain an output state $|\hat{\phi}\rangle$ such that it is guaranteed that:

$$d_{\text{tr}}(|\hat{\phi}\rangle, |\phi\rangle) \leq \frac{\varepsilon}{2}, \tag{S75}$$

with a probability of at least $1 - \delta/3$. Our output state is $|\hat{\psi}\rangle := \hat{G}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle)$, and the information about such a state is provided in the output by providing the orthogonal matrix $\hat{O} \in \mathrm{O}(2n)$, which identifies $\hat{G}$, and the t-qubit state $|\hat{\phi}\rangle$.

Considering the trace distance between $|\hat{\psi}\rangle$ and $|\psi\rangle$ and applying the triangle inequality with $\hat{G}(|\phi\rangle \otimes |0^{n-t}\rangle)$ as the reference state, we have:

$$d_{\text{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq d_{\text{tr}}(|\hat{\phi}\rangle, |\phi\rangle) + d_{\text{tr}}(|\phi\rangle \otimes \left|0^{n-t}\right\rangle, \hat{G}^\dagger |\psi\rangle), \tag{S76}$$

where in the last step we use the unitary-invariance of the trace distance and $d_{\text{tr}}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle, |\phi\rangle \otimes |0^{n-t}\rangle) = d_{\text{tr}}(|\hat{\phi}\rangle, |\phi\rangle)$. The algorithm's overall failure probability is contingent on the potential failure of any of the three subroutines—specifically, correlation matrix estimation, measurement of the last $n-t$ qubits, and the tomography protocol. Each subroutine is associated with a failure probability of at most $\delta/3$. Consequently, by the union bound, the algorithm's total failure probability is at most δ. Utilizing Eqs.(S74),(S75),(S76) and assuming the case in which the algorithm does not fail, we deduce $d_{\text{tr}}(|\hat{\psi}\rangle, |\psi\rangle) \leq \varepsilon$. The overall sample complexity is determined by the number of copies needed to estimate the correlation matrix $N_c(n, \varepsilon_c, \delta/3)$ plus the copies m for tomography, i.e., a total number of copies

$$N = \left\lceil \frac{256n^5}{\varepsilon^4} \log\left(\frac{12n^2}{\delta}\right) + 2N_{\text{tom}}\left(t, \frac{\varepsilon}{2}, \frac{\delta}{3}\right) + 24\log\left(\frac{3}{\delta}\right) \right\rceil, \tag{S77}$$

suffices, which is $\mathcal{O}(\mathrm{poly}(n) + \exp(t))$. On the other hand, the time complexity involves post-processing of the estimated correlation matrix, requiring $\mathcal{O}(n^3)$ time, and the time-complexity for full-state tomography which is $\mathcal{O}(\exp(t))$. □

Remark 45. *The output state of Algorithm 1 is $|\hat{\psi}\rangle := \hat{G}(|\hat{\phi}\rangle \otimes |0^{n-t}\rangle)$. Specifically, to provide a classical representation of $|\hat{\psi}\rangle$ in the output, it suffices to give the orthogonal matrix $\hat{O} \in \mathrm{O}(2n)$ associated with $\hat{G}$ and the classical description of the t-qubit state $|\hat{\phi}\rangle$. Therefore, the memory necessary to store the classical description of the state outputted by Algorithm 1 is $\mathcal{O}(\mathrm{poly}(n, 2^t))$, similarly to its time and sample complexity.*

Supplementary Material IV: Testing t-compressible states

In this section, we address property testing problem, i.e. the problem of determining whether a state is close or far from the set of states t-compressible states (or equivalently we test the Gaussian dimension of a state). We begin by establishing an upper bound on the trace distance between a state and the set of t-compressible Gaussian states. Subsequently, we present a lower bound on the same quantity. Finally, we leverage these two bounds to develop a testing algorithm for t-compressible Gaussian states.

We note that the testing problem in the context of fermionic Gaussian states ($t = 0$) was also unsolved. However, a forthcoming paper [67] addresses the testing problem for general, possibly mixed, fermionic Gaussian states. Here, we generalize the results presented in [67] regarding pure Gaussian testing to the scenario of t-compressible Gaussian states, using ideas developed in [67].

A. Approximate t-compressible state

We observed in Lemma 34 that when $n - t$ normal eigenvalues of a state's correlation matrix are precisely one, the state is a t-compressible state. However, when these eigenvalues are close to one, we may inquire about the existence of a t-compressible state in close proximity. This inquiry is formalized in the subsequent Proposition 46.

Proposition 46 (Check the closeness to a t-compressible Gaussian state)**.** *Let $|\psi\rangle$ be a quantum state. Let $\{\lambda_i\}_{i=1}^n$ be the normal eigenvalues of its correlation matrix ordered in increasing order. Then, there exists a t-compressible Gaussian state $|\psi_t\rangle$ such that:*

$$d_{\mathrm{tr}}(|\psi_t\rangle , |\psi\rangle) \leq \sqrt{\sum_{k=t+1}^{n} \frac{1}{2}(1-\lambda_k)}. \tag{S78}$$

In particular, $|\psi_t\rangle$ can be chosen as $|\psi_t\rangle := G_O(|\phi\rangle \otimes |0^{n-t}\rangle)$, where G_O is the Gaussian unitary associated with the orthogonal matrix $O \in \mathrm{O}(2n)$ that puts the correlation matrix of $|\psi\rangle$ in its normal form (Lemma 16), and $|\phi\rangle \otimes |0^{n-t}\rangle$ is the state obtained by projecting the state $G_O^\dagger |\psi\rangle$ onto the zero state on the last $n - t$ qubits.

Proof. We can define the state $|\psi'\rangle := G_O^\dagger |\psi\rangle$. We have:

$$\mathrm{Tr}(|\psi'\rangle\!\langle\psi'| \, Z_k) = C(\psi')_{2k-1,2k} = \Lambda_{2k-1,2k} = \lambda_k = 1 - (1 - \lambda_k), \tag{S79}$$

for each $k \in \{t + 1, \dots , n\}$. By using that $Z_k = 2 \, |0\rangle\!\langle 0|_k - I$, we have:

$$\mathrm{Tr}(|\psi'\rangle\!\langle\psi'| \, |0\rangle\!\langle 0|_k) = 1 - \frac{(1-\lambda_k)}{2} \tag{S80}$$

By Quantum Union Bound (Lemma 40), we have:

$$d_{\mathrm{tr}}(|\psi'\rangle , |\phi\rangle \otimes |0^{n-t}\rangle) \leq \sqrt{\sum_{k=t+1}^{n} \frac{(1-\lambda_k)}{2}}. \tag{S81}$$

Therefore, by using the unitarity invariance of the trace-norm, we can conclude. □

From this, it readily follows that trace distance between the state and the set of t-compressible pure Gaussian states $\mathcal{G}_t$ is upper bounded by:

$$\min_{|\phi_t\rangle \in \mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle , |\phi_t\rangle) \leq \sqrt{(n-t)\frac{(1-\lambda_{t+1})}{2}}. \tag{S82}$$

B. Lower bound on the trace distance from the set of t-compressible states

In this section, we establish a lower bound on the trace distance of a state from the set of t-compressible Gaussian states. We denote the set of pure t-compressible Gaussian states as $\mathcal{G}_t$. In the following proof, we follow the derivation presented in Ref. [67] for the case of pure Gaussian states ($t = 0$), extending it to t-compressible states.

Proposition 47. *Let $|\psi\rangle$ be a quantum state, and let $\{\lambda_i\}_{i=1}^n$ be the normal eigenvalues of its correlation matrix, ordered in increasing order. The lower bound on the trace distance between the state and the set of t-compressible pure Gaussian states $\mathcal{G}_t$ is given by:*

$$\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \geq \frac{1}{2}(1-\lambda_{t+1}) \tag{S83}$$

Proof. Consider an arbitrary operator O with $\|O\|_\infty \leq 1$, to be fixed later. Then, we have:

$$\begin{aligned}\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) &= \min_{|\phi_t\rangle\in\mathcal{G}_t} \frac{1}{2}\| \, |\psi\rangle\!\langle\psi| - |\phi_t\rangle\!\langle\phi_t| \, \|_1 &\text{(S84)}\\ &\geq \min_{|\phi_t\rangle\in\mathcal{G}_t} \frac{1}{2}|\operatorname{Tr}(O(|\psi\rangle\!\langle\psi| - |\phi_t\rangle\!\langle\phi_t|))|, &\text{(S85)}\end{aligned}$$

where in the last step, we used Holder's inequality.

Let $C(|\psi\rangle)$ and $C(|\phi_t\rangle)$ be the correlation matrices of $|\psi\rangle$ and $|\phi_t\rangle$, respectively. Since $C(|\psi\rangle) - C(|\phi_t\rangle)$ is real and anti-symmetric, it can be brought into its normal form $C(|\psi\rangle) - C(|\phi_t\rangle) = Q^T\Lambda' Q$, where $\Lambda' = \bigoplus_{j=1}^n i\sigma'_j Y$ and $\{\sigma'_j\}_{j=1}^n$ are the normal eigenvalues of $C(|\psi\rangle) - C(|\phi_t\rangle)$ and $Q \in \mathrm{O}(2n)$ is an orthogonal matrix (Lemma 16).

Now, choose the operator O in the form $O = U_Q^\dagger i\gamma_{2k-1}\gamma_{2k}U_Q$, where $k \in [n]$ and U_Q is a Gaussian unitary associated with the orthogonal matrix $Q \in \mathrm{O}(2n)$. Note that $\|O\|_\infty = 1$. Fix k as a value of j that maximizes $|\sigma'_j|$. Thus, we have:

$$\begin{aligned}|\operatorname{Tr}(O(|\psi\rangle\!\langle\psi| - |\phi_t\rangle\!\langle\phi_t|))| &= |[C(U_Q|\psi\rangle) - C(U_Q|\phi_t\rangle)]_{2k-1,2k}| &\text{(S86)}\\ &= |[Q(C(|\psi\rangle) - C(|\phi_t\rangle))Q^T]_{2k-1,2k}| &\text{(S87)}\\ &= |\sigma'_k| &\text{(S88)}\\ &= \max_{j\in[n]} |\sigma'_j| &\text{(S89)}\\ &= \|C(|\psi\rangle) - C(|\phi_t\rangle)\|_\infty, &\text{(S90)}\end{aligned}$$

where in the first step we used the definition of correlation matrix, in the second step we used Lemma 15 and in the last step we used the fact that the largest normal eigenvalues of an anti-symmetric matrix corresponds to the infinity norm of the matrix. Therefore, combining with (S85), we have:

$$\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \geq \frac{1}{2}\min_{|\phi_t\rangle\in\mathcal{G}_t} \|C(|\psi\rangle) - C(|\phi_t\rangle)\|_\infty. \tag{S91}$$

Now, by applying Lemma 39, we have:

$$\|C(|\psi\rangle) - C(|\phi_t\rangle)\|_\infty \geq |\lambda(C(|\psi\rangle)_{t+1} - \lambda(C(|\phi_t\rangle)_{t+1}|, \tag{S92}$$

where $\lambda(C)_{t+1}$ denotes the $t+1$-th smallest normal eigenvalue of a correlation matrix C. Since $|\phi_t\rangle$ is a t-compressible Gaussian state, its Gaussian dimension is $n-t$ (because of Proposition 35), hence its $t+1$-th smallest normal eigenvalue must be one. Therefore, the desired lower bound is obtained. □

C. Testing the Gaussian dimension of a state

We present an efficient algorithm (Algorithm 3) for property testing of t-compressible states, where $\mathcal{G}_t$ represents the set of n-qubits t-compressible Gaussian states, or equivalently the set of states with $n-t$ Gaussian dimension. The algorithm takes copies of a state $|\psi\rangle$ as input and determines whether $\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \leq \varepsilon_A$ or $\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \geq \varepsilon_B$, with the promise that one of these cases is true, where $\varepsilon_B > \varepsilon_A \geq 0$.

We provide the details of the testing algorithm in Algorithm 3. The correctness of this algorithm is established by the following theorem, the proof of which follows the same steps as proofs presented in [67].

Theorem 48 (Efficient t-Compressible Gaussian Testing). *Let $|\psi\rangle$ be an n-qubit pure state. Assume $\varepsilon_B, \varepsilon_A \in [0,1]$ such that $\varepsilon_B > \sqrt{(n-t)\varepsilon_A}$, $\delta \in (0,1]$, and $\varepsilon_{\mathrm{corr}} = (\frac{\varepsilon_B^2}{n-t} - \varepsilon_A)$. Assume that $|\psi\rangle$ is such that $\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) \leq \varepsilon_A$ or $\min_{|\phi_t\rangle\in\mathcal{G}_t} d_{\mathrm{tr}}(|\psi\rangle, |\phi_t\rangle) > \varepsilon_B$. Then, Algorithm 3 can discriminate between these two scenarios using $N = \lceil 16(n^3/\varepsilon_{\mathrm{corr}}^2)\log\big(4n^2/\delta\big)\rceil$ single-copy measurements of the state $|\psi\rangle$ with a probability of success at least $1-\delta$.*

```
Algorithm 3: Property Testing Algorithm for $t$-Compressible Gaussian States
Input: Error thresholds $\varepsilon_A, \varepsilon_B$, failure probability $\delta$. $N := \lceil 16(n^3/\varepsilon_{\text{corr}}^2)\log\big(4n^2/\delta\big)\rceil$ copies of the pure state $|\psi\rangle$, where
    $\varepsilon_{\text{corr}} = (\frac{\varepsilon_B^2}{n-t} - \varepsilon_A)$. Let $\varepsilon_{\text{test}} := \Big(\frac{\varepsilon_B^2}{n-t} + \varepsilon_A\Big)$.
Output: Output either "$\varepsilon_A$-close to the set of $t$-compressible states" or "$\varepsilon_B$-far from $t$-compressible states set".
Step 1: Estimate the entries of the correlation matrix using $N$ single-copy measurements, resulting in the estimated $2n \times 2n$ matrix $\hat{\Gamma}$;
Step 2: Find $\{\hat{\lambda}_k\}_{k=1}^n$, which corresponds to the ordered normal eigenvalues of $\hat{\Gamma}$;
Step 3: if $\hat{\lambda}_{t+1} \geq 1 - \varepsilon_{\text{test}}$ then
    Output: "$\varepsilon_A$-close to the set of $t$-compressible states".
else
    Output: "$\varepsilon_B$-far from $t$-compressible states set."
```

Proof. Let $\varepsilon_{\text{corr}} > 0$ be an accuracy parameter to be fixed later. By Lemma 38, with $N \geq 8(n^3/\varepsilon_{\text{corr}}^2)\log\big(4n^2/\delta\big)$ single-copy measurements, we can find a matrix $\hat{\Gamma}$ such that, with probability at least $1-\delta$, it holds that $\left\|\hat{\Gamma} - \Gamma(|\psi\rangle)\right\|_\infty \leq \varepsilon_{\text{corr}}$. This implies that for all $k \in [n]$, we have $|\hat{\lambda}_k - \lambda_k| \leq \varepsilon_{\text{corr}}$, where $\{\hat{\lambda}_k\}_{k=1}^n, \{\lambda_k\}_{k=1}^n$ are the normal eigenvalues of $\hat{\Gamma}$ and $\Gamma(|\psi\rangle)$ respectively. Let $\varepsilon_{\text{test}}$ be a parameter to fix later. If $\hat{\lambda}_{t+1} \geq 1 - \varepsilon_{\text{test}}$, we aim to show that $\min_{|\phi_t\rangle \in \mathcal{G}_t} d_{\text{tr}}(|\psi\rangle, |\phi_t\rangle) \leq \varepsilon_B$, otherwise, we aim to show that $\min_{|\phi_t\rangle \in \mathcal{G}_t} d_{\text{tr}}(|\psi\rangle, |\phi_t\rangle) > \varepsilon_A$. Thus, we first assume that $\hat{\lambda}_{t+1} \geq 1 - \varepsilon_{\text{test}}$. From Lemma 46, we have that:

$$\min_{|\phi_t\rangle \in \mathcal{G}_t} d_{\text{tr}}(|\psi\rangle, |\phi_t\rangle) \leq \sqrt{\frac{(n-t)}{2}(1-\lambda_{t+1})} \leq \sqrt{\frac{(n-t)}{2}(1-\hat{\lambda}_{t+1}+\varepsilon_{\text{corr}})} \leq \sqrt{\frac{(n-t)}{2}(\varepsilon_{\text{test}}+\varepsilon_{\text{corr}})}. \tag{S93}$$

Therefore we need to ensure that $\sqrt{\frac{(n-t)}{2}(\varepsilon_{\text{test}}+\varepsilon_{\text{corr}})} \leq \varepsilon_B$. Let us analyze now the case in which $\hat{\lambda}_{t+1} < 1 - \varepsilon_{\text{test}}$. From Lemma 47, we have:

$$\min_{|\phi_t\rangle \in \mathcal{G}_t} d_{\text{tr}}(|\psi\rangle, |\phi_t\rangle) \geq \frac{1}{2}(1-\lambda_{t+1}) \geq \frac{1}{2}(1-\hat{\lambda}_{t+1}-\varepsilon_{\text{corr}}) > \frac{1}{2}(\varepsilon_{\text{test}}-\varepsilon_{\text{corr}}) \tag{S94}$$

Therefore, we impose that $\frac{\varepsilon_{\text{test}}-\varepsilon_{\text{corr}}}{2} \geq \varepsilon_A$. The two mentioned inequalities are satisfied by choosing $\varepsilon_{\text{test}} = (\frac{\varepsilon_B^2}{n-t} + \varepsilon_A)$ and $\varepsilon_{\text{corr}} = (\frac{\varepsilon_B^2}{n-t} - \varepsilon_A)$, by assuming that $\varepsilon_B > \sqrt{(n-t)\varepsilon_A}$. □

Supplementary Material V: Pseudorandomness from t-doped Gaussian states and time complexity lower bound

We have presented an algorithm for learning t-doped fermionic Gaussian states with a time complexity scaling as $\mathcal{O}(\text{poly}(n, 2^t))$ (assuming that the Majorana locality κ of each non-Gaussian gate is constant in the number of qubits). Thus, as long as $t = \mathcal{O}(\log(n))$, the algorithm is efficient, i.e., the total run-time is polynomial in the number of qubits. In this section, we delve into establishing lower bounds on the time complexity for learning t-doped fermionic Gaussian states. We begin by demonstrating that, under a well-believed cryptography assumption [43–45, 64–66], no algorithm can learn t-doped fermionic Gaussian states with time complexity scaling in t as $\mathcal{O}(\text{poly}(t))$. This rules out efficient algorithms if t scales polynomially with the number of qubits n. However, under a stronger cryptography assumption [43–46], we can establish that when t scales *slightly* faster than logarithmically in the number of qubits n, i.e., $t = \tilde{\omega}(\log(n))$, there exists no efficient algorithm to learn t-doped fermionic Gaussian states, where we defined $\tilde{\omega}(\log(n)) := \omega(\log(n)\text{polyloglog}(n))$.

A. t-doped Gaussian states cannot be learned in polynomial time in t

Our cryptography assumption relies on the conjecture that a specific problem, namely "Learning With Errors over Rings" RingLWE [64], is hard to solve by quantum computers [43–45, 64–66]. Detailed definitions and discussions about RingLWE can be found in [64]. Informally, RingLWE is a variant of the more general "Learning With Errors" (LWE) problem specialized to polynomial rings over finite fields, where the LWE problem is to distinguish random linear equations, perturbed by a small amount of noise, from truly uniform ones.

Crucial to our proof is a lemma, adapted from [63] (which strongly relies on previous work [43, 47, 48]), presented below:

Lemma 49 (Adapted from Theorem 14 in [63])**.** *Assume that* RingLWE *cannot be solved by quantum computers in polynomial time. Then, there exists a set $\mathcal{S}_{\mathrm{PRS}}$ of k-qubits pure quantum states, known as pseudorandom quantum states, with the following properties:*

1. *Any state in $\mathcal{S}_{\mathrm{PRS}}$ can be prepared using $\tilde{\mathcal{O}}(k)$ Toffoli and Hadamard gates (here, $\tilde{\mathcal{O}}(\cdot)$ hides* $\mathrm{polylog}(\cdot)$ *factors).*

2. *States in the set $\mathcal{S}_{\mathrm{PRS}}$ cannot be learned in time complexity $\mathcal{O}(\mathrm{poly}(t))$ by quantum computers. More specifically, let $\rho \in \mathcal{S}_{\mathrm{PRS}}$ be an unknown quantum state. Then there is no quantum algorithm that, using $\mathcal{O}(\mathrm{poly}(k))$ copies of ρ and computational time, with probability at least $2/3$ outputs a classical description of a state $\hat{\rho}$ which can be prepared in polynomial time on a quantum computer such that $\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq 1/8$.*

Now we use this Lemma to show that there is no algorithm for learning t-doped states with a $\mathcal{O}(\mathrm{poly}(t))$ computational time scaling in t.

Proposition 50 (No $\mathrm{poly}(t)$ algorithm to learn t-doped states)**.** *Assume that* RingLWE *cannot be solved by quantum computers in polynomial time. Then there is no quantum algorithm that, given access to copies of a t-doped fermionic Gaussian n-qubits state ρ and with a time complexity scaling in t as $\mathcal{O}(\mathrm{poly}(t))$, outputs a classical description of a quantum state $\hat{\rho}$ such that it can be prepared in polynomial time on a quantum computer and, with probability at least $2/3$, it holds that $\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq 1/8$.*

Proof. Consider an n-qubit state of the form $|\phi\rangle \otimes |0^{n-k}\rangle$, where $|\phi\rangle$ is a k-qubit state in the set $\mathcal{S}_{\mathrm{PRS}}$ defined in Lemma 49. Let $|\phi\rangle = U_{\mathrm{PRS}}\,|0^k\rangle$, prepared by a unitary U_{PRS} that can be implemented using $\tilde{\mathcal{O}}(k)$ Hadamard and Toffoli gates, as per Lemma 49. The Toffoli gates can be implemented in turn using Hadamard, CNOT, T-gates, and T-gates inverse. For each gate in the system, utilizing a standard SWAP-exchange trick, we can make any gate acting on some qubits of the system to act only on the first two qubits through a cascade of SWAP gates. This incurs a total overhead factor of $\mathcal{O}(k)$ in the total number of gates. The SWAP gates between nearest-neighbor qubits are local non-Gaussian gates, since they can be expressed as $\mathrm{SWAP}_{i,i+1} = e^{-i\frac{\pi}{4}} \exp\big(i\frac{\pi}{4}(X_iX_{i+1} + Y_iY_{i+1} + Z_iZ_{i+1})\big)$, which have Majorana locality equal to 4 (due to the Jordan-Wigner mapping). Also the other gates, now acting on the first two qubits, are (possibly) non-Gaussian gates with Majorana locality at most 4. This is because the Pauli operators in the generator of each gate can be expressed in terms of Majorana operators via the Jordan-Wigner transformation. This results in a total of $t = \tilde{\mathcal{O}}(k^2)$ local non-Gaussian gates required to prepare the state. Thus, the $|\phi\rangle$ is a t-doped Gaussian state with $\kappa = 4$ Majorana local non-Gaussian gates. Now, due to Lemma 49, there exists no learning algorithm to learn such a state in time $\mathcal{O}(\mathrm{poly}(k)) = \mathcal{O}(\mathrm{poly}(t))$, with error less than $1/8$ and probability of success at least $2/3$. □

B. Learning $\tilde{\omega}(\log(n))$-doped Gaussian states is hard

The previous Proposition rules out efficient algorithms when $t = \Omega(\mathrm{poly}(n))$. However, our proposed algorithm is not anymore efficient when $t = \tilde{\omega}(\log(n))$, while it is efficient for $t = \mathcal{O}(\log(n))$. If we were to make the stronger assumption, namely that RingLWE cannot be solved by quantum computers in sub-exponential time [43–46], then we can rule out that efficient algorithm for $t = \tilde{\omega}(\log(n))$ exists (which means faster than $\omega(\log(n))$ but hiding polyloglog factors). For showing this, we need first the following Lemma adapted by [63].

Lemma 51 (Adapted from Theorem 14 and 15 in [63])**.** *Assume that* RingLWE *cannot be solved by quantum computers in sub-exponential time. Then, there exists a set $\mathcal{S}_{\mathrm{PRS}}$ of k-qubit pure quantum states, known as pseudorandom quantum states, with the following properties:*

1. *Any state in $\mathcal{S}_{\mathrm{PRS}}$ can be prepared using $\tilde{\mathcal{O}}(k)$ Toffoli and Hadamard gates (here, $\tilde{\mathcal{O}}(\cdot)$ hides* $\mathrm{polylog}(\cdot)$ *factors).*

2. *Any algorithm to learn states from the set $\mathcal{S}_{\mathrm{PRS}}$ must have $\exp(\Omega(k))$ time complexity. More specifically, let $\rho \in \mathcal{S}_{\mathrm{PRS}}$ be an unknown quantum state. Then any quantum algorithm that, by querying copies of ρ, with probability at least $2/3$ outputs a classical description of a state $\hat{\rho}$ which can be prepared in sub-exponential time on a quantum computer such that $\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq 1/8$, must have $\exp(\Omega(k))$ time-complexity.*

Now we use this to prove the following Proposition, also stated informally in the main text as Theorem 5. It reaches stronger conclusion than Proposition 50, but at the cost of stronger cryptography assumption. The idea of the following proof is to use a more compact qubits-to-fermion mapping than Jordan-Wigner, namely a modification of the one introduced by Kitaev [23], which would allow to create pseudorandom quantum states with no overhead in the number of non-Gaussian gates compared to the number of Toffoli and Hadamard gates. In the following, we recall that $\tilde{\omega}(\log(n))$ is defined as $\tilde{\omega}(\log(n)) := \omega(\log(n)\mathrm{polyloglog}(n)))$.

Proposition 52 (Learning $\tilde{\omega}(\log(n))$-doped Gaussian states is hard)**.** *Assume that* RingLWE *cannot be solved by quantum computers in sub-exponential time. Then, there is no efficient (i.e.,* $\mathcal{O}(\mathrm{poly}(n))$ *time) quantum algorithm that, by querying copies of a* $\tilde{\omega}(\log(n))$*-doped Gaussian state* ρ*, with probability at least* $2/3$ *outputs a description of a state* $\hat{\rho}$ *which can be prepared in polynomial time on a quantum computer such that* $\mathrm{d}_{\mathrm{tr}}(\rho,\hat{\rho}) \leq 1/8$*.*

Proof. Following a similar approach as in the proof of Proposition 50, we begin by defining a state $|\phi\rangle \otimes |0^{n-k}\rangle$, where $|\phi\rangle = U_{\mathrm{PRS}}\,|0^k\rangle$ represents a k-qubit state in the set $\mathcal{S}_{\mathrm{PRS}}$ as defined in Lemma 51. This state can be efficiently prepared using a unitary U_{PRS} with $\tilde{\mathcal{O}}(k)$ Hadamard and Toffoli gates, which, in turn, can be implemented using Hadamard gates, CNOTs, T-gates, and their inverses. In contrast to the previous proof in Proposition 50, an application of the same argument would not yield the desired conclusion due to the unfavorable quadratic overhead introduced by the SWAP-exchange trick in the number of non-Gaussian gates. That trick was necessary due to the use of Jordan-Wigner transformation. However, we can employ a more efficient qubits-to-fermions mapping, specifically a modified version of the one introduced by Kitaev [23]. Hereafter, we will refer to it as the "Kitaev encoding." Our objective is to construct a fermionic state encoding $|\phi\rangle$ using a circuit of size $\tilde{\mathcal{O}}(k)$ composed of Gaussian and $\kappa = 4$ local non-Gaussian gates. We employ a mapping of k qubits into $2k$ fermionic modes using Majorana operators $\{\gamma_{\alpha,j} \,|\, j \in [k],\, \alpha \in \{0,\,x,\,y,\,z\}\}$. These $4k$ Majorana operators are defined in terms of $4k$ Pauli strings via Jordan-Wigner, with an arbitrarily fixed operator ordering. We are now going to leverage the formalism and basics of stabilizer codes, for more in-depth information, refer to [75]. The Kitaev encoding involves defining a stabilizer code of $2k$ physical qubits encoded in k logical qubits, characterized by the following k stabilizer generators $\{s_j\}_{j=1}^{k}$ and logical Pauli operators $\{X_j^{\mathrm{KE}}, Z_j^{\mathrm{KE}}\}_{j=1}^{k}$:

$$s_j := \gamma_{0,j}\gamma_{x,j}\gamma_{y,j}\gamma_{z,j}, \tag{S95}$$

$$X_j^{\mathrm{KE}} := i\gamma_{y,j}\gamma_{z,j}, \tag{S96}$$

$$Z_j^{\mathrm{KE}} := i\gamma_{x,j}\gamma_{y,j}. \tag{S97}$$

for each $j \in [k]$. Note that these operators explicitly satisfy the algebraic conditions on stabilizer generators and logical Pauli operators. The Kitaev encoding is associated to a Clifford transformation V_{KE} such that:

$$V_{\mathrm{KE}} X_j V_{\mathrm{KE}}^{\dagger} = X_j^{\mathrm{KE}}, \tag{S98}$$

$$V_{\mathrm{KE}} Z_j V_{\mathrm{KE}}^{\dagger} = Z_j^{\mathrm{KE}}, \tag{S99}$$

for each $j \in [k]$, and:

$$V_{\mathrm{KE}} Z_j V_{\mathrm{KE}}^{\dagger} = s_j, \tag{S100}$$

for each $j \in \{k+1,\dots,2k\}$. The last equation ensures that $V_{\mathrm{KE}}\,|0^{2k}\rangle$ is an eigenstate with $+1$ eigenvalue for each of the stabilizer generators $\{s_j\}_{j=1}^{k}$, while Eq.(S99) implies that $V_{\mathrm{KE}}\,|0^{2k}\rangle$ is an eigenstate with $+1$ eigenvalue for each $\{Z_j^{\mathrm{KE}}\}_{j=1}^{k}$. Thus, $V_{\mathrm{KE}}\,|0^{2k}\rangle$ is a valid "logical zero" stabilizer state. Exploiting the fact that $V_{\mathrm{KE}}\,|0^{2k}\rangle$ is an eigenstate with $+1$ eigenvalues of $\{Z_j^{\mathrm{KE}}\}_{j=1}^{k}$ and $\{s_j Z_j^{\mathrm{KE}}\}_{j=1}^{k}$, its density matrix can be written as:

$$V_{\mathrm{KE}}\,|0^{2k}\rangle\!\langle 0^{2k}|\,V_{\mathrm{KE}}^{\dagger} = \prod_{j=1}^{k}\left(\frac{I + s_j Z_j^{\mathrm{KE}}}{2}\right)\prod_{j=k}^{2k}\left(\frac{I + Z_j^{\mathrm{KE}}}{2}\right) = \prod_{j=1}^{k}\left(\frac{I - i\gamma_{0,j}\gamma_{z,j}}{2}\right)\prod_{j=k}^{2k}\left(\frac{I + i\gamma_{x,j}\gamma_{y,j}}{2}\right). \tag{S101}$$

From this, we observe that $V_{\mathrm{KE}}\,|0^{2k}\rangle$ is a fermionic Gaussian state because it can be written in the form of Eq.(S4), noting that signed permutation matrices are orthogonal matrices. Moreover, we denote $Y_j^{\mathrm{KE}} := -iZ_j^{\mathrm{KE}}X_j^{\mathrm{KE}} = i\gamma_{x,j}\gamma_{z,j}$. The Kitaev encoding, as defined, ensures that the local qubit gates are mapped onto local fermionic ones. In particular, the gates of the circuit U_{PRS} that prepares the pseudorandom state $|\phi\rangle = U_{\mathrm{PRS}}\,|0^k\rangle$— the Hadamard H, CNOT, and T-gate — are, up to an overall phase, mapped onto

$$\mathrm{H}_j^{\mathrm{KE}} := V_{\mathrm{KE}}\mathrm{H}_j V_{\mathrm{KE}}^{\dagger} = V_{\mathrm{KE}}\left(Z_j\frac{I + iY_j}{\sqrt{2}}\right)V_{\mathrm{KE}}^{\dagger} = Z_j^{\mathrm{KE}}\frac{I + iY_j^{\mathrm{KE}}}{\sqrt{2}} = e^{-\frac{\pi}{2}\gamma_{x,j}\gamma_{y,j}}e^{-\frac{\pi}{4}\gamma_{z,j}\gamma_{x,j}}, \tag{S102}$$

$$\mathrm{CNOT}_{j,l}^{\mathrm{KE}} := V_{\mathrm{KE}}\mathrm{CNOT}_{j,l}V_{\mathrm{KE}}^{\dagger} = e^{i\frac{\pi}{4}(1 - Z_j^{\mathrm{KE}})(I - X_l^{\mathrm{KE}})} = e^{i\frac{\pi}{4}(I - i\gamma_{x,j}\gamma_{y,j})(I - i\gamma_{y,l}\gamma_{z,l})}, \tag{S103}$$

$$\mathrm{T}_j^{\mathrm{KE}} := V_{\mathrm{KE}}\mathrm{T}_j V_{\mathrm{KE}}^{\dagger} = e^{i\frac{\pi}{8}Z_j^{\mathrm{KE}}} = e^{-\frac{\pi}{8}\gamma_{x,j}\gamma_{y,j}}, \tag{S104}$$

for each $j \neq l \in [k]$. The only non-Gaussian among these is the encoding of the CNOT gate, which has Majorana locality $\kappa = 4$. This implies that the encoding of the circuit U_{PRS}, i.e. $U_{\mathrm{PRS}}^{\mathrm{KE}} := V_{\mathrm{KE}}U_{\mathrm{PRS}}V_{\mathrm{KE}}^{\dagger}$, is a t-doped fermionic Gaussian unitary with local non-Gaussian gates and $t = \tilde{\mathcal{O}}(k)$. Thus, we have that the Kitaev encoding of the pseudorandom state $|\phi\rangle = U_{\mathrm{PRS}} \left|0^k\right\rangle$ is:

$$|\phi\rangle_{\mathrm{KE}} := V_{\mathrm{KE}} |\phi\rangle \otimes \left|0^k\right\rangle = V_{\mathrm{KE}} U_{\mathrm{PRS}} \left|0^{2k}\right\rangle = U_{\mathrm{PRS}}^{\mathrm{KE}} V_{\mathrm{KE}} \left|0^{2k}\right\rangle . \tag{S105}$$

Since $V_{\mathrm{KE}} \left|0^{2k}\right\rangle$ is a Gaussian state and $U_{\mathrm{PRS}}^{\mathrm{KE}}$ is a t-doped Gaussian unitary with $t = \tilde{\mathcal{O}}(k)$, then $V_{\mathrm{KE}} |\phi\rangle \otimes \left|0^k\right\rangle$ is a t-doped Gaussian state with $t = \tilde{\mathcal{O}}(k)$. The Majorana locality of each non-Gaussian gate is at most 4.

Using an arbitrary algorithm $\mathcal{A}$ for learning a t-doped fermionic Gaussian state, we will now define a protocol for learning the pseudorandom state $|\phi\rangle$. Given a copy of a state $|\phi\rangle$ on k qubits, we use k auxiliary qubits in state $|0\rangle$ and apply the Clifford transformation V_{KE}. This means it can be produced by a circuit with $O(k^2)$ 2-qubit gates [76]. The resulting $|\phi\rangle_{\mathrm{KE}}$ can be input to $\mathcal{A}$ as a copy of a t-doped fermionic Gaussian state for $t = \tilde{\mathcal{O}}(k)$. Using the number of copies of $|\phi\rangle$ given by sample complexity of $\mathcal{A}$, we learn a description of a state $\hat{\rho}_{\mathrm{KE}}$ which, with probability at least $2/3$, satisfies:

$$d_{\mathrm{tr}}(\hat{\rho}_{\mathrm{KE}}, \rho_{\mathrm{KE}}) \leq \frac{1}{8}, \tag{S106}$$

where we defined ρ_{KE} to be the density matrix associated with $|\phi\rangle_{\mathrm{KE}}$. By defining $\hat{\rho} := \mathrm{Tr}_{\{k+1,\dots,2k\}} \left(V_{\mathrm{KE}}^{\dagger} \hat{\rho}_{\mathrm{KE}} V_{\mathrm{KE}} \right)$, where $\mathrm{Tr}_{\{k+1,\dots,2k\}}(\cdot)$ indicates the partial trace with respect to the qubits $\{k+1, \dots, 2k\}$, we also have:

$$d_{\mathrm{tr}}(\hat{\rho}, |\phi\rangle\!\langle\phi|) \leq d_{\mathrm{tr}}(V_{\mathrm{KE}}^{\dagger} \hat{\rho}_{\mathrm{KE}} V_{\mathrm{KE}}, |\phi\rangle\!\langle\phi| \otimes \left|0^k\right\rangle\!\left\langle 0^k\right|) = d_{\mathrm{tr}}(V_{\mathrm{KE}}^{\dagger} \hat{\rho}_{\mathrm{KE}} V_{\mathrm{KE}}, V_{\mathrm{KE}}^{\dagger} \rho_{\mathrm{KE}} V_{\mathrm{KE}}) = d_{\mathrm{tr}}(\hat{\rho}_{\mathrm{KE}}, \rho_{\mathrm{KE}}) \leq \frac{1}{8}, \tag{S107}$$

where in the first step we used that the partial trace does not increase the trace distance between two states [77]. Hence, we found a state $\hat{\rho}$ which is in trace distance close to the target state $|\phi\rangle\!\langle\phi|$. To recap, we produced the learning algorithm for a pseudorandom state $|\phi\rangle$ from a learning algorithm for t-doped fermionic Gaussian states. The pseudorandom state learning algorithm has the same sample complexity as the fermionic one, and the time complexity $T_{\mathrm{PRS}} = S_{\mathrm{f}} \cdot O(k^2) + T_{\mathrm{f}}$ where T_{f} and S_{f} are time and sample complexity of the fermionic learner. If there is a fermionic learner whose time and sample complexity scale subexponentially in k, the same property carries over to the pseudorandom states learner. By Lemma 51, this would contradict the cryptographic assumption that RingLWE cannot be solved by quantum computers in sub-exponential time. Hence, the time complexity of the fermionic learner needs to be $\exp(\Omega(k))$. If $k = \omega(\log(n))$, then this implies that any algorithm to learn t-doped fermionic Gaussian states with $t = \tilde{\mathcal{O}}(k) = \omega(\log(n)\mathrm{polyloglog}(n))$ must be inefficient, i.e., its time complexity must be $\omega(\mathrm{poly}(n))$. □

Concept learning of parameterized quantum models from limited measurements

Beng Yee Gan,[1, *] Po-Wei Huang,[1] Elies Gil-Fuster,[2, 3] and Patrick Rebentrost[1, 4, †]

[1] *Centre for Quantum Technologies, National University of Singapore, Singapore 117543*
[2] *Dahlem Center for Complex Quantum Systems,*
Freie Universität Berlin, 14195 Berlin, Germany
[3] *Fraunhofer Heinrich Hertz Institute, 10587 Berlin, Germany*
[4] *Department of Computer Science, National University of Singapore, Singapore 117417*

(Dated: July 26, 2024)

Classical learning of the expectation values of observables for quantum states is a natural variant of learning quantum states or channels. While the current learning-theoretic framework establishes the sample complexity and the number of measurement shots per sample required for learning such statistical quantities, the interplay between these two variables has not been adequately quantified before. In this work, we quantify and demonstrate the asymmetrical effects of the two variables on the performance of concept learning. Specifically, increasing the sample size enhances the learning performance of classical machines, even with single-shot estimates, while the improvements from increasing measurements become asymptotically trivial beyond a constant factor. When the total queries to quantum systems is fixed, such asymmetrical effects imply an asymmetrical trade-off between them. Through bias-variance-noise decomposition, we further show the practical impact of finite measurement noise on the training of classical machines. Finally, we apply the framework to study the impact of measurement noise on the classical surrogation of parameterized quantum circuit models. Our work provides new tools to analyse the operational influence of finite measurement noise in classical learning of quantum systems.

I. INTRODUCTION

The potential computational capabilities of quantum computers have garnered much interest in recent years from both academia and industry. In particular, it has been suggested that quantum computers have the potential to simulate quantum systems with an exponential speedup compared to classical computers [1, 2]. However, these hard-to-simulate computational tasks could potentially be efficiently learned by classical machines given access to data extracted from the associated quantum processes [3–11]. Such a learning task relies on quantum and classical computers alike to extract relevant information from quantum states via quantum measurements [12, 13] and subsequently to conduct learning of the desired properties of quantum states. Some of these quantum properties can be formulated and represented by mathematical models, which we can learn using classical learning algorithms. Examples of such *quantum models* include expectation values of quantum observables given a variational quantum circuit [14] or ground state properties of quantum systems [9–11]. Understanding how classical machines can learn quantum models is therefore essential, as it sheds light on the potential and limitations of quantum information processing.

Quantum systems exhibit inherent probabilistic behaviour, and measurements on such systems are typically subjected to statistical fluctuations. When only a limited number of measurements are made on a quantum model, the observed outcomes may deviate from the true underlying quantum models due to the measurement/shot noise. Hence, apart from the number of training data inputs N_1, the number of measurement shots (per data input) N_s is also a key quantity in determining the learning performance of classical learners. Current works often consider shot noise as an error term that needs to be mitigated and rely on its minimization to ensure learnability [8, 9, 11]. In these scenarios, the effects of altering N_1 and N_s are typically discussed separately, with N_s assumed to be sufficient enough as to not affect the analysis regarding N_1 and the learning performance.

In this work, we discuss asymmetrical effects that these two quantities have on the performance of classical machines in learning quantum models. That is, increasing N_1 enhances the learning performance of classical models, even when observed outcomes are estimated with limited measurement shots, e.g., in the single-shot limit [15] when $N_s = 1$. On the other hand, for a fixed training data size N_1, we find that improvements in learning performances from increasing the number of measurement shots N_s become asymptotically trivial beyond a constant factor.

In practice, extrinsic factors such as monetary budgets force one to fix the total number of queries to quantum models, thereby coupling N_1 and N_s since increasing N_1 will reduce N_s and vice versa[1]. This poses an interesting learning-theoretic question: *given a fixed number of queries to quantum models, will classical machines learn better with training datasets consisting of more inputs with noisier labels (larger N_1 but smaller N_s) or fewer in-*

* gan.bengyee@u.nus.edu
† patrick@comp.nus.edu.sg

[1] The simplest method of defining the total cost of querying the quantum model we wish to learn is $N = N_1 N_s$.

puts with cleaner labels (smaller N_1 but larger N_s)? Our analytical results show that, asymptotically, it is always better to sample from different inputs when sampling a data point incurs the same cost as conducting a duplicate measurement. The optimal performance is achieved when labels are estimated with only one measurement shot. As shown in Figure 1, our classical machines learn better with training datasets consisting of more inputs with the noisiest labels. Yet, realistically, it is cheaper to produce more samples for a fixed parameter setting in quantum models than to change the parameter settings each time. In this scenario, we analytically show that there exists an optimal pair of N_1 and N_s that will maximize the performance of the classical models.

Our analysis is based on the learning-theoretic framework of *probabilistic concepts* (p-concept) [16]. Stemming from the probabilistic nature of quantum measurements, there is no deterministic mapping of the input data to the observed outcomes (known in statistical learning theory as a *concept* [17]) that can capture the behaviour of the quantum model. Nonetheless, there is some structure to this uncertainty. That is, quantum models represent the conditional expectation of their unbiased estimators. As this is precisely how p-concepts are defined, one could formulate quantum models as p-concepts.

The p-concept setting was first introduced in a quantum setup in Scott Aaronson's seminal paper [18] and subsequently in Refs. [19–22]. While these works, along with our own, identify shot noise as structural randomness that allows us to cast quantum models as p-concepts, they primarily focus on the usage of the fat-shattering dimension, a complexity measure that shows the expressiveness of the set of p-concepts we are interested in learning. In these prior work, the fat-shattering dimension is used to quantify the difficulty of learning quantum states [18–20], measurements [21], and quantum circuits [22]. In contrast, our work utilizes kernel theory and the respective learnability results to investigate the impact of shot noise in learning quantum models using classical machine learning models. Furthermore, our framework disentangles the contributions of the classical representation of quantum models, the size of the training dataset, and the number of measurement shots, providing a new perspective to investigate their individual roles in learning quantum models.

We further assess the impacts of shot noise on the actual training of classical machines. Following the bias-variance-noise decomposition, we show the implicit impacts of shot noise on the bias and variance of classical models. Specifically, high shot noise will lead to high variance in classical models, which is consistent with observations in the literature [23, 24]. Finally, we apply our framework to numerically study the impact of shot noise on the classical surrogation of parameterized quantum circuit models. The numerical results are consistent with our theoretical predictions.

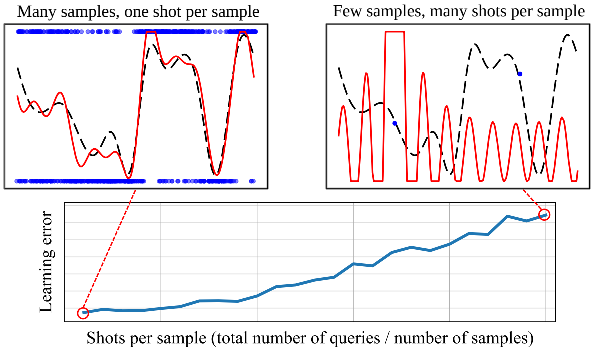


FIG. 1. Fixing the total number of queries to quantum models imposes constraints on the number of inputs and the number of shots per input: noisier (more accurate) estimates [BLUE DOTS] of the target function [BLACK-DASHED LINE] are acquired if more (fewer) inputs are considered. Classical machines trained with these inputs and associated function estimates will output the prediction [RED SOLID LINE].

II. PRELIMINARIES

In this section, we will first introduce two frameworks in statistical learning theory that we use to provide learning guarantees, the deterministic concept learning framework and the probabilistic concept learning framework. Then, we will provide a brief introduction to the types of quantum models considered in this work.

A. Probabilistic concept learning

Let $\mathcal{X} = \mathbb{R}^m$ and $\mathcal{Y} \subset \mathbb{R}$ be the data and label spaces, respectively. Further, we assume that data points $\boldsymbol{x}$ are independently and identically distributed (i.i.d.) according to some unknown but fixed distribution $p(\boldsymbol{x})$ and the label space $\mathcal{Y}$ is a compact and convex subspace of $\mathbb{R}$.

In the learning-theoretic setting, there are two types of functions of interest: *concept* and *hypothesis*. A concept c is a function that maps the data space to the label space, i.e., $c : \mathcal{X} \to \mathcal{Y}$. A particular set of these functions with specific properties forms a *concept class* $\mathcal{C} \subseteq \mathcal{Y}^{\mathcal{X}}$. In the deterministic learning setting, a concept maps data points $\boldsymbol{x} \in \mathcal{X}$ to associated labels $y \in \mathcal{Y}$, i.e., a data sample is given by $(\boldsymbol{x}, y)$ where $\boldsymbol{x}$ is sampled from $p(\boldsymbol{x})$ and $y = c(\boldsymbol{x})$. Similarly, a hypothesis is defined as $h : \mathcal{X} \to \mathcal{Y}$, and a subset of these functions forms a *hypothesis class* $\mathcal{H} \subseteq \mathcal{Y}^{\mathcal{X}}$. Then, given a collection of samples $\mathcal{S} = (\boldsymbol{x}_i, c(\boldsymbol{x}_i))_{i=1}^{N_1}$where $\boldsymbol{x}_i \sim p(\boldsymbol{x})$, a learning algorithm selects a hypothesis $h \in \mathcal{H}$ such that the difference between $h(\boldsymbol{x})$ and the corresponding label $y = c(\boldsymbol{x})$ is low under some performance measure.

The *probabilistic concept* (p-concept) and the p-concept class are defined in a similar fashion.

Definition 1 (p-concept)**.** *Let $P_{\boldsymbol{x}}(\mathcal{Y})$ be a conditional probability distribution over the label space $\mathcal{Y}$, with probability density specified as $p(y|\boldsymbol{x})$ for each input $\boldsymbol{x} \in \mathcal{X}$.*

We call p-concept *a function* $c : \mathcal{X} \to \mathcal{Y}$ *defined as the conditional expectation value of* y *given* $\boldsymbol{x}$ *arising from* p*:*

$$c : \mathcal{X} \to \mathcal{Y} \tag{1}$$

$$\boldsymbol{x} \mapsto c(\boldsymbol{x}) = \mathbb{E}_{y\sim p(y|\boldsymbol{x})}[y]. \tag{2}$$

Definition 2 (p-concept class)**.** *Let* $\mathcal{P} \subseteq \{P_{\boldsymbol{x}}(\mathcal{Y})\}$ *be a subset of all conditional probability distributions over the label space. For each distribution* $P_{\boldsymbol{x}}(\mathcal{Y}) \in \mathcal{P}$*, which specifies the conditional distribution* $p(y|\boldsymbol{x})$ *of* y *given* $\boldsymbol{x}$*, the corresponding* p*-concept is defined as per Definition 1. Then, a* p-concept class *is the class of functions* $\mathcal{C}$ *that corresponds to all functions arising from the set* $\mathcal{P}$ *of probability distributions:*

$$\mathcal{C} := \{c : \boldsymbol{x} \mapsto \mathbb{E}_{y\sim p(y|\boldsymbol{x})}[y] \,|\, P_{\boldsymbol{x}}(\mathcal{Y}) \in \mathcal{P}\}. \tag{3}$$

Noteworthy is that defining this concept class explicitly from a set of conditional distributions does not impose any limitations on what these functions can be. For any function $f \in \mathcal{Y}^{\mathcal{X}}$, one can always interpret it as a p-concept in an infinite number of ways. For instance, one could consider simply the probability distribution that always returns the value of the function $p(y|\boldsymbol{x}) = \delta(y - f(\boldsymbol{x}))$[2]. Alternatively, one could consider any random function $\xi(\boldsymbol{x})$ with zero mean $\mathbb{E}[\xi(\boldsymbol{x})] = 0$, and then one obtains a p-concept as the expectation value of the random function $f(\boldsymbol{x})+\xi(\boldsymbol{x})$. Indeed, there are infinitely many different probability distributions that give rise to the same p-concept class[3]. Nonetheless, some of these distributions can be generated via physically realizable processes, which are the focus of this work.

Contrasting with the deterministic learning setting, in the p-concept learning setting, the samples $(\boldsymbol{x}, y)$ are obtained by sampling the joint distribution $\mathcal{D} = p(\boldsymbol{x})p(y|\boldsymbol{x})$ with $c(\boldsymbol{x}) = \mathbb{E}_{y\sim p(y|\boldsymbol{x})}[y]$. In this work, we further consider a flexible setting that allows for access to $p(y|\boldsymbol{x})$. That is, given a data point $\boldsymbol{x}$, we can obtain multiple i.i.d. random labels from $p(y|\boldsymbol{x})$, e.g., $y_1, \dots, y_{N_s} \sim p(y|\boldsymbol{x})$, and use these labels to estimate the empirical mean of the random labels $\bar{y}_{N_s} = \frac{1}{N_s}\sum_{i=1}^{N_s} y_i$. Such sampling then averaging procedure can be directly modelled as the sampling process $(\boldsymbol{x}, \bar{y}_{N_s}) \sim \bar{\mathcal{D}}_{N_s} = p(\boldsymbol{x})p(\bar{y}_{N_s}|\boldsymbol{x})$ where $\bar{y}_{N_s}$ is distributed with variance $\sigma^2_{\bar{y}_{N_s}|\boldsymbol{x}} = \sigma^2_{y|\boldsymbol{x}}/N_s$ and $\sigma^2_{y|\boldsymbol{x}} = \mathrm{Var}_{y\sim p(y|\boldsymbol{x}_i)}[y]$. By construction, for all $N_s \in \mathbb{N}$, $p(\bar{y}_{N_s}|\boldsymbol{x})$ gives the same p-concept as $p(y|\boldsymbol{x})$, i.e.,

$$c(\boldsymbol{x}) = \mathbb{E}_{y\sim p(y|\boldsymbol{x})}[y] = \mathbb{E}_{\bar{y}_{N_s}\sim p(\bar{y}_{N_s}|\boldsymbol{x})}[\bar{y}_{N_s}]. \tag{4}$$

For ease of notation, we let $c(\boldsymbol{x}) := \mathbb{E}_{\bar{y}_{N_s}}[\bar{y}_{N_s}|\boldsymbol{x}]$ and implicitly assume the dependence of $\bar{y}_{N_s}$ and $\bar{\mathcal{D}}_{N_s}$ on N_s, and denote them as $\bar{y}$ and $\bar{\mathcal{D}}$, respectively.

In the p-concept learning setting, a learning algorithm similarly select a hypothesis h from a hypothesis class $\mathcal{H}$ such that the difference between $h(\boldsymbol{x})$ and the corresponding p-concept $c(\boldsymbol{x})$ is low under some performance measure. Here, we define two different performance measures: explicit and implicit loss. In particular, the explicit loss of h is defined as

$$\ell_{\mathrm{expl}}(h) = (h(\boldsymbol{x}) - c(\boldsymbol{x}))^2 \tag{5}$$

while the implicit loss of h is defined as

$$\ell_{\mathrm{impl}}(h) = (h(\boldsymbol{x}) - \bar{y})^2. \tag{6}$$

That is, the explicit loss directly measures the performance of h concerning the target p-concept $c(\boldsymbol{x})$, while the implicit loss indirectly quantifies the differences between $h(\boldsymbol{x})$ and $c(\boldsymbol{x})$ through the noisy labels $\bar{y}$ as $c(\boldsymbol{x}) = \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]$. Averaging both losses over all data points yields their respective risks: explicit risk

$$R_{\mathrm{expl}}(h) := \mathop{\mathbb{E}}_{(\boldsymbol{x},\bar{y})\sim\bar{\mathcal{D}}}[(h(\boldsymbol{x}) - c(\boldsymbol{x}))^2] \tag{7}$$

and implicit risk

$$R_{\mathrm{impl}}(h) := \mathop{\mathbb{E}}_{(\boldsymbol{x},\bar{y})\sim\bar{\mathcal{D}}}[(h(\boldsymbol{x}) - \bar{y})^2]. \tag{8}$$

The decomposition of $R_{\mathrm{impl}}(h)$, i.e.,

$$R_{\mathrm{impl}}(h) = R_{\mathrm{expl}}(h) + \mathop{\mathbb{E}}_{(\boldsymbol{x},\bar{y})\sim\bar{\mathcal{D}}}[(\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}] - \bar{y})^2] \tag{9}$$

$$= R_{\mathrm{expl}}(h) + R_{\mathrm{impl}}(\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]), \tag{10}$$

shows that the implicit and explicit risks are related by a constant shift. Hence, a small $R_{\mathrm{impl}}(h)$ implies a small $R_{\mathrm{expl}}(h)$ and vice versa.

In practice, the distribution $\bar{\mathcal{D}}$ and the exact p-concept $c(\boldsymbol{x})$ are inaccessible as we only have access to finite samples drawn from the distribution $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$ with $(\boldsymbol{x}_i, \bar{y}_i) \sim \bar{\mathcal{D}}$ and $c(\boldsymbol{x}) = \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]$. Therefore, instead of minimizing the implicit or explicit risks, we will minimize the empirical (implicit) risk

$$\widehat{R}(h) := \frac{1}{N_1}\sum_{i=1}^{N_1}(h(\boldsymbol{x}_i) - \bar{y}_i)^2. \tag{11}$$

using samples $\mathcal{S}$ to obtain the optimal hypothesis that well approximates the underlying p-concept rather than the noisy label. That is, we aim to achieve low R_{expl} by minimizing $\widehat{R}$. Note that we have provide a glossary of error definitions in Table I for ease of reference.

There is nothing that formally distinguishes a p-concept from a "regular" concept in the probably approximately correct (PAC) framework [16, 17]. Instead, the role of the probability distribution only comes forward when we talk about the learnability of such concepts.

[2] In this case, the p-concepts reduce to the "regular" concepts defined in Ref. [17].

[3] The original definition of p-concepts given by Kearns and Schapire [16] is simply a generalization of *concepts* in PAC learning [17] in terms of the function range, while the actual probabilistic component is defined with the learnability of p-concept classes. Here we take a slightly different approach and define p-concepts such that the element of probability is captured within the definition of p-concepts itself.

Name	Notation	Definition
Explicit loss	$\ell_{\text{expl}}(h)$	$(h(\boldsymbol{x}) - c(\boldsymbol{x}))^2$
Implicit loss	$\ell_{\text{impl}}(h)$	$(h(\boldsymbol{x}) - \bar{y})^2$
Explicit risk	$R_{\text{expl}}(h)$	$\mathbb{E}_{(\boldsymbol{x},\bar{y})\sim\bar{\mathcal{D}}}[(h(\boldsymbol{x})-c(\boldsymbol{x}))^2]$
Implicit risk	$R_{\text{impl}}(h)$	$\mathbb{E}_{(\boldsymbol{x},\bar{y})\sim\bar{\mathcal{D}}}[(h(\boldsymbol{x}) - \bar{y})^2]$
Empirical risk	$\widehat{R}(h)$	$\frac{1}{N_1}\sum_{i=1}^{N_1}(h(\boldsymbol{x}_i) - \bar{y}_i)^2$

TABLE I. Glossary of error terms used in our paper. Explicit (implicit) loss and risk are associated with the p-concept $c(\boldsymbol{x})$ (noisy labels $\bar{y}$), while the empirical risk is the empirical version of the *implicit* risk. We have subsumed the subscript in the empirical risk for ease of notation.

Definition 3 (p-concept learning)**.** *Let $N_s \in \mathbb{N}$ be the number of random labels (per data input) and $\mathcal{P} = \{p(\bar{y}|\boldsymbol{x})\}$ be a set of conditional probability distributions over $\mathcal{Y}$ associated with a p-concept class*

$$\mathcal{C} := \{c : \boldsymbol{x} \mapsto \mathbb{E}_{\bar{y}\sim p(\bar{y}|\boldsymbol{x})}[\bar{y}] \,|\, p(\bar{y}|\boldsymbol{x}) \in \mathcal{P}\}. \tag{12}$$

We say $\mathcal{C}$ is p-concept learnable *if there exists an algorithm $\mathcal{A}$ such that:*

1. *for any error tolerance ε and success probability δ,*
2. *for any conditional distribution $p(\bar{y}|\boldsymbol{x}) \in \mathcal{P}$ and corresponding p-concept $c \in \mathcal{C}$ in the class, and*
3. *for any probability distribution $p(\boldsymbol{x})$,*

the learning algorithm $\mathcal{A}$, when given as input a training set $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$, where $(\boldsymbol{x}_i)_{i=1}^{N_1} \sim D^{N_1}$, and each $\bar{y}_i \sim p(\bar{y}|\boldsymbol{x})$, produces a hypothesis h fulfilling

$$\mathbb{P}\left(R_{\text{expl}}(h) \leq \varepsilon\right) \geq 1 - \delta, \tag{13}$$

where $R_{\text{expl}}(h)$ is the risk functional defined in Equation (7) and the probability is over both: the sampling of training sets $(\boldsymbol{x}_i)_{i=1}^{N_1}$ of size N_1 and the sampling of random labels $\bar{y}$ conditional on each $\boldsymbol{x}_i$.

Further, $\mathcal{C}$ is efficiently p-concept learnable *if $\mathcal{A}$ has runtime polynomial in $1/\varepsilon$, $1/\delta$, and $\sigma^2_{\bar{y}|\boldsymbol{x}}$, the conditional variance of $\bar{y}$ given $\boldsymbol{x}_i$ for each $i \in \{1, \dots, N_1\}$. (Runtime efficiency implies sample efficiency, runtime of $\mathcal{A}$ upperbounds N_1).*

When there is no uncertainty in the given label, the p-concept learning model will reduce to the PAC learning model [17]. This is captured in Definition 3 by letting $N_s \to \infty$, and in this regime, we have $R_{\text{impl}}(\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]) = 0$ hence $R_{\text{expl}}(h) = R_{\text{impl}}(h)$.

1. Hypothesis class for modelling probabilistic concepts

To model the p-concepts, we consider the following hypothesis class

$$\mathcal{H} = \left\{h(\boldsymbol{x}) = u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle)\,;\, \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x}) \in \mathbb{R}^p\right\}, \tag{14}$$

where $u : \mathbb{R} \to \mathcal{Y}$ is an L-Lipschitz function that matches the label space $\mathcal{Y}$, $\boldsymbol{w}$ are weight vectors with bounded 2-norm $\|\boldsymbol{w}\|_2 \leq B$ and $\boldsymbol{\phi} : \mathbb{R}^m \to \mathbb{R}^p$ is the feature map that maps $\boldsymbol{x}$ to a higher dimensional feature space with $p > m$ and $\|\phi(\boldsymbol{x})\|_2 \leq 1$, and $\langle\cdot\,,\cdot\rangle$ is the usual inner product. This hypothesis class consists of two components (i) the feature map $\boldsymbol{\phi}(\boldsymbol{x})$ and (ii) the link function u, each serving different roles.

The feature map dictates the class of realizable functions and given two feature vectors $\boldsymbol{\phi}(\boldsymbol{x}), \boldsymbol{\phi}(\boldsymbol{x}')$, their inner product is equal to the kernel function

$$k(\boldsymbol{x}, \boldsymbol{x}') = \langle \boldsymbol{\phi}(\boldsymbol{x}), \boldsymbol{\phi}(\boldsymbol{x}')\rangle. \tag{15}$$

Interestingly, one could express the same class of functions in terms of the kernel. Computing the kernel function $k(\boldsymbol{x}, \boldsymbol{x}')$ directly without explicitly evaluating the feature vectors and their inner products is known as the kernel trick. Note that $\mathcal{H}$ reduces to the typical kernel machines when u is set to be the identity function.

The function u, on the other hand, provides us extra flexibility to incorporate the information about the p-concepts. As discussed, one does not necessarily have access to the exact p-concept $c(\boldsymbol{x})$ but rather to the samples $(\boldsymbol{x}, \bar{y}) \sim \bar{\mathcal{D}} = p(\boldsymbol{x})p(\bar{y}|\boldsymbol{x})$. Direct optimizing kernel machines with the empirical risk $\widehat{R}(\cdot)$ using the training samples $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$ yields

$$g(\boldsymbol{x}) = \sum_{i=1}^{N_1} a_i k(\boldsymbol{x}, \boldsymbol{x}_i). \tag{16}$$

However, this kernel-based model might be too expressive for p-concept modelling as it tends to overfit the noisy labels. Crucially, the link function u can be used to restrict the size of the model class, allowing us to suppress their tendency to overfit. For the sake of clarity, we will postpone the illustrations of the above-mentioned role of u to the latter sections as the examples could be more appropriately understood in the quantum context.

Now, we are ready to express the p-concepts in terms of the hypothesis class. That is,

$$\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}] = c(\boldsymbol{x}) = u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle + \xi(\boldsymbol{x})), \tag{17}$$

where $\xi(\boldsymbol{x}) \in [-M, M]$ is some noise function with $\mathbb{E}_{\boldsymbol{x}}[\xi(\boldsymbol{x})^2] \leq \epsilon_1$ that captures how well one can approximate p-concepts using hypotheses from $\mathcal{H}$. By the L-lipschitz property of u and $\mathbb{E}_{\boldsymbol{x}}[\xi(\boldsymbol{x})^2] \leq \epsilon_1$, we have

$$R_{\text{expl}}(h) = \mathbb{E}_{\bar{\mathcal{D}}}[(h(\boldsymbol{x}) - c(\boldsymbol{x}))^2] \leq L^2\epsilon_1. \tag{18}$$

That is, low ϵ_1 implies low approximation error of $c(\boldsymbol{x})$ using $h \in \mathcal{H}$. This approximation enables us to systematically reduce the learning task to the search of appropriate feature map $\boldsymbol{\phi}(\boldsymbol{x})$, the link function u and the design of efficient algorithms to learn the weight vector $\boldsymbol{w}$.

B. The family of parameterized quantum models

In this work, we are interested in learning a family of parameterized quantum models $f_{\boldsymbol{\theta}}(\boldsymbol{x})$

$$\mathcal{F} = \{f_{\boldsymbol{\theta}}(\boldsymbol{x}) = \mathrm{tr}(\rho_{\boldsymbol{\theta}}(\boldsymbol{x})O) \,|\, \boldsymbol{\theta} \in \Theta\}\,. \tag{19}$$

where $\rho_{\boldsymbol{\theta}}(\boldsymbol{x})$ are parameterized quantum states with parameters $\boldsymbol{\theta} \in \Theta = \mathbb{R}^r$ and input data $\boldsymbol{x} \in \mathcal{X} = \mathbb{R}^m$ while O is an arbitrary Hermitian observable. The quantum states $\rho_{\boldsymbol{\theta}}(\boldsymbol{x}) = \mathcal{M}_{\boldsymbol{\theta},\boldsymbol{x}}(\rho_0)$ could be prepared by applying parameterized quantum channels $\mathcal{M}_{\boldsymbol{\theta},\boldsymbol{x}}(\cdot)$ on some initial state ρ_0. In particular, we will focus on specific quantum channels that are generated by parameterized quantum circuits (PQCs). We remark that our analysis can be directly extended to other quantum channels including ground state preparation channels [9–11].

1. PQCs and their classical Fourier representations

Let $\boldsymbol{x} = (x_1, \ldots, x_m) \in \mathcal{X} = [0, 2\pi)^m$ be a vector of data points, $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_m) \in \Theta = [0, 2\pi)^r$ be a vector of parameters, $U(\boldsymbol{x}, \boldsymbol{\theta})$ be the unitary that represents the PQCs, $|\mathbf{0}\rangle = |0\rangle^{\otimes n}$ and O be an arbitrary Hermitian observable. We define the PQC model as

$$f_{\boldsymbol{\theta}}(\boldsymbol{x}) = \langle \mathbf{0}| \, U^\dagger(\boldsymbol{x}, \boldsymbol{\theta}) O U(\boldsymbol{x}, \boldsymbol{\theta}) \, |\mathbf{0}\rangle\,. \tag{20}$$

For a given $U(\cdot, \boldsymbol{\theta})$ and O, we define the PQC model class $\mathcal{F}_{U,O}$ as

$$\mathcal{F}_{U,O} = \left\{ f_{\boldsymbol{\theta}}(\cdot) = \langle \mathbf{0}| \, U^\dagger(\cdot, \boldsymbol{\theta}) O U(\cdot, \boldsymbol{\theta}) \, |\mathbf{0}\rangle \ \middle|\ \boldsymbol{\theta} \in \Theta \right\} \tag{21}$$

for all $\boldsymbol{x} \in \mathcal{X}$.

The parameterized unitary $U(\boldsymbol{x}, \boldsymbol{\theta})$ consists of a sequence of two different types of parameterized quantum gates. The first type of parameterized quantum gates is controlled by parameters $\boldsymbol{\theta}$, while the second type embeds data points x_i into the PQCs via unitary evolution

$$V_{(j,k)}(x_j) = e^{-iH_k^{(j)} x_j}, \tag{22}$$

generated by some Hamiltonian $H_k^{(j)}$. Given this parameterization strategy, it is well-known that PQC models could be written as a Fourier series[4] [29, 30]

$$f_{\boldsymbol{\theta}}(\boldsymbol{x}) = \sum_{\boldsymbol{\omega} \in \tilde{\Omega}} c_{\boldsymbol{\omega}}(\boldsymbol{\theta}) e^{i\langle \boldsymbol{\omega}, \boldsymbol{x}\rangle}, \tag{23}$$

where the frequency spectrum $\tilde{\Omega}$ is determined by the ensemble of eigenvalues of embedding Hamiltonian $\{H_k^{(j)}\}_{j,k}$ and the coefficients $c_{\boldsymbol{\omega}}(\boldsymbol{\theta})$ depend on the quantum gates parameterized by $\boldsymbol{\theta}$.

Equation (23) can be further simplified by noting that the non-zero frequencies in $\tilde{\Omega}$ come in pairs, i.e., $\boldsymbol{\omega}, -\boldsymbol{\omega} \in \tilde{\Omega}$, allowing us to split $\tilde{\Omega}$ into two components. That is, $\tilde{\Omega} := \Omega \cup (-\Omega)$ with $\Omega \cap (-\Omega) = \{\boldsymbol{\omega}_0\}$, where $\boldsymbol{\omega}_0 = (0, \ldots, 0) \in \tilde{\Omega}$ is the vector of zero frequencies. Let $\Omega = \{\boldsymbol{\omega}_0, \boldsymbol{\omega}_1, \ldots, \boldsymbol{\omega}_{|\Omega|}\}$ and for all $\boldsymbol{\omega} \in \Omega \backslash \{\boldsymbol{\omega}_0\}$, we have

$$a_{\boldsymbol{\omega}}(\boldsymbol{\theta}) := c_{\boldsymbol{\omega}}(\boldsymbol{\theta}) + c_{-\boldsymbol{\omega}}(\boldsymbol{\theta}) \tag{24}$$

$$b_{\boldsymbol{\omega}}(\boldsymbol{\theta}) := i(c_{\boldsymbol{\omega}}(\boldsymbol{\theta}) - c_{-\boldsymbol{\omega}}(\boldsymbol{\theta})). \tag{25}$$

Given this definition, Equation (23) can be equivalently written as

$$f_{\boldsymbol{\theta}}(\boldsymbol{x}) = c_{\boldsymbol{\omega}_0}(\boldsymbol{\theta}) + \sum_{i=1}^{|\Omega|-1} (a_{\boldsymbol{\omega}_i}(\boldsymbol{\theta}) \cos(\langle \boldsymbol{\omega}_i, \boldsymbol{x}\rangle) + b_{\boldsymbol{\omega}_i}(\boldsymbol{\theta}) \sin(\langle \boldsymbol{\omega}_i, \boldsymbol{x}\rangle)) \tag{26}$$

Identifying the corresponding weight vectors $\boldsymbol{w}$

$$\boldsymbol{w}_F(\boldsymbol{\theta}) = \sqrt{|\Omega|} \begin{pmatrix} c_{\boldsymbol{\omega}_0}(\boldsymbol{\theta}) \\ a_{\boldsymbol{\omega}_1}(\boldsymbol{\theta}) \\ b_{\boldsymbol{\omega}_1}(\boldsymbol{\theta}) \\ \vdots \\ a_{\boldsymbol{\omega}_{|\Omega|-1}}(\boldsymbol{\theta}) \\ b_{\boldsymbol{\omega}_{|\Omega|-1}}(\boldsymbol{\theta}) \end{pmatrix}^{\mathsf{T}} \tag{27}$$

and the trigonometric polynomial feature map

$$\boldsymbol{\phi}_F(\boldsymbol{x}) = \frac{1}{\sqrt{|\Omega|}} \begin{pmatrix} 1 \\ \cos(\langle \boldsymbol{\omega}_1, \boldsymbol{x}\rangle) \\ \sin(\langle \boldsymbol{\omega}_1, \boldsymbol{x}\rangle) \\ \vdots \\ \cos\left(\langle \boldsymbol{\omega}_{|\Omega|-1}, \boldsymbol{x}\rangle\right) \\ \sin\left(\langle \boldsymbol{\omega}_{|\Omega|-1}, \boldsymbol{x}\rangle\right) \end{pmatrix} \tag{28}$$

enables us to express the PQC model as a linear model with respect to the feature map $\boldsymbol{\phi}_F$, i.e.,

$$f_{\boldsymbol{\theta}}(\boldsymbol{x}) = \langle \boldsymbol{w}_F(\boldsymbol{\theta}), \boldsymbol{\phi}_F(\boldsymbol{x})\rangle, \tag{29}$$

and the associated kernel function is given by $k_F(\boldsymbol{x}, \boldsymbol{x}') = \langle \boldsymbol{\phi}_F(\boldsymbol{x}), \boldsymbol{\phi}_F(\boldsymbol{x}')\rangle$.

2. Data extraction from parameterized quantum models

In general, one does not have direct access to $f_{\boldsymbol{\theta}}(\boldsymbol{x})$. Instead, they are estimated using finite samples from measurement procedures such as direct measurement or classical shadow methods, as described in Appendix A. We denote outputs of such estimation procedures as $\bar{y}$ and their dependency on the data point $\boldsymbol{x}$, parameter $\boldsymbol{\theta}$, and the number of measurement shots N_s are implicitly assumed. In addition, they are unbiased estimators of $f_{\boldsymbol{\theta}}(\boldsymbol{x})$, i.e.,

$$f_{\boldsymbol{\theta}}(\boldsymbol{x}) = \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}, \boldsymbol{\theta}]. \tag{30}$$

[4] The Fourier expansion in this work mainly follows the treatment in Ref. [25, 26] but equivalent Fourier representation of PQC models can be obtained by other Fourier expansion methods [27, 28]

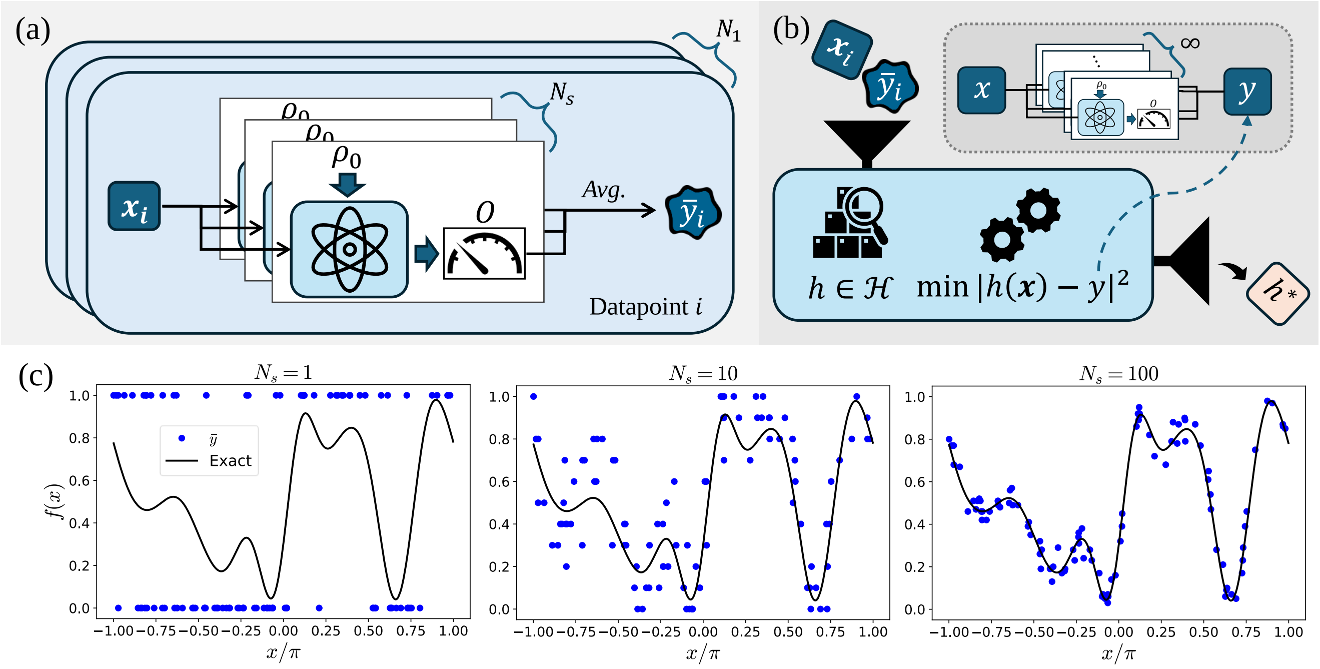


FIG. 2. Concept learning of parameterized quantum models. (a) To learn quantum models, one needs to probe the quantum model with N different input data points $\boldsymbol{x}$, and construct an estimator of the quantum model $y = f(\boldsymbol{x})$ conditioned on the input. Such estimators $\bar{y}$ can be constructed by taking the average over N_s duplicate quantum measurements. (b) Using data pairs $(\boldsymbol{x}_i, \bar{y}_i)$ collected from the quantum model, the task is to classically learn a representation h^* of the quantum model such that the output of classical representation $h(\boldsymbol{x})$ is close to the underlying expected output $y = f(\boldsymbol{x})$ of the quantum model for any arbitrary $\boldsymbol{x}$. As illustrated in (c), the number of measurement shots N_S will determine the closeness between the estimator $\bar{y}$ (blue dots) and the underlying expected value $f(x)$ (black solid line).

For ease of notation, we will drop the conditional dependency of the expectation on $\boldsymbol{\theta}$ from now on.

Now, we describe the procedures for obtaining labelled data points from a given $f_{\boldsymbol{\theta}}$. Without loss of generality, we let $p(\boldsymbol{x})$ be a uniform distribution of input $\boldsymbol{x}$. As depicted in Figure 2 (a), a set of N i.i.d. samples of $\boldsymbol{x}$ is first drawn from $p(\boldsymbol{x})$ and subsequently input to the quantum model to collect their associated labels $\bar{y}$ via the procedures described in Appendix A using N_s measurement repetitions. This gives the set of data $\mathcal{S} = \{\boldsymbol{x}_i, \bar{y}_i\}_{i=1}^{N}$. Shown in Figure 2 (c) are the labels $\bar{y}$ estimated with $N_s = 1, 10, 100$.

III. PARAMETERIZED QUANTUM MODELS AS PROBABILISTIC CONCEPTS

One can immediately deduce from Equation (30) that parameterized quantum models (PQMs) are p-concepts. Now, we will show that the hypothesis class defined in Section II A 1 is an appropriate model class for the learning of PQMs. Modelling PQMs using the hypothesis from $\mathcal{H}$, as defined in Equation (14), assumes the following: there exist a feature map $\boldsymbol{\phi}(\boldsymbol{x})$, a function u, a weight vector $\boldsymbol{w}$, and a noise function $\xi(\boldsymbol{x})$ such that the PQMs

Algorithm 1: The learning algorithm

```
Input: Labelled training data $\{(\boldsymbol{x}_i, \bar{y}_i)\}_{i=1}^{N_1} \in \mathcal{X} \times \mathcal{Y}$,
       non-decreasing $L$-Lipschitz function
       $u : \mathbb{R} \to \mathcal{Y}$, kernel function $k$ corresponding to
       feature map $\boldsymbol{\phi}$, learning rate $\lambda > 0$, number of
       iterations $T$, labelled held-out data of size $N_2$
       $\{(\boldsymbol{p}_j, \bar{q}_j)\}_{j=1}^{N_2} \in \mathcal{X} \times \mathcal{Y}$
$\alpha^i := 0 \in \mathbb{R}^{N_1}$
for $t = 1, \ldots, T$ do
    $h^t(\boldsymbol{x}) := u\left(\sum_{i=1}^{N_1} \alpha_i^t k(\boldsymbol{x}, \boldsymbol{x}_i)\right)$
    for $i = 1, 2, \ldots, N_1$ do
        $\alpha_i^{t+1} := \alpha_i^t + \frac{\lambda}{N_1}(\bar{y}_i - h^t(\boldsymbol{x}_i))$
Output: $h^r$ where
        $r = \arg\min_{t \in \{1,\ldots,T\}} \frac{1}{N_2} \sum_{j=1}^{N_2} (\bar{q}_j - h^t(\boldsymbol{p}_j))^2$
```

can be expressed as

$$\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}] = \mathrm{tr}(\rho_{\boldsymbol{\theta}}(\boldsymbol{x})O) = u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle + \xi(\boldsymbol{x})), \qquad (31)$$

with $||\boldsymbol{w}||_2 \le B$, $\xi(\boldsymbol{x}) \in [-M, M]$, and $\mathbb{E}_{\boldsymbol{x}}[\xi(\boldsymbol{x})^2] \le \epsilon_1$. Hence, the aim here is to find an appropriate function u that contains information on the PQM as well as construct the feature map $\boldsymbol{\phi}(\boldsymbol{x})$ that efficiently approximates a PQM.

A. Algorithm for concept learning of parameterized quantum models

By expressing the PQMs in terms of the hypothesis in $\mathcal{H}$, we systematically reduce the modelling problem to the search of the appropriate feature map $\boldsymbol{\phi}(\boldsymbol{x})$, link function u, and optimal weight $\boldsymbol{w}^*$. As the first two attributes are highly dependent on the problem at hand, we will defer their discussion to Section IV. In this section, we will assume $\boldsymbol{\phi}(\boldsymbol{x})$ and u are known and focus on the algorithm part of the problem.

Consider a PQM $\mathrm{tr}(\rho(\boldsymbol{x})O)$ that can be approximated by a feature map $\boldsymbol{\phi}(\boldsymbol{x})$ and a known L-Lipschitz non-decreasing function $u : \mathbb{R} \to \mathcal{Y}$, as per Equation (31). The task of learning PQMs could be formulated as the search of the optimal weight vector $\boldsymbol{w}^*$ such that the output hypothesis $h^*(\boldsymbol{x}) = u(\langle \boldsymbol{w}^*, \boldsymbol{\phi}(\boldsymbol{x})\rangle)$ minimizes the explicit risk

$$R_{\mathrm{expl}}(h^*) = \mathbb{E}_{\bar{\mathcal{D}}}[(u(\langle \boldsymbol{w}^*, \boldsymbol{\phi}(\boldsymbol{x})\rangle) - \mathrm{tr}(\rho(\boldsymbol{x})O))^2]. \quad (32)$$

As discussed in Section II A, we will only have access to finite samples drawn from the distribution $\bar{\mathcal{D}}$. Hence, we will be minimizing the empirical risk $\widehat{R}(h)$ in Equation (11) using some training samples $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$ with $(\boldsymbol{x}_i, \bar{y}_i) \sim \bar{\mathcal{D}}$ instead of $R_{\mathrm{expl}}(h)$. Note that the extra u in the empirical risk makes the optimization non-convex. As detailed in Figure 2 (b), while the classical machine learns from a noisy dataset consisting of shot noise from quantum measurements, our objective is to enable the classical machine to approximate the underlying p-concept of the PQM, i.e., the expected value of the measured outcomes of PQMs.

Shown in Algorithm 1 is an iterative-based method that learns PQMs under some mild assumptions. While our algorithm is derived from the iterative method in Ref. [31], we extended the provable guarantee of the original algorithm to include the number of measurement shots N_s used to estimate $\bar{y}$ and show its operational role in the algorithm. The analytical guarantee enables us to understand the contributions of errors and the intuitive explanation of the working principle of Algorithm 1 is provided in Appendix B 1.

Theorem 1 (p-concept learnability of PQMs). *We are given a quantum observable O such that $\|O\|_\infty = \Delta$. With this observable, we have quantum model whose expected output can be expressed as a classical representation as follows: $\mathrm{tr}(\rho(\boldsymbol{x})O) = u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle + \xi(\boldsymbol{x}))$, where $u : \mathbb{R} \to [-\Delta, \Delta]$ is a known L-Lipschitz non-decreasing function, $\xi : \mathbb{R}^m \to [-M, M]$ such that $\mathbb{E}_{\boldsymbol{x}}[\xi(\boldsymbol{x})^2] \leq \epsilon_1$, $\|\boldsymbol{w}\|_2 \leq B$, and $\|\phi(\boldsymbol{x})\|_2 \leq 1$. Considering a training dataset of N_1 i.i.d. samples of $\boldsymbol{x}$ as input to the quantum model, and whose label is the sample mean of the output of the quantum model sampled over N_s measurements. Let the conditional variance of an individual measurement averaged over all $\boldsymbol{x}$ be $\bar{\sigma}$. For $\delta \in (0, 1)$, with probability $1-\delta$, setting the learning rate $\lambda = \frac{1}{L}$ and given a validation dataset size of $N_2 = \mathcal{O}(N_1 \Delta^2 \log(\frac{T}{\delta}))$, after $T = \mathcal{O}(\frac{BL}{\epsilon_4})$ iterations, Algorithm 1 outputs a hypothesis $h \in \mathcal{H}$ such that*

$$R_{\mathrm{expl}}(h) \leq \mathcal{O}(L\Delta\sqrt{\epsilon_1} + L\Delta M \epsilon_2 + LB\Delta\epsilon_3 + LB\epsilon_4 + \Delta^2\epsilon_5), \quad (33)$$

where $\epsilon_2 = \sqrt[4]{\frac{\log(\frac{1}{\delta})}{N_1}}$, $\epsilon_3 = \sqrt{\frac{1}{N_1}}$, $\epsilon_4 = \sqrt{\frac{\bar{\sigma}\log(\frac{1}{\delta})}{N_1 N_s}}$, $\epsilon_5 = \sqrt{\frac{\log(\frac{1}{\delta})}{N_1}}$, and $\bar{\sigma} = \mathbb{E}_{\boldsymbol{x}}[\sigma^2_{y|\boldsymbol{x}}]$.

The proof of this theorem can be found in Appendix B 2. As shown in Equation (33), four different error sources will affect the performance of the models: (i) the approximation error ϵ_1, (ii) the data sampling errors ϵ_2 and ϵ_5, (iii) the learnability error ϵ_3, and (iv) the label sampling error ϵ_4. Firstly, the approximation error ϵ_1 captures the intrinsic error that can be achieved by our hypothesis class as it tells us how far away our hypothesis $h(\boldsymbol{x})$ is from the true function $\mathrm{tr}(\rho(\boldsymbol{x})O)$ we wish to learn, i.e., $\mathbb{E}_{\boldsymbol{x}}[\xi(\boldsymbol{x})^2] \leq \epsilon_1$. It is therefore impossible to obtain a small risk if the approximation error is high to begin with. On the other hand, the data sampling errors ϵ_2 and ϵ_5 capture the statistical noise arising from the finite data samples provided to the learning algorithm while the learnability error ϵ_3 stems from Rademacher complexity and quantifies the hardness of learning with the given hypothesis class. Both of these errors can be minimized by providing more data samples. Lastly, the label sampling error ϵ_4 is influenced by three attributes, the averaged variance $\mathbb{E}_{\boldsymbol{x}}[\sigma^2_{y|\boldsymbol{x}}]$, the number of training data points N_1, and the number of measurement shots N_s. Increasing either N_1 or N_s could reduce the label sampling error. Additionally, a measurement scheme that results in smaller variance will require fewer training data points and measurement shots to achieve a smaller ϵ_4 error.

B. Asymmetrical effects of N_1 and N_s

While the individual implications of all four types of errors are straightforward to deduce, jointly analysing the last three sources of error leads to an interesting observation regarding the asymmetrical effects of N_1 and N_s on classical learning of quantum models. On the one hand, increasing N_s can only decrease the label sampling error ϵ_4 but not the data sampling errors ϵ_2 and ϵ_5 and the learnability error ϵ_3. On the other hand, increasing N_1 will simultaneously decrease all three errors, and ϵ_4 approaches 0 regardless of the value of N_s. Consequently, one could set $N_s = 1$ when N_1 is sufficiently large. This observation aligns with intuition, as the labels are dependent on the parameters. By sampling across the training points, one effectively samples across various labels, thereby providing a reasonable estimation of quantum models. In contrast, increasing the resolution of the labels does not provide extra information on other data points. This observation is summarised in Corollary 1 and numerically illustrated in Figure 3 (a). For simplicity, we assume $\delta = 0.01$, and $\bar{\sigma} = L = B = \Delta = 1$.

Corollary 1 (Asymmetrical effects of N_1 and N_s)**.** *Let all variables defined as per Theorem 1. For the hypothesis class $\mathcal{H}$ with link function u, feature map $\boldsymbol{\phi}(\boldsymbol{x})$ and weight vector $\boldsymbol{w}$ with $\mathrm{tr}(\rho(\boldsymbol{x})O) = u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle) \in \mathcal{H}$, i.e., $\mathbb{E}_{\boldsymbol{x}}[\xi(\boldsymbol{x})^2] = 0$, Algorithm 1 will output a hypothesis $h \in \mathcal{H}$ such that*

$$R_{\mathrm{expl}}(h) \leq c_1\sqrt{\frac{1}{N_1}} + c_2\sqrt{\frac{1}{N_1 N_s}} + c_3\sqrt{\frac{1}{N_1}}, \tag{34}$$

where $c_1 = \mathcal{O}(LB\Delta)$, $c_2 = \mathcal{O}\left(LB\sqrt{\bar{\sigma}\log\left(\frac{1}{\delta}\right)}\right)$, $c_3 = \mathcal{O}\left(\Delta^2 \log\left(\frac{1}{\delta}\right)\right)$, and N_1 and N_s contribute asymmetrically to $R(h)$. That is, for a constant N_1, $R(h) \not\to 0$ when $N_s \to \infty$, but $R(h) \to 0$ when $N_1 \to \infty$ regardless of the value of N_s. Note that $\epsilon_1 = 0$ implies $M = 0$ by definition.

The overall analysis shows that for a sufficiently large N_1, classical models can learn quantum models that have efficient classical representation even when target labels are estimated with limited measurement shots, e.g., $N_s = 1$. Conversely, when such efficient classical representation cannot be found, $\mathrm{tr}(\rho(\boldsymbol{x})O)$ is not learnable even when N_1 and N_s are infinite. Corollary 1 further shows that N_s plays a less significant role than N_1 in the classical learning of quantum models. In other words, shot noise is not a fundamental concern in classical learning of quantum models as its role can be easily substituted by N_1.

C. Trade-offs between N_1 and N_s

In an ideal world, one would choose N_1 and N_s as large as possible to minimize the explicit risk. However, external constraints like financial budgets and time limitations might significantly restrict the total number of queries to a quantum model. Thus, a more realistic setting is to first consider a fixed number of queries to quantum models, and N_1 and N_s are subsequently decided.

In general, producing more samples for a fixed parameter setting in an experiment is much cheaper and faster than changing the parameter settings each time. Changing parameters incurs an additional cost that may stem from preprocessing subroutines, classical transpilation and optimization of the circuits or platform-dependent factors regarding the hardware we are executing the quantum circuits on. For example, the penalty cost for superconducting quantum computers would be larger than for trapped-ion quantum computers, as it is relatively cheaper to produce more samples for a fixed parameter set than to change the parameter setting each time in the former platform [32]. To quantify such costs for easier discussion, we assume that these costs can be quantitatively evaluated to be some multiple $\gamma \in \mathbb{R}_+$ of the cost to run a repetition of quantum circuits that have already been configured. That is, we assume changing the parameter setting once will incur extra cost of γ shots.

Considering the total measurement budget for training, we find that $N_{\mathrm{tot}} = N_1 \cdot (N_s + \gamma)$. Fixing the total measurement budget N_{tot} implies a trade-off between N_1 and N_s: increasing N_1 will reduce N_s and vice versa. This poses an interesting learning-theoretic question: *given a fixed N_{tot}, will classical machines learn better with training datasets consisting of more inputs/parameters with noisier labels (larger N_1 but smaller N_s) or fewer inputs with cleaner labels (smaller N_1 but larger N_s)?* As shown in Corollary 2, when N_1 and N_s are treated equally ($\gamma = 0$), asymptotically, it is generally better to sample more inputs, i.e., $(N_1^*, N_s^*) = (N_{tot}, 1)$. When there is an extra cost for changing the parameter settings, i.e., $\gamma > 0$, there exists a pair of optimal input size N_1^* and the shot number N_s^* that minimize the explicit risk. These observations are numerically illustrated in Figure 3 (b). For simplicity, we assume $\delta = 0.01$, and $\bar{\sigma} = L = B = \Delta = 1$.

Corollary 2 (Trade-off between N_1 and N_s)**.** *Consider the setting as per Corollary 1. For a given fix total measurement budget for training $N_{\mathrm{tot}} \in \mathbb{N}$ and a fix penalty cost $\gamma \in \mathbb{R}_+$, N_1 and N_s are determined by $N_{\mathrm{tot}} = N_1 \cdot (N_s + \gamma)$. Respecting this constraint, Algorithm 1 will output a hypothesis $h \in \mathcal{H}$ such that*

$$R_{\mathrm{expl}}(h) \leq c_1\sqrt{\frac{N_s + \gamma}{N_{\mathrm{tot}}}} + c_2\sqrt{\frac{N_s + \gamma}{N_{\mathrm{tot}} N_s}} + c_3\sqrt{\frac{N_s + \gamma}{N_{\mathrm{tot}}}}. \tag{35}$$

When $\gamma = 0$, the upper bound of the explicit risk $R_{\mathrm{expl}}(h)$ reduces to

$$R_{\mathrm{expl}}(h) \leq c_1\sqrt{\frac{N_s}{N_{\mathrm{tot}}}} + c_2\sqrt{\frac{1}{N_{\mathrm{tot}}}} + c_3\sqrt{\frac{N_s}{N_{\mathrm{tot}}}} \tag{36}$$

which is minimized when $N_s = 1$. When $\gamma > 0$, there exists a pair of optimal input data size and shot number (N_1^*, N_s^*) where

$$N_1^* = \frac{N_{tot}}{N_s^* + \gamma} \quad \textit{and} \quad N_s^* = \left(\frac{c_2 \gamma}{c_1 + c_3}\right)^{\frac{2}{3}} \tag{37}$$

that minimizes our upper bound of $R_{\mathrm{expl}}(h)$.

Note that the optimal value of N_s does not correlate with N_{tot}, but depends on the constant penalty cost γ. Hence, setting $N_s = 1$ regardless of the value of γ would only increase $R_{\mathrm{expl}}(h)$ by a factor of $\sqrt{1+\gamma}$, retaining learnability up to a constant factor for single measurement learning.

Taking a closer examination at N_s, we check whether other factors apart from the device-dependent cost γ affect the value of N_s. Delving into the definitions of the terms c_1, c_2, and c_3, we note that the terms L, Δ, and δ are constants that either depend on the problem setting or can be set arbitrarily. B, on the other hand, is directly

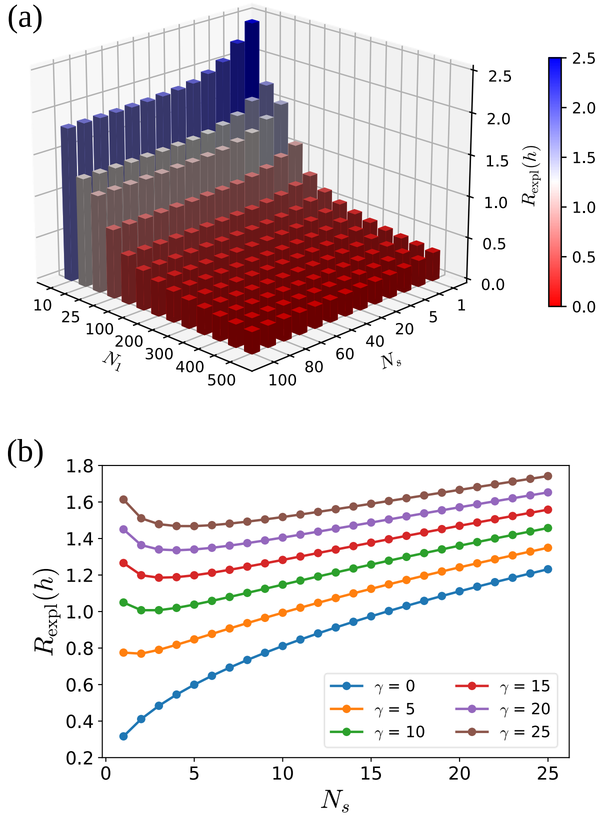


FIG. 3. The respective numerical illustrations of Corollary 1 and Corollary 2 with $\delta = 0.01$, and $\bar{\sigma} = L = B = \Delta = 1$. (a) The plot shows the asymmetrical effect of the number of training samples N_1 and the number of measurement shots N_s to the explicit risk $R_{\mathrm{expl}}(h)$. (b) For a fixed total measurement budget N_{tot}, the optimal pair of N_1 and N_s will change with γ. When $\gamma = 0$, the optimal shot number is $N_s = 1$ but it depends on γ when $\gamma > 0$. All curves are computed with $N_{tot} = 600$ and $N_s = \{1, 2, 3, \ldots, 24, 25\}$.

related to the expressibility of the hypothesis h used to model the quantum model. *Does the expressibility B of the hypothesis h affect the number of shots N_s required?*

Plugging in $c_1 = \mathcal{O}(B)$, $c_2 = \mathcal{O}(B)$, $c_3 = \mathcal{O}(1)$, we note that in terms of B, $N_s = \mathcal{O}\left(\frac{B}{B+K}\right)$, where K is a constant. While N_s is indeed dependent on B, its dependency can be upper bounded by a constant as $N_s \to \mathcal{O}(1)$ as B grows. Hence, even in cases where the expressibility of the hypothesis h we use to exactly model the quantum model scales exponentially, the number of shots required to sample each data is still limited to a constant value.

D. Shot-noise dependent bias-variance trade-off

An alternative framework for analyzing the occurrences of different error terms commonly seen in machine learning analysis is the bias-variance-noise decomposition. Here, we provide a summary with the full introduction deferred to Appendix C.

Optimizing the empirical risk $\widehat{R}(h)$ using different training datasets $\mathcal{S}$ would yield different trained models $h_{\mathcal{S}}(\boldsymbol{x})$. The bias then measures, on average, how much $h_{\mathcal{S}}$ deviates from the ground truth f

$$\mathbf{Bias}_{\mathcal{S}} := \mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - f(\boldsymbol{x}), \tag{38}$$

while the variance

$$\mathbf{Var}_{\mathcal{S}} := \mathbb{E}_{\mathcal{S}}\left[(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - h_{\mathcal{S}}(\boldsymbol{x}))^2\right] \tag{39}$$

measures the fluctuations among the trained models. As the expectation is taken over all possible training datasets of the same size, therefore, the bias and variance will be dependent on the complexity of the hypothesis class, the number of training data points N_1 and the number of random labels N_s.

The average of the explicit risk over all possible training datasets will then have the following decomposition, whose derivation is also found in Appendix C:

$$\mathbb{E}_{\mathcal{S}}[R_{\mathrm{expl}}(h_{\mathcal{S}})] = \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Bias}^2_{\mathcal{S}}\right] + \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Var}_{\mathcal{S}}\right]. \tag{40}$$

where

$$\mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Bias}^2_{\mathcal{S}}\right] := \mathbb{E}_{\boldsymbol{x}}\left[(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - f(\boldsymbol{x}))^2\right] \quad \text{and} \tag{41}$$

$$\mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Var}_{\mathcal{S}}\right] := \mathbb{E}_{\boldsymbol{x},\mathcal{S}}\left[(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - h_{\mathcal{S}}(\boldsymbol{x}))^2\right] \tag{42}$$

are the averaged bias squared and averaged variance, respectively. This decomposition shows that the shot noise has an indirect impact on the performance of classical machine learning models and this impact can be studied by analysing the statistical quantities $\mathbf{Bias}^2_{\mathcal{S}}$ and $\mathbf{Var}_{\mathcal{S}}$. Intuitively, high shot noise implies high variance in the labels, indirectly leading to high variance in the models, and further induces overfitting. We will provide a simple example in Section IV to illustrate how shot noise affects the bias-variance trade-off.

Equation (33) and Equation (40) appear to be unrelated to each other. On the one hand, the algorithm-specific Equation (33) gives a probabilistic guarantee on the performance of each trained model. On the other hand, the algorithm-agnostic Equation (40) provides an understanding of the average behaviour of the overall hypothesis class. One can however observe the similarities between the two by directly comparing Equation (33) and Equation (40). Specifically, the first term in Equation (33) can be understood as the bias of the models since it quantifies the asymptotic error that is achievable by the models while the second term captures the finite sampling noise of the bias; the other three terms inform on the variance of the model. Interestingly, the shot-noise dependent variance is captured by ϵ_4 and Figure 3 essentially captures the variance dependence on the number of training data points and number of measurement shots.

IV. CLASSICAL SURROGATES OF PQC MODELS AS PROBABILISTIC CONCEPTS

As a direct example, we apply our theoretical framework to create a classical surrogate of parameterized quantum circuit (PQC) models [8]. Treating PQC models as p-concepts enables us to study the impact of shot noise on constructing their corresponding classical surrogates. In particular, we observed asymmetrical effects from both the number of training data points and the number of measurement shots, as well as the potential for using a relatively small number of measurement shots to surrogate PQC models. As predicted by our theoretical analysis, the bias and variance of the classical surrogates are highly dependent on the strength of the shot noise. Finally, we highlight the role of the link function in our surrogate models in suppressing their variance in the presence of the shot noise.

We wish to emphasize that our work aims to provide a generic framework to analyse the learnability of PQMs in the presence of shot noise. Therefore, in this example, we will consider the feature map proposed in the literature [29, 30], but our framework is readily adaptable to future proposals of efficient feature maps. In addition, our results can be easily extended to other types of PQMs by replacing the quantum channel with appropriate substitutes.

A. Classical approximation of PQC models

In this section, we will briefly discuss the existing methods for approximating PQC models classically. As described in Section II B 1, PQC models can be written as $f_{\boldsymbol{\theta}}(\boldsymbol{x}) = \langle \boldsymbol{w}_F(\boldsymbol{\theta}), \boldsymbol{\phi}_F(\boldsymbol{x})\rangle$. Therefore, the immediate choice of feature map for modelling PQC models classically is the full trigonometric polynomial feature map $\boldsymbol{\phi}_F(\boldsymbol{x})$. However, the associated model class could be too expressive thus it might overfit the training data points [8]. In addition, the size of the frequency spectrum could be exponential in the data dimension, which becomes intractable for classical computers. Instead, one could hope to exploit some structure of the PQC to construct an efficient feature map $\boldsymbol{\phi}(\boldsymbol{x})$ to approximate the PQC models

$$\langle \mathbf{0}| U^\dagger(\boldsymbol{x},\boldsymbol{\theta}) O U(\boldsymbol{x},\boldsymbol{\theta}) |\mathbf{0}\rangle \approx \langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle. \tag{43}$$

According to our notation above, we would use the noise function $\xi(\boldsymbol{x})$ to refer to the approximation error $\xi(\boldsymbol{x}) = \langle \boldsymbol{w}_F, \boldsymbol{\phi}_F(\boldsymbol{x})\rangle - \langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle$. We drop the explicit $\boldsymbol{\theta}$ dependence of $\boldsymbol{w}_F$ and ξ for ease of notation.

One approach would be to construct $\boldsymbol{\phi}$ as a truncated version of $\boldsymbol{\phi}_F$. This would take advantage of the fact that the high-frequency components of PQC models that are subjected to Pauli noise [27] typically make smaller contributions than lower frequency terms. Thus, Fourier series with an appropriate level of truncation can be used to model PQC models without compromising much of the accuracy. This approach assumes that we know which components to truncate ahead of time, though, and that might be unrealistic for practical scenarios.

As an alternative, one can utilize a popular technique from machine learning called Random Fourier Features (RFF) [33], used to efficiently approximate the high-dimensional inner product $\langle \boldsymbol{w}_F(\boldsymbol{\theta}), \boldsymbol{\phi}_F(\boldsymbol{x})\rangle$ by randomly selecting only a few of its dominant terms [25, 26]. Using RFF amounts to performing a truncation of the Hilbert space, with the only difference being that the selection of components that are kept is probabilistic. RFF has been proposed as an approach to "dequantize" PQC-based quantum machine learning models by exploiting the efficient low-dimensional feature map $\boldsymbol{\phi}$ in Ref. [25]. On the other hand, Ref. [26] discusses the applicability of RFF in terms of which PQCs are likely to admit the efficient approximation. In both these references, the task is not to *learn* the classically efficient representation of the PQC but rather to show that a given downstream task can be learned efficiently classically, without ever running the PQC. Even though the specific task is not the same, we observe that the main limitation in learning quantum models comes from an efficient classical representation, which deeply aligns with the use of RFF. In Appendix D we formally discuss how the performance guarantees of RFF bring about learnability in the sense introduced in Sections II and III. Also, we wish to emphasize that the efficient classical representation of PQCs is still under active research, but our work could be directly adapted if efficient feature maps were found.

B. Modelling PQCs with and without link functions

In this section, we will discuss the operational role of the link function u in the surrogation of PQC models. Without loss of generality, we let $O = |\mathbf{0}\rangle\langle\mathbf{0}|$, hence we have

$$f_{\boldsymbol{\theta}}(\boldsymbol{x}) = |\langle \mathbf{0}| U(\boldsymbol{x},\boldsymbol{\theta}) |\mathbf{0}\rangle|^2 = \langle \boldsymbol{w}, \boldsymbol{\phi}_{\mathrm{RFF}}(\boldsymbol{x})\rangle + \xi(\boldsymbol{x}), \tag{44}$$

and $f_{\boldsymbol{\theta}}(\cdot) \in \mathcal{F}_{U,|\mathbf{0}\rangle\langle\mathbf{0}|}$. To model the probabilistic function $f_{\boldsymbol{\theta}}(\boldsymbol{x})$, we consider the following hypothesis class

$$\mathcal{H}_{\mathrm{RFF}} = \{h(\boldsymbol{x}) = u(\langle \boldsymbol{w}, \boldsymbol{\phi}_{\mathrm{RFF}}(\boldsymbol{x})\rangle), \|\boldsymbol{w}\|_2 \leq B\} \tag{45}$$

where u is the clipping function

$$u(x) = \begin{cases} 0, & x < 0 \\ x, & 0 \leq x \leq 1 \\ 1, & x > 1 \end{cases}, \tag{46}$$

a 1-Lipschitz function that enforces the matching of co-domains of the hypothesis class $\mathcal{H}$ and $|\langle \mathbf{0}| U(\boldsymbol{x},\boldsymbol{\theta}) |\mathbf{0}\rangle|^2$ while ensuring the output of the linear hypothesis h within range $[0,1]$ is not distorted. Note that the link function has no impact on $f_{\boldsymbol{\theta}}(\boldsymbol{x})$ since $f_{\boldsymbol{\theta}}(\boldsymbol{x}) \in [0,1]$.

To provide context regarding the value of B, we note that similar to the full Fourier representation of PQC models, the weight vectors of the RFF feature map can also be written as

$$\boldsymbol{w} = \sqrt{D} \begin{pmatrix} a_{\tilde{\boldsymbol{\omega}}_1}(\boldsymbol{\theta}) \\ b_{\tilde{\boldsymbol{\omega}}_1}(\boldsymbol{\theta}) \\ \vdots \\ a_{\tilde{\boldsymbol{\omega}}_D}(\boldsymbol{\theta}) \\ b_{\tilde{\boldsymbol{\omega}}_D}(\boldsymbol{\theta}) \end{pmatrix}^{\intercal} \tag{47}$$

where D is the dimension of the random Fourier feature map $\boldsymbol{\phi}_{\text{RFF}}$ and $\tilde{\boldsymbol{\omega}}_i \in \Omega$ are the sampled frequencies from the original Fourier spectrum Ω. Following general algorithm-independent results in statistical learning theory on RFFs [34, 35], we assume that the value $|a_{\tilde{\boldsymbol{\omega}}_i}(\boldsymbol{\theta})|$ and $|b_{\tilde{\boldsymbol{\omega}}_i}(\boldsymbol{\theta})|$ are bounded by some constant K. Note that $\|\boldsymbol{w}\|_2 \leq KD \in \mathcal{O}(D)$.

Combining Theorem 1 with the results from the RFF approximation yield Corollary 3.

Corollary 3. *Consider the hypothesis class $\mathcal{H}_{\text{RFF}}$ as defined in Equation (45), a target function $f(\boldsymbol{x}) \in \mathcal{F}_{U,|\mathbf{0}\rangle\langle\mathbf{0}|}$, and variables as defined in Theorem 1. Let $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$ be the training dataset with $\bar{y}_i$ estimated with N_s measurement shots. Running Algorithm 1 with $\mathcal{S}$ will yield $h \in \mathcal{H}_{\text{RFF}}$ such that*

$$R_{\text{expl}}(h) \leq \mathcal{O}\left(\sqrt{\epsilon_1} + M\epsilon_2 + D\left[\epsilon_3 + \epsilon_4\right] + \epsilon_5\right), \tag{48}$$

where $\epsilon_2 = \sqrt[4]{\frac{\log\left(\frac{1}{\delta}\right)}{N_1}}$, $\epsilon_3 = \sqrt{\frac{1}{N_1}}$, $\epsilon_4 = \sqrt{\frac{\bar{\sigma}\log\left(\frac{1}{\delta}\right)}{N_1 N_s}}$, $\epsilon_5 = \sqrt{\frac{\log\left(\frac{1}{\delta}\right)}{N_1}}$, *and* $\bar{\sigma} = \mathbb{E}_{\boldsymbol{x}}[\sigma^2_{\lambda|\boldsymbol{x}}]$.

Here, we exploited the information about the co-domain of the target p-concepts to design an appropriate link function u that restricts the size of the hypothesis class. To illustrate the impact of limiting the hypothesis class size, we relax the co-domains matching constraint, i.e., set u to be the identity map, hence the hypothesis class considered becomes

$$\mathcal{G}_{\text{RFF}} = \left\{g(\boldsymbol{x}) = \langle \boldsymbol{w}, \boldsymbol{\phi}_{\text{RFF}}(\boldsymbol{x})\rangle, \|\boldsymbol{w}\|_2 \leq B\right\}. \tag{49}$$

The most straightforward method to learn $f_{\boldsymbol{\theta}}(\boldsymbol{x})$ under this relaxed formulation is to directly minimize the empirical risk $\widehat{R}(h)$ given a sample $\mathcal{S}$ sampled from the distribution $\mathcal{D}$, which we call empirical risk minimization (ERM).

We can formulate the above as a quadratically constrained quadratic program as follows:

$$\boldsymbol{w}^* = \underset{\boldsymbol{w}, \|\boldsymbol{w}\|_2 \leq B}{\arg\min} \frac{1}{|\mathcal{S}|} \sum_{(\boldsymbol{x}, \bar{y}) \in \mathcal{S}} |\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle - \bar{y}|^2, \tag{50}$$

which can be efficiently solved by convex optimization methods such as interior point methods [36] or projected gradient descent. Alternatively, by including the constraint in the loss with Lagrangian multipliers, the problem can be formulated as a ridge regression task. Various prior work use this formulation to tackle learning problems involving PQCs [8, 25, 26].

Lemma 1. *Consider the hypothesis class $\mathcal{G}_{\text{RFF}}$ as defined in Equation (49), a target function $f(\boldsymbol{x}) \in \mathcal{F}_{U,|\mathbf{0}\rangle\langle\mathbf{0}|}$, and variables as defined in Theorem 1. Let $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$ be the training dataset with $\bar{y}_i$ estimated with N_s measurement shots. Optimizing Equation (50) with $\mathcal{S}$ will yield $g_{\mathcal{S}}^{\text{ERM}} \in \mathcal{G}_{\text{RFF}}$ such that*

$$R_{\text{expl}}(g_{\mathcal{S}}^{\text{ERM}}) \leq \mathcal{O}\left(\epsilon_1 + D^2\sqrt{\frac{\log\frac{1}{\delta}}{N_1}}\right). \tag{51}$$

The proof of this lemma can be found in Appendix E. Similar to Equation (48), one could understand Equation (51) from the bias and variance perspective, i.e., the first term informs the bias of the model while the second term tells us about the model's variance. Firstly, the inclusion of the link function u in the hypothesis class $\mathcal{H}$ results in a class of model that has higher bias as compared to hypothesis class $\mathcal{G}$ hence leads to a quadratic increase in error ϵ_1. Consequently, $\mathcal{H}$ that is higher in bias will have a lower variance, and we can observe the separate and asymmetrical effects of the data sampling and shot noises on the explicit risk. Removing the link function leads to higher variance in $\mathcal{G}$, and the sensitivity to shot and data sampling noises becomes indistinguishable. The relationship between errors in these two generalization bounds essentially manifests the bias-variance trade-off. Further, such results showcase the fact the ERM-based hypothesis selection can still generalize with a constant number of measurements provided that we have abundant data points.

We note that without the application of the link function u in our modelling, classical models are much more susceptible to shot noise. Our theoretical results of Corollary 2 and Lemma 1 imply that in order to learn labels obtained from constant number measurements, without the link function u, classical algorithms may require up to data points N_1 that are square of what is needed for models with the link function u. In the following section, we numerically showcase this property.

V. NUMERICAL VALIDATION ON THE ROLE OF SHOT NOISE

In this section, we will provide numerical verifications of our theoretical results, validating the operational roles of shot noise in learning quantum models.

A. Numerical settings

We consider the data re-uploading model [37] for one-dimensional data points x in our numerical demonstra-

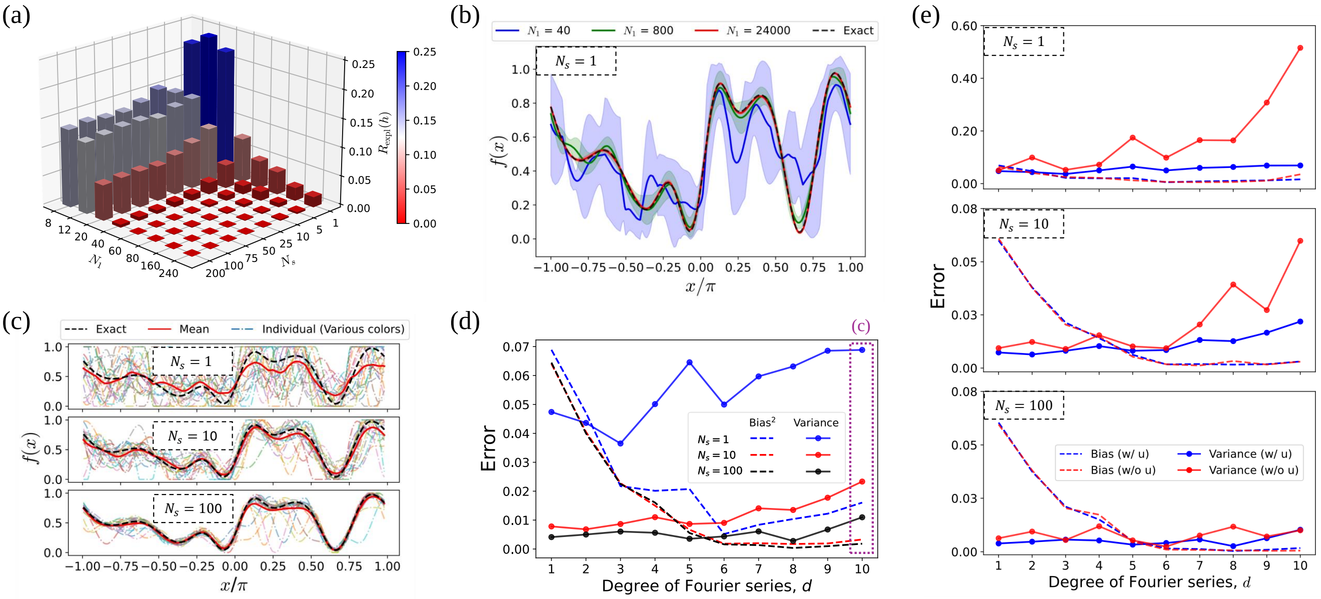


FIG. 4. (a) The averaged explicit risk for different numbers of training data points N_1 and number of measurement shots N_s. The overall trends agreed with the theoretical prediction in Figure 3: for a fixed N_1, the explicit risk saturated after some threshold value of N_s, but the explicit risk can be reduced by increasing N_1 regardless of the value of N_s. (b) When the model in $\mathcal{H}_{10}$ are presented with a sufficiently large dataset, i.e., $N_1 = 24000$, the exact function (black dashed line) can be learned even if the labels are estimated with one measurement shot. (c) Twenty different trained models (dotted dashed line of various colours) from $\mathcal{H}_{10}$ and their mean predictors (solid red line) for $N_1 = 1, 10, 100$. Increasing N_s reduces the shot noise, hence reducing the spread of the trained models. (d) The bias-variance trade-off curve. The bias and variance of the trained models in (c) are calculated and plotted in the purple dotted box. The rest of the values are computed using similar procedures as per (c) for $\mathcal{H}_d$ with $d = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Both the bias and variance decrease when N_s increases, illustrating the shot-noise dependent bias-variance trade-off. (e) Bias and variance for models with and without the link function u. The models without the link function are more expressive, hence they are more susceptible to the shot noise, i.e., they have a higher tendency to overfit the shot noise. Increasing N_s will reduce the shot noise, hence suppressing the shot-noise-induced variance. Note that the same target function is considered in all these numerical experiments.

tion

$$f_{\boldsymbol{\theta}}(x) = \left|\langle 0|\,\mathrm{Rot}\left(\boldsymbol{\theta}^{L_r+1}\right)\,\Pi_{l=1}^{L_r}\left[R_X(x)\mathrm{Rot}\left(\boldsymbol{\theta}^{l}\right)\right]|0\rangle\right|^2, \tag{52}$$

where $\boldsymbol{\theta} = (\boldsymbol{\theta}^1, \ldots, \boldsymbol{\theta}^{L_r+1})$ is the set of rotational angles, $\mathrm{Rot}(\boldsymbol{\theta}^l) = R_Z(\theta_3^l)R_Y(\theta_2^l)R_Z(\theta_1^l)$ is the universal single qubit unitary gate, L_r is the number of layer repetitions, and $R_P(\cdot)$ are the Pauli rotation unitary gates with $P \in \{X, Y, Z\}$. While we considered only the single qubit data re-uploading model with one-dimensional data points, it is straightforward to generalize our results to the multi-qubit model or with multi-dimensional data points. As described, the data re-uploading model can be expressed as a truncated Fourier series

$$f_{\boldsymbol{\theta}}(x) = c_0(\boldsymbol{\theta}) + \sum_{\omega=1}^{L_r} a_\omega(\boldsymbol{\theta})\cos(\omega x) + b_\omega(\boldsymbol{\theta})\sin(\omega x), \tag{53}$$

with Fourier spectrum $\Omega_{L_r}^+ = \{1, \ldots, L_r\}$ while the Fourier coefficients are dependent solely on $\boldsymbol{\theta}$ and their associated unitaries.

Now, we will describe our numerical setting. Firstly, we considered fixed randomly generated angles $\boldsymbol{\theta}$ in our numerical demonstrations, and this set of angles is used for all numerical experiments. Therefore, we will drop the dependency on $\boldsymbol{\theta}$ from now on. In addition, we set $L_r = 10$ for the data re-uploading model to generate a degree 10 Fourier series. Such a target function is sufficiently complex for us to observe various impacts of shot noise in learning $f(x)$. Finally, this numerical example does not require the utilization of random Fourier features, as the model under consideration is rather straightforward; therefore, the truncation method suffices. Specifically, we consider the following truncated Fourier series as our hypothesis class

$$\mathcal{H}_d = \left\{ h_d(x) = u\left(\nu_0 + \sum_{\omega=1}^{d} \alpha_\omega \cos(\omega x) + \beta_\omega \sin(\omega x)\right)\right\} \tag{54}$$

where $\nu_0, \alpha_\omega, \beta_\omega \in \mathbb{R}$, $u(\cdot)$ is the clipping function as defined in Equation (46) and $d \in \mathbb{N}$ controls the degree of the truncated Fourier series, hence the complexity of $\mathcal{H}_d$. For all numerical experiments, the number of training steps T is fixed as 50, and 500 testing data points are used to evaluate the performance of trained models. To distinguish the hypothesis class with and without the link function, we denote $\mathcal{H}_d$ with the identity link function as $\mathcal{G}_d$. Note that all datasets are extracted using the procedures described in Section II B 2.

B. Asymmetrical effects of N_1 and N_s

To begin with, we investigate the asymmetry dependent of the explicit risk on the number of training data points N_1 and the number of measurement shots N_s. In particular, we set $d = 10$ such that the approximation error $\epsilon_1 = 0$, i.e., when $\nu_0 = c_0$, $\alpha_\omega = a_\omega$, and $\beta_\omega = b_\omega$ for all $\omega \in \Omega_{10}^{+}$, enabling us to isolate the impact of these two attributes. In this example, the ratio of the number of training data points N_1 to the number of validation data points N_2 is N_1:N_2 = 8:2 with total data points $N = \{10, 15, 25, 50, 75, 100, 200, 300\}$. That is, we trained the model in $\mathcal{H}_{10}$ with different pairwise combinations of $N_1 = \{8, 12, 20, 40, 60, 80, 160, 240\}$ training data points and $N_s = \{1, 5, 10, 25, 50, 75, 100, 200\}$ measurement shots using Algorithm 1 under $T = 50$ training iterations, and the optimal model is chosen using $N_2 = \{2, 3, 5, 10, 15, 20, 40, 60\}$ validation data points for the respective value of N_1. Finally, the explicit risk is estimated with 500 testing data points and we averaged the explicit risk over 5 random instances of training and validation datasets.

The results shown in Figure 4 (a) agreed with our theoretical prediction in Figure 3, validating the asymmetrical effects of N_1 and N_s as described in Corollary 1. In particular, it shows the decreasing trend of explicit risk with the increase of N_1 while keeping $N_s = 1$. This observation is further validated by Figure 4 (b), where the exact function can be learned when the model is presented with sufficiently large training data points with labels estimated using one measurement repetition, i.e., $N_1 = 2.4 \times 10^4$ and $N_s = 1$. The three solid curves in Figure 4 (b) are the mean predictors obtained using training datasets of size $N_1 = \{40, 800, 24000\}$ and validation datasets of size $N_2 = \{10, 200, 600\}$ respectively. Each of these mean predictors is averaged over 5 different training instances and the shaded regions are the standard deviations of the predictions. As expected, increasing N_1 reduces the standard deviations of the predictors and improves the mean predictions.

C. Shot-noise dependent bias-variance trade-off

As discussed in Section III D, training models with different finite-size training datasets will yield different trained models. This phenomenon is observed in Figure 4 (c) where 20 distinct trained models from $\mathcal{H}_{10}$, i.e., dashed-dotted lines of different colours, each trained with different training datasets of size 40 are different across $N_s = 1, 10, 100$. In addition, the reducing fluctuations of the trained models with increasing N_s demonstrated the N_s-dependent relationship between these trained models. As N_1 is sufficiently large, the prediction accuracy can be improved by increasing N_s and this is reflected in Figure 4 (c) where the mean predictor is approaching the exact function as N_s increases. These two observations can otherwise be captured by computing two statistical quantities, the squared bias

$$\mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Bias}_{\mathcal{S}}^2\right] := \mathbb{E}_{\boldsymbol{x}}\left[\left(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - f(\boldsymbol{x})\right)^2\right] \tag{55}$$

and the variance

$$\mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Var}_{\mathcal{S}}\right] := \mathbb{E}_{\boldsymbol{x},\mathcal{S}}\left[\left(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - h_{\mathcal{S}}(\boldsymbol{x})\right)^2\right]. \tag{56}$$

In particular, we compute their empirical versions using the trained models as per Figure 4 (c) using 500 testing data points. The computed values are plotted in Figure 4 (d) at $d = 10$, i.e., the points in the purple dotted box. As expected the bias and variance reduce when N_s increases.

These exact settings and procedures as per Figure 4 (c) are repeated to obtain trained models from $\mathcal{H}_d$ for $d = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and these models are then used to compute their respective bias and variance. Plotting their bias and variance yields the bias-variance trade-off curve, as shown in Figure 4 (d). Across $N_s = 1, 10, 100$, the bias (variance) consistently decreases (increases) with increasing d. This observation is consistent with the bias-variance trade-off concept, where less complex models (in our case, $\mathcal{H}_d$ with lower d) will have higher bias but with lower variance. In contrast, the highly complicated models will have lower bias but with higher variance. The former type of model tends to underfit the training data while the latter is more likely to overfit the training data. In addition, Figure 4 (d) illustrates the shot-noise dependent bias-variance trade-off as described in Section III D: Increase N_s will reduce the bias and variance of the models.

Using the same settings as per Figure 4 (d) but a different training procedure, we extract the bias and variance of the hypothesis without the link function u, i.e., $\mathcal{G}_d$. Specifically, there is an exact analytical solution if we solve Equation (50) using kernel ridge regression and we use the validation dataset to choose the optimal regularization strength out of $C = \{0.006, 0.015, 0.03, 0.0625, 0.125, 0.25, 0.5, 1.0, 2.0, 5.0, 8.0, 16.0, 32.0, 64.0, 128.0, 256, 512, 1024\}$. Then, their bias and variance are compared against the hypothesis equipped with the link function in Figure 4 (e) and these numerical results are in agreement with the theoretical analysis in Section IV B. That is, the variance of $\mathcal{G}_d$ is significantly higher than their counterpart when N_s is low. High shot noise implies that the estimated labels would be very different from their exact values and a more expressive model class like $\mathcal{G}_d$ will have a higher tendency to overfit the shot noise, lending to a higher

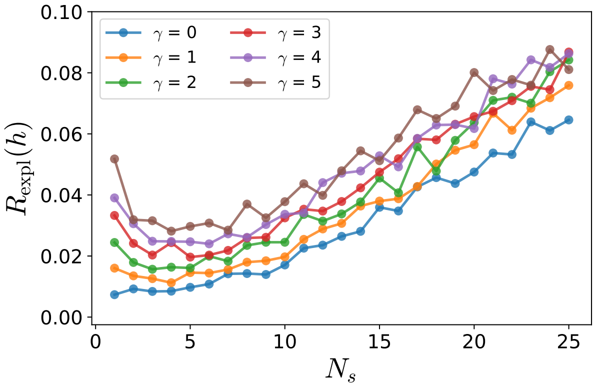


FIG. 5. The trade-off between N_1 and N_s is considered under a fixed total measurement budget of $N_{\mathrm{tot}} = 600$ for $\gamma = \{0, 1, 2, 3, 4, 5\}$ and $N_s = \{1, 2, 3, \ldots, 24, 25\}$. When N_1 and N_s are treated equally, i.e., $\gamma = 0$, the optimal pair of N_1 and N_s is given by $(N_1^*, N_s^*) = (600, 1)$. As γ increases, more measurement shots are required, hence smaller N_1, to achieve better model performance. However, there will be a threshold beyond which the performance of models worsens.

variance. Increasing N_s reduces the shot noise but the finite data sampling noise remains. This explains the reducing but non-vanishing variance for both $\mathcal{H}_d$ and $\mathcal{G}_d$ when N_s increases as well as the success of current learning protocol using $\mathcal{G}_d$ [8, 10, 11]. Interestingly, the model's bias with the link function matches well with the one without. In summary, the link function helps suppress the shot noise-induced variance by restricting the expressivity of the hypothesis class.

D. Trade-off between N_1 and N_s

Finally, we numerically investigate the trade-off between N_1 and N_s under a fixed total measurement budget of N_{tot}. Recall that the relationship between N_{tot}, N_1, and N_s is given by $N_{\mathrm{tot}} = (N_1 + N_2)(N_s + \gamma)$, where γ is the penalty cost and N_2 is the size of validation dataset. The inclusion of N_2 captures the resource constraint for choosing the optimal time step T^*. Here, we let $N_{\mathrm{tot}} = 600$, $\gamma = \{0, 1, 2, 3, 4, 5\}$, and the ratio of N_1 to N_2 be 8:2. Furthermore, we set $N_s = \{1, 2, 3, \ldots, 24, 25\}$ giving different combinations of N_1 and N_2. Repeating the similar procedures as per Figure 4 (a) over 60 random instances of training and validation datasets for the above-mentioned settings yields Figure 5. As predicted by Corollary 2, for a fixed N_{tot} and when $\gamma = 0$, the performance of classical machines can be enhanced by reducing N_s, and the optimality is achieved when $N_s = 1$. On the other hand, the optimal pair of N_1 and N_s depends on the penalty cost when $\gamma > 0$; the larger the γ, the higher the N_s required to achieve optimal model performance.

VI. DISCUSSION

Finite measurement or shot noise is an intrinsic quantum phenomenon. Such noise is always present in the estimation of quantum models; hence, classical machines will unavoidably encounter shot noise when learning quantum models. Therefore, it is crucial to understand whether shot noise could increase the difficulty for classical machines to learn quantum models, or if it is just a statistical feature that can be well-handled by classical models.

By formulating parameterized quantum models as probabilistic concepts, we show that classical machines can learn quantum models with efficient classical representation in the presence of shot noise. Said otherwise, the fundamental hardness of learning quantum models depends on the existence of efficient classical representation, while the impact of shot noise is only prominent when there is an insufficient number of training data points. When sufficient training data points are provided, classical learning of quantum models is possible even when the labels are estimated with limited measurement shots. This asymmetrical effect of the number of training data and measurement repetitions arises from the differences in information gained when sampling each component. That is, one effectively samples across various labels when sampling across the training points but increasing the resolution of the labels does not provide extra information on other data points.

Each quantum measurement, be it on a fixed or different parameter setting, counts as a query to quantum models. While unlimited queries to quantum models are desired, our limited time and monetary resources force us to wisely distribute our budget to maximize the information extracted from quantum models. That is, one has to choose to train the classical machines with datasets consisting of either more inputs with noisier labels or fewer inputs with cleaner labels. If sampling across parameter settings does not incur extra cost compared to sampling quantum models with the same parameter setting, then the classical machine would learn better with datasets consisting of more inputs but with the noisiest labels. Otherwise, the optimal budget partition would depend on the cost differences between measurements with fixed and different parameter settings.

While the hardness of learning quantum models classically is not dictated by the shot noise, it has an impact on the actual training of classical machines. For a given set of training data points $\{\boldsymbol{x}_i\}_{i=1}^{N_1}$, different label sampling instances will yield different training datasets, i.e., $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$ or $\mathcal{S}' = (\boldsymbol{x}_i, \bar{y}'_i)_{i=1}^{N_1}$. Each dataset will produce an associated trained model. We capture this model's sensitivity to variation of labels through the bias-variance-noise decomposition and show that the link function can suppress this undesired sensitivity by restricting the size of the hypothesis class. Finally, we use our framework for the classical surrogation of parameterized quantum circuit models, and our theoretical analysis correctly predicts the behaviours of classical surrogates in the presence of shot noise.

Viewed from other angles, our work provides a framework to study the impact of classical approximation and shot noise on learning quantum models classically. Future works could focus on searching for good classical approximations, and our framework could be directly adapted to handle shot noise. An interesting direction is to combine our framework with the analysis in Ref. [38] to investigate the classical learnability of the parameterized quantum circuit models that are free of barren plateaus. This will provide an alternative perspective on the relationship between classical simulability and learnability of parameterized quantum models [39]. Shallow parameterized quantum circuits usually admit efficient classical representation, yet they might experience exponential concentration if observables are not chosen carefully [40]. This setting is suitable to push the limits of our framework to check if classical machines can still learn such models under the influence of exponential concentration.

Finally, the core of our framework is the assumption that the parameterized quantum models represent the conditional unbiased expectation of their unbiased estimators. However, estimators might not be unbiased after some post-processing operations. An example of such post-processing operations is quantum error mitigation. It will be interesting to investigate the role of shot noise in the biased regime.

ACKNOWLEDGMENTS

The authors thank Yuxuan Du, Naixu Guo, Hela Mhiri, and Manuel Rudolph for discussions. This work is supported by the National Research Foundation, Singapore, and A*STAR under its CQT Bridging Grant and its Quantum Engineering Programme under grant NRF2021-QEP2-02-P05. EGF is supported by a Google PhD Fellowship, the Einstein Foundation (Einstein Research Unit on Quantum Devices), BMBF (Hybrid), and BMWK (EniQmA).

[1] R. P. Feynman, Simulating physics with computers, Int. J. Theor. Phys. **21**, 467 (1982).

[2] S. Lloyd, Universal quantum simulators, Science **273**, 1073–1078 (1996).

[3] H.-Y. Huang, M. Broughton, M. Mohseni, R. Babbush, S. Boixo, H. Neven, and J. R. McClean, Power of data in quantum machine learning, Nat. Commun. **12**, 2631 (2021).

[4] H.-Y. Huang, S. Chen, and J. Preskill, Learning to predict arbitrary quantum processes, PRX Quantum **4**, 040337 (2023).

[5] H. Zhao, L. Lewis, I. Kannan, Y. Quek, H.-Y. Huang, and M. C. Caro, Learning quantum states and unitaries of bounded gate complexity (2023), arXiv:2310.19882 [quant-ph].

[6] L. Zhao, N. Guo, M.-X. Luo, and P. Rebentrost, Provable learning of quantum states with graphical models (2023), arXiv:2309.09235 [quant-ph].

[7] A. Anshu and S. Arunachalam, A survey on the complexity of learning quantum states, Nat. Rev. Phys. **6**, 59–69 (2023).

[8] F. J. Schreiber, J. Eisert, and J. J. Meyer, Classical surrogates for quantum learning models, Phys. Rev. Lett. **131**, 100803 (2023).

[9] H.-Y. Huang, R. Kueng, G. Torlai, V. V. Albert, and J. Preskill, Provably efficient machine learning for quantum many-body problems, Science **377**, eabk3333 (2022).

[10] L. Lewis, H.-Y. Huang, V. T. Tran, S. Lehner, R. Kueng, and J. Preskill, Improved machine learning algorithm for predicting ground state properties, Nat. Commun. **15**, 895 (2024).

[11] Y. Che, C. Gneiting, and F. Nori, Exponentially improved efficient machine learning for quantum many-body states with provable guarantees (2023), arXiv:2304.04353 [quant-ph].

[12] S. Aaronson, Shadow tomography of quantum states, SIAM J. Comput. **49**, STOC18 (2020).

[13] C. Huang, F. Zhang, M. Newman, J. Cai, X. Gao, Z. Tian, J. Wu, H. Xu, H. Yu, B. Yuan, M. Szegedy, Y. Shi, and J. Chen, Classical simulation of quantum supremacy circuits (2020), arXiv:2005.06787 [quant-ph].

[14] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles, Variational quantum algorithms, Nature Reviews Physics **3**, 625–644 (2021).

[15] E. Recio-Armengol, J. Eisert, and J. J. Meyer, Single-shot quantum machine learning (2024), arXiv:2406.13812 [quant-ph].

[16] M. J. Kearns and R. E. Schapire, Efficient distribution-free learning of probabilistic concepts, J. Comput. Syst. Sci. **48**, 464–497 (1994).

[17] L. G. Valiant, A theory of the learnable, Commun. ACM **27**, 1134–1142 (1984).

[18] S. Aaronson, The learnability of quantum states, Proc. R. Soc. A: Math. Phys. Eng. Sci. **463**, 3089 (2007).

[19] A. Rocchetto, Stabiliser states are efficiently PAC-learnable, Quantum Inf. Comput. **18**, 541 (2018).

[20] A. Rocchetto, S. Aaronson, S. Severini, G. Carvacho, D. Poderini, I. Agresti, M. Bentivegna, and F. Sciarrino, Experimental learning of quantum states, Sci. Adv. **5**, eaau1946 (2019).

[21] H.-C. Cheng, M.-H. Hsieh, and P.-C. Yeh, The learnability of unknown quantum measurements, Quantum Inf. Comput. **16**, 615–656 (2016).

[22] M. C. Caro and I. Datta, Pseudo-dimension of quantum circuits, Quantum Mach. Intell. **2**, 14 (2020).

[23] B. Neal, S. Mittal, A. Baratin, V. Tantia, M. Scicluna, S. Lacoste-Julien, and I. Mitliagkas, A modern take on the bias-variance tradeoff in neural networks (2019), arXiv:1810.08591 [cs.LG].

[24] Z. Yang, Y. Yu, C. You, J. Steinhardt, and Y. Ma, Rethinking bias-variance trade-off for generalization of neural networks, in *Proceedings of the 37th International Conference on Machine Learning*, Proceedings of Ma-

chine Learning Research, Vol. 119, edited by H. D. III and A. Singh (PMLR, 2020) pp. 10767–10777.

[25] J. Landman, S. Thabet, C. Dalyac, H. Mhiri, and E. Kashefi, Classically approximating variational quantum machine learning with random Fourier features (2022), arXiv:2210.13200 [quant-ph].

[26] R. Sweke, E. Recio, S. Jerbi, E. Gil-Fuster, B. Fuller, J. Eisert, and J. J. Meyer, Potential and limitations of random Fourier features for dequantizing quantum machine learning (2023), arXiv:2309.11647 [quant-ph].

[27] E. Fontana, M. S. Rudolph, R. Duncan, I. Rungger, and C. Cîrstoiu, Classical simulations of noisy variational quantum circuits (2023), arXiv:2306.05400 [quant-ph].

[28] N. A. Nemkov, E. O. Kiktenko, and A. K. Fedorov, Fourier expansion in variational quantum algorithms, Phys. Rev. A **108**, 032406 (2023).

[29] F. J. Gil Vidal and D. O. Theis, Input redundancy for parameterized quantum circuits, Front. Phys. **8**, 297 (2020).

[30] M. Schuld, R. Sweke, and J. J. Meyer, Effect of data encoding on the expressive power of variational quantum-machine-learning models, Phys. Rev. A **103**, 032430 (2021).

[31] S. Goel and A. R. Klivans, Learning neural networks with two nonlinear layers in polynomial time, in *Proceedings of the Thirty-Second Conference on Learning Theory*, Proceedings of Machine Learning Research, Vol. 99, edited by A. Beygelzimer and D. Hsu (PMLR, 2019) pp. 1470–1499.

[32] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, Experimental comparison of two quantum computing architectures, Proc. Natl. Acad. Sci. **114**, 3305 (2017).

[33] A. Rahimi and B. Recht, Random features for large-scale kernel machines, in *Advances in Neural Information Processing Systems*, Vol. 20, edited by J. Platt, D. Koller, Y. Singer, and S. Roweis (Curran Associates, Inc., 2007).

[34] A. Rahimi and B. Recht, Weighted sums of random kitchen sinks: Replacing minimization with randomization in learning, in *Advances in Neural Information Processing Systems*, Vol. 21, edited by D. Koller, D. Schuurmans, Y. Bengio, and L. Bottou (Curran Associates, Inc., 2008).

[35] A. Rahimi and B. Recht, Uniform approximation of functions with random bases, in *2008 46th Annual Allerton Conference on Communication, Control, and Computing* (2008) pp. 555–561.

[36] S. Boyd and L. Vandenberghe, Interior-point methods, in *Convex Optimization* (Cambridge University Press, 2004) p. 561–630.

[37] A. Pérez-Salinas, A. Cervera-Lierta, E. Gil-Fuster, and J. I. Latorre, Data re-uploading for a universal quantum classifier, Quantum **4**, 226 (2020).

[38] M. Cerezo, M. Larocca, D. García-Martín, N. Diaz, P. Braccia, E. Fontana, M. S. Rudolph, P. Bermejo, A. Ijaz, S. Thanasilp, E. R. Anschuetz, and Z. Holmes, Does provable absence of barren plateaus imply classical simulability? Or, why we need to rethink variational quantum computing (2023), arXiv:2312.09121 [quant-ph].

[39] M. Hinsche, M. Ioannou, A. Nietner, J. Haferkamp, Y. Quek, D. Hangleiter, J.-P. Seifert, J. Eisert, and R. Sweke, One T gate makes distribution learning hard, Phys. Rev. Lett. **130**, 240602 (2023).

[40] M. Cerezo, A. Sone, T. Volkoff, L. Cincio, and P. J. Coles, Cost function dependent barren plateaus in shallow parametrized quantum circuits, Nat. Commun. **12** (2021).

[41] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, Nat. Phys. **16**, 1050 (2020).

[42] N. Guo, F. Pan, and P. Rebentrost, Estimating properties of a quantum state by importance-sampled operator shadows (2023), arXiv:2305.09374 [quant-ph].

[43] J. M. Kohler and A. Lucchi, Sub-sampled cubic regularization for non-convex optimization, in *Proceedings of the 34th International Conference on Machine Learning*, Proceedings of Machine Learning Research, Vol. 70, edited by D. Precup and Y. W. Teh (PMLR, 2017) pp. 1895–1904.

[44] P. L. Bartlett and S. Mendelson, Rademacher and Gaussian complexities: risk bounds and structural results, J. Mach. Learn. Res. **3**, 463–482 (2002).

[45] S. M. Kakade, K. Sridharan, and A. Tewari, On the complexity of linear prediction: Risk bounds, margin bounds, and regularization, in *Advances in Neural Information Processing Systems*, Vol. 21, edited by D. Koller, D. Schuurmans, Y. Bengio, and L. Bottou (Curran Associates, Inc., 2008).

[46] M. Ledoux and M. Talagrand, *Probability in Banach Spaces* (Springer Berlin Heidelberg, 1991).

[47] M. Mohri, A. Rostamizadeh, and A. Talwalkar, *Foundations of Machine Learning*, 2nd ed. (The MIT Press, 2018).

[48] A. M. Childs and N. Wiebe, Hamiltonian simulation using linear combinations of unitary operations, Quantum Inf. Comput. **12** (2012).

[49] E. Gil-Fuster, J. Eisert, and V. Dunjko, On the expressivity of embedding quantum kernels, Mach. Learn. Sci. Technol. **5**, 025003 (2024).

[50] E. Gil-Fuster, J. Eisert, and C. Bravo-Prieto, Understanding quantum machine learning also requires rethinking generalization, Nat. Commun. **15** (2024).

[51] M. C. Caro, E. Gil-Fuster, J. J. Meyer, J. Eisert, and R. Sweke, Encoding-dependent generalization bounds for parametrized quantum circuits, Quantum **5**, 582 (2021).

[52] S. Jerbi, L. J. Fiderer, H. Poulsen Nautrup, J. M. Kübler, H. J. Briegel, and V. Dunjko, Quantum machine learning beyond kernel methods, Nat. Commun. **14**, 517 (2023).

Appendix A: Sampling and estimation methods on PQMs

1. Direct sampling-based estimation

The most straightforward method is to generate estimations by directly conducting measurements on the target observable. Plugging in the eigendecomposition of the observable O, i.e., $O = \sum_{k=1}^{K} \lambda^{(k)} \left|\lambda^{(k)}\right\rangle \left\langle\lambda^{(k)}\right|$ in $f(\boldsymbol{x}) =$

$\mathrm{tr}(\rho(\boldsymbol{x})O)$ yields

$$f(\boldsymbol{x}) = \sum_{k=1}^{K} \lambda^{(k)} \left\langle \lambda^{(k)} \right| \rho(\boldsymbol{x}) \left| \lambda^{(k)} \right\rangle , \tag{A1}$$

where $0 \leq \left\langle \lambda^{(k)} \right| \rho(\boldsymbol{x}) \left| \lambda^{(k)} \right\rangle \leq 1 \ \forall k$, $\lambda^{(k)} \in \mathbb{R}$, and $\sum_{k=1}^{K} \left\langle \lambda^{(k)} \right| \rho(\boldsymbol{x}) \left| \lambda^{(k)} \right\rangle = 1$. The random measurement processes of $\rho(\boldsymbol{x})$ in the eigenbasis $\left| \lambda^{(k)} \right\rangle$ can be modelled as sampling of eigenvalue $\lambda^{(k)}$ from the associated probability distribution, i.e., $\lambda \sim p_{\boldsymbol{x}}(\lambda)$ with $\lambda \in \Lambda = \{\lambda^{(k)}\}_{k=1}^{K}$ and $p_{\boldsymbol{x}}(\lambda) = \langle \lambda | \rho(\boldsymbol{x}) | \lambda \rangle$.

Given N_s i.i.d. measurement outcomes $\{\lambda_i\}_{i=1}^{N_s}$, one could estimate $f(\boldsymbol{x})$ by the empirical mean

$$\bar{y}_D = \frac{1}{N_s} \sum_{i=1}^{N_s} \lambda_i . \tag{A2}$$

where we have implictly assumed the dependence of $\bar{y}_D$ on $\boldsymbol{x}$, i.e., $\bar{y}_D \equiv \bar{y}_D(\boldsymbol{x})$. The finite-measurement-outcome mean $\bar{y}_D$ is an unbiased estimator of $f(\boldsymbol{x})$

$$f(\boldsymbol{x}) = \mathbb{E}_{\bar{y}_D} \left[\bar{y}_D | \boldsymbol{x} \right] \tag{A3}$$

with variance $\sigma^2_{\bar{y}_D|\boldsymbol{x}} = \sigma^2_{\lambda|\boldsymbol{x}} / N_s$.

It is however generally hard to measure $\rho(\boldsymbol{x})$ in the eigenbasis of the observable. In typical scenarios, one would normally consider a linear combination of M Pauli observables P_i, i.e., $O = \sum_{i=1}^{M} a_i P_i$ with $a_i \in \mathbb{R}$, and the eigenbasis of such an observable is non-trivial to find. To estimate the original observable expectation value, one will typically measure the expectation value of $\rho(\boldsymbol{x})$ against each Pauli observable and then linearly combine them with the associated weights a_i

$$\mathrm{tr}(\rho(\boldsymbol{x})O) = \sum_{i=1}^{M} a_i \, \mathrm{tr}(\rho(\boldsymbol{x}) P_i). \tag{A4}$$

While each Pauli estimator is unbiased for the associated Pauli observable, the joint estimators of $\mathrm{tr}(\rho(\boldsymbol{x})O)$ constructed by summing these Pauli estimators need not be unbiased.

2. Shadow-based estimation

Alternatively, estimating measurement results using classical shadows [41] also introduces structural noise to our framework, allowing training based on random measurements as opposed to direct measurements, which may be much more costly in practice.

Recall that in the classical shadows protocol, to estimate properties of a quantum state ρ, one first evolves the quantum state using a unitary U sampled from a tomographically complete unitary ensemble $\mathcal{U}$ and performs measurements on the computational basis $|\hat{b}\rangle \in \{0,1\}^n$ and the bit-string b is observed with probability $\Pr\left[\hat{b} = b\right] = \langle b | U \rho U^\dagger | b \rangle$. From the measurement outcome, one can construct a classical snapshot $\hat{\rho} = \mathcal{M}_{\mathcal{U}}^{-1}(U^\dagger |\hat{b}\rangle\langle\hat{b}| U)$ where we apply an inverted quantum channel $\mathcal{M}_{\mathcal{U}}^{-1}$ determined by the unitary ensemble $\mathcal{U}$. This classical snapshot is an unbiased estimator for the density matrix, i.e., $\rho = \mathbb{E}_{U,|\hat{b}\rangle}[\hat{\rho}]$.

The classical snapshot serves as a good estimator for the parameterized quantum state when applied to a suitable set of Hermitian observables $\{H_1, H_2, \cdots, H_M\}$. For example, the classical snapshots can be used to estimate the function $f(\boldsymbol{x}) = \mathrm{tr}(\rho(\boldsymbol{x})O)$ with $O = \sum_{i=1}^{M} a_i P_i$, i.e., $\bar{y}_{CS} = \mathrm{tr}(\bar{\rho}(\boldsymbol{x})O)$ where $\bar{\rho} = \frac{1}{N_s} \sum_{i=1}^{N_s} \hat{\rho}_i$ is the averaged sum of N_s classical snapshots. It is straightforward to show that such an estimator is an unbiased estimator of $f(\boldsymbol{x})$

$$f(\boldsymbol{x}) = \mathbb{E}_{\bar{y}_{CS}} \left[\bar{y}_{CS} | \boldsymbol{x} \right] . \tag{A5}$$

Other unbiased shadow estimation techniques based on random sampling such as operator shadows [42] can also be used to produce the unbiased estimators for the quantum models.

Appendix B: Details on the learning algorithm

1. Intuitive understanding on the working principle of Algorithm 1

Algorithm 1 works similarly to gradient descent algorithm. Take the following empirical risk

$$\widehat{R} = \frac{1}{2N_1}\sum_{j=1}^{N_1} |y_j - u\left(\langle w, \boldsymbol{\phi}(\boldsymbol{x_j})\rangle\right)|^2 \tag{B1}$$

We can then upper bound the gradient as follows:

$$\frac{\partial \widehat{R}}{\partial \boldsymbol{w}} \leq \frac{L}{N_1}\sum_{j=1}^{N_1}(u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x_j})\rangle) - y_j)\boldsymbol{\phi}(\boldsymbol{x_j}) \tag{B2}$$

By introducing kernelization to linear models, one can set $\boldsymbol{w} = \sum_{i=1}^{N_1} \alpha_i \boldsymbol{\phi}(\boldsymbol{x_i})$. Setting the upper bound as the gradient step with a learning rate of $\frac{1}{L^2}$, we see that in each step, the value of α_j has an update of

$$\Delta\alpha_j = \frac{u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x_j})\rangle) - y_j}{LN_1} = \frac{u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x_j})\rangle) - y_j}{LN_1} = \frac{u\left(\sum_{i=1}^{N_1} \alpha_i k(\boldsymbol{x_i}, \boldsymbol{x_j})\right) - y_j}{LN_1}, \tag{B3}$$

giving us the update in Algorithm 1.

Due to initialization of parameters to zero, which is akin to interior point methods, the algorithm provides implicit norm regularization of the parameters. This property, in addition to the limitation of gradient steps taken, provides the theoretical guarantees as shown in Theorem 1, which we show in the following section.

2. Proof of Theorem 1

We are given the output range $\mathcal{Y} = [-\Delta, \Delta]$. Let $\bar{\Gamma} := \frac{1}{N_1}\sum_{i=1}^{N_1}(\bar{y}_i - u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x}_i)\rangle + \xi(\boldsymbol{x}_i)))\boldsymbol{\phi}(\boldsymbol{x}_i)$, $\bar{\Gamma}^t := \frac{1}{N_1}\sum_{i=1}^{N_1}(\bar{y}_i - u(\langle \boldsymbol{w}^t, \boldsymbol{\phi}(\boldsymbol{x}_i)\rangle))\boldsymbol{\phi}(\boldsymbol{x}_i)$ and $\chi := \frac{1}{N_1}\sum_{i=1}^{N_1}\xi(\boldsymbol{x}_i)^2$. We apply the Lemma 11 from Ref. [31] to the empirical mean $\bar{y}$.

Lemma B.1. *At iterative t in Algorithm 1, suppose $\|\boldsymbol{w}^t - \boldsymbol{w}\| \leq B$ for $B > 1$, then if $\|\bar{\Gamma}\| \leq \epsilon_4 < 1$, then*

$$\|\boldsymbol{w}^t - \boldsymbol{w}\|^2 - \|\boldsymbol{w}^{t+1} - \boldsymbol{w}\|^2 \geq \lambda\left(\left(\frac{2}{L} - \lambda\right)\hat{R}(h^t) - 2\Delta\sqrt{\chi} - 2B\epsilon_4 - \lambda\epsilon_4^2 - 2\Delta\lambda\epsilon_4\right), \tag{B4}$$

where λ is the regularization parameter.

Using Lemma B.1 with $\lambda = 1/L$, we have

$$\|\boldsymbol{w}^t - \boldsymbol{w}\|^2 - \|\boldsymbol{w}^{t+1} - \boldsymbol{w}\|^2 \geq \frac{1}{L}\left(\frac{\hat{R}(h^t)}{L} - 2\Delta\sqrt{\chi} - 2B\epsilon_4 - \frac{\epsilon_4^2}{L} - \frac{2\Delta\epsilon_4}{L}\right). \tag{B5}$$

For each iteration t of Algorithm 1, one of the following two cases needs to be satisfied

$$\text{Case 1: } \|\boldsymbol{w}^t - \boldsymbol{w}\|^2 - \|\boldsymbol{w}^{t+1} - \boldsymbol{w}\|^2 > \frac{B\epsilon_4}{L} \tag{B6}$$

$$\text{Case 2: } \|\boldsymbol{w}^t - \boldsymbol{w}\|^2 - \|\boldsymbol{w}^{t+1} - \boldsymbol{w}\|^2 \leq \frac{B\epsilon_4}{L}. \tag{B7}$$

Let t^* be the first iteration where Case 2 holds. We show that such an iteration exists. Assume the contradictory, that is, Case 2 fails for each iteration. Since $\|\boldsymbol{w}^0 - \boldsymbol{w}\|_2^2 = \|\boldsymbol{0} - \boldsymbol{w}\|_2^2 \leq B^2$ by assumption, however,

$$B^2 \geq \|\boldsymbol{w}^0 - \boldsymbol{w}\|_2^2 \geq \|\boldsymbol{w}^0 - \boldsymbol{w}\|_2^2 - \|\boldsymbol{w}^k - \boldsymbol{w}\|_2^2 \tag{B8}$$

$$= \sum_{t=0}^{k-1}\left(\|\boldsymbol{w}^t - \boldsymbol{w}\|_2^2 - \|\boldsymbol{w}^{t+1} - \boldsymbol{w}\|_2^2\right) \geq \frac{kB\epsilon_4}{L}, \tag{B9}$$

for k iterations. Hence, in at most $T \geq \frac{BL}{\epsilon_4}$ iterations Case 1 will be violated and Case 2 will have to be true. Combining Equation (B5) and Case 2 yield

$$\hat{R}(h^t) \leq 2L\Delta\sqrt{\chi} + 3BL\epsilon_4 + \epsilon_4^2 + 2\Delta\epsilon_4 \tag{B10}$$

What remains to be done is to bound χ and to obtain N_s in terms of ϵ_4. Similar to Ref. [31], we could bound χ using Hoeffding's inequality

$$\sqrt{\chi} \leq \sqrt{\epsilon_1} + \mathcal{O}\left(M\sqrt[4]{\frac{\log(1/\delta)}{N_1}}\right), \tag{B11}$$

and therefore by observing that $B \propto \Delta$, we have

$$\hat{R}(h^t) \leq \mathcal{O}\left(L\Delta\sqrt{\epsilon_1} + LM\sqrt[4]{\frac{\log(1/\delta)}{N_1}} + BL\epsilon_4\right). \tag{B12}$$

By definition, we have that $(\bar{y}_i - u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x}_i)\rangle + \xi(\boldsymbol{x}_i)))\boldsymbol{\phi}(\boldsymbol{x}_i)$ are zero mean i.i.d. random variables with bounded norm, so we can use the following vector Bernstein inequality to bound the norm of $\bar{\Gamma}$.

Lemma B.2 (Vector Bernstein inequality (Lemma 18 from [43]))**.** *Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$ be independent zero-mean vector-valued random variables with common dimension d and they are uniformly bounded and also the variance is bounded above $\mathbb{E}[\|\boldsymbol{x}_i\|^2] \leq \sigma^2$. Let*

$$\boldsymbol{z} = \frac{1}{N}\left\|\sum_{i=1}^{N}\boldsymbol{x}_i\right\|_2. \tag{B13}$$

Then we have for $0 \leq \epsilon \leq \sigma^2/\mu$

$$P[\|\boldsymbol{z}\| \geq \epsilon] \leq \exp\left(-\frac{N\epsilon^2}{8\sigma^2} + \frac{1}{4}\right). \tag{B14}$$

Before using the vector Bernstein inequality, we need to compute the variance of $\|(\bar{y} - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])\boldsymbol{\phi}(\boldsymbol{x})\|$ where $\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}] = u(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle + \xi(\boldsymbol{x}))$, i.e., $\mathbb{E}_{\bar{\mathcal{D}}}[\|(\bar{y} - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])\boldsymbol{\phi}(\boldsymbol{x})\|^2]$ as $\mathbb{E}_{\bar{\mathcal{D}}}[\|(\bar{y} - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])\boldsymbol{\phi}(\boldsymbol{x})\|] = 0$ by definition. Therefore,

$$\begin{aligned}
\mathbb{E}_{\bar{\mathcal{D}}}\left[\|(\bar{y} - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])\boldsymbol{\phi}(\boldsymbol{x})\|^2\right] &= \mathbb{E}_{\bar{\mathcal{D}}}\left[(\bar{y} - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])^2\|\boldsymbol{\phi}(\boldsymbol{x})\|^2\right] && \text{(B15)}\\
&\leq \mathbb{E}_{\bar{\mathcal{D}}}\left[(\bar{y} - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])^2\right] && \text{(B16)}\\
&= \mathbb{E}_{\bar{\mathcal{D}}}\left[\bar{y}^2 - 2\bar{y}\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}] + \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]^2\right] && \text{(B17)}\\
&= \mathbb{E}_{\boldsymbol{x}}\mathbb{E}_{\bar{y}|\boldsymbol{x}}\left[\bar{y}^2 - 2\bar{y}\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}] + \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]^2\right] && \text{(B18)}\\
&= \mathbb{E}_{\boldsymbol{x}}\left[\mathbb{E}_{\bar{y}}[\bar{y}^2|\boldsymbol{x}] - \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]^2\right] && \text{(B19)}\\
&= \mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{\bar{y}|\boldsymbol{x}}\right] && \text{(B20)}\\
&= \frac{\mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{y|\boldsymbol{x}}\right]}{N_s} && \text{(B21)}
\end{aligned}$$

We can therefore bound $\|\bar{\Gamma}\|$ by letting $\sigma = \frac{\mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{y|\boldsymbol{x}}\right]}{N_s}$

$$P(\|\bar{\Gamma}\| \leq \epsilon_4) \geq 1 - \exp\left(-\frac{N_1 N_s \epsilon_4^2}{8\mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{y|\boldsymbol{x}}\right]} + \frac{1}{4}\right). \tag{B22}$$

For a probability of $1 - \delta$, number of training samples N_1, and number of measurement repetitions N_s, we can achieve $\|\bar{\Gamma}\| \leq \epsilon_4$ with

$$\epsilon_4 = \sqrt{\frac{8\mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{y|\boldsymbol{x}}\right]}{N_1 N_s}\left(\log\left(\frac{1}{\delta}\right) + \frac{1}{4}\right)}. \tag{B23}$$

To bound $R(h^{t^*})$ with $\hat{R}(h^{t^*})$, we require the following results:

Theorem B.1 (Theorem 8, [44]; Formulation of Theorem 21, [31]). *Let $\mathcal{L} : \mathcal{Y}' \times \mathcal{Y} \to \mathbb{R}_+$ be a loss function upper bounded by $b > 0$ and such that for any fixed y, $y' \to \mathcal{L}(y', y)$ is L-Lipschitz for some $L > 0$. Given function class $\mathcal{F} \subset (\mathcal{Y}')^{\mathcal{X}}$, for any $f : \mathcal{X} \to \mathcal{Y}' \in \mathcal{F}$, and for any sample $\mathcal{S}$ from distribution $\mathcal{D}$ of size N,*

$$\left| \mathbb{E}_{\mathcal{D}} \left[\mathcal{L}(f(x), y)\right] - \frac{1}{N} \sum_{(x,y)\in\mathcal{S}} \mathcal{L}(f(x), y) \right| \leq 4L\mathfrak{R}_N(\mathcal{F}) + 2b\sqrt{\frac{\log 2/\delta}{2N}}, \tag{B24}$$

where $\mathfrak{R}_N(\mathcal{H})$ is the expected value of the empirical Rademacher complexity of the function class $\mathcal{F}$ over all samples of size N.

Plugging the generalization, we have the following result for all hypotheses $h \in \mathcal{H}$.

$$R_{\text{expl}}(h) \leq \hat{R}(h) + 8\Delta\mathfrak{R}_{N_1}(\mathcal{H}) + 2\Delta^2\sqrt{\frac{\log(\frac{2}{\delta})}{2N_1}}. \tag{B25}$$

Next, to compute the empirical Rademacher complexity of $\mathcal{H}$, we use the following results:

Theorem B.2 (Lemma 22, [44] or Theorem 1, [45]; Formulation of Theorem 22, [31]). *Let $\mathcal{X}$ be a subset of an inner product space such that for all $\boldsymbol{x} \in \mathcal{X}$, $\|\boldsymbol{x}\|_2 \leq X$, and let $\mathcal{W} = \{\boldsymbol{x} \to \langle \boldsymbol{w}, \boldsymbol{x} \rangle, \|\boldsymbol{w}\|_2 \leq W\}$. Then it holds that*

$$\mathfrak{R}_N(\mathcal{W}) \leq \frac{XW}{\sqrt{N}}, \tag{B26}$$

Lemma B.3 (Talagrand's lemma, Corollary 3.17, [46]; Formulation of Lemma 5.7, [47]). *Let $\Phi : \mathbb{R} \to \mathbb{R}$ be a L-Lipschitz function. Then for any hypothesis set $\mathcal{F}$ of real-valued functions, the following holds:*

$$\mathfrak{R}_N(\Psi \circ \mathcal{F}) \leq L\mathfrak{R}_N(\mathcal{F}), \tag{B27}$$

Noting that our hypothesis class $\mathcal{H}$ in question is a linear class with a L-Lipschitz function applied to it, with the constraints $\|\boldsymbol{w}\|_2 \leq B$ and $\|\boldsymbol{\phi(x)}\|_2 \leq 1$ combining the above two results, we get

$$\mathfrak{R}_{N_1}(\mathcal{H}) \leq \frac{BL}{\sqrt{N_1}}, \tag{B28}$$

Finally, we can make use of Rademacher complexity to bound $R(h^t)$

$$R_{\text{expl}}(h^{t^*}) \leq \hat{R}(h^{t^*}) + \mathcal{O}\left(BL\Delta\sqrt{\frac{1}{N_1}} + \Delta^2\sqrt{\frac{\log(1/\delta)}{N_1}} \right) \tag{B29}$$

$$= \mathcal{O}\left(L\Delta\sqrt{\epsilon_1} + L\Delta M\sqrt[4]{\frac{\log(1/\delta)}{N_1}} + BL\Delta\sqrt{\frac{1}{N_1}} + BL\sqrt{\frac{\bar{\sigma}}{N_1 N_s}\left(\log\left(\frac{1}{\delta}\right)\right)} + \Delta^2\sqrt{\frac{\log(1/\delta)}{N_1}} \right) \tag{B30}$$

where $\bar{\sigma} = \mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{y|\boldsymbol{x}}\right]$. The last step is to show that we can indeed find a hypothesis satisfying the above guarantee. Using the Hoeffding inequality and union bound, one could show that $N_2 \geq O\left(N_1\Delta^2 \log(\frac{T}{\delta^2})\right)$ validation data points suffice to choose the optimal hypothesis h^{t^*} at time step t^* that satisfies Equation (B30).

Appendix C: Bias-variance-noise decomposition

For a given training dataset $\mathcal{S} = (\boldsymbol{x}_i, \bar{y}_i)_{i=1}^{N_1}$, one would obtain an associated trained model $h_{\mathcal{S}}(\boldsymbol{x})$ by optimizing the empirical risk $\widehat{R}(h)$ using some optimization methods such as the gradient descent algorithm. Further, different training datasets $\mathcal{S}'$ would yield different trained models $h_{\mathcal{S}'}(\boldsymbol{x})$, each associated with explicit risk $R_{\text{expl}}(h_{\mathcal{S}})$ and $R_{\text{expl}}(h_{\mathcal{S}'})$, respectively. This observation begs the question of how these trained models are related to each other and the target concept $c(\boldsymbol{x}) = \mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]$.

To address the above-mentioned questions, we introduce a machine learning concept known as the bias-variance trade-off. The bias of machine learning models informs their consistent errors and it is defined as

$$\mathbf{Bias}_{\mathcal{S}} := \mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - f(\boldsymbol{x}). \tag{C1}$$

Since $f(\boldsymbol{x})$ is independent of $\mathcal{S}$, one could express the bias as $\mathbf{Bias}_{\mathcal{S}} = \mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x}) - f(\boldsymbol{x})]$. Low bias suggests that on average the trained models $h_{\mathcal{S}}(\boldsymbol{x})$ are close to the target function, and typically machine learning models with larger model class sizes will have lower bias. Yet, models with low bias need not be optimal as they tend to be more sensitive to variations in training data; such models are said to have high variance where the variance of the model is defined as

$$\mathbf{Var}_{\mathcal{S}} := \mathbb{E}_{\mathcal{S}}\left[\left(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - h_{\mathcal{S}}(\boldsymbol{x})\right)^2\right]. \tag{C2}$$

It should be clear from the definition that the bias and variance are dependent on the complexity of the hypothesis class, the number of training data points N_1 and the number of random labels N_s.

The above-mentioned bias-variance trade-off can be studied by analysing the average behaviour of the trained models under the constraints of finite training data points and labels, which we capture by taking the expectation value over all possible training data sets $\mathcal{S}$ with the same N_1 and N_s, which we denote $\mathbb{E}_{\mathcal{S}|N_1,N_s}[R_{\text{impl}}(h_{\mathcal{S}})]$ where $R_{\text{impl}}(h_{\mathcal{S}}) = \mathbb{E}_{\bar{\mathcal{D}}}[(h_{\mathcal{S}}(\boldsymbol{x}) - \bar{y})^2]$ is the implicit risk of $h_{\mathcal{S}}(\cdot)$ as defined in Equation (8).

This averaged risk quantifies the overall performance of the hypothesis class $\mathcal{H}$ under all realization of training datasets of size N_1, with empirical means estimated using N_s random labels. Furthermore, $R_{\text{impl}}(h) = R_{\text{expl}}(h) + \bar{\sigma}_{N_S}$ implies

$$\mathbb{E}_{\mathcal{S}|N_1,N_s}[R_{\text{impl}}(h_{\mathcal{S}})] = \mathbb{E}_{\mathcal{S}|N_1,N_s}[R_{\text{expl}}(h_{\mathcal{S}})] + \bar{\sigma}_{N_S}, \tag{C3}$$

where $\mathbb{E}_{\mathcal{S}|N_1,N_s}[R_{\text{expl}}(h_{\mathcal{S}})]$ is the averaged explicit risk and $R_{\text{impl}}(\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}]) := \bar{\sigma}_{N_S} = \mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{\bar{y}|\boldsymbol{x}}\right] = \frac{1}{N_s}\mathbb{E}_{\boldsymbol{x}}\left[\sigma^2_{y|\boldsymbol{x}}\right]$ is the irreducible error that lower bounds the implicit risk on unseen sample. Note that in the asymptotic regime ($N_1 \to \infty$), the variance goes to 0 as the finite data sampling noise diminishes, and one would consistently obtain the optimal model in $\mathcal{H}$ that achieves the optimal explicit risk $R_{\text{expl}}(h)$. In addition, the strength of the irreducible error is controllable by the number of random samples N_s. In particular, $\bar{\sigma}_{N_S} \to 0$ as $N_s \to \infty$ and therefore $\mathbb{E}_{\mathcal{S}|N_1,N_s\to\infty}[R_{\text{impl}}(h_{\mathcal{S}})] \to \mathbb{E}_{\mathcal{S}|N_1,N_s\to\infty}[R_{\text{expl}}(h_{\mathcal{S}})]$.

We can then further decompose the explicit risk averaged over all dataset.

$$\begin{aligned}
\mathbb{E}_{\mathcal{S}}[R_{\text{expl}}(h_{\mathcal{S}})] &= \mathbb{E}_{\boldsymbol{x},\mathcal{S}}\left[\left(h_{\mathcal{S}}(\boldsymbol{x}) - c(\boldsymbol{x})\right)^2\right] && \text{(C4)}\\
&= \mathbb{E}_{\boldsymbol{x},\mathcal{S}}\left[\left(h_{\mathcal{S}}(\boldsymbol{x}) - \mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] + \mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - c(\boldsymbol{x})\right)^2\right] && \text{(C5)}\\
&= \mathbb{E}_{\boldsymbol{x}}\left[\left(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - c(\boldsymbol{x})\right)^2\right] + \mathbb{E}_{\boldsymbol{x},\mathcal{S}}\left[\left(\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\boldsymbol{x})] - h_{\mathcal{S}}(\boldsymbol{x})]\right)^2\right] && \text{(C6)}\\
&= \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Bias}^2_{\mathcal{S}}\right] + \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Var}_{\mathcal{S}}\right]. && \text{(C7)}
\end{aligned}$$

In summary, we have

$$\begin{aligned}
\mathbb{E}_{\mathcal{S}|N_1,N_s}[R_{\text{expl}}(h_{\mathcal{S}})] &= \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Bias}^2_{\mathcal{S}}\right] + \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Var}_{\mathcal{S}}\right], \quad \text{and} && \text{(C8)}\\
\mathbb{E}_{\mathcal{S}|N_1,N_s}[R_{\text{impl}}(h_{\mathcal{S}})] &= \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Bias}^2_{\mathcal{S}}\right] + \mathbb{E}_{\boldsymbol{x}}\left[\mathbf{Var}_{\mathcal{S}}\right] + \bar{\sigma}_{N_s}. && \text{(C9)}
\end{aligned}$$

Appendix D: Random Fourier feature models

1. Classical approximation of PQC functions

Let $\mathcal{F}_{U,O}$ and $\boldsymbol{\phi}_F(\boldsymbol{x})$ be the PQC concept class and feature map as defined in Equation (21) and Equation (28), respectively. In addition, let $k_F(\boldsymbol{x},\boldsymbol{x}') = \langle\boldsymbol{\phi}_F(\boldsymbol{x}),\boldsymbol{\phi}_F(\boldsymbol{x}')\rangle$ be the kernel of $\boldsymbol{\phi}_F(\boldsymbol{x})$.

Our goal of learning PQCs corresponds to taking $\mathcal{F}_{U,O}$ as our concept class. It is a still-unresolved question which PQCs provably give rise to function families that can or cannot be well approximated by kernel-based function families, but it is known that PQCs exist which cannot. Nonetheless, we offer a generic PQC construction whose functions are guaranteed to be well-approximated by a kernel-based hypothesis family. The recipe we propose does not exactly match the typical PQCs used by practitioners, but it is generic enough that it may become useful in the future. The construction relies on the Linear Combination of Unitaries (LCU) framework [48] and resembles constructions proposed in e.g. Refs. [49, 50].

Let k_F be a kernel that can be well-approximated as an Embedding Quantum Kernel (EQK) [49] on n qubits, meaning there exists a data-dependent unitary gate $U(\boldsymbol{x})$ such that

$$\sup_{\boldsymbol{x},\boldsymbol{x}'\in\mathcal{X}}\left|k_F(\boldsymbol{x},\boldsymbol{x}') - |\langle\mathbf{0}|U^\dagger(\boldsymbol{x})U(\boldsymbol{x}')|\mathbf{0}\rangle|^2\right|^2 \leq \epsilon \tag{D1}$$

for almost every $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}$. Then, given $N \in \mathbb{N}$, a vector of real numbers $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^N$, and a set of inputs $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$, consider a PQC over $n + \lceil \log(N) \rceil$ qubits. The circuit starts on the all-0 state, and the unitary $U(\boldsymbol{x})$ is applied on the first n-qubits. In parallel, we perform amplitude encoding of $\boldsymbol{\alpha}$ on the other $\lceil \log(N) \rceil$ qubits of the auxiliary register. Next, we define a controlled operation CU_i which, conditional on the auxiliary register being in state $|i\rangle$ for $i \in \{1, \ldots, N\}$ applies $U^\dagger(\boldsymbol{x}_i)$ on the main register. It follows that these controlled operations commute $[CU_i, CU_j] = 0$. We need only apply all such controlled gates in sequence, then: $\prod_{i=1}^N CU_i$, and measure the probability of the first n-qubits being in the all-0 state at the end (together with a diagonal observable on the auxiliary register that takes care of the negative signs in $\boldsymbol{\alpha}$). For notational ease, we do not explicitly write the extra observable on the auxiliary register, and we write only the projector on the all-0 state. This means that the functions can take negative values even though they are defined as the absolute square of a complex number. This way, given $\boldsymbol{\alpha}$ and $\boldsymbol{x}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$ we have defined a PQC in the form of a unitary $W(\boldsymbol{\alpha}, \boldsymbol{x}, (\boldsymbol{x}_i)_i)$, and produces as output a function in the kernel-based hypothesis family:

$$|\langle \mathbf{0} | W(\boldsymbol{\alpha}, \boldsymbol{x}, (\boldsymbol{x}_i)_i) | \mathbf{0} \rangle|^2 = \sum_{i=1}^N \alpha_i |\langle \mathbf{0} | U^\dagger(\boldsymbol{x}) U(\boldsymbol{x}') | \mathbf{0} \rangle|^2. \tag{D2}$$

From the ϵ-approximation of the initial kernel k_F via the EQK defined by U, it follows that each function of the form $\sum_{i=1}^N \alpha_i k(\boldsymbol{x}, \boldsymbol{x}_i)$ can be approximated by a function in $\mathcal{F}_{W, |\mathbf{0}\rangle\langle\mathbf{0}|}$, by taking the same $\boldsymbol{\alpha}$ vector and the same set of inputs $(\boldsymbol{x}_i)_i$. Without loss of generality, we assume the parameter vector $\boldsymbol{\alpha}$ has bounded norm $\|\boldsymbol{\alpha}\|_2^2 \leq B$:

$$\begin{aligned}
&\sup_{\boldsymbol{x} \in \mathcal{X}} \left| \left(\sum_{i=1}^N \alpha_i k_F(\boldsymbol{x}, \boldsymbol{x}_i) \right) - |\langle \mathbf{0} | W(\boldsymbol{\alpha}, \boldsymbol{x}, (\boldsymbol{x}_i)_i) | \mathbf{0} \rangle|^2 \right|^2 && \text{(D3)}\\
&= \sup_{\boldsymbol{x} \in \mathcal{X}} \left| \sum_{i=1}^N \alpha_i \left(k_F(\boldsymbol{x}, \boldsymbol{x}_i) - |\langle \mathbf{0} | U^\dagger(\boldsymbol{x}) U(\boldsymbol{x}_i) | \mathbf{0} \rangle|^2 \right) \right|^2 && \text{(D4)}\\
&\leq \|\boldsymbol{\alpha}\|^2 \sum_{i=1}^N \sup_{x \in \mathcal{X}} \left| k_F(\boldsymbol{x}, \boldsymbol{x}_i) - |\langle \mathbf{0} | U^\dagger(\boldsymbol{x}) U(\boldsymbol{x}_i) | \mathbf{0} \rangle|^2 \right|^2 && \text{(D5)}\\
&\leq B^2 \epsilon && \text{(D6)}
\end{aligned}$$

Altogether, this recipe allows us to construct a PQC whose associated function family is the same as a given kernel-based function family. For Algorithm 1 to succeed as a classical learner of this function family, then, we need only be able to evaluate the kernel k_F efficiently classically. It is known that the complexity of evaluating the trigonometric kernels that result from quantum embeddings is upper-bounded by the cardinality of the frequency spectrum $\tilde{\Omega}$ arising from the encoding strategy.

2. Approximating PQCs with random Fourier features

If the PQC $U(\boldsymbol{x}, \boldsymbol{\theta})$ is such that its corresponding feature map is of polynomial dimension $|\tilde{\Omega}| \in \mathcal{O}(\mathrm{poly}(m))$, then we know we can classically express the corresponding function exactly: $\langle \mathbf{0} | U^\dagger(\boldsymbol{x}, \boldsymbol{\theta}) O U(\boldsymbol{x}, \boldsymbol{\theta}) | \mathbf{0} \rangle = \langle \boldsymbol{w}_F, \boldsymbol{\phi}_F(\boldsymbol{x}) \rangle$, where the real-valued vector $\boldsymbol{w}_F$ is efficiently storable in classical memory. Refs. [8, 51] offer a discussion on what encoding strategies connected to families of PQCs will result in Fourier spectra of polynomial size. It is nevertheless known that many natural encoding strategies result in an exponentially large Fourier spectrum, where we cannot rely on an exact realization of the PQC function as a classical linear map. Some of these cases have been recently analyzed in Refs. [26, 27] under the lens of Random Fourier Features (RFF) [33]. The main idea in RFF is to efficiently approximate the high-dimensional inner product $\langle \boldsymbol{w}_F, \boldsymbol{\phi}_F(\boldsymbol{x}) \rangle$ by sampling a few of its dominant terms.

For instance, consider an encoding strategy which gives rise to an exponentially large Fourier spectrum $|\Omega| \propto \exp(m)$. Then, the inner product

$$\langle \boldsymbol{w}, \boldsymbol{\phi}_F(\boldsymbol{x}) \rangle = \sum_{j=1}^{2|\Omega|-1} w_j \phi_{F,j}(\boldsymbol{x}) \tag{D7}$$

cannot be classically evaluated in general due to its containing many terms. Now consider a specific PQC $U(\boldsymbol{x}, \boldsymbol{\theta})$ with this encoding strategy, but which is structured enough that we know that some entries of the weight vector are more dominant than others, in that they contribute more to the sum. One way to capture this would be by considering a probability distribution over the Fourier spectrum $P(\Omega)$, where the probability associated with a specific frequency is proportional to the magnitude squared of its coefficients $p(\boldsymbol{\omega}) = a_{\boldsymbol{\omega}}^2 + b_{\boldsymbol{\omega}}^2$. Without loss of generality, we assume the coefficients are alreadyproperly normalized. Then, what the RFF algorithm prescribes we do is sample a number D of frequencies from such a distribution $\tilde{\boldsymbol{\omega}} \sim P^D$, and then consider the classical efficient feature map $\boldsymbol{\phi}_{\mathrm{RFF}}(\boldsymbol{x})$ consisting of only those frequencies:

$$\boldsymbol{\phi}_{\mathrm{RFF}}(\boldsymbol{x}) = \frac{1}{\sqrt{D}} \begin{pmatrix} \cos\langle \tilde{\boldsymbol{\omega}}_1, \boldsymbol{x}\rangle \\ \sin\langle \tilde{\boldsymbol{\omega}}_1, \boldsymbol{x}\rangle \\ \vdots \\ \cos\langle \tilde{\boldsymbol{\omega}}_D, \boldsymbol{x}\rangle \\ \sin\langle \tilde{\boldsymbol{\omega}}_D, \boldsymbol{x}\rangle \end{pmatrix}. \tag{D8}$$

The sampled frequencies $\tilde{\boldsymbol{\omega}}$ are all in the original Fourier spectrum $\tilde{\boldsymbol{\omega}}_i \in \Omega$, so $\boldsymbol{\phi}_{\mathrm{RFF}}(\boldsymbol{x})$ is just an appropriately renormalized subvector of the full $\boldsymbol{\phi}_F(\boldsymbol{x})$. This smaller feature map gives rise to the hypothesis family:

$$\mathcal{H}_{\mathrm{RFF}} = \{u(\langle \boldsymbol{w}, \boldsymbol{\phi}_{\mathrm{RFF}}(\boldsymbol{x})\rangle) \,|\, \boldsymbol{w} \in \mathbb{R}^D\}. \tag{D9}$$

Then, if the PQC function is such that it can in principle be approximated as a linear map of rank D [52], it follows from Refs. [25, 26, 33] that the RFF hypothesis family should contain a good approximation to the function. In the context of this work, this means that Algorithm 1 should be able to learn the initial PQC function by using $\mathcal{H}_{\mathrm{RFF}}$ as a hypothesis class.

The remaining question is, again, how to specify the right $\mathcal{H}_{\mathrm{RFF}}$ for a given PQC of interest, modelled by the function family $\mathcal{F}_{U,O}$. The ultimate general-case answer is not fully resolved [26], but we provide a recipe to, given an RFF-approximable EQK k, construct a corresponding PQC.

Let k be a kernel that can be approximated as the inner product of a feature map $\boldsymbol{\phi}$ of polynomial size (in particular, this could be the randomized feature map produced by the RFF algorithm):

$$\sup_{\boldsymbol{x},\boldsymbol{x}' \in \mathcal{X}} \left| k(\boldsymbol{x}, \boldsymbol{x}') - \langle \boldsymbol{\phi}(\boldsymbol{x}), \boldsymbol{\phi}(\boldsymbol{x}')\rangle \right|^2 \leq \epsilon, \tag{D10}$$

for almost every $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}$. Let further $U(\boldsymbol{x})$ be a quantum embedding that implements the feature map $\boldsymbol{\phi}(\boldsymbol{x})$ (w.l.o.g. we take $\boldsymbol{\phi}$ to be properly normalized):

$$\sup_{\boldsymbol{x},\boldsymbol{x}' \in \mathcal{X}} \left| |\langle \mathbf{0} | U^\dagger(\boldsymbol{x}) U(\boldsymbol{x}') | \mathbf{0}\rangle|^2 - \langle \boldsymbol{\phi}(\boldsymbol{x}), \boldsymbol{\phi}(\boldsymbol{x}')\rangle \right|^2 \leq \epsilon'. \tag{D11}$$

Then the same LCU construction we used before also results in a PQC whose function family approximates the function family of the RFF-based kernel, which in turn approximates the function family of the original kernel. With triangular inequality, it follows that this PQC construction approximates the original kernel-based function family. Since Algorithm 1 can provably learn the kernel-based function family, it follows it can also learn this PQC family.

Appendix E: Proof of Lemma 1

To discuss the explicit risk of the ERM given the hypothesis class $\mathcal{H}$ in Equation (45), we use the following result in statistical learning theory:

Proposition E.1 (Proposition 4.1, [47])**.** *Let $\mathcal{D}$ be a distribution over $\mathcal{X} \times \mathcal{Y}$. Let $\mathcal{L} : \mathcal{Y}' \times \mathcal{Y} \to \mathbb{R}_+$ be a loss function. Considering a hypothesis class $\mathcal{F}$ that maps $\mathcal{X}$ to $\mathcal{Y}'$, For any sample $\mathcal{S}$ from distribution $\mathcal{D}$, for hypotheses $f \in \mathcal{F}$, the following holds:*

$$\mathbb{E}_{\mathcal{D}}[\mathcal{L}(f_{\mathcal{S}}^{\mathrm{ERM}}(\boldsymbol{x}), y)] - \inf_{f \in \mathcal{F}} \mathbb{E}_{\mathcal{D}}[\mathcal{L}(f(\boldsymbol{x}), y)] \leq 2 \sup_{f \in \mathcal{F}} \left| \mathbb{E}_{\mathcal{D}}[\mathcal{L}(f(\boldsymbol{x}), y)] - \frac{1}{|\mathcal{S}|} \sum_{(\boldsymbol{x}, y) \in \mathcal{S}} \mathcal{L}(f(\boldsymbol{x}), y) \right|. \tag{E1}$$

Considering the implicit loss function ℓ_{impl} for the loss function $\mathcal{L}$ in the above proposition, we get

$$R_{\mathrm{impl}}(h_{\mathcal{S}}^{\mathrm{ERM}}) - \inf_{h \in \mathcal{H}} R_{\mathrm{impl}}(h) \leq 2 \sup_{h \in \mathcal{H}} |R_{\mathrm{impl}}(h) - \widehat{R}(h)|. \tag{E2}$$

Noting that $R_{\text{impl}}(h) = R_{\text{expl}}(h) + R_{\text{impl}}(\mathbb{E}_{\bar{y}}[\bar{y}|\boldsymbol{x}])$, we can see that

$$R_{\text{expl}}(h_{\mathcal{S}}^{\text{ERM}}) - \inf_{h\in\mathcal{H}} R_{\text{expl}}(h) \leq 2 \sup_{h\in\mathcal{H}} |R_{\text{impl}}(h) - \widehat{R}(h)|. \tag{E3}$$

By definition, we know that

$$\inf_{h\in\mathcal{H}} R_{\text{expl}}(h) = \inf_{h\in\mathcal{H}} \mathbb{E}_{\bar{\mathcal{D}}}[(h(\boldsymbol{x}) - c(\boldsymbol{x}))^2] \leq \mathbb{E}_{\bar{\mathcal{D}}}[(\langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle - \langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle + \xi(\boldsymbol{x}))^2] = \mathbb{E}_{\bar{\mathcal{D}}}[\xi(\boldsymbol{x})^2] \leq \epsilon_1. \tag{E4}$$

Hence we see that

$$R_{\text{expl}}(h_{\mathcal{S}}^{\text{ERM}}) \leq \epsilon_1 + 2 \sup_{h\in\mathcal{H}} |R_{\text{impl}}(h) - \widehat{R}(h)|. \tag{E5}$$

We now find error bounds on the right-hand side of the previous proposition. To do so, we require the following results obtainable by combining Theorem 8 and Lemma 22 from [44]:

Theorem E.1 (Theorem 11.11, [47])**.** *Given distribution $\mathcal{D}$ over $\mathcal{X} \times \mathcal{Y}$, let $k : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ be a positive semidefinite kernel, $\Phi : \mathcal{X} \to \mathbb{H}$ be the feature map associated with kernel k, and hypothesis class $\mathcal{H} = \{\boldsymbol{x} \to \langle \boldsymbol{w}, \boldsymbol{\phi}(\boldsymbol{x})\rangle, \|\boldsymbol{w}\|_{\mathbb{H}} \leq \Lambda\}$. Assume there exists $r, M > 0$ such that $k(\boldsymbol{x}, \boldsymbol{x}) \leq r^2$ and for all hypotheses $h : \mathcal{X} \to \mathcal{Y}' \in \mathcal{H}$ and all $(\boldsymbol{x}, y) \in \mathcal{D}$, $|h(\boldsymbol{x}) - y| \leq M$. Then for any sample $\mathcal{S}$ from $\mathcal{D}$ of size N, the generalization bound is as follows:*

$$\left| \mathop{\mathbb{E}}_{(\boldsymbol{x},y)\sim\mathcal{D}} \left[|h(\boldsymbol{x}) - y|^2\right] - \frac{1}{N} \sum_{(\boldsymbol{x},y)\in\mathcal{S}} |h(\boldsymbol{x}) - y|^2 \right| \in \mathcal{O}\left(\frac{M\Lambda r}{\sqrt{N}} + M^2 \sqrt{\frac{\log\frac{1}{\delta}}{N}} \right). \tag{E6}$$

Plugging in our error losses and range of $\mathcal{H}$, we note that $\Lambda, M \in \mathcal{O}(D)$ and $r = 1$. We then obtain the following generalization bound for $\mathcal{H}$.

$$|R_{\text{impl}}(h) - \widehat{R}(h)| \in \mathcal{O}\left(D^2 \sqrt{\frac{\log\frac{1}{\delta}}{N_1}} \right), \tag{E7}$$

Note that this result yields a better result than the Rademacher-based generalization bound proposed by Caro *et al.* [51] by a logarithmic factor if we use the entire Fourier spectrum instead of RFF. We can then write the explicit risk for the ERM as follows:

$$R_{\text{expl}}(h_{\mathcal{S}}^{\text{ERM}}) \in \mathcal{O}\left(\epsilon_1 + D^2 \sqrt{\frac{\log\frac{1}{\delta}}{N_1}} \right). \tag{E8}$$

Advantage of Quantum Machine Learning from General Computational Advantages

Hayata Yamasaki[1] * Natsuto Isogai[1] † Mio Murao[1] ‡

[1] *Department of Physics, Graduate School of Science, The University of Tokyo*
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033

Abstract. A key milestone of quantum machine learning (QML) is to demonstrate its advantage over classical methods in accelerating supervised learning with classical data. Previously, QML's proven advantages were limited to learning tasks constructed based on Shor's algorithms. We here construct supervised learning tasks with provable advantage based on general quantum computational advantages beyond Shor's algorithms. We construct a polynomial-time QML algorithm for solving these tasks even though these tasks have exponentially many candidates of functions to be learned. At the same time, we prove the hardness of achieving these tasks for any polynomial-time classical method. We also clarify protocols for preparing classical data of this learning task for its experimental demonstration. These results pave the way to exploit various quantum advantages in computing functions for demonstrating QML's advantages.

Keywords: Quantum machine learning, PAC learning, Quantum advantage, Supervised learning

1 Introduction

Machine learning supervised by big data supports our daily lives in today's world. Quantum machine learning (QML) attracts growing attention as an emerging field of research to further accelerate and scale up the learning by taking advantage of quantum computation [1, 2]. Due to its importance and potential, QML has gathered substantial attention among the community of recent AQIS conferences [3–5]. Quantum computation is believed to achieve significant speedup in solving various computational problems over conventional classical computation [6, 7]. The central goal of supervised learning is, however, not solving the computational problems themselves but finding and making a correct prediction on unseen data under the supervision of given sample data [8–11]. A far-reaching milestone in the field of QML is to demonstrate the advantage of QML, i.e., an end-to-end acceleration in accomplishing this goal of learning in such a way that any possible classical learning method would never be able to achieve.

However, it has been challenging to realize this milestone due to our limited theoretical understanding of the learning tasks with the advantage of QML. Representative QML algorithms such as those in Refs. [12–17] have theoretically guaranteed upper bounds of their runtime, and it is indeed hard for existing classical algorithms to achieve the same learning tasks as these QML algorithms within a comparable runtime; nevertheless, these facts are insufficient to provably rule out the possibility of the potential existence of classical learning methods achieving the comparable runtime. For example, the quantum algorithm for recommendation systems was initially claimed to achieve an exponential speedup compared to the existing classical algorithms at the time [13], but it turned out in later research that the quantum algorithm achieves only a polynomial speedup compared to the best possible classical algorithm due to a breakthrough in designing a quantum-inspired classical algorithm for solving the same task [18]. Prior to our work, the advantage of QML based on general types of quantum computational advantages has only shown for a limited class of learning problems that can be simply solved by a brute-force algorithm trying each solution candidate one by one [19, 20]; however, in practice, machine learning algorithms never try all the possible candidates of the functions to be learned, which is infeasible in many cases. Of interest here are more difficult yet common learning problems where the number of candidates is exponential. In this regime, the advantage of QML in accelerating supervised learning with classical data has been proven only based on the quantum computational advantage of Shor's algorithms [21–23] to solve integer factoring and discrete logarithms [19, 20, 24–26]. The existing techniques to prove the hardness of learning for all possible classical methods use a cryptographic argument essentially depending on the specific mathematical structure of discrete logarithms and integer factoring [8, 9, 19, 20, 24–27], which do not straightforwardly generalize. A fundamental open question in the theory of QML has been what types of quantum computational advantages, beyond that of Shor's algorithms, lead to learning tasks to demonstrate the end-to-end acceleration of the learning; to address this question, novel techniques need to be established to prove the classical hardness of learning beyond the realm of Shor's algorithms.

Also from a practical perspective, toward the experimental demonstration of the advantages of QML, Shor's algorithms are challenging to realize with near-term quantum technologies [28], confronting as an obstacle to the demonstration. One reason for this practical challenge is rooted in the fact that Shor's algorithms need to compete with the well-established classical algorithms for integer factoring that run only within subexponential time, which is much shorter than exponential time [29–31]. For this reason, a milestone in realizing Shor's algorithms is often set to factorize a relatively

*hayata.yamasaki@gmail.com
†natsuto.isogai@phys.s.u-tokyo.ac.jp
‡murao@phys.s.u-tokyo.ac.jp

large integer, such as a 2048-bit integer [28]. On the other hand, apart from Shor's algorithms, polynomial-time quantum algorithms can also solve other types of computational problems that are potentially harder for classical algorithms, such as those relevant to topological data analysis (TDA) [32–36], Pell's equation [37, 38], and BQP-complete problems [39–45]. For the classically hard problems, one could potentially use a much smaller size of the problem instance, e.g., with much less than 2048-bit inputs, to demonstrate the quantum computational advantages. In view of this, the solution to the above open question on the relation between quantum computational advantages and the advantage of QML will also constitute a significant step to the practical demonstration as well as the fundamental understanding of QML.

2 Summary of Main Result

In this work, we address this open question by showing that quantum advantages in computing functions *in general* lead to the provable end-to-end advantage of QML in conducting supervised learning with classical data, without specifically depending on Shor's algorithms. Significantly, our results hold for learning problems with exponentially many candidates of the functions to be learned in terms of the problem size.

To address the above question, we explicitly construct a family of classification tasks in a conventional setting of supervised learning with classical sample data, i.e., in a probably approximately correct (PAC) learning model [8, 9, 46], using a general class of functions that can be computed efficiently in polynomial time for a large fraction of inputs by quantum algorithms but not by any classical algorithm (even under the supervision of data). In a classification task, for an unknown function c to be learned (called a concept), one is initially given sample data of inputs x from a target distribution $x \sim \mathcal{D}$ and the corresponding outputs $c(x) = 0$ or $c(x) = 1$ of binary labels. Using these samples, the classification task aims to find and make a correct prediction (called a hypothesis) that should coincide with $c(x)$ for a large fraction of $x \sim \mathcal{D}$. We study classification tasks that have a common structure to those widely appearing in conventional machine learning; in particular, we consider tasks that can be solved by a commonly used learning method called feature mapping and linear separation (see Fig. 1 of Technical Manuscript). In this approach, the learning algorithm first maps an input x to another vector $f(x)$ and subsequently classifies x in the space of $f(x)$. This mapping f is known as a feature map, transforming x in the input space into the corresponding feature $f(x)$ in the feature space that encapsulates essential information for the classification. The sets of x satisfying $c(x) = 0$ and $c(x) = 1$ are mapped into $\mathcal{F}_0$ and $\mathcal{F}_1$ of $f(x)$, respectively. The feature map here should be designed so that $\mathcal{F}_0$ and $\mathcal{F}_1$ have linear separability, i.e, the property that a hyperplane in the feature space should be able to distinguish between $\mathcal{F}_0$ and $\mathcal{F}_1$ [47]. The goal of the learning task is to find the hyperplane and use it to make a correct prediction for $x \sim \mathcal{D}$.

Our key discovery is that the advantage of QML stems from the feature mapping that makes the learning feasible for quantum computation but hard for classical computation; in our QML framework, we convert the input x into a bit string representing their feature $f(x)$ by a feature map f that can be computed efficiently by quantum computation but not by classical computation. The feature space for these bit strings is represented as a vector space over a finite field (see Technical Manuscript for details). Remarkably, for our learning task, we show that f can be arbitrarily chosen from a general class of functions that can be, roughly speaking, computed efficiently within a polynomial time by quantum algorithms (for a large fraction of inputs $x \sim \mathcal{D}$ with a high probability) but not by classical algorithms (even with a polynomial-size advice string, e.g., sample data). We call a function in this class a *quantumly advantageous function* (see also Technical Manuscript for the precise definition). In the previous work on the provable advantage of QML, the choice of such a feature map was limited to those computed by Shor's algorithms, which has been undermining the applicability of QML. By contrast, our results make it possible to use arbitrary quantumly advantageous functions as feature maps in QML to obtain the following theorem.

Theorem 1 *(informal, see also Technical Manuscript): Advantage of QML from general computational advantages. For any quantumly advantageous function f under any target distribution $\mathcal{D}$, we construct a quantum algorithm that can find and make a correct prediction in our learning task within a polynomial time; by contrast, we prove that no polynomial-time classical algorithm can achieve this.*

Construction of polynomial-time QML algorithm. We construct a polynomial-time quantum algorithm for solving our learning task using a polynomial amount of classical sample data. This quantum algorithm is simply implementable by a variant of the conventional learning method: feature mapping by quantum computation to map the input classical data into the corresponding bit strings representing their features, followed by linear separation by classical computation to find an appropriate hyperplane in the feature space to achieve the classification. While the feature space of these bit strings is discrete, our algorithm finds a hyperplane by solving a system of linear equations using Gaussian elimination. A technical challenge in constructing our algorithm is that the learning algorithm does not necessarily find the true hyperplane of the unknown concept c to be learned but may output an approximate estimate of the hyperplane; nevertheless, our analysis shows that any hyperplane learned by our algorithm leads to a correct prediction for a large fraction of $x \sim \mathcal{D}$ with a high probability to achieve the learning task (see Technical Manuscript for details).

Provable classical hardness At the same time, under the assumption that no polynomial-time classical algorithm can compute the quantumly advantageous function used in our construction (yet, importantly, without any cryptographic assumption specifically depending on Shor's algorithms), we prove that no polynomial-time classical algorithm can accomplish this learning task. The feature mapping and the linear separation may also be applicable to some of the previous works on the advantage of QML [24], but a more crucial difference arises from the techniques for proving the classical hardness. In particular, a feature map constructed in Ref. [24] used Shor's algorithms to transform an input into a feature in a feature space, which was taken as a space of functions called the reproducing kernel Hilbert space (RKHS) in the kernel method [10, 11] to show a polynomial-time quantum learning algorithm. However, the existing techniques for proving the classical hardness of such learning tasks needed to use a cryptographic argument on the hardness of solving computational problems depending on the specific mathematical structure of discrete logarithms and integer factoring [8, 9, 19, 20, 24–27] and do not straightforwardly generalize. By contrast, we develop techniques for analyzing our learning task with its feature space formulated as the vector space of bit strings (i.e., the vector space over a finite field), making it possible to prove the classical hardness for any quantumly advantageous function in general (see Technical Manuscript for details).

Protocol for demonstrating the provable advantage of QML Furthermore, we clarify a protocol for preparing the classical sample data to demonstrate this provable advantage of QML in the experiments. For the demonstration, we propose a two-party setup, where a party A is in charge of preparing the classical sample data, and the other party B receives the data from A to perform the learning (see also Fig. 2 of Technical Manuscript). We here put A and B on equal footing by allowing both to compute the feature map f by quantum computation. Note that in the previous work on the advantage of QML based on Shor's algorithms [19, 20, 24–26], the data for their learning tasks were able to be prepared by classical computation, but this classical data preparation was possible by assuming a special property of cryptographic primitives (i.e., *classically one-way* permutation, which is hard to invert efficiently by classical computation but is invertible efficiently by quantum computation). We also show that A's data preparation for our task is possible in the same way by only using classical computation if we use the classically one-way permutations for f (see Technical Manuscript for details). These results pave the way to the practical demonstration of the provable advantage of QML in experiments, via realizing any quantum algorithms for computing quantumly advantageous functions without necessarily depending on Shor's algorithms.

3 Impact

In conclusion, our work successfully bridges the gap between the advantage of QML (in finding and making a correct prediction from given samples) and quantum computational advantages (in computing functions), disclosing the origin of the advantage of QML stemming from the computation of *any* quantumly advantageous functions. The existing works on the provable advantages of QML were limited to the realm of Shor's algorithms [19, 20, 24–26] or to that of brute-force algorithms that are not applicable to the super-polynomial number of candidates [19, 20]. By contrast, our results open vast opportunities to use a general class of quantum algorithms beyond Shor's algorithms to enjoy the provable advantage of QML, such as those relevant to topological data analysis (TDA) [32–36], Pell's equation [37, 38], and BQP-complete problems [39–45] (see Technical Manuscript for details of these examples). In different settings from ours, advantages of using quantum computation have been shown in a learning setting with quantum data obtained from quantum experiments [48–53] and also in a distribution learning setting [54–56]; still, it is not straightforward to apply these quantum algorithms to accelerate the common learning tasks in the era of big data, as represented by supervised learning with classical data. By contrast, our approach offers a QML framework that can address this common type of learning task. A merit of our QML framework is that it is simply implementable by using any quantumly advantageous function for feature mapping, followed by classically performing linear separation in the feature space.

Also from a broader perspective, in applications of machine learning, state-of-the-art classical learning methods such as deep learning heuristically design the feature maps, e.g., by adapting the architectures of deep neural networks [57]. The theoretical analysis of optimized choices of feature maps for given data is challenging even in classical cases, but empirical facts suggest that the classification tasks for real-world data often reduce to applying feature maps designed by such artificial neural networks followed by linear separation [57]. In view of the success of the artificially designed feature maps, it is crucial to allow as large classes of functions as possible to create more room for the heuristic optimization of the feature maps. Advancing ahead, our QML framework makes it possible to design the feature maps flexibly, using arbitrary quantumly advantageous functions to attain the provable advantage of QML. Toward the demonstration of the advantage of QML, an experimental challenge still remains in seeking how to realize quantum computation to surpass the capability of classical computation, and yet our QML framework opens a way to transcend all possible classical learning methods by exploiting *any* realization of quantumly advantageous functions for the feature maps.

Note: After this work had appeared in arXiv, Ref. [58] also showed a result in a similar direction, i.e., shows a provable advantage of QML over any classical methods for learning problems with exponentially many candidates, using another technique. We believe that this fact also supports a common interest and a high impact of our results in the field of QML.

References

[1] P. Wittek, *Quantum Machine Learning: What Quantum Computing Means to Data Mining* (Elsevier, 2014).

[2] M. Schuld and F. Petruccione, *Machine learning with quantum computers* (Springer, 2021).

[3] S. Bhattacharjee, M. M. Fuad, and A. K. M. F. Hossain, in *23rd Asian Quantum Information Science Conference (AQIS 2023)* (2023).

[4] L. Banchi, J. Pereira, and S. Pirandola, in *22nd Asian Quantum Information Science Conference (AQIS 2022)* (2022).

[5] H. Yamasaki, S. Subramanian, S. Sonoda, and M. Koashi, in *21st Asian Quantum Information Science Conference (AQIS 2021)* (2021).

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, 2011).

[7] S. Arora and B. Barak, *Computational complexity: A Modern Approach* (Cambridge University Press, 2009).

[8] M. J. Kearns, *The computational complexity of machine learning* (MIT press, 1990).

[9] M. J. Kearns and U. Vazirani, *An introduction to computational learning theory* (MIT press, 1994).

[10] B. Schölkopf and A. J. Smola, *Learning with kernels: support vector machines, regularization, optimization, and beyond* (MIT press, 2002).

[11] F. Bach, *Learning Theory from First Principles* (2023).

[12] P. Rebentrost, M. Mohseni, and S. Lloyd, Phys. Rev. Lett. **113**, 130503 (2014).

[13] I. Kerenidis and A. Prakash, in *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 67, edited by C. H. Papadimitriou (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2017) pp. 49:1–49:21.

[14] Z. Zhao, J. K. Fitzsimons, and J. F. Fitzsimons, Phys. Rev. A **99**, 052331 (2019).

[15] H. Yamasaki, S. Subramanian, S. Sonoda, and M. Koashi, in *Advances in Neural Information Processing Systems*, Vol. 33, edited by H. Larochelle, M. Ranzato, R. Hadsell, M. Balcan, and H. Lin (Curran Associates, Inc., 2020) pp. 13674–13687.

[16] H. Yamasaki and S. Sonoda, "Exponential error convergence in data classification with optimized random features: Acceleration by quantum machine learning," (2022), arXiv:2106.09028 [quant-ph] .

[17] H. Yamasaki, S. Subramanian, S. Hayakawa, and S. Sonoda, in *Proceedings of the 40th International Conference on Machine Learning*, ICML'23 (JMLR.org, 2023).

[18] E. Tang, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019 (Association for Computing Machinery, New York, NY, USA, 2019) p. 217–228.

[19] C. Gyurik and V. Dunjko, "On establishing learning separations between classical and quantum machine learning with classical data," (2023), arXiv:2208.06339 [quant-ph] .

[20] C. Gyurik and V. Dunjko, "Exponential separations between classical and quantum learners," (2023), arXiv:2306.16028 [quant-ph] .

[21] P. W. Shor, in *Proceedings 35th annual symposium on foundations of computer science* (Ieee, 1994) pp. 124–134.

[22] P. W. Shor, SIAM Journal on Computing **26**, 1484 (1997).

[23] P. W. Shor, SIAM Review **41**, 303 (1999).

[24] Y. Liu, S. Arunachalam, and K. Temme, Nature Physics **17**, 1013 (2021).

[25] R. A. Servedio and S. J. Gortler, SIAM Journal on Computing **33**, 1067 (2004).

[26] J. Perez-Guijarro, A. Pages-Zamora, and J. R. Fonollosa, IEEE Transactions on Quantum Engineering , 1 (5555).

[27] M. Kearns and L. Valiant, J. ACM **41**, 67–95 (1994).

[28] C. Gidney and M. Ekerå, Quantum **5**, 433 (2021).

[29] H. W. Lenstra and C. Pomerance, Journal of the American Mathematical Society **5**, 483 (1992).

[30] J. P. Buhler, H. W. Lenstra, and C. Pomerance, in *The development of the number field sieve*, edited by A. K. Lenstra and H. W. Lenstra (Springer Berlin Heidelberg, Berlin, Heidelberg, 1993) pp. 50–94.

[31] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, IEEE Security & Privacy **20**, 80 (2022).

[32] S. Lloyd, S. Garnerone, and P. Zanardi, Nature communications **7**, 10138 (2016).

[33] R. Hayakawa, Quantum **6**, 873 (2022).

[34] B. Ameneyro, G. Siopsis, and V. Maroulas, in *2022 IEEE/ACM 7th Symposium on Edge Computing (SEC)* (2022) pp. 387–392.

[35] I. Y. Akhalwaya, S. Ubaru, K. L. Clarkson, M. S. Squillante, V. Jejjala, Y.-H. He, K. Naidoo, V. Kalantzis, and L. Horesh, "Towards quantum advantage on noisy quantum computers," (2022), arXiv:2209.09371 [quant-ph] .

[36] S. McArdle, A. Gilyén, and M. Berta, "A streamlined quantum algorithm for topological data analysis with exponentially fewer qubits," (2022), arXiv:2209.12887 [quant-ph] .

[37] S. Hallgren, in *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (Association for Computing Machinery, New York, NY, USA, 2002) p. 653–658.

[38] S. Hallgren, J. ACM **54** (2007).

[39] M. H. Freedman, M. Larsen, and Z. Wang, Communications in Mathematical Physics **227**, 605 (2002).

[40] P. Wocjan and S. Zhang, "Several natural bqp-complete problems," (2006), arXiv:quant-ph/0606179 [quant-ph] .

[41] D. Aharonov, V. Jones, and Z. Landau, in *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '06 (Association for Computing Machinery, New York, NY, USA, 2006) p. 427–436.

[42] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009).

[43] D. Aharonov and I. Arad, New Journal of Physics **13**, 035019 (2011).

[44] S. Gharibian and F. Le Gall, in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022 (Association for Computing Machinery, New York, NY, USA, 2022) p. 19–32.

[45] S. Gharibian, R. Hayakawa, F. L. Gall, and T. Morimae, "Improved hardness results for the guided local hamiltonian problem," (2022), arXiv:2207.10250 [quant-ph] .

[46] L. G. Valiant, Commun. ACM **27**, 1134–1142 (1984).

[47] T. M. Cover, IEEE Transactions on Electronic Computers **EC-14**, 326 (1965).

[48] H.-Y. Huang, R. Kueng, and J. Preskill, Phys. Rev. Lett. **126**, 190505 (2021).

[49] D. Aharonov, J. Cotler, and X.-L. Qi, Nature communications **13**, 887 (2022).

[50] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (2022) pp. 574–585.

[51] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Science **376**, 1182 (2022).

[52] H.-Y. Huang, S. Chen, and J. Preskill, "Learning to predict arbitrary quantum processes," (2023), arXiv:2210.14894 [quant-ph] .

[53] F. Meier and H. Yamasaki, "Energy-consumption advantage of quantum computation," (2023), arXiv:2305.11212 [quant-ph] .

[54] J.-G. Liu and L. Wang, Phys. Rev. A **98**, 062324 (2018).

[55] R. Sweke, J.-P. Seifert, D. Hangleiter, and J. Eisert, Quantum **5**, 417 (2021).

[56] N. Pirnay, R. Sweke, J. Eisert, and J.-P. Seifert, Phys. Rev. A **107**, 042416 (2023).

[57] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning* (MIT Press, 2016).

[58] R. Molteni, C. Gyurik, and V. Dunjko, "Exponential quantum advantages in learning quantum observables from classical data," (2024), arXiv:2405.02027 [quant-ph] .

Advantage of Quantum Machine Learning from General Computational Advantages

Hayata Yamasaki*,[1,*] Natsuto Isogai*,[1] and Mio Murao[1]
(Hayata Yamasaki and Natsuto Isogai contributed equally to this work.)
[1] *Department of Physics, Graduate School of Science,*
The Univerisity of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

An overarching milestone of quantum machine learning (QML) is to demonstrate the advantage of QML over all possible classical learning methods in accelerating a common type of learning task as represented by supervised learning from classical data. However, the provable advantages of QML in supervised learning have been known so far only for the learning tasks designed for using the advantage of specific quantum algorithms, i.e., Shor's algorithms. Here we explicitly construct an unprecedentedly broader family of supervised learning tasks with classical data to offer the provable advantage of QML based on general quantum computational advantages, progressing beyond Shor's algorithms. Our learning task is feasibly achievable by executing a general class of functions that can be computed efficiently in polynomial time for a large fraction of inputs by arbitrary quantum algorithms but not by any classical algorithm. We prove the hardness of achieving this learning task for any possible polynomial-time classical learning method. We also clarify protocols for preparing the classical data to demonstrate this learning task in experiments. These results open vast opportunities to exploit a variety of quantum advantages in computing functions for the realization of provably advantageous QML.

Introduction.— Machine learning technologies supervised by big data serve as one of the core infrastructures to support our daily lives. Quantum machine learning (QML) attracts growing attention as an emerging field of research to further accelerate and scale up the learning by taking advantage of quantum computation [1, 2]. Quantum computation is believed to achieve significant speedup in solving various computational problems over conventional classical computation [3, 4]. The central goal of supervised learning is, however, not solving the computational problems themselves but finding and making a correct prediction on unseen data under the supervision of given sample data [5–8]. A far-reaching milestone in the field of QML is to demonstrate the advantage of QML, i.e., an end-to-end acceleration in accomplishing this goal of learning in such a way that any possible classical learning method would never be able to achieve.

However, it has been challenging to realize this milestone due to our limited theoretical understanding of the learning tasks with the advantage of QML. Representative QML algorithms such as those in Refs. [9–14] have theoretically guaranteed upper bounds of their runtime, and it is indeed hard for existing classical algorithms to achieve the same learning tasks as these QML algorithms within a comparable runtime; nevertheless, these facts are insufficient to provably rule out the possibility of the potential existence of classical learning methods achieving the comparable runtime. For example, the quantum algorithm for recommendation systems was initially claimed to achieve an exponential speedup compared to the existing classical algorithms at the time [10], but it turned out in later research that the quantum algorithm achieves only a polynomial speedup compared to the best possible classical algorithm due to a breakthrough in designing a quantum-inspired classical algorithm for solving the same task [15]. It is possible to prove the advantage of QML in accelerating particular types of supervised learning with classical data, as shown in Refs. [16–20]; yet problematically, such learning tasks are mostly based on the quantum computational advantage of Shor's algorithms to solve integer factoring and discrete logarithms [21–23], and the techniques to prove the hardness of learning for all possible classical methods use a cryptographic argument essentially depending on the specific mathematical structure of discrete logarithms and integer factoring [5, 6, 16–20, 24], which do not straightforwardly generalize. References [18, 19] also study the advantage of QML based on more general quantum computational advantages than that of Shor's algorithms, but this technique was limited to learning problems with only polynomially many possible functions to be learned, which are learnable just by a brute-force algorithm. By contrast, of interest here are the learning problems with exponentially many possible functions to be learned, which require more efficient learning algorithms than such a brute-force approach yet commonly appear in practical machine learning. A fundamental open question in the theory of QML has been what types of quantum computational advantages, beyond that of Shor's algorithms, lead to the end-to-end quantum acceleration in solving such learning problems with exponentially many possibilities; to address this question, novel techniques need to be established to prove the classical hardness of learning beyond the realm of Shor's algorithms.

Also from a practical perspective, toward the experimental demonstration of the advantages of QML, Shor's algorithms are challenging to realize with near-term quantum technologies [25], confronting as an obstacle to the demonstration. One reason for this practical challenge is rooted in the fact that Shor's algorithms need

[*] hayata.yamasaki@gmail.com

to compete with the well-established classical algorithms for integer factoring that run only within subexponential time, which is much shorter than exponential time [26–28]. For this reason, a milestone in realizing Shor's algorithms is often set to factorize a relatively large integer, such as a 2048-bit integer [25]. On the other hand, apart from Shor's algorithms, polynomial-time quantum algorithms can also solve other types of computational problems that are potentially harder for classical algorithms, such as those relevant to topological data analysis (TDA) [29–33], BQP-complete problems [34–40], and Pell's equation [41, 42]. For the classically hard problems, one could potentially use a much smaller size of the problem instance, e.g., with much less than 2048-bit inputs, to demonstrate the quantum computational advantages. In view of this, the solution to the above open question on the relation between quantum computational advantages and the advantage of QML will also constitute a significant step to the practical demonstration as well as the fundamental understanding of QML.

In this work, we address this open question by showing that quantum advantages in computing functions *in general* lead to the provable end-to-end advantage of QML in supervised learning with classical data, even for exponentially many possible functions to be learned. Our results do not specifically depend on Shor's algorithms. In particular, using a general class of functions that can be computed efficiently in polynomial time for a large fraction of inputs by quantum algorithms but not by any classical algorithm (even under the supervision of data), we explicitly construct a family of classification tasks in a conventional setting of supervised learning from classical sample data, i.e., in a probably approximately correct (PAC) learning model [5, 6, 43]. This classification task may require finding a correct classifier function among exponentially many possibilities for labeling the input data. We construct a polynomial-time quantum algorithm for solving our learning task using a polynomial amount of classical sample data. This quantum algorithm is simply implementable by a variant of the conventional learning method: feature mapping by quantum computation to map the input classical data into the corresponding bit strings representing their features, followed by linear separation by classical computation to find an appropriate hyperplane in the feature space to achieve the classification. At the same time, we prove that no polynomial-time classical algorithm can accomplish this learning task. Furthermore, we provide a protocol for preparing the classical sample data to demonstrate this advantage of QML in the experiments. These results open vast opportunities for anyone to use a general class of quantum algorithms of their favorite to achieve provably advantageous QML over any classical learning method even for the learning problems with exponentially many possibilities, progressing beyond the previous approach in Refs. [16–20].

Formulation of learning tasks.— We describe the setting of learning and the formulation of our learning task. Our analysis is based on a conventional setting of supervised learning, i.e., the PAC learning model [5, 6, 43]. See Methods on the definition of the PAC learning model.

Following the convention of the PAC learning, we formulate our concept class $\mathcal{C}_N$, i.e., a set of functions $c \in \mathcal{C}_N$ to be learned, which classify an N-bit input x coming from a target probability distribution $\mathcal{D}_N$ into binary-labeled categories specified by $c(x) = 0$ or $c(x) = 1$. Our formulation is in line with a conventional learning approach based on feature mapping and linear separation (Fig. 1). In this approach, the learning algorithm first maps an input x to another vector $f(x)$ and subsequently classifies x in the space of $f(x)$. This mapping f is known as a feature map, transforming x in the input space into the corresponding feature $f(x)$ in the feature space that encapsulates essential information for the classification. The sets of x satisfying $c(x) = 0$ and $c(x) = 1$ are mapped into $\mathcal{F}_0$ and $\mathcal{F}_1$ of $f(x)$, respectively. The feature map here should be designed so that $\mathcal{F}_0$ and $\mathcal{F}_1$ have linear separability, i.e, the property that a hyperplane in the feature space should be able to distinguish between $\mathcal{F}_0$ and $\mathcal{F}_1$ [44]. More formally, there should exist a vector s in the feature space and a threshold t such that

$$f(x) \cdot s \leq t \text{ for } c(x) = 0; \quad f(x) \cdot s > t \text{ for } c(x) = 1. \tag{1}$$

The equation $f(x) \cdot s = t$ represents the hyperplane to separate $\mathcal{F}_0$ and $\mathcal{F}_1$ specified by the unknown target concept c to be learned. The concept class of c is learnable by converting the given input samples using the feature map, followed by finding this hyperplane, i.e., its parameter s, using the corresponding output samples. Once we find s, for a new input x drawn from $\mathcal{D}_N$, we can make a correct prediction of $c(x)$ by evaluating a hypothesis $h(x)$ in a hypothesis class, which classifies x based on the value of $f(x) \cdot s$.

Based on this approach, we construct our concept class $\mathcal{C}_N = \{c_s\}_s$ parameterized by s in the vector space $\mathbb{F}_2^D$ over a finite field, where $\mathbb{F}_2 = \{0, 1\}$ is the finite field representing a bit, and D is the dimension of the feature space $\mathbb{F}_2^D$. Each concept c_s is a function from the input space $\{0, 1\}^N$ to binary labels $\{0, 1\}$. With some choice of the feature map $f_N : \{0, 1\}^N \to \mathbb{F}_2^D$, we here define c_s as

$$c_s(x) := f_N(x) \cdot s \in \mathbb{F}_2 = \{0, 1\}, \tag{2}$$

where $f_N(x) \cdot s$ is the bitwise inner product in $\mathbb{F}_2^D$. This concept class is designed in accordance with the convention in machine learning based on feature mapping and linear separation as in (1), yet using the finite fields as the feature space (i.e., $f_N(x) \cdot s = t := 0$ or $f_N(x) \cdot s = 1$).

Advantage of QML from general quantum computational advantages.— To seek the advantage of QML, we study our concept class in (2) with an appropriate choice of the feature map f_N. Remarkably, for our concept class, we show that f_N can be arbitrarily chosen from, roughly speaking, a general class of functions that can be computed efficiently within a polynomial time by quantum

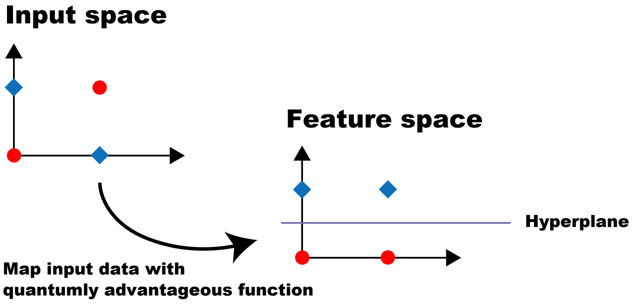


FIG. 1. A conventional learning approach based on feature mapping and linear separation, which our work also follows. Inputs x in the input space (red circles with output labels $c(x)=0$ and blue squares with $c(x)=1$) are mapped into the corresponding features $f(x)$ in the feature space by a feature map f. Then, using the features $f(x)$ of the input samples and the corresponding output samples $c(x)$, we find a hyperplane linearly separating the sets of features for $c(x)=0$ and $c(x)=1$ as in (1) to achieve the learning. In our learning tasks, we use quantumly advantageous functions as f.

algorithms but not by classical algorithms. In the following, we introduce this general class of functions for f_N, followed by describing how the advantage of QML emerges from this general quantum advantage in computing f_N.

Under a target distribution $\mathcal{D}_N$, we choose the feature map f_N to be any function in a general class denoted by

$$\{(f_N,\mathcal{D}_N)\}_N \in \mathsf{HeurFBQP}\setminus(\mathsf{HeurFBPP/rpoly}), \qquad (3)$$

as defined more precisely in the following (see also Supplementary Information for more details). We call a function in this class a *quantumly advantageous function* under $\mathcal{D}_N$.

In (3), we require that $f_N(x)$ should be efficiently computable by a quantum algorithm for a large fraction of x drawn from $\mathcal{D}_N$, and the set $\mathsf{HeurFBQP}$ of pairs of the function f_N and the distribution $\mathcal{D}_N$ represents those satisfying this requirement. In the computational complexity theory, a (worst-case) complexity class FBQP [45] conventionally represents a set of functions $f_N(x)$ that is efficiently computable by a quantum algorithm for all x even for the worst-case input [1], but for PAC learning, it suffices to work on a *heuristic* complexity class $\mathsf{HeurFBQP}$ that requires the efficiency not all but only a large fraction of x [46, 47]. More precisely, $\{(f_N,\mathcal{D}_N)\}_N \in \mathsf{HeurFBQP}$ requires that there exists a quantum algorithm $\mathcal{A}(x,\mu,\nu)$ that should run, for any N and $0<\mu,\nu<1$, within a polynomial runtime $O(\mathsf{poly}(N,1/\mu,1/\nu))$ to output $f_N(x)$ correctly for a large fraction $1-\mu$ of inputs x drawn from $\mathcal{D}_N$ with a high probability at least $1-\nu$, i.e.,

$$\Pr_{x\sim\mathcal{D}_N}\left[\Pr\left[\mathcal{A}(x,\mu,\nu)=f_N(x)\right]\geq 1-\nu\right]\geq 1-\mu, \qquad (4)$$

where the inner probability is taken over the randomness of $\mathcal{A}$.

At the same time, in (3), we require that $f_N(x)$ should not be efficiently computable by any classical (randomized) algorithm for the large fraction of x even with the help of the sample data, and to meet this requirement, it suffices to consider the relative complement of the set $\mathsf{HeurFBPP/rpoly}$ as in (3). In the complexity theory, $\mathsf{HeurFBPP}$ can be considered to be the classical analog of $\mathsf{HeurFBQP}$ while FBPP the classical analog of FBQP, indicating that the functions $f_N(x)$ are efficiently computable from the given input x by a classical randomized algorithm. Additionally, in the setting of PAC learning, the sample data are also initially given apart from x. The use of the sample data is not necessarily limited to the learning, but the data may also potentially help the classical algorithm to compute $f_N(x)$ itself more efficiently [18, 19, 48]. The parameters of hypotheses learned from the data given according to a data distribution can be seen as a random bit string of polynomial length $O(\mathsf{poly}(N,1/\mu,1/\nu,1/\xi))$ that could potentially make the computation more efficient with a high probability at least $1-\xi$, known as the randomized advice string α in the complexity theory [49]. To address this issue, we require that $f_N(x)$ should remain hard to compute by any classical algorithm even with an arbitrary polynomial-length randomized advice string α. More precisely, $\{(f_N,\mathcal{D}_N)\}_N \notin \mathsf{HeurFBPP/rpoly}$ requires that no classical (randomized) algorithm $\mathcal{A}(x,\alpha,\mu,\nu,\xi)$ with a randomized advice $\alpha\sim\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}$ of length $O(\mathsf{poly}(N,1/\mu,1/\nu,1/\xi))$ sampled from an advice distribution $\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}$ should run, for any N and $0<\mu,\nu,\xi<1$, in a polynomial time $O(\mathsf{poly}(N,1/\mu,1/\nu,1/\xi))$ to output $f_N(x)$ correctly with a high probability at least $1-\nu$ for a large fraction $1-\xi$ of α for a large fraction $1-\mu$ of x from $\mathcal{D}_N$, i.e.,

$$\Pr_{x\sim\mathcal{D}_N}\left[\Pr_{\alpha\sim\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}}\left[\Pr\left[\mathcal{A}(x,\alpha,\mu,\nu,\xi)=f_N(x)\right]\right.\right.$$
$$\left.\left.\geq 1-\nu\right]\geq 1-\xi\right]\geq 1-\mu, \qquad (5)$$

where the most inner probability is taken over the randomness of $\mathcal{A}$. The previous work on the advantage of QML [16–20] used a cryptographic argument specifically depending on discrete logarithms and integer factoring to prove the classical hardness of their learning tasks, but we here identify that we can use the heuristic complexity class $\mathsf{HeurFBPP/rpoly}$ to rule out the existence of polynomial-time classical learning algorithms for our learning tasks. Note that the heuristic complexity class was also used in Refs. [18, 19] for providing conditions

[1] Note that Ref. [45] defines FBQP as a class of search problems, i.e., computation of functions having a set of multiple outputs for each input, but we consider f_N to have a single output $f_N(x)$ for each input x.

of the concept classes that offer the advantage of QML, but their results were limited to polynomial-size concept classes learnable by a brute-force algorithm that just tries all the concepts in the concept class; by contrast, we here apply the heuristic complexity class to the computation of feature maps, which makes it possible to construct exponential-size concept classes beyond the reach of such a brute-force approach.

Our main result proves that for *any* choice of the quantumly advantageous functions f_N in (3), our exponential-size concept class in (2) leads to the advantage of QML. In particular, the main result is summarized as follows. (See also Methods for the more precise definitions of the efficient learnability of the concept and the efficient evaluatability of the hypothesis.)

Theorem 1 (Advantage of QML from general computational advantages)**.** *Under any target distribution $\mathcal{D}_N$ over N-bit inputs, for any quantumly advantageous function f_N under $\mathcal{D}_N$, the concept class $\mathcal{C}_N$ defined in (2) with f_N is quantumly efficiently learnable, and for this $\mathcal{C}_N$, we can construct a quantumly efficiently evaluatable hypothesis class. By contrast, $\mathcal{C}_N$ is not classically efficiently learnable by any classically efficiently evaluatable hypothesis class.*

Importantly, Theorem 1 establishes the advantage of QML in supervised learning with exponential-size concept classes using arbitrary quantumly advantageous functions, in contrast with the fact that the existing techniques for proving the advantage of QML [16–20] were limited to using the advantage of Shor's algorithms. In Methods, to prove Theorem 1, we explicitly construct polynomial-time quantum algorithms for learning the concept and evaluating the hypothesis; at the same time, we prove that no classical algorithm can evaluate hypotheses that correctly predict the concepts in our concept class.

For our concept, the quantum algorithms for the learning and the evaluation are implementable by the simple approach of feature mapping and linear separation: in our case, the feature mapping uses the quantum algorithm in (4), and the linear separation is performed only by classical computing. A technical challenge in constructing our algorithms is that the learning algorithm does not necessarily find the true parameter s of the target concept c_s but may output an estimate $\tilde{s}$ with $\tilde{s} \neq s$; nevertheless, our analysis shows that the parameter $\tilde{s}$ learned by our algorithm leads to a correct hypothesis $h_{\tilde{s}}$ satisfying $h_{\tilde{s}}(x) = c_s(x)$ for a large fraction of x with high probability (see Methods for details).

The feature mapping and the linear separation may also be applicable to some of the previous works on the advantage of QML [16], but a more crucial difference arises from the techniques for proving the classical hardness. In particular, a feature map constructed in Ref. [16] used Shor's algorithms to transform an N-bit input into a feature in a feature space, which was taken as a space of functions called the reproducing kernel Hilbert space (RKHS) in the kernel method [7, 8] to show a polynomial-time quantum learning algorithm. However, the existing techniques for proving the classical hardness of such learning tasks needed to use a cryptographic argument on the hardness of solving computational problems depending on the specific mathematical structure of discrete logarithms and integer factoring [5, 6, 16–20, 24] and do not straightforwardly generalize. By contrast, we develop techniques for analyzing our learning task with its feature space formulated as the vector space over a finite field, making it possible to prove the classical hardness for any quantumly advantageous function in general (see Methods for details).

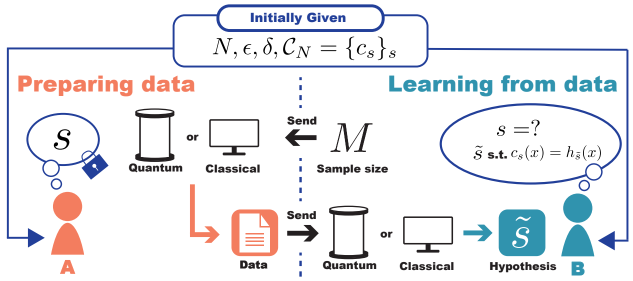


FIG. 2. A setup for demonstrating the advantage of QML in supervised learning by two parties A and B, where A is in charge of preparing the classical sample data, and B receives the data from A to perform the learning. The parties A and B are initially given the problem size N, the error parameter ϵ, the significance parameter δ, and the concept class $\mathcal{C}_N = \{c_s\}_s$ in (2) by choosing the feature map as a quantumly advantageous function f_N. The party A chooses a D-bit parameter s of the target concept c_s, which is kept as A's secret. To learn c_s, the party B decides the number M of sample data to be used for B's learning and lets A know M. Then, A prepares M input-output sample data as described in the main text and sends the data to B. Using the given data, B performs the algorithms in Theorem 1 to find a D-bit string $\tilde{s}$ and make a prediction for new inputs x by the hypothesis $h_{\tilde{s}}(x) = f_N(x) \cdot \tilde{s}$ so that the error in estimating true $c_s(x)$ should be below ϵ with high probability at least $1 - \delta$.

Lastly, due to the generality of the quantumly advantageous functions, Theorem 1 opens unprecedented opportunities for realizing the provable advantages of QML in supervised learning beyond the realm of Shor's algorithms, e.g., in the fields relevant to TDA [29–33], BQP-complete problems [34–40], and Pell's equation [41, 42]. See Methods for more details.

Protocol for preparing classical sample data for the experimental demonstration.— To embody the opportunities of demonstrating the advantage of QML in experiments, we clarify the protocol for preparing the classical sample data for our concept class $\mathcal{C}_N$ in (2).

For the demonstration, we consider a two-party setting, where a party A is in charge of preparing the classical sample data, and the other party B receives the data from A to perform the learning (Fig. 2). Initially, A and B are given the problem size N, the error parameter ϵ, and the significance parameter δ. Let $\mathcal{D}_N$ be a target distribution, and suppose that A can load a sequence of inputs x sampled from $\mathcal{D}_N$ (e.g., from some input data storage), with each x loadable in a unit time. Note that the exact description of the true distribution $\mathcal{D}_N$ may be unknown to both A and B throughout the learning. In addition, A and B are given the concept class $\mathcal{C}_N$ determined by choosing the feature map f_N as a quantumly advantageous function under $\mathcal{D}_N$. Given this initial setup, B decides the number $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ of sample data to be used for B's learning and lets A know M (see Supplementary Information for the precise choice of M). Then, A chooses the parameter $s \in \mathbb{F}_2^D$ of the target concept $c_s \in \mathcal{C}_N$ arbitrarily (e.g., by sampling s uniformly at random). For the given M and this choice of c_s, A is in charge of preparing M input-output pairs of sample data and giving the data to B while keeping s as A's secret. The task for B is to find a vector $\tilde{s} \in \mathbb{F}_2^D$ using the M data sent from A and make a prediction for new inputs x drawn from $\mathcal{D}_N$ by the hypothesis $h_{\tilde{s}}(x) = f_N(x) \cdot \tilde{s}$ so that the error in estimating true $c_s(x)$ should be below ϵ with high probability at least $1 - \delta$.

For A, we propose a data-preparation protocol using quantum computation in the same way as B using quantum computation for learning, while we will also discuss another protocol using only classical computation later. To prepare the data, A first loads M inputs $x_1, \ldots, x_M$ drawn from $\mathcal{D}_N$. Then, using the quantum algorithm (4) for computing f_N, A prepares the corresponding M outputs denoted by $\mathcal{A}(x_1), \ldots, \mathcal{A}(x_M)$. While the outputs $\mathcal{A}(x)$ may not always be the same as $f_N(x)$ due to the randomness of the quantum algorithm, our analysis shows that, with an appropriate choice of parameters μ and ν in (4), A can make the error in these M outputs negligibly small by only using a polynomial time of quantum computation (see Supplementary Information for details). Finally, A send $\{x_m, \mathcal{A}(x_m)\}_{m=1}^{M}$ to B as the M data.

Note that in the previous work on the advantage of QML based on Shor's algorithms [16–20], the data for their learning tasks were able to be prepared by classical computation, but we here put A and B on equal footing by allowing both to compute f_N by quantum computation. In the previous work, the data were prepared by assuming a special property of cryptographic primitives (i.e., *classically one-way* permutation, which is hard to invert efficiently by classical computation but is invertible efficiently by quantum computation). In Supplementary Information, we show that the data preparation for our concept class is also possible by only using classical computation if we construct f_N using the classically one-way permutations.

Then, the protocol for achieving B's task reduces to running the quantum learning and evaluation algorithms in Theorem 1. To compare these quantum algorithms with classical algorithms, we also propose to perform B's task by only using classical computation for several small problem sizes N. In particular, from the (superpolynomial) runtimes of classically computing f_N for the several choices of small N, we propose to perform extrapolation to estimate the constant factors in the (superpolynomial, potentially exponential) scaling of the runtime of this classical method for larger N. The demonstration of the advantage of QML is successfully achieved by realizing the polynomial-time quantum algorithms in experiments for an appropriate choice of N to outperform the classical algorithms with the estimated superpolynomial runtime.

Discussion and outlook.— In this work, we have proved that a general class of quantum advantages in computing functions, characterized by $\mathsf{HeurFBQP} \setminus (\mathsf{HeurFBPP/rpoly})$ in (3), lead to the end-to-end advantage of QML in a task of supervised learning with classical data, even for exponentially many possible functions to be learned. We have clarified the polynomial-time quantum algorithms to find and make a correct prediction and have also proved the hardness of this learning task for any possible polynomial-time classical method. Whereas such advantage of QML was shown only for specific cases of using the advantage of Shor's algorithms in previous research [16–20], our results make it possible to use the general quantum advantages in computing functions beyond that of Shor's algorithms, such as those relevant to topological data analysis (TDA), BQP-complete problems, and Pell's equation. Furthermore, we propose protocols to prepare the classical sample data for the experimental demonstration of this advantage of QML. These results solve the fundamental open question about characterizing which types of quantum computational advantages lead to the advantage of QML in accelerating supervised learning, making it possible to exploit all the quantumly advantageous functions for QML.

Our results also constitute a significant step toward the practical demonstration of the advantage of QML in experiments. For implementation with near-term quantum technologies, heuristic QML algorithms have been studied widely [50–53], but no analysis provides a classically hard (yet quantumly feasible) instance of the learning tasks; even more problematically, no analysis provides bounds of the runtime and the success probability of these heuristic QML algorithms. In different settings, advantages of using quantum computation have been shown in a learning setting with quantum data obtained from quantum experiments [54–59] and also in a distribution learning setting [60–62]; still, it is not straightforward to apply these quantum algorithms to accelerate the common learning tasks in the era of big data, as represented by supervised learning from classical data. By contrast, our approach offers a QML framework that can address this type of learning task. A merit of our QML framework is that it is simply implementable by using any quantumly advantageous function for feature mapping, followed by classically performing linear separation in the feature space, which our framework takes as the space of bit strings representing features.

Also from a broader perspective, in applications of machine learning, state-of-the-art classical learning methods such as deep learning heuristically design the feature maps, e.g., by adapting the architectures of deep neural networks [63]. The theoretical analysis of optimized choices of feature maps for given data is challenging even in classical cases, but empirical facts suggest that the classification tasks for real-world data often reduce to applying feature maps designed by such artificial neural networks followed by linear separation [63]. In view of the success of the artificially designed feature maps, it is crucial to allow as large classes of functions as possible to create more room for the heuristic optimization of the feature maps. Advancing ahead, our QML framework makes it possible to design the feature maps flexibly, using arbitrary quantumly advantageous functions to attain the provable advantage of QML. It also turns out that a large dimension of the feature space is not even a prerequisite for the advantage of QML in our framework, as opposed to a common yet unproven folklore on the potential relevance of large dimension [50–53]; after all, we have proved that the advantage of QML stems solely from the quantum advantages in computing functions without any further requirement for their mathematical structure. Toward the demonstration of the advantage of QML, an experimental challenge still remains in seeking how to realize quantum computation to surpass the capability of classical computation, and yet our QML framework opens a way to transcend all possible classical learning methods by exploiting *any* realization of quantumly advantageous functions for the feature maps.

ACKNOWLEDGEMENTS

We acknowledge Casper Gyurik and Vedran Dunjko for the discussion and comments. This work was supported by JST PRESTO Grant Number JPMJPR201A, JPMJPR23FC, JSPS KAKENHI Grant Number JP23K19970, and MEXT Quantum Leap Flagship Program (MEXT QLEAP) JPMXS0118069605, JPMXS0120351339. This work was supported by JST PRESTO Grant Number JPMJPR201A, JPMJPR23FC, JSPS KAKENHI Grant Number JP23K19970, and MEXT Quantum Leap Flagship Program (MEXT QLEAP) JPMXS0118069605, JPMXS0120351339.

AUTHOR CONTRIBUTIONS

H.Y. and N.I. contributed equally to this work. H.Y., N.I., and M.M. contributed to the conception of the work. H.Y. and N.I. contributed to the analysis and interpretation in the work and the preparation of the initial draft. H.Y., N.I., and M.M. contributed to the revision of the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary Information is available for this paper. Correspondence and requests for materials should be addressed to Hayata Yamasaki.

METHODS

In Methods, we summarize the probabilistically approximately correct (PAC) learning model, sketch the proof of our main result, i.e., Theorem 1 in the main text, and provide examples of new directions of quantum machine learning (QML) based on Theorem 1.

Throughout the paper, we use the following notations. Let $\mathbb{N}$ be the set of all natural numbers $1, 2, \ldots$. Let $\mathbb{F}_2 = \{0, 1\}$ denote the finite field of order 2, i.e., for $0, 1 \in \mathbb{F}_2$,

$$\begin{aligned} 0+0&=0, & 0\times 0&=0,\\ 0+1&=1, & 0\times 1&=0,\\ 1+0&=1, & 1\times 0&=0,\\ 1+1&=0, & 1\times 1&=1. \end{aligned} \tag{6}$$

Note that $\{0, 1\}$ and $\mathbb{F}_2$ may be the same set, but we will use $\mathbb{F}_2$ for representing the feature space, where we use the bitwise arithmetics in (6), while we will use $\{0, 1\}$ in the other cases. Let $\mathsf{poly}(x)$ denote a polynomial of x. Unless otherwise stated, we use N as the length of input bit strings for a family of computational problems. For a probability distribution $\mathcal{D}$ over the set $\mathcal{X}$, we denote by $x \sim \mathcal{D}$ to mean that x is drawn from the distribution $\mathcal{D}$. A probability $\mathbf{Pr}_{x\sim\mathcal{D}}[\cdots]$ indicates that the probability is taken for the random draw of x according to distribution $\mathcal{D}$.

PAC learning model.— We summarize the definition of the PAC learning model based on Ref. [6]. See also Supplementary Information for further details.

In the PAC learning model, for a problem size N, a specification of a set of functions $\mathcal{C}_N$, called a concept class, is initially given. Each function $c \in \mathcal{C}_N$ is called a concept, which maps an N-bit input x to a Boolean-valued output $c(x) \in \{0, 1\}$ (i.e., a label of x in classification). For some unknown choice of a concept $c \in \mathcal{C}_N$ called the target concept, the learning algorithm is given a polynomial number of samples $\{x_m, c(x_m)\}_{m=1}^{M}$, which are pairs of inputs with each x_m drawn from a target probability distribution $\mathcal{D}_N$ and the corresponding outputs $c(x_m)$. Note that the previous work [16–19] on the advantage of QML studied a restricted setting that only allows for uniform distribution in the choice of the target distribution $\mathcal{D}_N$, but in our work, $\mathcal{D}_N$ can be an arbitrary distribution over the N bits without this restriction. Using the given sample data, the learning algorithm is designed to find a function, termed a hypothesis h, from a set $\mathcal{H}_N$ of functions called a hypothesis class, so as to make a correct prediction on c by h.

In the PAC learning model, the ability to find the correct hypothesis for the target concept using the given samples is called the learnability of a concept class under a target distribution [6]. In particular, for the problem size N, the error parameter $\epsilon > 0$, and a confidence parameter $\delta > 0$, a concept class $\mathcal{C}_N$ is *quantumly (classically) efficiently learnable* under $\mathcal{D}_N$ if there exists a quantum (classical randomized) learning algorithm $\mathcal{A}$ that finds a hypothesis h such that

$$\mathrm{error}(h) \coloneqq \mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}[h(x) \neq c(x)] < \epsilon. \tag{7}$$

with high probability at least $1-\delta$, using a polynomial number of samples $\{x_m, c(x_m)\}_{i=1}^{M}$ ($M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$) within a polynomial time complexity $t_{\mathcal{A}} = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ (see also Supplementary Information for more details).

The ability to efficiently evaluate the hypothesis identified from the samples is also crucial in the PAC learning model, which is called evaluatability [6]. By definition of the learnability, the learned hypothesis may inevitably have some error on a nonzero fraction ϵ of x drawn from $\mathcal{D}_N$, and the definition of evaluatability here also inherits this point. In particular, for $\epsilon, \delta > 0$, we say that a hypothesis class $\mathcal{H}_N$ is *quantumly (classically) efficiently evaluatable* under $\mathcal{D}_N$ if, given a hypothesis h, there exists a quantum (classical randomized) evaluation algorithm $\mathcal{A}$ that can compute $h(x)$ for a large fraction $1-\epsilon$ of new inputs x drawn from $\mathcal{D}_N$ with high probability at least $1-\delta$ in terms of the randomness of the (randomized) algorithm $\mathcal{A}$, within a polynomial time complexity $t_{\mathcal{A}} = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ (see also Supplementary Information for more details).

Quantum learning and evaluation algorithms and classical hardness for our concept class.— Within the PAC learning model, we sketch the proof of our main result, i.e., Theorem 1 in the main text. In particular, for our concept class, we construct a polynomial-time quantum algorithm for learning the concept to output the corresponding hypothesis in a hypothesis class. Then, we also construct a polynomial-time quantum algorithm for evaluating the hypothesis in the hypothesis class. Finally, we prove the hardness of the evaluation of the hypotheses in the hypothesis class for any possible polynomial-time classical algorithm. See also Supplementary Information for more details.

Our quantum learning algorithm starts with using a quantum algorithm $\mathcal{A}$ in (4) to compute the feature map $f_N(x_m)$ for each of the given samples $\{(x_m, c_s(x_m))\}_{m=1}^{M}$. Note that the features output by $\mathcal{A}$, denoted by $\{\mathcal{A}(x_m)\}_{m=1}^{M}$, may not exactly coincide with the features $\{f_N(x_m)\}_{m=1}^{M}$ in general due to the randomness of the quantum algorithm, but our analysis shows that the learning algorithm can feasibly make the failure probability negligibly small. Our learning algorithm then classically performs Gaussian elimination to solve a system of linear equations for a variable $\tilde{s} \in \mathbb{F}_2^D$

$$\begin{aligned} \mathcal{A}(x_1)\cdot\tilde{s} &= c_s(x_1),\\ \mathcal{A}(x_2)\cdot\tilde{s} &= c_s(x_2),\\ &\vdots\\ \mathcal{A}(x_M)\cdot\tilde{s} &= c_s(x_M), \end{aligned} \tag{8}$$

subsequently outputting a solution $\tilde{s}$ as an estimate of the parameter of the hypothesis. For $\tilde{s}$, we construct the hypothesis $h_{\tilde{s}}$ by

$$h_{\tilde{s}}(x) \coloneqq f_N(x)\cdot\tilde{s}. \tag{9}$$

A technical challenge in our construction of the learning algorithm arises from the fact that the solutions $\tilde{s}$ of the system of the linear equations in (8) may not be unique. After all, we work on a general setting allowing any target distribution $\mathcal{D}_N$, any quantumly advantageous function f_N, and any quantum algorithm $\mathcal{A}$ to compute f_N approximately as in (4); thus, it may happen that

$$\tilde{s} \neq s. \tag{10}$$

For the worst-case input $x \in \{0,1\}^N$, it may indeed happen that

$$h_{\tilde{s}}(x) \neq c_s(x). \tag{11}$$

It is thus nontrivial to prove that the hypothesis $h_{\tilde{s}}$ given by (9) can predict the target concept c_s correctly as required for the learnability. We nevertheless prove that any of the solutions $\tilde{s}$ of (8) (even if (10) is the case) leads to a correct hypothesis

$$h_{\tilde{s}}(x) = c_s(x) \tag{12}$$

for a large fraction of input x drawn from $\mathcal{D}_N$ with a high probability. In other words, our analysis proves that the fraction of x causing (11) can be made negligibly small by our polynomial-time quantum learning algorithm, leading to the quantumly efficient learnability of our concept class (see Supplementary Information for details).

As for the quantum algorithm for evaluating the hypothesis, with the parameter $\tilde{s}$ learned, the evaluation algorithm aims to estimate $f_N(x)\cdot\tilde{s}$ in (9). For a new input x drawn from $\mathcal{D}_N$, our evaluation algorithm simply uses the quantum algorithm $\mathcal{A}$ in (4) to compute $\mathcal{A}(x)$, i.e., an estimate of $f_N(x)$. The output $\mathcal{A}(x)$ of $\mathcal{A}$ may be different from $f_N(x)$ in general due to the randomness of the quantum algorithm, but we show that the error can be made negligibly small within a polynomial time. Then, our algorithm takes the (bitwise) inner product of $\mathcal{A}(x)$ and the given parameter $\tilde{s}$, which we prove leads to a correct evaluation of $h(x)$ for a large fraction of input x with a high probability, leading to the quantumly efficient evaluatability (see Supplementary Information for details).

Finally, the classical hardness is proved by contradiction, as with the established arguments in the computational learning theory [5, 6]. In particular, we prove that if all concepts $c_s(x)$ ($s \in \mathbb{F}_2^D$) of our concept class in (2) were classically efficiently learnable by some hypotheses $h_s(x)$ that are classically efficiently evaluatable by polynomial-time classical algorithms, then the feature map $f_N(x)$ in (2) would be computed by a polynomial-time classical algorithm using these classical evaluation algorithms, contradicting to the assumption that f_N is a quantumly advantageous function. To prove the classical hardness of learning for the exponential-size concept classes as in our case, the previous work on the advantage of QML relied on a cryptographic argument that specifically depends on Shor's algorithms [16–20]; by contrast, our proof technique developed here does not depend on such a specific property of Shor's algorithms but is applicable to any quantumly advantageous function in general.

For this development, our key idea is to use the property of the vector space $\mathbb{F}_2^D$ over the finite field used as the feature space in our construction. In particular, for the standard basis $\{s_d\}_{d=1}^D$ of this D-dimensional vector space $\mathbb{F}_2^D$ (i.e., $s_1 = (1,0,\ldots,0,0)^\top, \ldots, s_D = (0,0,\ldots,0,1)^\top$), suppose that the concepts $c_{s_d}(x)$ for $d = 1,\ldots,D$ are efficiently learnable by classically efficiently evaluatable hypotheses $h_{s_d}(x)$. Then, observing that the bitwise inner product $c_{s_d}(x) = f_N(x) \cdot s_d$ yields the dth bit of $f_N(x)$, we use the corresponding hypotheses $h_{s_d}(x)$ to construct an estimate of $f_N(x)$ as

$$\tilde{f}_N(x) = \begin{pmatrix} h_{s_1}(x) \\ h_{s_2}(x) \\ \vdots \\ h_{s_D}(x) \end{pmatrix} \in \mathbb{F}_2^D. \tag{13}$$

Thus, the polynomial-time classical algorithms for evaluating the hypotheses would be able to compute each element of this vector and thus approximate $f_N(x)$ well with high probability, which contradicts the fact that f_N is a quantumly advantageous function. Therefore, our concept class that includes the concepts $c_{s_d}(x)$ for $d = 1,\ldots,D$ is not classically efficiently learnable by any classically efficiently evaluatable hypothesis class (see Supplementary Information for details).

New directions of QML based on quantumly advantageous functions.— Our results in Theorem 1 of the main text open unprecedented opportunities for using a variety of quantum algorithms to demonstrate the advantage of QML, progressing beyond Shor's algorithms. We here propose several promising candidates of such quantum algorithms relevant to the following different areas.

1. *Topological data analysis (TDA).*— Quantum algorithms for computing an estimation of normalized Betti numbers and other topological invariants [29–33] gather considerable attention due to their potential applications to TDA, an area of data science using mathematical tools on topology. The functions computed by these quantum algorithms are leading candidates of the quantumly advantageous functions since techniques for proving the computational hardness are also known in multiple relevant cases under conventional assumptions in the complexity theory [64–69]. Classical sample data given in terms of bit strings can also be used as the input to some of these quantum algorithms, without necessarily using oracles for the input to these algorithms; for example, given N input points constituting a Vietoris-Rips (VR) complex, the quantum algorithm in Ref. [30] computes an approximation of the normalized persistent Betti number with accuracy $O(1/\mathsf{poly}(N))$ with probability at least $1-O(1/\mathsf{poly}(N))$. In this case, the function that this quantum algorithm computes can be used as a feature map $f_N : \{0,1\}^{O(\mathsf{poly}(N))} \to \mathbb{F}_2^{O(\log(N))}$, from which we can construct our concept class according to (2). Note that the normalized persistent Betti number may have a different value from the (original) persistent Betti number due to the normalization factor, but independently of such mathematical structure, our results lead to the advantage of QML for our concept class.

2. *BQP-complete problems.*— It is indeed a variant of long-standing open problems in the complexity theory to prove the existence of the quantumly advantageous functions unconditionally without any computational hardness assumption; however, a natural candidate for the quantumly advantageous functions is the functions relevant to the hardest problems in the scope of the polynomial-time quantum algorithms, known as BQP-complete problems [34–40]. For instance, the function used for the local unitary-matrix average eigenvalue (LUAE) problem in Ref. [35] yields such a candidate. Given an N-bit string b and a $O(\mathsf{poly}(N))$-bit string representing an $O(\mathsf{poly}(N))$-size quantum circuit to implement a $2^N \times 2^N$ unitary matrix U, let $\{\lambda_j\}_j$ denote the set of eigenvalues of U with the corresponding set $\{|\nu_j\rangle\}_j$ of eigenvectors. Then, the LUAE problem involves computation of an estimate of the average eigenvalue $\bar{\lambda} = \sum_{j=1}^{2^N} |\langle b|\nu_j\rangle|^2 \lambda_j$ up to precision $O(1/\mathsf{poly}(N))$ with probability at least $1 - O(1/\mathsf{poly}(N))$ [35]. Thus, the function to be computed in the LUAE problem provides a feature map $f_N : \{0,1\}^{O(\mathsf{poly}(N))} \to \mathbb{F}_2^{O(\log(N))}$, from which we can construct our concept class according to (2). We remark that this construction is based on the worst-case complexity class BQP, but for our concept class, we can indeed choose f_N based on the hardest problems in the heuristic complexity class HeurFBQP, which is potentially even broader than the worst-case complexity class. Also note that Refs. [18, 19] considered using instances of BQP-

complete problems themselves as the polynomial-size concept classes that provide the advantage of QML, but since their construction uses BQP-complete problems directly as the concept classes, the connection between quantum advantages in the learning of concept classes and the computation of functions was elusive; by contrast, our contribution is to bridge this connection by using quantumly advantageous functions appearing in the BQP-complete problems to introduce new, different concept classes.

3. *Cryptographic problems beyond the scope of Shor's algorithms.*— Shor's algorithms [21–23] stand as polynomial-time quantum algorithms to solve integer factoring and discrete logarithms relevant to Rivest–Shamir–Adleman (RSA) cryptosystem [70], and no existing classical algorithm can solve these problems within a polynomial time. But it still remains an unsolved open problem whether these are hard to compute for any possible polynomial-time classical algorithm apart from the existing ones. If an efficient classical algorithm for solving these problems were found in the future, the previously known advantage of QML depending on Shor's algorithms would also cease to survive. Even in such a case, our results open a chance that the advantage of QML can still survive based on another cryptographic problem that can be harder than those solved by Shor's algorithms. For example, given an N-bit nonsquare positive integer d for Pell's equation $x^2 - dy^2 = 1$, the first $O(\mathsf{poly}(N))$ digits of $\ln\left(x_1 + y_1\sqrt{d}\right)$ for its least positive solution (x_1, y_1) can be computed with a high probability exponentially close to one by a polynomial-time quantum algorithm [41, 42]; at the same time, even if one has a polynomial-time classical algorithm for solving integer factoring and discrete logarithms, it is unknown if one can obtain a polynomial-time classical algorithm for this computation, which is relevant to a key exchange system based on the principal ideal problem [71] (see Refs. [41, 42] for details). This computations yields a feature map $f_N : \{0,1\}^N \to \mathbb{F}_2^{O(\mathsf{poly}(N))}$, from which we can construct our concept class according to (2). This construction provides an example of exponential-size concept classes in N leading to the advantage of QML without depending on the computational advantage of Shor's algorithms, which has been challenging to establish as long as one uses techniques in the existing work [16–20].

DATA AVAILABILITY

No data is used in this study.

CODE AVAILABILITY

No code is used in this study.

SUPPLEMENTARY INFORMATION

Supplementary Information of "Advantage of Quantum Machine Learning from General Computational Advantages" is organized as follows. Section A gives settings and definitions of a learning model and quantum computational advantage. Section B provides our learning task and proof of the advantage of quantum machine learning (QML) in solving our learning task. Section C describes a setup for demonstrating this advantage of QML and presents protocols for preparing the classical sample data for the demonstration.

Appendix A: Setting and definition

In this section, we present settings and definitions relevant to our work. In Section A 1, we define a model of probably and approximately correct (PAC) learning [5, 6, 43] to be analyzed in this work and also define the advantage of QML. In Section A 2, we define quantum advantages in computing a function, which we will use to show the advantage of QML.

1. PAC learning model

The analysis in our work will be based on a conventional model of learning called the PAC learning model in Ref. [6]. Let $\mathcal{D}_N$ be any unknown target probability distribution supported on an input space $\mathcal{X}_N \subseteq \{0,1\}^N$ of N bits. In our work, a concept class $\mathcal{C}_N$ over $\mathcal{X}_N$ is a set of functions from the input space to the set of binary labels. Consequently, a concept $c \in \mathcal{C}_N$ is a function such that $c : \mathcal{X}_N \to \{0,1\}$. A sample is denoted as $(x, c(x))$, which is a pair of the input and the output for the concept. Let $\mathbf{EX}(c, \mathcal{D}_N)$ be a procedure (oracle) that returns a labeled sample $(x, c(x))$ within a unit time upon each call, where x is drawn randomly and independently according to $\mathcal{D}_N$. Note that the samples $(x, c(x))$ from $\mathbf{EX}(c, \mathcal{D}_N)$ are given in terms of classical bit strings throughout this paper. In this setting, we can consider $\mathcal{X} = \bigcup_{N\geq 1} \mathcal{X}_N$ and $\mathcal{C} = \bigcup_{N\geq 1} \mathcal{C}_N$ to define an infinite family of learning problems of increasing input lengths.

In the PAC learning model, a learning algorithm will have access to samples from $\mathbf{EX}(c, \mathcal{D}_N)$ for an unknown target concept c, which is chosen from a given concept class $\mathcal{C}_N$. Using the samples, the learning algorithm will find a hypothesis h from a hypothesis class $\mathcal{H}_N$ so that h should approximate c. We define a measure of approximation error between hypothesis h and unknown concept c as

$$\mathrm{error}(h) = \mathbf{Pr}_{x\sim\mathcal{D}_N}[c(x) \neq h(x)]. \tag{A1}$$

The learning algorithm only sees input-output samples of the unknown target concept c. The algorithm may not have to directly deal with the representation of true c, i.e., a symbolic encoding of c in terms of a bit string. However, it still matters which representation the algorithm chooses for its hypothesis h since the learning algorithm needs to output the representation of h. To deal with these representations more formally, consider a representation scheme $\mathcal{R}$ for a concept class $\mathcal{C}_N$, which is a function $\mathcal{R} : \Sigma^* \to \mathcal{C}_N$ with $\Sigma = \{0,1\}$ denoting a bit and $\Sigma^* := \bigcup_{N\geq 1} \Sigma^N$ denoting the set of bit strings. We call any string $\sigma \in \Sigma^*$ such that $\mathcal{R}(\sigma) = c$ a representation of c. For $\mathcal{R}$, we here consider the length of the bit string $\sigma \in \Sigma^*$ to be the size of each representation σ, which we write $\mathrm{size}(\sigma)$. A representation of hypothesis h can be formulated in the same way by replacing c with h and $\mathcal{C}_N$ with $\mathcal{H}_N$.

The learning task is divided into two main parts. One is to find, using the samples, a representation of the hypothesis h that approximates the target concept c well, and the other is to make a prediction by evaluating $h(x)$ correctly for a new input $x \in \mathcal{X}_N$ and the learned representation of h. First, we define efficient learnability as shown below. This definition requires that the algorithm find and output the representation of the appropriate hypothesis h for the target concept c within a polynomial time. Note that this definition implies that the representation of the hypotheses h should also be of at most polynomial length. Conventionally, the PAC learning model may require that it be learnable for all distributions [6], but we can here observe that learning tasks in practice usually deal with data given from a particular distribution; for example, in the classification of images of dogs and cats, the learning algorithm does not have to work for any distribution over the images, but it suffices to deal with a given distribution supported on the meaningful images such as those of dogs and cats. Based on this observation, our model requires that it be learnable for a given (unknown) target distribution. Note that throughout the learning, the learning algorithm does not have to estimate the description of the target distribution itself, but it only suffices to learn the target concept c by the hypothesis h.

Definition S1 (Efficient learnability). *For any problem size $N \in \mathbb{N}$, let $\mathcal{C}_N$ be a concept class and $\mathcal{D}_N$ be a target distribution over an input space $\mathcal{X}_N \subseteq \{0,1\}^N$ of N bits. We say that $\mathcal{C}_N$ is quantumly (classically) efficiently learnable under the target distribution $\mathcal{D}_N$ if there exists a hypothesis class $\mathcal{H}_N$ and a quantum (classical randomized) algorithm $\mathcal{A}$ with the following property: for every concept $c \in \mathcal{C}_N$, and for all $0 < \epsilon, \delta < 1$, if $\mathcal{A}$ is given access to $\mathbf{EX}(c, \mathcal{D}_N)$ in addition to ϵ and δ, then $\mathcal{A}$ runs in a polynomial time*

$$t_{\mathcal{A}}(\mathbf{EX}, \epsilon, \delta) = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta)), \tag{A2}$$

to output a representation of hypothesis $h \in \mathcal{H}_N$ satisfying, with probability at least $1 - \delta$,

$$\mathrm{error}(h) \leq \epsilon, \tag{A3}$$

where the left-hand side is given by (A1). The probability is taken over the random examples drawn from the *calls of* $\mathbf{EX}(c, \mathcal{D}_N)$ *and the randomness used in the randomized algorithm* $\mathcal{A}$*. The number of calls of* $\mathbf{EX}(c, \mathcal{D}_N)$ *(i.e., the number of samples) and the size of the output representation of the hypothesis are bounded by the runtime.*

As for the evaluation of the learned hypothesis, we give a definition of efficient evaluatability below. This definition requires that, given an input x and a representation σ_h of a hypothesis h, the algorithm should evaluate $h(x)$ correctly in a polynomial time for a large fraction of x with high probability. The representation of a hypothesis used in this definition can be, in general, an arbitrary polynomial-length bit string representing the hypothesis. In particular, in the case of the previous work [16–20] on the advantage of QML using Shor's algorithms for solving integer factoring and discrete logarithms [21–23], a classical algorithm may be able to prepare samples on its own; by contrast, in our general setting, samples are given from the oracle **EX** as in Definition S1, and we do not necessarily require that the evaluation algorithms should be able to simulate **EX** to prepare the samples on their own. (For example, in Section C 2, we will discuss the preparation of samples by quantum computation rather than classical computation, so the classical algorithm may not be able to prepare the samples on its own.) In this learning setting, at best, an evaluation algorithm may be able to use the given samples encoded in the polynomial-length representation of the hypothesis as an extra input to the algorithm, which may not be prepared by the algorithm on its own but can be used for the algorithm to compute $h(x)$ more efficiently [18, 19, 48]. In addition to this encoding of a polynomial amount of sample data used in the learning, the representation of the hypothesis can even include any polynomial-length bit string to help the evaluation algorithm compute the hypothesis even more efficiently (which may be prepared potentially using an exponential runtime if we do not assume efficient learnability). In complexity theory, such an extra probabilistic input (apart from x) to make the computation potentially more efficient is known as a randomized advice string [49], as described in more detail in Section A 2. Note that it would be more conventional in the computational complexity theory to use an advice string given deterministically [4], but we here consider the samples and the representation of the hypothesis obtained from the samples as special instances of the randomized advice string since the samples in the PAC learning are given probabilistically from a data distribution. Also, in a conventional setting, efficient evaluation in the PAC model may mean that the hypothesis can be evaluated in worst-case polynomial time [6]. However, recalling the above observation that practical learning tasks deal with data from a more specific target distribution, we see that it may be too demanding to require that the hypothesis h should be evaluated efficiently for all possible $x \in \mathcal{X}_N$ even in the worst case; rather, it makes more sense to require that we should be able to evaluate $h(x)$ efficiently for x drawn from the target distribution of interest with a sufficiently high probability. In the complexity theoretical terms, this requirement can be captured by the notion of heuristic polynomial time [46, 47]; accordingly, we define efficient evaluatability based on heuristic complexity, as shown below. Since the heuristic hardness implies the worst-case hardness, proving the hardness of efficient evaluation for our learning model immediately leads to the conventional worst-case hardness of efficient evaluation in the learning (see also Section A 2 for more discussion on the difference and relation between these hardness results).

Definition S2 (Efficient evaluatability)**.** *For any problem size* $N \in \mathbb{N}$*, let* $\mathcal{C}_N$ *be a concept class and* $\mathcal{D}_N$ *be a target distribution over an input space* $\mathcal{X}_N \subseteq \{0,1\}^N$ *of* N *bits. We say that the hypothesis class* $\mathcal{H}_N$ *is quantumly (classically) efficiently evaluatable under the target distribution* $\mathcal{D}_N$ *if there exists a quantum (classical randomized) algorithm* $\mathcal{A}$ *such that for all* $N \in \mathbb{N}$, $0 < \epsilon, \delta < 1$, *and a* $O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$*-length bit string* σ_h *representing any hypothesis* $h \in \mathcal{H}_N$*,* $\mathcal{A}$ *runs in a polynomial time for all* $x \in \mathcal{X}_N$

$$t_{\mathcal{A}}(x, \sigma_h, \epsilon, \delta) = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta)), \tag{A4}$$

to output $\mathcal{A}(x, \sigma_h, \epsilon, \delta)$ *satisfying*

$$\Pr_{x \sim \mathcal{D}_N} \left[\Pr\left[\mathcal{A}(x, \sigma_h, \epsilon, \delta) = h(x)\right] \geq 1 - \delta\right] \geq 1 - \epsilon, \tag{A5}$$

where the inner probability is taken over the randomness of the randomized algorithm $\mathcal{A}$*.*

From Definitions S1 and S2, a learning task can be divided into four categories CC, CQ, QC, and QQ [18, 19], which means that whether the learning task is classically or quantumly efficiently learnable and whether it is classically or quantumly efficiently evaluatable, respectively. It is known that the categories CQ and QQ are equivalent unless the hypothesis class is fixed [19]. Note that Refs. [19] defined these categories based on the worst-case complexity, but the categories for our definitions may be different in that Definitions S1 and S2 are given based on the heuristic complexity. In our work, we will study the advantage of QML in the sense of $\mathsf{CC}\,/\,\mathsf{QQ}$ separation, following the previous work [16, 17] on the advantage of QML; i.e., we will construct a learning task in QQ but not in CC.

Finally, we remark that the learnability and the evaluatability are different in that Definition S1 requires that the hypothesis h should be found in polynomial time with a high probability, and Definition S2 requires that h should be evaluated. Efficient learnability itself does not require that the learned hypothesis should be efficiently used for making a prediction via its evaluation, and efficient evaluatability itself does not require that the representation of the hypothesis should be obtained efficiently in learning from the samples. However, to achieve the end-to-end acceleration of QML, we eventually need both quantumly efficient learnability and quantumly efficient evaluatability simultaneously, which our analysis aims at. Correspondingly, for the classical hardness of the learning tasks, our interest is to rule out the possibility that the best classical method achieves efficient learnability and efficient evaluatability simultaneously.

2. Quantum computational advantage

In this section, we present the computational complexity classes relevant to our analysis of the advantage of QML. Our analysis will use a general class of functions that are efficient to compute by quantum computation but hard by classical computation, based on the complexity classes defined here.

In the following, we will start by presenting the worst-case, average-case, and heuristic computational complexity classes [46, 47], whose difference arises from the fraction of the inputs for which the problem can be solved in polynomial time. Then, we will present the complexity classes for computing functions by classical randomized algorithms and quantum algorithms. Finally, we will explain advice strings, which are, roughly speaking, bit strings given to the algorithm in addition to the input to help solve the problem efficiently.

We introduce three cases of complexity classes: worst-case, average-case, and heuristic polynomial time. A complexity class is conventionally defined as a worst-case class; for example, the class P of (worst-case) polynomial time is a family of decision problems such that all the inputs of the problems in the family can be solved within a polynomial time in terms of the length of the input bit strings (even for the worst-case choice of the input) [4]. Accordingly, the existing analyses of the advantage of QML in previous research were also based on the worst-case complexity classes, requiring that the algorithm should be able to evaluate the hypothesis $h(x)$ for all $x \in \mathcal{X}_N$ [16–19]. However, this requirement is too demanding in our setting; after all, the PAC learning model allows for errors depending on a given target distribution. In the learning as in Definitions S1 and S2, it suffices to learn and evaluate $h(x)$ efficiently only for a sufficiently large fraction of x on the support of the given target distribution, rather than all x. Intuitively, in the classification of images for example, it suffices to learn and evaluate $h(x)$ efficiently for meaningful images on the support of the true probability distribution of samples, and whether $h(x)$ can be evaluated for all possible images including those never appearing in the real-world data is irrelevant in practice. To capture this difference, we here take into account average-case and heuristic complexity classes [46, 47]. The class of worst-case polynomial time is the class of decision problems that are solvable in polynomial time. Whereas P is a class of decision problems, average-case polynomial time AvgP and heuristic polynomial time HeurP are the classes of *distributional* decision problems that consist not only of decision problems but also of the target probability distributions of the input. In solving the distributional problems, the runtime of an algorithm may probabilistically change depending on the input given from the distribution. The runtime of solving the problem in AvgP should be polynomial in input length on average over inputs given from the distribution [72], which may allow, e.g., an exponentially long runtime to obtain a correct answer for an exponentially small fraction of the inputs. On the other hand, HeurP requires that the runtime of correctly solving the problem should be polynomial only for a sufficiently large fraction of (yet not all) the inputs from the distribution, and for the rest of the small fraction of the inputs, the algorithm may output a wrong answer [46, 47]. Note that in the heuristic class, the average runtime of correctly solving the problem is not necessarily bounded. By definition, the worst-case complexity class is contained in the average-case class, and the average-case class in the heuristic class; i.e., it is shown that $\mathsf{P} \subseteq \mathsf{AvgP} \subseteq \mathsf{HeurP}$ [73]. More formally, we define the worst-case, average-case, and heuristic classes with reference to P as follows. Note that for our analysis of learning, only the worst-case and heuristic classes are relevant, while the average-case classes are discussed here for clarity of presentation; thus, we may stop mentioning the average-case classes after this definition.

Definition S3 (Worst-case, average-case, and heuristic polynomial time [46, 47, 72])**.** *We define the worst-case, average-case, and heuristic complexity classes, namely,* P*,* AvgP*, and* HeurP*, respectively, as follows.*

1. *A decision problem, i.e., a function $L : \{0,1\}^* \to \{0,1\}$ with a single-bit output, is in P if there exists a deterministic classical algorithm $\mathcal{A}$ such that for every N and every input $x \in \{0,1\}^N$, $\mathcal{A}$ outputs $L(x)$ in $\mathsf{poly}(N)$ time.*

2. *A distributional problem $(L, \mathcal{D})$ is in AvgP if there exists a deterministic classical algorithm $\mathcal{A}$ and a constant d such that for every N*
$$\mathbb{E}_{x\sim\mathcal{D}_N}\left[\frac{t_{\mathcal{A}}(x)^{\frac{1}{d}}}{N}\right] = O(1), \tag{A6}$$
where $t_{\mathcal{A}}(x)$ is the time taken to calculate $L(x)$ by $\mathcal{A}$, and $\mathbb{E}_{x\sim\mathcal{D}_N}[\cdots]$ is the expected value over x drawn from $\mathcal{D}_N$.

3. *A distributional problem $(L, \mathcal{D})$ is in HeurP if there exists a deterministic classical algorithm $\mathcal{A}$ such that for every N and all $0 < \mu < 1$, the runtime $t_{\mathcal{A}}(x, \mu)$ of $\mathcal{A}$ for every input x in the support of $\mathcal{D}_N$ is $t_{\mathcal{A}}(x, \mu) = O(\mathsf{poly}(N, 1/\mu))$, and the output $\mathcal{A}(x, \mu)$ of $\mathcal{A}$ satisfies*
$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}[\mathcal{A}(x,\mu) = L(x)] \geq 1 - \mu. \tag{A7}$$

Next, we define the classes of problems solvable by a (classical) randomized algorithm. In Definition S3, we use a deterministic classical algorithm to solve problems.

By contrast, in the randomized algorithms, we need to take into account errors arising from the randomization. Corresponding to P and HeurP, we define the two classes of problems for randomized algorithms as follows.

Definition S4 (Worst- and heuristic bounded-error probabilistic polynomial time [46, 47]). *We define a worst-case class* BPP *and a heuristic class* $\mathsf{HeurBPP}$ *for classical randomized algorithms as follows.*

1. *A decision problem L is in BPP if there exists a classical randomized algorithm $\mathcal{A}$ such that for every N and every input $x \in \{0,1\}^N$, the runtime $t_{\mathcal{A}}(x)$ of $\mathcal{A}$ is $t_{\mathcal{A}}(x) = O(\mathsf{poly}(N))$, and the output $\mathcal{A}(x)$ of $\mathcal{A}$ satisfies*
$$\mathbf{Pr}[\mathcal{A}(x) = L(x)] \geq 2/3, \tag{A8}$$
where the probability is taken over the randomness of $\mathcal{A}$.

2. *A distributional problem $(L, \mathcal{D})$ is in $\mathsf{HeurBPP}$ if there exists a classical randomized algorithm such that for every N and all $0 < \mu < 1$, the runtime $t_{\mathcal{A}}(x,\mu)$ of $\mathcal{A}$ for every input x in the support of $\mathcal{D}_N$ is $t_{\mathcal{A}}(x,\mu) = O(\mathsf{poly}(N, 1/\mu))$, and the output $\mathcal{A}(x,\mu)$ of $\mathcal{A}$ satisfies*
$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}[\mathbf{Pr}[\mathcal{A}(x,\mu) = L(x)] \geq 2/3] \geq 1-\mu, \tag{A9}$$
where the inner probability of $\mathcal{A}(x,\mu) = L(x)$ is taken over randomness of $\mathcal{A}$.

Whereas we have so far explained complexity classes of decision problems, i.e., those for computing functions with a single-bit output, our analysis will use a Boolean function with a single multi-bit output for each N-bit input
$$f_N : \{0,1\}^N \to \{0,1\}^{D(N)}, \tag{A10}$$
where $D : \mathbb{N} \to \mathbb{N}$ is any function satisfying $D(N) = O(\mathsf{poly}(N))$, and we may abbreviate $D(N)$ as D in the following of this paper. Accordingly, we define the complexity classes of function problems, i.e., problems of computing such multi-bit output functions f_N. For the heuristic complexity class, we also refer to a family of problems $\{(f_N, \mathcal{D}_N)\}_{N\in\mathbb{N}}$ as distributional function problems. Whenever f_N is used in the following of this paper, it refers to a function with a single multi-bit output for each input. Note that the complexity classes of function problems may also be defined as those of search problems, which can be considered to be the problems of computing functions with many possible outputs for each input, and the algorithms aim to search for one of the possible outputs for a given input. But even if one considers such a more general definition, functions f_N relevant to our analysis are those with a single output for each input; correspondingly, we here present the definitions using the single-output functions for simplicity.

Definition S5 (Worst-case and heuristic distributional function bounded-error polynomial time). *We define a worst-case class* FBPP *and a heuristic class* $\mathsf{HeurFBPP}$ *for computing multi-bit output functions as follows.*

1. *Given $R_N := \{(x, f_N(x))\}_{x\in\{0,1\}^N}$ and $R := \bigcup_N R_N$, the relation R is in FBPP if there exists a randomized classical algorithm $\mathcal{A}$ such that for all N, every input $x \in \{0,1\}^N$, and all $0 < \nu < 1$, the runtime $t_{\mathcal{A}}(x,\nu)$ of $\mathcal{A}$ is $t_{\mathcal{A}}(x,\nu) = O(\mathsf{poly}(N, 1/\nu))$, and the output $\mathcal{A}(x,\nu)$ of $\mathcal{A}$ satisfies*
$$\mathbf{Pr}[(x, \mathcal{A}(x,\nu)) \in R_N] \geq 1-\nu, \tag{A11}$$
where the probability is taken over the randomness of $\mathcal{A}$.

2. *A distributional function problem $F = \{(f_N, \mathcal{D}_N)\}_{N\in\mathbb{N}}$ is in $\mathsf{HeurFBPP}$ if there exists a classical randomized algorithm $\mathcal{A}$ such that for all N and all $0 < \mu, \nu < 1$, the runtime $t_{\mathcal{A}}(x,\mu,\nu)$ of $\mathcal{A}$ for every input $x \in \{0,1\}^N$ in the support of $\mathcal{D}_N$ is $t_{\mathcal{A}}(x,\mu,\nu) = O(\mathsf{poly}(N, 1/\mu, 1/\nu))$, and the output $\mathcal{A}(x,\mu,\nu)$ of $\mathcal{A}$ satisfies*
$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}[\mathbf{Pr}[\mathcal{A}(x,\mu,\nu) = f_N(x)] \geq 1-\nu] \geq 1-\mu, \tag{A12}$$
where the inner probability of $\mathcal{A}(x,\mu,\nu) = f_N(x)$ is taken over randomness of $\mathcal{A}$.

We next define the classes FBQP and $\mathsf{HeurFBQP}$ of problems efficiently solvable by quantum algorithms. The classes defined so far are the computational complexity classes for deterministic or randomized classical algorithms, but we here define FBQP and $\mathsf{HeurFBQP}$ using quantum algorithms in place of the classical algorithms. The class $\mathsf{HeurFBQP}$ will be used for our construction of learning tasks in Definition S8 of Section B 1 to prove the advantage of QML. Note that we have $\mathsf{FBQP} \subseteq \mathsf{HeurFBQP}$ in the same way as $\mathsf{P} \subseteq \mathsf{HeurP}$. Working on $\mathsf{HeurFBQP}$, we aim to make it possible to use a potentially larger class of computational advantages of heuristic quantum algorithms captured by $\mathsf{HeurFBQP}$ rather than FBQP, so as to achieve a wider class of learning tasks more efficiently.

Definition S6 (Worst-case and heuristic distributional function bounded-error quantum polynomial time). *We define a worst-case class* FBQP *and a heuristic class* $\mathsf{HeurFBQP}$ *for quantum algorithms as follows.*

1. *Given $R_N = \{(x, f_N(x))\}_{x\in\{0,1\}^N}$ and $R = \bigcup_N R_N$, the relation R is in FBQP if there exists a quantum algorithm $\mathcal{A}$ such that for all N, every input $x \in \{0,1\}^N$, all $0 < \nu < 1$, the runtime $t_{\mathcal{A}}(x,\nu)$ of $\mathcal{A}$ is $t_{\mathcal{A}}(x,\nu) = O(\mathsf{poly}(N, 1/\nu))$, and the output $\mathcal{A}(x,\nu)$ of $\mathcal{A}$ satisfies*
$$\mathbf{Pr}[(x, \mathcal{A}(x,\nu)) \in R_N] \geq 1-\nu, \tag{A13}$$
where the probability is taken over the randomness of $\mathcal{A}$.

2. *A distributional function problem $F = \{(f_N, \mathcal{D}_N)\}_{N\in\mathbb{N}}$ is in* HeurFBQP *if there exists a quantum algorithm $\mathcal{A}$ such that for all N and all $0 < \mu, \nu < 1$, the runtime $t_{\mathcal{A}}(x, \mu, \nu)$ of $\mathcal{A}$ for every input $x \in \{0,1\}^N$ in the support of $\mathcal{D}_N$ is $t_{\mathcal{A}}(x, \mu, \nu) = O(\mathsf{poly}(N, 1/\mu, 1/\nu))$, and the output $\mathcal{A}(x, \mu, \nu)$ of $\mathcal{A}$ satisfies*

$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}[\mathbf{Pr}[\mathcal{A}(x, \mu, \nu) = f_N(x)] \geq 1-\nu] \geq 1-\mu, \quad \text{(A14)}$$

where the inner probability of $\mathcal{A}(x, \mu, \nu) = f_N(x)$ is taken over randomness of $\mathcal{A}$.

Finally, we introduce the complexity classes with randomized advice strings [49]. As discussed in Section A 1, the analysis of the efficient evaluatability in the PAC learning model needs to take into account the randomized advice strings of at most $O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ length [18, 19, 48]. To capture the power of the bit strings representing the hypotheses to be evaluated, we consider the complexity classes with a polynomial-length randomized advice string as follows.

Definition S7 (Worst-case and heuristic distributional function bounded-error polynomial time with randomized advice)**.** *We define a worst-case class* FBPP/rpoly *and a heuristic class* HeurFBPP/rpoly *with advice as follows.*

1. *Given $R_N = \{(x, f_N(x))\}_{x\in\{0,1\}^N}$ and $R = \bigcup_N R_N$, the relation R is in* FBPP/rpoly *if there exists a randomized classical algorithm $\mathcal{A}$ such that for all N, every input $x \in \{0,1\}^N$, and all $0 < \nu, \xi < 1$, there exists an advice distribution $\mathcal{D}^{\mathrm{adv}}_{N,\nu,\xi}$ over $\{0,1\}^{O(\mathsf{poly}(N,1/\nu,1/\xi))}$ such that the runtime $t_{\mathcal{A}}(x, \alpha, \nu, \xi)$ of $\mathcal{A}$ is $t_{\mathcal{A}}(x, \alpha, \nu, \xi) = O(\mathsf{poly}(N, 1/\nu, 1/\xi))$, and the output $\mathcal{A}(x, \alpha, \nu, \xi)$ of $\mathcal{A}$ satisfies*

$$\mathop{\mathbf{Pr}}_{\alpha\sim\mathcal{D}^{\mathrm{adv}}_{N,\nu,\xi}}[\mathbf{Pr}[(x, \mathcal{A}(x, \alpha, \nu, \xi)) \in R_N] \geq 1-\nu] \geq 1-\xi, \quad \text{(A15)}$$

where the inner probability is taken over the randomness of $\mathcal{A}$.

2. *A distributional function problem $F = \{(f_N, \mathcal{D}_N)\}_{N\in\mathbb{N}}$ is in* HeurFBPP/rpoly *if there exists a randomized classical algorithm $\mathcal{A}$ such that for all N and all $0 < \mu, \nu, \xi < 1$, there exists an advice distribution $\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}$ over $\{0,1\}^{O(\mathsf{poly}(N,1/\mu,1/\nu,1/\xi))}$ such that the runtime $t_{\mathcal{A}}(x, \alpha, \mu, \nu, \xi)$ of $\mathcal{A}$ for every input $x \in \{0,1\}^N$ in the support of $\mathcal{D}_N$ is $t_{\mathcal{A}}(x, \alpha, \mu, \nu, \xi) = O(\mathsf{poly}(N, 1/\mu, 1/\nu, 1/\xi))$, and the output $\mathcal{A}(x, \alpha, \mu, \nu, \xi)$ of $\mathcal{A}$ satisfies*

$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}\left[\mathop{\mathbf{Pr}}_{\alpha\sim\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}}[\mathbf{Pr}[\mathcal{A}(x, \alpha, \mu, \nu, \xi) = f_N(x)] \geq 1-\nu] \geq 1-\xi\right] \geq 1-\mu, \quad \text{(A16)}$$

where the probability of $\mathcal{A}(x, \alpha, \mu, \nu, \xi) = f_N(x)$ is taken over randomness of $\mathcal{A}$.

We similarly define other possible classes such as FP by combining the above definitions.

Appendix B: Advantage of QML from general quantum computational advantages

In this section, we prove that, for general quantum computational advantages, we can correspondingly construct learning tasks that are hard for classical computation but can be efficiently solved by quantum computation, within the conventional framework of supervised learning (i.e., in the PAC model formulated in Section A 1). In previous work [16–20], the advantage of QML was observed under the computational hardness assumption for a specific type of problem, such as that solved by Shor's algorithms. References [18, 19] also provide a learning problem with the advantage of QML based on more general quantum computational advantages than that of Shor's algorithms, but the concept class therein was limited to be polynomial-size ones, which can be straightforwardly solved by a brute-force algorithm. In contrast, the learning tasks introduced here will have exponential-size concept classes and yet will still be based on general types of quantum computational advantages, i.e., arbitrary functions in HeurFBQP \(HeurFBPP/rpoly) rather than just that of Shor's algorithms. In Section B 1, we explicitly give the concept class of these learning tasks as linear separation problems in the space of bits. In Section B 2, we construct polynomial-time quantum algorithms for learning and evaluation in our learning tasks. In Section B 3, we rigorously prove the classical hardness of the learning tasks.

1. Formulation of learning tasks

In this section, we construct learning tasks using general types of quantum advantages based on complexity classes introduced in Section A 2.

First, we define the general complexity class of functions to be used for formulating our learning task. Although Refs. [18, 19] studied conditions on the complexity classes that potentially lead to the advantage of QML, the analyses in Refs. [18, 19] were based on worst-case complexity [18, 19] and were not able to explicitly construct the learning tasks satisfying their conditions in general. By contrast, we here identify an appropriate class of functions using the heuristic complexity classes, so that we can use any functions in this class for our explicit construction of the learning tasks with the provable advantage of QML. The class that we use is given as follows.

Definition S8 (Quantumly advantageous functions)**.** *For a distributional functions problem $\{(f_N, \mathcal{D}_N)\}_{N\in\mathbb{N}}$ in*

$$\{(f_N, \mathcal{D}_N)\}_N \in \textsf{\textit{HeurFBQP}}\backslash(\textsf{\textit{HeurFBPP/rpoly}}), \tag{B1}$$

we call f_N a quantumly advantageous function under the target distribution $\mathcal{D}_N$.

As presented in the main text, the quantumly advantageous functions may include various functions beyond those computed by Shor's algorithms. Since we use heuristic complexity classes, the class of functions in Definition S8 is even larger than the class defined by the worst-case complexity classes, as discussed in Section A 2. For example, our definition does not rule out the possibility of using heuristic quantum algorithms such as the variational quantum algorithms (VQAs) for seeking evidence of the utility of QML based on the heuristic complexity class [74], in case one finds a variant of such quantum algorithms that are faster than classical algorithms for most of the inputs.

We define our concept class using the quantumly advantageous functions below. In the existing work [16–19] on the advantage of QML, the target distribution was limited to the uniform distribution, and the task was dependent on the specific mathematical structure of the functions computed by Shor's algorithms; by contrast, we allow for an arbitrary target distribution $\mathcal{D}_N$ over N bits, and we can use an arbitrary quantumly advantageous function without specifically depending on Shor's algorithms.

Definition S9 (Concept class for the advantage of QML from general computational advantages)**.** *For any N, $D = O(\mathsf{poly}(N))$, any target distribution $\mathcal{D}_N$ over an input space $\mathcal{X}_N \subseteq \{0,1\}^N$ of N bits, and any quantumly advantageous function $f_N : \{0,1\}^N \to \mathbb{F}_2^D$ under $\mathcal{D}_N$, we define a concept class $\mathcal{C}_N$ over the input space $\mathcal{X}_N$ as $\mathcal{C}_N = \{c_s\}_{s\in\mathbb{F}_2^D}$ with its concept c_s for each parameter $s \in \mathbb{F}_2^D$ given by*

$$c_s(x) := f_N(x) \cdot s \in \mathbb{F}_2 = \{0,1\}, \tag{B2}$$

where $f_N(x) \cdot s$ for $f_N(x), s \in \mathbb{F}_2^D = \{0,1\}^D$ is a bitwise inner product in the vector space $\mathbb{F}_2^D$ over the finite field.

2. Construction of polynomial-time quantum algorithms for learning and evaluation

In this section, we show polynomial-time quantum algorithms for learning concepts in the concept class in Definition S9 and for evaluating hypotheses in the hypothesis class for this concept class. A challenge here arises from the fact that our concept class $\mathcal{C}_N$ in Definition S9 may have an exponential size in N. To see the importance of addressing this challenge, recall that, for example, Refs. [18, 19] also analyzed the advantage of QML based on general quantum computational advantages, but their results were only applicable to polynomial-size concept classes so that their concept classes should be efficiently learnable by a brute-force quantum algorithm that just tries all the concepts in the concept class. However, our interest here is whether QML can learn concepts without such a brute-force approach. Advancing ahead, our results overcome such limitations by constructing QML algorithms achieving efficient learning and evaluation for the exponential-size concept classes, of which we will also prove the hardness for any classical learning methods in Sec. B 3. Below, we first describe our learning algorithm (Algorithm S1) and prove the quantum efficient learnability for our concept class. We then describe our evaluation algorithm (Algorithm S2) and prove the quantum efficient evaluatability for the hypothesis class constructed for our concept class.

We first describe our quantum algorithm for learning. Our algorithm for learning a target concept in our concept class is given by Algorithm S1. The concept class $\mathcal{C}_N = \{c_s : s \in \mathbb{F}_2^D\}$ is defined in Definition S9 for any (unknown) target distribution $\mathcal{D}_N$ over $\mathcal{X}_N \subseteq \mathbb{F}_2^N$ and any quantumly advantageous function $f_N : \{0,1\}^N \to \mathbb{F}_2^D$. Let c_s denote the unknown target concept to be learned from the samples by the algorithm, where s is the true parameter of the target concept. For any $\epsilon > 0$ and $\delta > 0$, our algorithm aims to achieve the learning in Definition S1, i.e., to output $\tilde{s}$ so that a hypothesis $h_{\tilde{s}}$ represented by $\tilde{s}$ should satisfy

$$\underset{x\sim\mathcal{D}_N}{\mathbf{Pr}}\left[h_{\tilde{s}}(x) \neq c_s(x)\right] \leq \epsilon \tag{B3}$$

with a high probability greater than or equal to $1-\delta$. To this goal, we set the internal parameters in Algorithm S1 as

$$M = \left\lceil \frac{D}{\epsilon} - 1 \right\rceil, \tag{B4}$$

$$\mu = \frac{\delta}{2M}, \tag{B5}$$

$$\nu = \frac{\delta}{2M}, \tag{B6}$$

where $\lceil x \rceil$ is the ceiling function, i.e., the smallest integer greater than or equal to x.

In Algorithm S1, M samples are initially loaded as the input, obtained from the oracle **EX** in the setting of the PAC learning model described in Section A 1. The M samples are denoted by $\{(x_m, c_s(x_m))\}_{m=1}^M$, where c_s is the (unknown) target concept to be learned from the samples by the algorithm. Then, the algorithm probabilistically computes the quantumly advantageous function f_N for each of the M input samples $x_1, \ldots, x_M$. By definition of the quantumly advantageous function f_N in $\mathsf{HeurFBQP}$ of (A14), we have a quantum algorithm $\mathcal{A}$ to achieve

$$\underset{x\sim\mathcal{D}_N}{\mathbf{Pr}}\left[\mathbf{Pr}\left[\mathcal{A}(x,\mu,\nu) = f_N(x)\right] \geq 1-\nu\right] \geq 1-\mu, \tag{B7}$$

with runtime

$$t_{\mathcal{A}}(x,\mu,\nu) = O\left(\left(\frac{N}{\mu\nu}\right)^{\alpha}\right), \tag{B8}$$

where $\alpha > 0$ is an upper bound of the degree of the polynomial runtime. To compute f_N, Algorithm S1 applies the quantum algorithm $\mathcal{A}$ to each of $x_1, \ldots, x_M$. We write the outputs of $\mathcal{A}$ as $\mathcal{A}(x_1), \ldots, \mathcal{A}(x_M) \in \mathbb{F}_2^D$, respectively, where we will omit μ and ν for simplicity of notation if it is obvious from the context. Note that $\mathcal{A}$ may not be a deterministic algorithm, and thus, we may have $\mathcal{A}(x_m) = f_N(x_m)$ only probabilistically. Using $\mathcal{A}(x_1), \ldots, \mathcal{A}(x_M)$ obtained from these computations, the algorithm performs Gaussian elimination by classical computation to solve a system of linear equations

$$\begin{aligned} \mathcal{A}(x_1) \cdot \tilde{s} &= c_s(x_1), \\ \mathcal{A}(x_2) \cdot \tilde{s} &= c_s(x_2), \\ &\vdots \\ \mathcal{A}(x_M) \cdot \tilde{s} &= c_s(x_M), \end{aligned} \tag{B9}$$

where the left-hand sides of the system of linear equations are the bitwise inner product in the space $\mathbb{F}_2^D$ of the D-dimensional vectors over the finite field. This step provides a solution

$$\tilde{s} = \begin{pmatrix} \tilde{s}_1 \\ \tilde{s}_2 \\ \vdots \\ \tilde{s}_D \end{pmatrix} \in \mathbb{F}_2^D \tag{B10}$$

of the system of linear equations. This system of linear equations always has the true parameter s of the target concept c_s as a solution but may have more than one solution if the set $\{\mathcal{A}(x_1), \ldots, \mathcal{A}(x_M)\}$ does not include a spanning set of D vectors in the D-dimensional vector space $\mathbb{F}_2^D$. The non-spanning cases indeed occur in our setting, especially when the support of $\mathcal{D}_N$ or the range of f_N is small, on which we impose no assumption for the generality of our learning task. Even if the system of linear equations has more than one solution, the algorithm can nevertheless adopt any solution of (B9) as $\tilde{s}$ in (B10). The learning algorithm outputs this parameter $\tilde{s}$ as a representation of the hypothesis given by

$$h_{\tilde{s}}(x) = f_N(x) \cdot \tilde{s}, \tag{B11}$$

where the right-hand side is the bitwise inner product in $\mathbb{F}_2^D$. The hypothesis class is then given by

$$\mathcal{H}_N := \{h_{\tilde{s}} : \tilde{s} \in \mathbb{F}_2^D\}. \tag{B12}$$

In the following, we will prove the efficient learnability of our concept class $\mathcal{C}_N$ by Algorithm S1. The proof is nontrivial since the parameter $\tilde{s}$ in (B10) output by our learning algorithm may not be exactly equal to true s of the target concept c_s but can be any of multiple possible solutions of the system of linear equations in (B9); i.e., we need to take into account the cases of

$$\tilde{s} \neq s. \tag{B13}$$

```
Algorithm S1 Quantum algorithm for learning a concept in the concept class in Definition S9
Input: Samples loaded from the oracle EX, $\epsilon > 0$, and $\delta > 0$.
Output: A $D$-bit representation $\tilde{s} \in \mathbb{F}_2^D$ of the hypothesis
    $h_{\tilde{s}}$ in (B11) in the hypothesis class in (B12) achieving
    the error below $\epsilon$ with high probability at least $1 - \delta$, as in (B3).
1: Load $M$ samples $(x_1, c_s(x_1)), \ldots, (x_M, c_s(x_M))$ from the
   oracle EX with $M$ given in (B4).
2: for $m = 1, \ldots, M$ do
3:     Perform the quantum algorithm $\mathcal{A}$ in (B7) for the input
       $x_m$ with the parameters $\mu$ and $\nu$ in (B5) and (B6),
       respectively, to obtain $\mathcal{A}(x_m)$.
4: end for
5: Perform Gaussian elimination by classical computation
   for solving the system of linear equations in (B9), using
   $\mathcal{A}(x_1), \ldots, \mathcal{A}(x_M)$ obtained in the previous steps and the
   output samples $c_s(x_1), \ldots, c_s(x_M)$ loaded initially, to obtain a solution $\tilde{s}$ in (B10).
6: return $\tilde{s}$.
```

```
Algorithm S2 Quantum algorithm for evaluating a hypothesis in the hypothesis class for the concept class in Definition S9
Input: A new input $x \in \mathcal{X}_N$ sampled from the target distribution $\mathcal{D}_N$,
    a parameter $\tilde{s} \in \mathbb{F}_2^D$ of the hypothesis $h_{\tilde{s}}$
    in (B11) in the hypothesis class (B12), $\epsilon > 0$, and $\delta > 0$.
Output: An estimate $\tilde{h} \in \{0, 1\}$ of the hypothesis $h_{\tilde{s}}(x)$ for
    the input $x$ achieving the error below $\epsilon$ with high probability at least $1 - \delta$, as in (B41).
1: Perform the quantum algorithm $\mathcal{A}$ in (B7) for the input
   $x$ with the parameters $\mu$ and $\nu$ in (B42) and (B43), respectively, to obtain $\mathcal{A}(x)$.
2: return $\tilde{h} = A_N(x) \cdot \tilde{s}$ in (B44).
```

We will nevertheless prove that we have

$$h_{\tilde{s}}(x) = c_s(x) \tag{B14}$$

for a large fraction of x with a high probability as required for the efficient learnability in Definition S1.

To achieve this proof, our key technique is to use the lemma below, which indicates that if we have sufficiently many samples $x_1, \ldots, x_M$, then for a new $(M+1)$th input x_{M+1} to be given in the future, we will be able to represent its feature $y_{M+1} = f_N(x) \in \mathbb{F}_2^D$ as a linear combination of those of the M samples, $y_1 = f_N(x_1), \ldots, y_M = f_N(x_M) \in \mathbb{F}_2^D$, with a high probability. Using this lemma, in our proof of efficient learnability, we will show that the learned hypothesis $h_{\tilde{s}}(x) = f_N(x) \cdot \tilde{s}$ with $\tilde{s}$ estimated from $y_1, \ldots, y_M$ will coincide with the target concept $c_s(x) = f_N(x) \cdot s$ with true s, by expanding $f_N(x)$ therein as the linear combination of $f_N(x_1), \ldots, f_N(x_M)$. In particular, we here give the following lemma.

Lemma S10 (Probability of linear combination)**.** *Suppose that M vectors $y_1,\ldots,y_M\in\mathbb{F}_2^D$ are sampled from any probability distribution on a D-dimensional vector space $\mathbb{F}_2^D$ over the finite field in an identically and identically distributed (IID) way. If the $(M+1)$th vector y is sampled from the same distribution, then y can be represented by a linear combination of the other M vectors $y_1,\ldots,y_M$, i.e.,*

$$y=\sum_{m=1}^{M}\alpha_m y_m \quad \text{for some } \alpha_m\in\mathbb{F}_2=\{0,1\}, \tag{B15}$$

with a high probability greater than or equal to

$$1-\frac{D}{M+1}. \tag{B16}$$

Proof. We write $y_{M+1}:=y$. Given any sequence $y_1,\ldots,y_{M+1}$ of the $M+1$ vectors, let m' be the number of nonzero vectors in $(y_1,\ldots,y_{M+1})$ such that the vector cannot be represented by a linear combination of the other M vectors. Let $p(m')$ denote the probability that the sequence $y_1,\ldots,y_{M+1}$ randomly chosen by the IID sampling includes exactly m' vectors that cannot be represented by a linear combination of the other M. Since the space $\mathbb{F}_2^D$ is D-dimensional, we always have

$$m'\leq D, \tag{B17}$$

that is,

$$\sum_{m'=0}^{D}p(m')=1. \tag{B18}$$

For example, we may have $m'=D$ in the cases where the sequence includes the D vectors that form a basis of the vector space $\mathbb{F}_2^D$, and the other $N-D$ vectors are zero vectors.

Conditioned on having these m' vectors in the sequence of $M+1$ vectors, the probability of (B15) is bounded by the probability of having one of the m' vectors out of the $M+1$ vectors as the $(M+1)$th vector, i.e.,

$$\begin{aligned}&\mathbf{Pr}\left[y_{M+1}\neq\sum_{m=1}^{M}\alpha_m y_m\quad\forall\alpha_m\in\mathbb{F}_2\middle|m'\right]\\ &=\frac{m'}{M+1} &\text{(B19)}\\ &\leq\frac{D}{M+1}, &\text{(B20)}\end{aligned}$$

where the first equality follows from the assumption of IID sampling, and the inequality in the last line from (B17). Therefore, it holds that

$$\begin{aligned}&\mathbf{Pr}\left[y_{M+1}\neq\sum_{m=1}^{M}\alpha_m y_m\quad\forall\alpha_m\in\mathbb{F}_2\right]\\ &=\sum_{m'=0}^{M}p(m')\,\mathbf{Pr}\left[y_{M+1}\neq\sum_{m=1}^{M}\alpha_m y_m\quad\forall\alpha_m\in\{0,1\}\middle|m'\right]\\ &\leq\left(\sum_{m'=0}^{M}p(m')\right)\frac{D}{M+1} &\text{(B21)}\\ &=\frac{D}{M+1}, &\text{(B22)}\end{aligned}$$

which yields the conclusion. □

Using Lemma S10, we prove that the concept class $\mathcal{C}_N$ in Definition S9 is quantumly efficiently learnable as follows.

Theorem S11 (Quantumly efficient learnability)**.** *For any N, $D=O(\mathsf{poly}(N))$, any target distribution $\mathcal{D}_N$ over the N-bit input space $\mathcal{X}_N\subseteq\{0,1\}^N$, and any quantumly advantageous function $f_N:\{0,1\}^N\to\mathbb{F}_2^D$ under $\mathcal{D}_N$, the concept class $\mathcal{C}_N$ in Definition S9 with f_N is quantumly efficiently learnable by Algorithm S1.*

Proof. In the following, we will first discuss the success probability of our algorithm and then analyze the error in the learning. Finally, we will provide an upper bound of the runtime.

Regarding the success probability of Algorithm S1, the probabilistic parts of the learning algorithm are the loading of the M samples $(x_1,c_s(x_1)),\ldots,(x_M,c_s(x_M))$ from the oracle **EX** and the computations of $f_N(x)$ for all $x\in\{x_1,\ldots,x_M\}$ by the quantum algorithm $\mathcal{A}$. The other parts, such as the Gaussian elimination, are deterministic, as shown in Algorithm S1. In loading the M samples, based on Lemma S10, we require that the feature map $f_N(x)$ for the next $(M+1)$th sample x from the same target distribution $\mathcal{D}_N$, which is to be evaluated after the learning from the M samples, should be represented as a linear combination of those of the M samples, $f_N(x_1),\ldots,f_N(x_M)$, with a high probability at least $1-\epsilon$; i.e., it should hold that

$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}\left[f_N(x)=\sum_{m=1}^{M}\alpha_m f_N(x_m)\right]\geq1-\epsilon. \tag{B23}$$

Using Lemma S10 with $y_1=f_N(x_1),\ldots,y_M=f_N(x_M)$, and $y=f_N(x)$, we see that, with M given by (B4), this requirement is fulfilled. Also, in the computations of f_N, we require that the probabilistic quantum algorithm $\mathcal{A}$ should simultaneously achieve

$$\mathcal{A}(x_1)=f_N(x_1),\ldots,\mathcal{A}(x_M)=f_N(x_M), \tag{B24}$$

with a high probability of at least $1-\delta$. For each $m\in\{1,\ldots,M\}$, due to (B7) and the union bound, we have $\mathcal{A}(x_m)=f_N(x_m)$ with a probability at least

$$1-(\mu+\nu); \tag{B25}$$

then, due to the union bound, the probability of having (B24) simultaneously is at least

$$1-M(\mu+\nu). \tag{B26}$$

Thus, with μ chosen as (B5) and ν as (B6), the requirement in (B24) is fulfilled. As a whole, the requirement in (B23) is always satisfied for our choice of M, and the requirement in (B24) is satisfied with a high probability at least $1-\delta$ for our choice of μ and ν, which guarantees that the overall success probability of the learning algorithm is lower bounded by $1-\delta$.

Given that the requirements in (B23) and (B24) are fulfilled, the error in learning as in Definition S1 is bounded as follows. Under (B23) and (B24), for any x satisfying

$$f_N(x) = \sum_{m=1}^{M} \alpha_m f_N(x_m), \tag{B27}$$

the hypothesis $h_{\tilde{s}}$ in (B11) parameterized by $\tilde{s} \in \mathbb{F}_2^D$ output by Algorithm S1 can correctly classify x as

$$\begin{aligned}
h_{\tilde{s}}(x) &= f_N(x) \cdot \tilde{s} && \text{(B28)}\\
&= \sum_{m=1}^{M} \alpha_m f_N(x_m) \cdot \tilde{s} && \text{(B29)}\\
&= \sum_{m=1}^{M} \alpha_m \mathcal{A}(x_m) \cdot \tilde{s} && \text{(B30)}\\
&= \sum_{m=1}^{M} \alpha_m c_s(x_m) && \text{(B31)}\\
&= \sum_{m=1}^{M} \alpha_m f_N(x_m) \cdot s && \text{(B32)}\\
&= f_N(x) \cdot s && \text{(B33)}\\
&= c_s(x), && \text{(B34)}
\end{aligned}$$

where (B29) follows from (B27), (B30) from (B24), and (B31) from (B9). Therefore, due to the requirement of (B23), we have

$$\mathbf{Pr}\left[h(x) = c_s(x)\right] \geq 1-\epsilon; \tag{B35}$$

that is, the error in (A1) is bounded by

$$\mathrm{error}(h) = \mathbf{Pr}\left[h(x) \neq c_s(x)\right] \leq \epsilon, \tag{B36}$$

as required for the learnability in Definition S1.

The runtime of Algorithm S1 is dominated by the computations of f_N by $\mathcal{A}$ and the Gaussian elimination. We first consider the runtime of computing f_M for the M samples $x_1, \ldots, x_M$. For each x_m with $m \in \{1, \ldots, M\}$, the runtime of the quantum algorithm $\mathcal{A}$ for computing f_N is given by $t_{\mathcal{A}}(x_m)$ in (B8); thus, the runtime of the M calculations is

$$\sum_{m=1}^{M} t_{\mathcal{A}}(x_m) = O\left(M\left(\frac{N}{\mu\nu}\right)^{\alpha}\right). \tag{B37}$$

In addition, the runtime of performing the Gaussian elimination to find a solution $\tilde{s} \in \mathbb{F}_2^D$ of the system of M linear equations in (B9) (with $D \leq M$ due to (B4)) is

$$O(M^3). \tag{B38}$$

In total, for M in (B4), μ in (B5), ν in (B6), and $D = O(\mathsf{poly}(N)) = O(N^{\beta})$ with some $\beta > 0$, the overall runtime of Algorithm S1 is upper bounded by

$$\begin{aligned}
&O\left(M\left(\frac{N}{\mu\nu}\right)^{\alpha}\right) + O(M^3)\\
&= O\left(\frac{N^{2\alpha\beta+\alpha+\beta}}{\delta^{2\alpha}\epsilon^{2\alpha+1}} + \frac{N^{3\beta}}{\epsilon^3}\right) && \text{(B39)}\\
&= O\left(\mathsf{poly}\left(N, \frac{1}{\epsilon}, \frac{1}{\delta}\right)\right), && \text{(B40)}
\end{aligned}$$

as required for efficient learnability in Definition S1. □

Next, we describe our quantum algorithm for evaluating the hypotheses for our concept class. Our quantum algorithm for evaluating a hypothesis $h_{\tilde{s}}$ in (B11) with the learned parameter $\tilde{s}$ is given by Algorithm S2, where the hypothesis class is in (B12). In our case, the parameter $\tilde{s}$ serves as the D-bit representation of the hypothesis, corresponding to σ_h in Definition S2 of the efficient evaluatability. For any $\epsilon > 0$ and $\delta > 0$, our evaluation algorithm aims to achieve the efficient evaluation in Definition S2; in particular, the evaluation algorithm aims to output an estimate $\tilde{h} \in \{0,1\}$ of the hypothesis $h_{\tilde{s}}(x)$ for the input x so as to satisfy

$$\mathop{\mathbf{Pr}}_{x\sim\mathcal{D}_N}\left[\mathbf{Pr}\left[\tilde{h} = h_{\tilde{s}}(x)\right] \geq 1-\delta\right] \geq 1-\epsilon, \tag{B41}$$

where the inner probability is taken over the randomness of the evaluation algorithm. To this goal, we set the internal parameters in Algorithm S2 as

$$\begin{aligned}
\mu &= \epsilon && \text{(B42)}\\
\nu &= \delta. && \text{(B43)}
\end{aligned}$$

In algorithm S2, an unseen input x is initially given by sampling from the target distribution $\mathcal{D}_N$. Then, the algorithm probabilistically computes the quantumly advantageous function f_N for the input x, using the same quantum algorithm $\mathcal{A}$ as that used in our learning algorithm, i.e., that in (B7) and (B8), yet with the parameters μ in (B42) and ν in (B43). We let $\mathcal{A}(x)$ denote the output of $\mathcal{A}$ in (B7) for the input x, where we will omit μ and ν for simplicity of notation if it is obvious from the context. Note that $\mathcal{A}$ may not be a deterministic algorithm; that is, we may have $\mathcal{A}(x) = f_N(x)$ only probabilistically, as shown in (B7). Finally, using the given parameter $\tilde{s}$ of the hypothesis $h_{\tilde{s}}$, the evaluation algorithm calculates the bitwise inner product of $\mathcal{A}(x)$ obtained from the above computation and $\tilde{s}$, so as to output

$$\tilde{h} \coloneqq \mathcal{A}(x) \cdot \tilde{s}. \tag{B44}$$

We now prove the quantumly efficient evaluatability of the hypothesis class $\mathcal{H}_N$ in (B12) by Algorithm S2 as follows.

Theorem S12 (Quantumly efficient evaluatability)**.** *For any N, $D = O(\mathsf{poly}(N))$, any target distribution $\mathcal{D}_N$ over the N-bit input space $\mathcal{X}_N \subseteq \{0,1\}^N$, and any quantumly advantageous function $f_N : \{0,1\}^N \to \mathbb{F}_2^D$ under $\mathcal{D}_N$, the hypothesis class $\mathcal{H}_N$ in* (B12) *with f_N, parameterized by $\tilde{s} \in \mathbb{F}^D$, is quantumly efficiently evaluatable by Algorithm S2.*

Proof. In the following, we will first discuss the success probability of our evaluation algorithm and then provide an upper bound of the runtime.

The probabilistic part of Algorithm S2 is confined solely to the computation of $f_N(x)$ by the quantum algorithm $\mathcal{A}$, and the other parts, such as the bitwise inner product, are deterministic. The requirement for this probabilistic part is that the quantum algorithm $\mathcal{A}$ should compute $f_N(x)$ correctly for a large fraction $1-\epsilon$ of the given input x with high probability at least $1-\delta$, i.e.,

$$\Pr_{x\sim\mathcal{D}_N}\left[\Pr\left[\mathcal{A}(x) = f_N(x)\right] \geq 1-\delta\right] \geq 1-\epsilon. \tag{B45}$$

Using $\mathcal{A}$ in (B7) with μ chosen as (B42) and ν as (B43), we fulfill this requirement. Conditioned on having

$$\mathcal{A}(x) = f_N(x), \tag{B46}$$

the output $\tilde{h}$ in (B44) becomes

$$\tilde{h} = \mathcal{A}(x)\cdot\tilde{s} = f_N(x)\cdot\tilde{s} = h_{\tilde{s}}(x). \tag{B47}$$

Consequently, Algorithm S2 outputs $\tilde{h}$ satisfying

$$\Pr_{x\sim\mathcal{D}_N}\left[\Pr\left[\tilde{h} = h_{\tilde{s}}(x)\right] \geq 1-\delta\right] \geq 1-\epsilon, \tag{B48}$$

as required for the evaulatability in Definition S2.

The runtime of Algorithm S2 is dominated by the computation of f_N by $\mathcal{A}$ and the bitwise inner product. We first consider the runtime $t_{\mathcal{A}}$ of $\mathcal{A}$ for the input x. We have the algorithm $\mathcal{A}$ satisfying (B8). Accordingly, with μ chosen as (B42) and ν as (B43), we have

$$t_{\mathcal{A}}(x) = O\left(\left(\frac{N}{\mu\nu}\right)^{\alpha}\right) \tag{B49}$$

$$= O\left(\left(\frac{N}{\epsilon\delta}\right)^{\alpha}\right). \tag{B50}$$

Also, the runtime of the bitwise inner product of vector in the D-dimensional vector space $\mathbb{F}_2^D$ over the finite field in (B44) is

$$O(D). \tag{B51}$$

Thus, for μ in (B42), ν in (B43), and $D = O(\mathsf{poly}(N)) = O(N^{\beta})$ with some $\beta > 0$, the overall runtime of Algorithm S2 is upper bounded by

$$O\left(\left(\frac{N}{\epsilon\delta}\right)^{\alpha}\right) + O(D) \tag{B52}$$

$$= O\left(\left(\frac{N}{\epsilon\delta}\right)^{\alpha}\right) + O\left(N^{\beta}\right) \tag{B53}$$

$$= O\left(\mathsf{poly}\left(N, \frac{1}{\epsilon}, \frac{1}{\delta}\right)\right), \tag{B54}$$

as required for the efficient evaluatablity in Definition S2. □

3. Provable hardness for any polynomial-time classical algorithm

In this section, we prove the classical hardness of efficient learning and efficient evaluation for our concept class in Definition S9. Our proof is given by contradiction; that is, we will prove that, assuming that there exists a classically efficient evaluatable hypothesis class (Definition S2) for classically efficient learnability (Definition S1) of our concept class, one would be able to construct a polynomial-time classical algorithm to compute a quantumly advantageous function f_N in Definition S8 using the polynomial-time classical algorithms for evaluating the hypotheses in this hypothesis class. This classical algorithm is presented in Algorithm S3. The rest of this section first describes this classical algorithm for the reduction of evaluating hypotheses to computing f_N and then provides the full proof of the classical hardness.

To see the significance of our construction of this classical algorithm for the reduction, recall that it has been challenging to prove the classical hardness of learning without relying on discrete logarithms or integer factoring, which are solved by Shor's algorithms; by contrast, our proof of the classical hardness is applicable to any quantumly advantageous function beyond the scope of Shor's algorithms. Note that, in this direction, Refs. [18, 19] have also considered a concept class to show the advantage of QML based on general quantum computational advantages, but their results were applicable only to polynomial-size concept classes that can be learned by a brute-force algorithm, and our interest here is exponential-size concept classes that cannot be learned in such a brute-force approach. The technique of the proof by contradiction itself may be well established in the complexity theory and also used info showing the classical hardness of learning in the previous works [5, 6, 16–20, 24]. However, the existing proofs of the classical hardness in these previous works essentially depend on a specific mathematical structure of discrete logarithms and integer factoring, so as to go through a cryptographic argument based on these computational problems. To go beyond the realm of Shor's algorithms, novel techniques without relying on the existing cryptographic approach need to be developed. In contrast with these existing works, for our exponential-size concept class with its feature space formulated as the space of bit strings, which is quantumly efficiently learnable and evaluatable as shown in Sec. B 2, we prove the classical hardness based on any quantumly advantageous func-

Algorithm S3 Classical algorithm for the reduction of evaluating the hypotheses for the concept class in Definition S9 to computing the quantumly advantageous function in Definition S8

```
Input: A new input $x \in \mathcal{X}_N$ sampled from the target distribution $\mathcal{D}_N$, $\mu, \nu, \xi > 0$, a randomized advice string $\alpha \sim \mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}$ in (B67) providing the representations $\alpha = (\sigma_{h_{s_1}}, \ldots, \sigma_{h_{s_D}})$ of $D$ hypotheses $h_{s_1}, \ldots, h_{s_D}$ in (B62) for the concept class $\mathcal{C}_N$ in Definition S9.
Output: An estimate $\tilde{f}$ of a quantumly advantageous function $\tilde{f}_N(x)$ for $\mathcal{C}_N$ achieving (B55) and (B56).
for $d = 1, \ldots, D$ do
    Perform the quantum algorithm $\mathcal{A}$ in (B64) and (B65) for $x$, $\sigma_{h_{s_1}}$, $\epsilon$ in (B59), and $\delta$ in (B60), to compute an estimate $\tilde{h}_{s_d} \in \{0,1\}$ of $h_{s_d}(x)$.
end for
return $\tilde{f} = \left(\tilde{h}_{s_1}, \ldots, \tilde{h}_{s_1}\right)^\top$ in (B66).
```

tions in Definition S8, without depending on any specific quantum algorithm such as Shor's algorithms.

To show this, for any target distribution $\mathcal{D}_N$, any quantumly advantageous function $f_N : \{0,1\}^N \to \mathbb{F}_2^D$ under $\mathcal{D}_N$ in Definition S8 with $D = O(\mathsf{poly}(N))$, and our concept class $\mathcal{C}_N$ in Definition S9, we assume that $\mathcal{C}_N$ is classically efficiently learnable as in Definition S2 by a hypothesis class $\mathcal{H}_N$, and the hypothesis class $\mathcal{H}_N$ is classically efficiently evaluatable as in Definition S2. Under this assumption, we construct a polynomial-time classical algorithm for the reduction of the efficient evaluation of the hypotheses in $\mathcal{H}_N$ to the computation of f_N, as shown in Algorithm S3, which will lead to the contradiction. Given an input x drawn from $\mathcal{D}_N$ and an appropriate choice of a polynomial-length randomized advice string α sampled from a advice distribution $\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}$ as in the definition of $\mathsf{HeurFBPP/rpoly}$ in (A16), the goal of Algorithm S3 is, for all $0 < \mu < 1$, $0 < \nu < 1$, and $0 < \xi < 1$, to output an estimate $\tilde{f} \in \mathbb{F}_2^D$ of $f_N(x)$ satisfying

$$\underset{x\sim\mathcal{D}_N}{\mathbf{Pr}}\left[\underset{\alpha\sim\mathcal{D}^{\mathrm{adv}}_{N,\mu,\nu,\xi}}{\mathbf{Pr}}\left[\mathbf{Pr}[\mathcal{A}(x,\alpha,\mu,\nu,\xi) = f_N(x)]\right.\right.$$
$$\left.\left.\geq 1-\nu\right] \geq 1-\xi\right] \geq 1-\mu, \tag{B55}$$

within runtime

$$t_{\mathcal{A}}(x,\alpha,\mu,\nu,\xi) = O\left(\mathsf{poly}\left(N, \frac{1}{\mu}, \frac{1}{\nu}, \frac{1}{\xi}\right)\right), \tag{B56}$$

where α will be given from distributions of the representations of D hypotheses in $\mathcal{H}_N$ as described below. To this goal, we set the internal parameters in Algorithm S3 as

$$\epsilon_{\mathrm{learn}} = \frac{\mu}{2D}, \tag{B57}$$

$$\delta_{\mathrm{learn}} = \frac{\xi}{D}, \tag{B58}$$

$$\epsilon_{\mathrm{eval}} = \frac{\mu}{2D}, \tag{B59}$$

$$\delta_{\mathrm{eval}} = \frac{\nu}{D}. \tag{B60}$$

In Algorithm S3, an input x drawn from the distribution $\mathcal{D}_N$ is initially given, and the representations of hypotheses for D concepts in our concept class $\mathcal{C}_N$ are also initially given. In particular, let

$$\{s_d \in \mathbb{F}_2^D\}_{d=1,\ldots,D} \tag{B61}$$

denote the standard basis of the D-dimensional vector space $\mathbb{F}_2^D$, where the dth element of the vector $s_d \in \mathbb{F}_2^D$ is 1, and all the other elements of s_d are 0. Then, under the assumption of the classically efficient learnability of $\mathcal{C}_N$, for each s_d and all $0 < \epsilon_{\mathrm{learn}}, \delta_{\mathrm{learn}} < 1$, there should exist a classical algorithm that outputs, with a high probability of at least $1 - \delta_{\mathrm{learn}}$, a representation $\sigma_{h_{s_d}}$ of a hypothesis h_{s_d} such that

$$\underset{x\sim\mathcal{D}_N}{\mathbf{Pr}}\left[h_{s_d}(x) \neq c_{s_d}(x)\right] \leq \epsilon_{\mathrm{learn}}, \tag{B62}$$

and $\sigma_{h_{s_d}}$ should be of polynomial length

$$\mathrm{size}\left(\sigma_{h_{s_d}}\right) = O\left(\left(\frac{N}{\epsilon_{\mathrm{learn}}\delta_{\mathrm{learn}}}\right)^{\eta}\right), \tag{B63}$$

where $\eta > 0$ is an upper bound of the degree of the polynomial length. Note that our proof of the hardness does not use the learning algorithm directly in Algorithm S3, but the assumption of classically efficient learnability is used to guarantee the existence of the hypotheses that approximate the concepts well and have polynomial-length representations, as in (B62) and (B63).

Furthermore, under the assumption of the classically efficient evaluatability of this hypothesis class, there should exist a classical (randomized) algorithm $\mathcal{A}$ such that for the representation $\sigma_{h_{s_d}}$ of each hypothesis h_{s_d} with s_d in (B61), and all $0 < \epsilon_{\mathrm{eval}}, \delta_{\mathrm{eval}} < 1$, the algorithm $\mathcal{A}$ outputs an estimate $\tilde{h}_{s_d} \in \{0,1\}$ of $h_{s_d}(x)$ satisfying

$$\underset{x\sim\mathcal{D}_N}{\mathbf{Pr}}\left[\mathbf{Pr}\left[\tilde{h}_{s_d} = h_{s_d}(x)\right] \geq 1 - \delta_{\mathrm{eval}}\right] \geq 1 - \epsilon_{\mathrm{eval}}, \tag{B64}$$

within polynomial runtime for all x in the support of $\mathcal{D}_N$

$$t_{\mathcal{A}}\left(x, \sigma_{h_{s_d}}, \epsilon_{\mathrm{eval}}, \delta_{\mathrm{eval}}\right) = O\left(\left(\frac{N}{\epsilon_{\mathrm{eval}}\delta_{\mathrm{eval}}}\right)^{\gamma}\right), \tag{B65}$$

where $\gamma > 0$ is an upper bound of the degree of the polynomial runtime.

Under this assumption on the classically efficient learnability and the classically efficient evaluatability, Algorithm S3 uses the classical evaluation algorithm $\mathcal{A}$ to compute each of the D hypotheses $h_{s_1}(x), \ldots, h_{s_D}(x)$ for the input x, to obtain $\tilde{h}_{s_1}, \ldots, \tilde{h}_{s_D}$. Note that $\mathcal{A}$ may not be a deterministic algorithm, and thus, we may have $\tilde{h}_{s_d} = h_{s_d}(x)$ only probabilistically. But if it holds that $\tilde{h}_{s_d} = h_{s_d}(x) = c_{s_d}(x)$, then $\tilde{h}_{s_d}$ is the dth bit of $f_N(x) \in \mathbb{F}_2^D$, as can be seen from (B2). Using this property of the vector space of bit strings, from the computed values $\tilde{h}_{s_1}, \ldots, \tilde{h}_{s_D} \in \{0,1\}$, Algorithm S3 outputs

$$\tilde{f} := \begin{pmatrix} \tilde{h}_{s_1} \\ \tilde{h}_{s_2} \\ \vdots \\ \tilde{h}_{s_D} \end{pmatrix} \in \mathbb{F}_2^D \tag{B66}$$

as an estimate of $f_N(x)$.

Using the reduction achieved by Algorithm S3, we prove that our concept class $\mathcal{C}_N$ is not classically efficiently learnable by any classically efficiently evaluatable hypothesis class. We also note that, in previous works [5, 16, 17, 24] of the classical hardness of learning tasks, efficient evaluatability was defined in terms of worst-case complexity; by contrast, motivated by the practical applicability as discussed in Section A 1, our definition of efficient evaluatablity in Definition S2 is in terms of heuristic complexity. Since the heuristic complexity classes include the corresponding worst-case complexity classes as discussed in Section A 2, our proof of the classical hardness of our learning tasks for the heuristic complexity implies the more conventional classical hardness for the worst-case complexity as well.

Theorem S13 (Classical hardness)**.** *For any N, $D = O(\mathsf{poly}(N))$, any target distribution $\mathcal{D}_N$ over the N-bit input space $\mathcal{X}_N \subseteq \{0,1\}^N$, and any quantumly advantageous function $f_N : \{0,1\}^N \to \mathbb{F}_2^D$ under $\mathcal{D}_N$, the concept class $\mathcal{C}_N$ in Definition S9 with f_N is not classically efficiently learnable by any classically efficiently evaluatable hypothesis class.*

Proof. We prove the statement by contradiction; i.e., we show that, under the assumption that $\mathcal{C}_N$ is classically efficiently learnable by some classically efficiently evaluatable hypothesis class, there should exist a classical randomized algorithm (Algorithm S3) with a polynomial-length randomized advice string α achieving (B55) and (B56) for the reduction to computing the quantum advantageous function f_N. In the following, we first analyze the length of α. Then, we consider the success probability of our algorithm for the reduction. Finally, we discuss the runtime of our algorithm for the reduction.

The length of the randomized advice string α is bounded as follows. We let the advice distribution $\mathcal{D}_{N,\mu,\nu,\xi}^{\mathrm{adv}}$ be the output distribution of the classical randomized algorithm for efficient learning that outputs the representations of the D hypothesis satisfying (B62) and (B63), and we use these representations as the randomized advice string

$$\alpha := \left(\sigma_{h_{s_1}}, \ldots, \sigma_{h_{s_D}}\right). \tag{B67}$$

Due to (B63), (B57), (B58), and $D = O(\mathsf{poly}(N)) = N^\beta$ for some $\beta > 0$, the total length of α is

$$\sum_{d=1}^{D} \mathrm{size}(\sigma_{h_{s_d}}) = O\left(D \times \left(\frac{N}{\epsilon_{\mathrm{learn}}\delta_{\mathrm{learn}}}\right)^\eta\right) \tag{B68}$$

$$= O\left(\frac{N^{\beta\eta+\beta+\eta}}{\mu^\eta}\right), \tag{B69}$$

as required for $\mathsf{HeurFBPP/rpoly}$ in (A16).

Regarding the success probability of Algorithm S3, conditioned on having α in (B67) with (B62) satisfied for all $d \in \{1, \ldots, D\}$ as in (B72), the remaining probabilistic parts of the algorithm are the input x from $\mathcal{D}_N$ inducing the error between the hypotheses $h_{s_1}(x), \ldots, h_{s_D}(x)$ and the true concepts $c_{s_1}(x), \ldots, c_{s_D}(x)$ in (B62), and the computations of the estimates $\tilde{h}_{s_1}, \ldots, \tilde{h}_{s_D}$ of the hypotheses $h_{s_1}(x), \ldots, h_{s_D}(x)$ by the evaluation algorithm $\mathcal{A}$ in (B64). The other parts, such as the output of $\tilde{f}$ from $\tilde{h}_{s_1}, \ldots, \tilde{h}_{s_D}$ in (B66), are deterministic, as shown in Algorithm S3. In Algorithm S3, we require that the representation α in (B67) of the D hypothesis $h_{s_1}(x), \ldots, h_{s_D}(x)$ sampled from $\mathcal{D}_{N,\mu,\nu,\xi}^{\mathrm{adv}}$ should simultaneously coincide with the true concepts $c_{s_1}(x), \ldots, c_{s_D}(x)$, i.e.,

$$h_{s_1}(x) = c_{s_1}(x), \ldots, h_{s_D}(x) = c_{s_D}(x). \tag{B70}$$

With our choice of $\epsilon_{\mathrm{learn}}$ in (B57) and δ_{learn} in (B58), due to (B62) and the union bound, this requirement is fulfilled for a large fraction of x at least

$$1 - D\epsilon_{\mathrm{learn}} = 1 - \frac{\mu}{2}, \tag{B71}$$

for a large fraction of the randomized advice string at least

$$1 - D\delta_{\mathrm{learn}} = 1 - \xi. \tag{B72}$$

In addition, we require that the estimates $\tilde{h}_{s_1}, \ldots, \tilde{h}_{s_D}$ simultaneously coincides with these hypotheses $h_{s_1}(x), \ldots, h_{s_D}(x)$, i.e.

$$\tilde{h}_{s_1} = h_{s_1}(x), \ldots, \tilde{h}_{s_D} = h_{s_D}(x). \tag{B73}$$

With our choice of ϵ_{eval} in (B59) and δ_{eval} in (B60), due to (B64) and the union bound, this requirement is fulfilled for a large fraction of x at least

$$1 - D\epsilon_{\mathrm{eval}} = 1 - \frac{\mu}{2}, \tag{B74}$$

with a high probability of at least

$$1 - D\delta_{\mathrm{eval}} = 1 - \nu. \tag{B75}$$

Given the requirements in (B70) and (B73), due to (B66), the output of Algorithm S3 is

$$\tilde{f} = \begin{pmatrix} \tilde{h}_{s_1} \\ \tilde{h}_{s_2} \\ \vdots \\ \tilde{h}_{s_D} \end{pmatrix} = \begin{pmatrix} c_{s_1}(x) \\ c_{s_2}(x) \\ \vdots \\ c_{s_D}(x) \end{pmatrix} = f_N(x), \tag{B76}$$

where the last equality follows from (B2) since $\{s_d\}_d$ is the standard basis of the D-dimensioanl vector space $\mathbb{F}_2^D$. Consequently, due to (B71), (B72), (B74), (B75), and the union bound, the requirements in (B70) and (B73) are simultaneously fulfilled for a large fraction of x at least

$$1-\mu, \tag{B77}$$

for a large fraction of α at least

$$1-\xi, \tag{B78}$$

with a high probability of at least

$$1-\nu, \tag{B79}$$

which yields the success probability of our algorithm as required for HeurFBPP/rpoly in (A16).

The runtime of Algorithm S3 is determined by the evaluations of the D hypotheses and the bitwise inner product. For any x and every $d \in 1, \ldots, D$, the runtime of the classical algorithm $\mathcal{A}$ for computing h_{s_d} is given by

$$t_{\mathcal{A}}\left(x, \sigma_{h_{s_d}}, \epsilon_{\text{eval}}, \delta_{\text{eval}}\right) = O\left(\left(\frac{N}{\epsilon_{\text{eval}}\delta_{\text{eval}}}\right)^{\gamma}\right), \tag{B80}$$

as shown in (B65). Thus, the runtime of the D evaluations is

$$\sum_{d=1}^{D} t_{\mathcal{A}}\left(x, \sigma_{h_{s_d}}, \epsilon_{\text{eval}}, \delta_{\text{eval}}\right) = O\left(D\left(\frac{N}{\epsilon_{\text{eval}}\delta_{\text{eval}}}\right)^{\gamma}\right). \tag{B81}$$

In addition, the runtime of the output of the D-dimensional vector $\tilde{f}$ in (B66) is

$$O(D). \tag{B82}$$

Due to (B81) and (B82), for ϵ_{eval} in (B59), δ_{eval} in (B60), and $D = O(N^{\beta})$ with some constant $\beta > 0$, the overall runtime of Algorithm S3 is upper bounded by

$$\begin{aligned} &O\left(D\left(\frac{N}{\epsilon_{\text{eval}}\delta_{\text{eval}}}\right)^{\gamma}\right) + O(D) \\ &= O\left(N^{\beta}\left(\frac{N^{\gamma}N^{\beta\gamma}N^{\beta\gamma}}{\mu^{\gamma}\nu^{\gamma}}\right)\right) \\ &= O\left(\frac{N^{2\beta\gamma+\beta+\gamma}}{\mu^{\gamma}\nu^{\gamma}}\right) \\ &= O\left(\mathsf{poly}\left(N, \frac{1}{\mu}, \frac{1}{\nu}\right)\right), \end{aligned} \tag{B83}$$

as required for HeurFBPP/rpoly in (A16).

Consequently, under the assumption that $\mathcal{C}_N$ is classically efficiently learnable by some classically efficiently evaluatable hypothesis class, one would be able to construct Algorithm S3 achieving (B55) and (B56); that is, the problem $\{(f_N, \mathcal{D}_N)\}$ would be in HeurFBPP/rpoly. This contradicts Definition S8 of the quantum advantageous function f_N. □

Appendix C: Data-preparation protocols for demonstrating advantage of QML from general computational advantages

In this section, we propose protocols for preparing the sample data for our learning tasks studied in Section B so as to demonstrate the advantage of QML using our learning tasks. A nontrivial part of our analysis of this data preparation is that the sample data can be prepared only probabilistically in our general setting; after all, the quantumly advantageous functions used for our concept class in Definition S9 are defined for probabilistic algorithms and heuristic complexity classes in general. Nevertheless, we provide feasible conditions for the correct data preparation. The rest of this section is organized as follows. In Section C 1, we provide a two-party setup for demonstrating the advantage of QML with one party preparing the data and the other learning from the data. In Section C 2, we describe a protocol using quantum computation to prepare the correct sample data with a high success probability for the demonstration. In Section C 3, we describe another protocol using classical computation to prepare the sample data with a high success probability for the demonstration, in special cases where the quantumly advantageous function is constructed based on a class of one-way permutation that is hard to invert by a polynomial-time classical algorithm but can be inverted by a polynomial-time quantum algorithm.

1. Setup for demonstrating advantage of QML from general computational advantages

This section provides a setup for demonstrating the advantage of QML. In other words, we propose a learning setting including data preparation.

In our setup, we consider two parties; a party A is in charge of data preparation, and the other party B receives sample data from A to perform learning. The party A uses either quantum or classical computers to prepare the data while B does not know how A has prepared the data. The data should be prepared in such a way that B can achieve the learning if B uses the quantum learning algorithm in Section B 2 but cannot if B is limited to any polynomial-time classical learning method as in Section B 3. See also the main text for an illustration of the setup.

The overall protocol for A and B demonstrating the advantage of QML in this setup is as follows. First, two parties A and B are given the problem size N, the concept class $\mathcal{C}_N = \{c_s\}_{s\in\mathbb{F}_2^D}$ specified by the quantumly advantageous function $f_N : \mathbb{F}_2^N \to \mathbb{F}_2^D$ under a target distribution $\mathcal{D}_N$ in Definition S9, the error parameter ϵ and the confidence parameter δ, where $D = O(\mathsf{poly}(N))$. Note that the description of $\mathcal{D}_N$ may be unknown to A and B throughout the protocol, but A has access to (an oracle to load) an $O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ amount of the inputs x sampled from $\mathcal{D}_N$ within a unit time per loading each input. Given these parameters, based on (B4), B determines the number of samples for learning as

$$M = \left\lceil \frac{D}{\epsilon} - 1 \right\rceil, \tag{C1}$$

where $\lceil \cdots \rceil$ is the ceiling function, and send M to A. Then, A decides the parameter s of the target concept c_s arbitrarily and keeps s as A's secret. For M and s, the task of A is to correctly prepare the M sample data

$$\{(x_m, c_s(x_m))\}_{m=1}^{M}, \tag{C2}$$

using a quantum or classical computer. After preparing the M data in (C2), A sends the data to B. Using the given sample data, the task of B is to find a parameter $\tilde{s} \in \mathbb{F}_2^D$ and make a prediction for new input x drawn from $\mathcal{D}_N$ by the hypothesis $h_{\tilde{s}}(x) = f(x) \cdot \tilde{s}$ so that the error should satisfy

$$\mathop{\mathbf{Pr}}_{x \sim \mathcal{D}_N} [h_{\tilde{s}}(x) \neq c_s(x)] \leq \epsilon \tag{C3}$$

with a high probability of at least $1 - \delta$.

Using Algorithm S1 and Algorithm S2, B can achieve this task with quantum computation within a polynomial time

$$O(\mathsf{poly}(N, 1/\epsilon, 1/\delta), \tag{C4}$$

and our analysis in Section B 3 shows that B cannot achieve this task with any polynomial-time classical method. In the following sections, we will construct A's algorithms for preparing the data in (C2) with a high probability of at least $1 - \delta$ within a polynomial time

$$O(\mathsf{poly}(N, 1/\epsilon, 1/\delta)). \tag{C5}$$

With a sufficient amount of correct data, one can conduct the learning and test the learned hypothesis. Thus, with A's data-preparation algorithm and B's learning and evaluation algorithms, our protocol in the above setup can demonstrate the advantage of QML.

2. Quantum algorithm for preparing data

In this section, we show how to prepare the sample data in (C2) for the concept class in Definition S9 based on a quantumly advantageous function f_N in Definition S8, using a quantum algorithm.

Algorithm S4 Quantum algorithm for data preparation

```
Input: The problem size $N$, the concept class $\mathcal{C}_N$ in Definition S9 with a quantumly advantageous function $f_N$, $\epsilon > 0$, $\delta > 0$, the number $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ of samples to be prepared (e.g., given by (C1)), the true parameter $s$ of the target concept, inputs sampled from a target distribution $\mathcal{D}_N$ to be loaded from an oracle.
Output: An estimate $\{(x_m, \tilde{c}_m)\}_{m=1}^{M}$ of the $M$ sample data $\{(x_m, c_s(x_m))\}_{m=1}^{M}$ satisfying (C6) with a high probability at least $1 - \delta$.
for $m = 1, \ldots, M$ do
    Load an input $x_m$ sampled from the target distribution $\mathcal{D}_N$ (with access to the oracle).
    Perform the quantum algorithm $\mathcal{A}$ in (B7) for computing $f_N$ for the input $x_m$ with the parameters $\mu$ and $\nu$ in (C7) and (C8), respectively, to obtain $\mathcal{A}(x_m)$.
    Compute $\tilde{c}_m = \mathcal{A}(x_m) \cdot s$ in (C9).
end for
return $\{(x_m, \tilde{c}_m)\}_{m=1}^{M}$.
```

The data-preparation algorithm is shown in Algorithm S4. As described in Section C 1, given the problem size N, the concept class $\mathcal{C}_N$ in Definition S9 with a quantumly advantageous function f_N, the error parameter ϵ, the significance parameter δ, the number $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ of samples to be prepared (e.g., given by (C1), yet we here describe the algorithm for general M), and the true parameter s of the target concept, we assume that Algorithm S4 has access to (an oracle to load) an $O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ amount of the inputs x sampled from $\mathcal{D}_N$ within a unit time per loading each input. Then, the goal of Algorithm S4 is to output an estimate $\{(x_m, \tilde{c}_m)\}_{m=1}^{M}$ of the data $\{(x_m, c_s(x_m))\}_{m=1}^{M}$ in (C2) with x_m drawn from the target distribution $\mathcal{D}_N$, so that it should hold with a high probability at least $1 - \delta$ that, for all m,

$$\tilde{c}_m = c_s(x_m). \tag{C6}$$

Note that the error parameter ϵ is not explicitly relevant to Algorithm S4 except for the possibility of M depending on ϵ. To this goal, we set the internal parameters in Algorithm S4 as

$$\mu = \frac{\delta}{2M}, \tag{C7}$$

$$\nu = \frac{\delta}{2M}. \tag{C8}$$

In Algorithm S4, for each $m = 1, \ldots, M$, we start with sampling x_m from the target distribution $\mathcal{D}_N$. Then, we use the quantum algorithm $\mathcal{A}$ in (B7) to compute the quantumly advantageous function f_N with μ in (C7) and ν in (C8), to obtain $\mathcal{A}(x_m)$ within a polynomial runtime in (B8), where μ and ν in (B7) may be omitted for simplicity of the presentation if obvious from the context. Finally, Algorithm S4 computes an estimate $\tilde{c}_m$ of $c_s(x_m)$ by

$$\tilde{c}_m \coloneqq \mathcal{A}(x_m) \cdot s, \tag{C9}$$

in accordance with the definition of c_s in (B2). After performing these computations for all m, the algorithm outputs

$$\{(x_m, \tilde{c}_m)\}_{m=1}^{M} \tag{C10}$$

as an estimate of the data $\{(x_m, c_s(x_m))\}_{m=1}^{M}$ in (C2).

The following theorem shows that this algorithm prepares the data in (C2) correctly with a high probability $1-\delta$ within a polynomial time.

Theorem S14 (The polynomial-time data preparation with a quantum algorithm)**.** *Given any N, ϵ, and δ, for any $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$, Algorithm S4 outputs the M sample data $\{(x_m, c_s(x_m))\}_{m=1}^{M}$ in (C2) with a high probability at least $1-\delta$ within a polynomial time*

$$O(\mathsf{poly}(N, 1/\epsilon, 1/\delta)). \tag{C11}$$

Proof. We will first discuss the success probability of Algorithm S4 and then provide an upper bound of the runtime.

The probabilistic parts of Algorithm S4 are the computations of f_N by the quantum algorithm $\mathcal{A}$. We require that for all $m \in \{1, \ldots, M\}$, the output $\mathcal{A}(x_m)$ of this quantum algorithm should coincide with $f_N(x_m)$ simultaneously, i.e.

$$\mathcal{A}(x_1) = f_N(x_1), \ldots, \mathcal{A}(x_M) = f_N(x_M). \tag{C12}$$

Given this requirement, the output of Algorithm S4 coincides with the data in (C2); that is, $\tilde{c}_m$ in (C9) satisfies

$$\tilde{c}_m = \mathcal{A}(x_m) \cdot s = f_N(x_m) \cdot s = c_s(x_m), \tag{C13}$$

by definition of c_s in (B2). With our choice of μ in (C7) and ν in (C8), due to the union bound, this requirement is fulfilled with a high probability at least

$$1 - M(\mu + \nu) = 1 - \delta, \tag{C14}$$

which yields the desired success probability.

The runtime of Algorithm S4 is determined by the computations of f_N and the bitwise inner product. Due to (B8) with the choice of μ in (C7) and ν in (C8), for $D = O(N^{\beta})$ with $\beta > 0$ and $M = O((\frac{N}{\epsilon\delta})^{\lambda})$ with $\lambda > 0$, we have the overall runtime

$$O\left(M\left(\left(\frac{N}{\mu\nu}\right)^{\alpha} + D\right)\right) \tag{C15}$$

$$= O\left(\frac{N^{\alpha+2\alpha\lambda+\lambda}}{\epsilon^{(2\alpha+1)\lambda}\delta^{2\alpha\lambda+2\alpha+\lambda}} + \frac{N^{\beta+\lambda}}{\epsilon^{\lambda}\delta^{\lambda}}\right) \tag{C16}$$

$$= O\left(\mathsf{poly}\left(N, 1/\epsilon, 1/\delta\right)\right), \tag{C17}$$

which yields the conclusion. □

3. Classical algorithm for preparing data based on classically one-way permutation

In this section, we show how to prepare the sample data in (C2) using a classical algorithm, for a concept class derived by replacing the quantumly advantageous function used in Definition S9 with an inverse of a classically one-way permutation introduced in the following.

We define the classically one-way permutation to derive the concept class for preparing the data with the classical algorithm.

Definition S15 (Classically one-way permutation)**.** *For N, let $f_N^{\mathrm{OWP}} : \{0,1\}^N \to \{0,1\}^N$ be a permutation (i.e., an N-bit one-to-one function), where we may write $\mathbb{F}_2^N = \{0,1\}^N$. We write*

$$x = f_N^{\mathrm{OWP}}(y), \tag{C18}$$

where sampling x from a probability distribution $\mathcal{D}_N$ with computing $y = f_N^{\mathrm{OWP}^{-1}}(x)$ is equivalent to sampling y from a probability distribution $\mathcal{D}_N^Y$ with computing (C18) under the condition that

$$\mathcal{D}_N = f_N^{\mathrm{OWP}}(\mathcal{D}_N^Y). \tag{C19}$$

We say that a permutation f_N^{OWP} is a classically one-way permutation f_N^{OWP} under $\mathcal{D}_N$ if the relation $R := \{R_N\}_{N\in\mathbb{N}}$ with $R_N := \{(y, f_N^{\mathrm{OWP}}(y))\}_{y\in\{0,1\}^N}$ is in FP*, and the distributional function problem $\{(f_N^{\mathrm{OWP}^{-1}}, \mathcal{D}_N)\}_{N\in\mathbb{N}}$ is in* HeurFBQP *but not in* HeurFBPP/rpoly*.*

We then introduce the following concept class by replacing the quantumly advantageous function in the concept class of Definition S9 with the classically one-way permutation in Definition S15.

Definition S16 (Concept class based on classically one-way permutation)**.** *For any N, any probability distribution $\mathcal{D}_N$ over $\mathbb{F}_2^N$, and any classically one-way permutation $f_N^{\mathrm{OWP}} : \mathbb{F}_2^N \to \{0,1\}^N$ under $\mathcal{D}_N$ in Definition S15, we define a concept class $\mathcal{C}_N^{\mathrm{OWP}}$ over the input space $\mathcal{X}_N$ as $\mathcal{C}_N^{\mathrm{OWP}} := \{c_s\}_{s\in\mathbb{F}_2^N}$, where $\mathcal{X}_N$ is the support of $\mathcal{D}_N$ in (C19), and c_s is a concept given by*

$$c_s(x) := f_N^{\mathrm{OWP}^{-1}}(x) \cdot s \in \mathbb{F}_2 = \{0,1\}, \tag{C20}$$

with $f_N^{\mathrm{OWP}^{-1}}(x) \cdot s$ denoting a bitwise inner product in the vector space $\mathbb{F}_2^N$ over the finite field.

By definition, the inverse $f_N^{\mathrm{OWP}^{-1}}$ of the classically one-way permutation f_N^{OWP} in Definition S16 is a special case of the quantumly advantageous functions in Definition S9. Therefore, the quantum efficient learnability, the quantum efficient evaluatability, and the classical hardness for this concept class follow from the same argument as Section B. Note that particular variants of classically one-way permutations f_N^{OWP} that can be inverted by Shor's algorithms are used in the previous work on the advantage of QML [16–19]. Since f_N^{OWP} is a permutation, if the target distribution $\mathcal{D}_N$ is uniform, then Algorithm S5 simply samples from the uniform distribution, which is assumed in Refs. [16–19]. By contrast, our analysis does not assume the uniform distribution, generalizing the settings in Refs. [16–19]. And even more importantly, the concept class in Definition S16 does not depend on specific cryptographic techniques for the classically one-way permutation f_N^{OWP} such as those invertible by Shor's algorithms, in the same way as the concept class in Definition S9 without depending on the specific

Algorithm S5 Classical algorithm for data preparation with classically one-way function

```
Input: The problem size $N$, the concept class $\mathcal{C}_N$ in Definition S16 with a classically one-way permutation $f_N^{\mathrm{OWP}}$,
    $\epsilon > 0$, $\delta > 0$, the number $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ of samples to be prepared (e.g., given by (C1)), the true
    parameter $s$ of the target concept, and parameters $y$ sampled from a probability distribution $\mathcal{D}_N^Y$ in (C19) to be
    loaded from an oracle.
Output: The $M$ sample data $\{(x_m, c_s(x_m))\}_{m=1}^M$ in (C21).
for $m = 1, \ldots, M$ do
    Load a parameter $y_m$ sampled from the distribution $\mathcal{D}_N^Y$ (with access to the oracle).
    Perform the deterministic classical algorithm in (C22) to compute $f_N^{\mathrm{OWP}}$ for $y_m$, to obtain $x_m = f_N^{\mathrm{OWP}}(y_m)$.
    Compute $c_s(x_m) = y_m \cdot s$ in (C24).
end for
return $\{(x_m, c_s(x_m))\}_{m=1}^M$.
```

mathematical structure of quantumly advantageous functions.

In the following, based on the setup described in Section C 1, we modify the protocol in such a way that the concept class is replaced with the above concept class based on a classically one-way permutation, and the party A has access to (an oracle to load) an $O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ amount of the parameters y in (C18) sampled from $\mathcal{D}_N^Y$ in (C19), in place of loading x, within a unit time per loading each y.

The classical data-preparation algorithm is shown in Algorithm S5. Given the problem size N, the concept class $\mathcal{C}_N$ in Definition S16 with a classically one-way permutation f_N^{OWP} under the probability distribution $\mathcal{D}_N$ in Definition S15, the error parameter ϵ, the significance parameter δ, the number $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$ of samples to be prepared (e.g., given by (C1), yet we here describe the algorithm for general M), the true parameter s of the target concept, and the parameters y to be loaded as assumed above, the goal of Algorithm S5 is to output M pairs of data

$$\{(x_m, c_s(x_m))\}_{m=1}^M, \tag{C21}$$

with each x_m drawn from the distribution $\mathcal{D}_N$, where (C21) is a variant of (C2) up to the change of the concept class to (C20). Note that the error parameter ϵ and the significance parameter δ are not explicitly relevant to Algorithm S5 except for the possibility of M depending on ϵ and δ. In Algorithm S5, for each $m = 1, \ldots, M$, we start with loading y_m sampled from the distribution $\mathcal{D}_N^Y$. Then, the algorithm computes the classically one-way permutation f_N^{OWP} for y_m. By definition of the classically one-way permutation $\{f_N^{\mathrm{OWP}}\}_{N \in \mathbb{N}} \in \mathsf{FP}$, we have a polynomial-time deterministic classical algorithm $\mathcal{A}$ to compute

$$x_m = \mathcal{A}(y_m) = f_N^{\mathrm{OWP}}(y_m) \tag{C22}$$

within runtime

$$t_{\mathcal{A}}(y_m) = O\left(N^{\zeta}\right), \tag{C23}$$

where $\zeta > 0$ is an upper bound of the degree of the polynomial runtime. Finally, Algorithm S5 computes $c_s(x_m)$ by

$$c_s(x_m) = y_m \cdot s, \tag{C24}$$

following the definition of c_s in (C20). After performing these computations for all m, Algorithm S5 outputs the data in (C21), i.e.,

$$\{(x_m, c_s(x_m))\}_{m=1}^M. \tag{C25}$$

The following theorem shows that Algorithm S5 prepares the data in (C21) correctly within a polynomial time.

Theorem S17 (The polynomial-time data preparation with a classical algorithm based on classically one-way functions)**.** *Given any N, ϵ, and δ, for any $M = O(\mathsf{poly}(N, 1/\epsilon, 1/\delta))$, Algorithm S5 outputs the M sample data $\{(x_m, c_s(x_m))\}_{m=1}^M$ in (C21) within a polynomial time*

$$O(\mathsf{poly}(N, 1/\epsilon, 1/\delta)). \tag{C26}$$

Proof. Algorithm S5 is a deterministic algorithm and has no error; thus, it suffices to discuss the runtime. The runtime of Algorithm S5 is determined by computing the classically one-way permutation f_N^{OWP} in Definition S15 for M inputs $y_1, \ldots y_M$ and bitwise inner product. Due to (C23), for $M = O((\frac{N}{\epsilon\delta})^{\lambda})$ with $\lambda > 0$, we have the overall runtime

$$O\left(M\left(N^{\zeta} + N\right)\right) \tag{C27}$$

$$= O\left(\frac{N^{\zeta+\lambda}}{\epsilon^{\lambda}\delta^{\lambda}}\right) \tag{C28}$$

$$= O\left(\mathsf{poly}\left(\frac{N}{\epsilon\delta}\right)\right), \tag{C29}$$

which yields the conclusion. □

[1] P. Wittek, *Quantum Machine Learning: What Quantum Computing Means to Data Mining* (Elsevier, 2014).

[2] M. Schuld and F. Petruccione, *Machine learning with quantum computers* (Springer, 2021).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*,

10th ed. (Cambridge University Press, 2011).

[4] S. Arora and B. Barak, *Computational complexity: A Modern Approach* (Cambridge University Press, 2009).

[5] M. J. Kearns, *The computational complexity of machine learning* (MIT press, 1990).

[6] M. J. Kearns and U. Vazirani, *An introduction to computational learning theory* (MIT press, 1994).

[7] B. Schölkopf and A. J. Smola, *Learning with kernels: support vector machines, regularization, optimization, and beyond* (MIT press, 2002).

[8] F. Bach, *Learning Theory from First Principles* (2023).

[9] P. Rebentrost, M. Mohseni, and S. Lloyd, Quantum support vector machine for big data classification, Phys. Rev. Lett. **113**, 130503 (2014).

[10] I. Kerenidis and A. Prakash, Quantum Recommendation Systems, in *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 67, edited by C. H. Papadimitriou (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2017) pp. 49:1–49:21.

[11] Z. Zhao, J. K. Fitzsimons, and J. F. Fitzsimons, Quantum-assisted gaussian process regression, Phys. Rev. A **99**, 052331 (2019).

[12] H. Yamasaki, S. Subramanian, S. Sonoda, and M. Koashi, Learning with optimized random features: Exponential speedup by quantum machine learning without sparsity and low-rank assumptions, in *Advances in Neural Information Processing Systems*, Vol. 33, edited by H. Larochelle, M. Ranzato, R. Hadsell, M. Balcan, and H. Lin (Curran Associates, Inc., 2020) pp. 13674–13687.

[13] H. Yamasaki and S. Sonoda, Exponential error convergence in data classification with optimized random features: Acceleration by quantum machine learning (2022), arXiv:2106.09028 [quant-ph].

[14] H. Yamasaki, S. Subramanian, S. Hayakawa, and S. Sonoda, Quantum ridgelet transform: Winning lottery ticket of neural networks with quantum computation, in *Proceedings of the 40th International Conference on Machine Learning*, ICML'23 (JMLR.org, 2023).

[15] E. Tang, A quantum-inspired classical algorithm for recommendation systems, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019 (Association for Computing Machinery, New York, NY, USA, 2019) p. 217–228.

[16] Y. Liu, S. Arunachalam, and K. Temme, A rigorous and robust quantum speed-up in supervised machine learning, Nature Physics **17**, 1013 (2021).

[17] R. A. Servedio and S. J. Gortler, Equivalences and separations between quantum and classical learnability, SIAM Journal on Computing **33**, 1067 (2004).

[18] C. Gyurik and V. Dunjko, On establishing learning separations between classical and quantum machine learning with classical data (2023), arXiv:2208.06339 [quant-ph].

[19] C. Gyurik and V. Dunjko, Exponential separations between classical and quantum learners (2023), arXiv:2306.16028 [quant-ph].

[20] J. Pérez-Guijarro, A. Pagés-Zamora, and J. R. Fonollosa, Relation between quantum advantage in supervised learning and quantum computational advantage, IEEE Transactions on Quantum Engineering , 1 (2023).

[21] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th annual symposium on foundations of computer science* (Ieee, 1994) pp. 124–134.

[22] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing **26**, 1484 (1997).

[23] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Review **41**, 303 (1999).

[24] M. Kearns and L. Valiant, Cryptographic limitations on learning boolean formulae and finite automata, J. ACM **41**, 67–95 (1994).

[25] C. Gidney and M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum **5**, 433 (2021).

[26] H. W. Lenstra and C. Pomerance, A rigorous time bound for factoring integers, Journal of the American Mathematical Society **5**, 483 (1992).

[27] J. P. Buhler, H. W. Lenstra, and C. Pomerance, Factoring integers with the number field sieve, in *The development of the number field sieve*, edited by A. K. Lenstra and H. W. Lenstra (Springer Berlin Heidelberg, Berlin, Heidelberg, 1993) pp. 50–94.

[28] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, The state of the art in integer factoring and breaking public-key cryptography, IEEE Security & Privacy **20**, 80 (2022).

[29] S. Lloyd, S. Garnerone, and P. Zanardi, Quantum algorithms for topological and geometric analysis of data, Nature communications **7**, 10138 (2016).

[30] R. Hayakawa, Quantum algorithm for persistent betti numbers and topological data analysis, Quantum **6**, 873 (2022).

[31] B. Ameneyro, G. Siopsis, and V. Maroulas, Quantum persistent homology for time series, in *2022 IEEE/ACM 7th Symposium on Edge Computing (SEC)* (2022) pp. 387–392.

[32] I. Y. Akhalwaya, S. Ubaru, K. L. Clarkson, M. S. Squillante, V. Jejjala, Y.-H. He, K. Naidoo, V. Kalantzis, and L. Horesh, Towards quantum advantage on noisy quantum computers (2022), arXiv:2209.09371 [quant-ph].

[33] S. McArdle, A. Gilyén, and M. Berta, A streamlined quantum algorithm for topological data analysis with exponentially fewer qubits (2022), arXiv:2209.12887 [quant-ph].

[34] M. H. Freedman, M. Larsen, and Z. Wang, A modular functor which is universal for quantum computation, Communications in Mathematical Physics **227**, 605 (2002).

[35] P. Wocjan and S. Zhang, Several natural bqp-complete problems (2006), arXiv:quant-ph/0606179 [quant-ph].

[36] D. Aharonov, V. Jones, and Z. Landau, A polynomial quantum algorithm for approximating the jones polynomial, in *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '06 (Association for Computing Machinery, New York, NY, USA, 2006) p. 427–436.

[37] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum algorithm for linear systems of equations, Phys. Rev. Lett. **103**, 150502 (2009).

[38] D. Aharonov and I. Arad, The bqp-hardness of approximating the jones polynomial, New Journal of Physics **13**, 035019 (2011).

[39] S. Gharibian and F. Le Gall, Dequantizing the quantum singular value transformation: Hardness and applications to quantum chemistry and the quantum pcp conjecture, in *Proceedings of the 54th Annual ACM SIGACT Sympo-*

sium on Theory of Computing, STOC 2022 (Association for Computing Machinery, New York, NY, USA, 2022) p. 19–32.

[40] S. Gharibian, R. Hayakawa, F. L. Gall, and T. Morimae, Improved hardness results for the guided local hamiltonian problem (2022), arXiv:2207.10250 [quant-ph].

[41] S. Hallgren, Polynomial-time quantum algorithms for pell's equation and the principal ideal problem, in *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (Association for Computing Machinery, New York, NY, USA, 2002) p. 653–658.

[42] S. Hallgren, Polynomial-time quantum algorithms for pell's equation and the principal ideal problem, J. ACM **54** (2007).

[43] L. G. Valiant, A theory of the learnable, Commun. ACM **27**, 1134–1142 (1984).

[44] T. M. Cover, Geometrical and statistical properties of systems of linear inequalities with applications in pattern recognition, IEEE Transactions on Electronic Computers **EC-14**, 326 (1965).

[45] S. Aaronson, The equivalence of sampling and searching, in *Computer Science – Theory and Applications*, edited by A. Kulikov and N. Vereshchagin (Springer Berlin Heidelberg, Berlin, Heidelberg, 2011) pp. 1–14.

[46] A. Bogdanov and L. Trevisan, Average-case complexity, Foundations and Trends® in Theoretical Computer Science **2**, 1 (2006).

[47] R. Impagliazzo, A personal view of average-case complexity, in *Structure in Complexity Theory Conference, Annual* (IEEE Computer Society, Los Alamitos, CA, USA, 1995) p. 134.

[48] H.-Y. Huang, M. Broughton, M. Mohseni, R. Babbush, S. Boixo, H. Neven, and J. R. McClean, Power of data in quantum machine learning, Nature Communications **12**, 2631 (2021).

[49] S. Aaronson, H. Buhrman, and W. Kretschmer, A Qubit, a Coin, and an Advice String Walk into a Relational Problem, in *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 287, edited by V. Guruswami (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2024) pp. 1:1–1:24.

[50] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, Quantum circuit learning, Phys. Rev. A **98**, 032309 (2018).

[51] M. Schuld and N. Killoran, Quantum machine learning in feature hilbert spaces, Phys. Rev. Lett. **122**, 040504 (2019).

[52] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, Supervised learning with quantum-enhanced feature spaces, Nature **567**, 209 (2019).

[53] M. Schuld, A. Bocharov, K. M. Svore, and N. Wiebe, Circuit-centric quantum classifiers, Phys. Rev. A **101**, 032308 (2020).

[54] H.-Y. Huang, R. Kueng, and J. Preskill, Information-theoretic bounds on quantum advantage in machine learning, Phys. Rev. Lett. **126**, 190505 (2021).

[55] D. Aharonov, J. Cotler, and X.-L. Qi, Quantum algorithmic measurement, Nature communications **13**, 887 (2022).

[56] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, Exponential separations between learning with and without quantum memory, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (2022) pp. 574–585.

[57] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Quantum advantage in learning from experiments, Science **376**, 1182 (2022).

[58] H.-Y. Huang, S. Chen, and J. Preskill, Learning to predict arbitrary quantum processes (2023), arXiv:2210.14894 [quant-ph].

[59] F. Meier and H. Yamasaki, Energy-consumption advantage of quantum computation (2023), arXiv:2305.11212 [quant-ph].

[60] J.-G. Liu and L. Wang, Differentiable learning of quantum circuit born machines, Phys. Rev. A **98**, 062324 (2018).

[61] R. Sweke, J.-P. Seifert, D. Hangleiter, and J. Eisert, On the Quantum versus Classical Learnability of Discrete Distributions, Quantum **5**, 417 (2021).

[62] N. Pirnay, R. Sweke, J. Eisert, and J.-P. Seifert, Superpolynomial quantum-classical separation for density modeling, Phys. Rev. A **107**, 042416 (2023).

[63] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning* (MIT Press, 2016).

[64] P. Scheiblechner, On the complexity of deciding connectedness and computing betti numbers of a complex algebraic variety, Journal of Complexity **23**, 359 (2007).

[65] H. Edelsbrunner and S. Parsa, On the computational complexity of betti numbers: Reductions from matrix rank, in *Proceedings of the 2014 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 152–160.

[66] C. Cade and P. M. Crichigno, Complexity of supersymmetric systems and the cohomology problem (2021), arXiv:2107.00011 [quant-ph].

[67] C. Gyurik, C. Cade, and V. Dunjko, Towards quantum advantage via topological data analysis, Quantum **6**, 855 (2022).

[68] M. Crichigno and T. Kohler, Clique homology is qma1-hard (2022), arXiv:2209.11793 [quant-ph].

[69] A. Schmidhuber and S. Lloyd, Complexity-theoretic limitations on quantum algorithms for topological data analysis (2022), arXiv:2209.14286 [quant-ph].

[70] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM **21**, 120–126 (1978).

[71] J. A. Buchmann and H. C. Williams, A key exchange system based on real quadratic fields extended abstract, in *Advances in Cryptology — CRYPTO' 89 Proceedings*, edited by G. Brassard (Springer New York, New York, NY, 1990) pp. 335–343.

[72] L. A. Levin, Average case complete problems, SIAM Journal on Computing **15**, 285 (1986).

[73] A. Nickelsen and B. Schelm, Average-case computations - comparing avgp, hp, and nearly-p, in *20th Annual IEEE Conference on Computational Complexity (CCC'05)* (2005) pp. 235–242.

[74] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, *et al.*, Variational quantum algorithms, Nature Reviews Physics **3**, 625 (2021).

Generalized Recipe for Quantum Reverse Processes via Bayesian Inversion

Clive Cenxin Aw,[1] Lin Htoo Zaw,[1] Maria Balanzó-Juandó,[2] and Valerio Scarani[1, 3]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

[2] *ICFO-Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain*

[3] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

(Dated: May 14, 2024)

This is an extended, non-technical abstract for AQIS.2024. It is for a presentation aimed to be an birds-eye overview on a generalized recipe for reverse processes via Bayesian inference. It takes most from PRX Quantum.5.010332 [1]. Some figures are also appended to the end of the document.

I. QUESTIONS TO SET THE STAGE

Reversibility is a central concept in physics and information science, from entropy to state recovery, noise and dissipation [2–8]. That said, there exists a plurality of approaches for characterizing it, some of which only apply in strictly defined, classical contexts. Given reversibility's fundamentality, a question arises: can we formalize the definition of reverse processes for any processes, classical or quantum?

This question is enhanced by a further puzzle: introducing an ancillary system, every irreversible process can always be seen as a marginal of a larger reversible global process [9, 10]. This is sometimes called the *dilation* of a channel (as in Stinespring dilations).

$$\mathcal{E}[\bullet] = \mathrm{Tr}_B\left[U(\bullet \otimes \beta)U^\dagger\right] \tag{1}$$

How, then, does reversal on marginal level compare to that in the global, dilated picture? Does "reversal and marginalization commute"? This has implications in physical implementation of recovery protocols, as it relates to the question of when can I reverse a process $\mathcal{R}[\mathcal{E}]$ with the same global dynamics (i.e. some unitary U) I used for the forward process $\mathcal{E}$. That is,

$$\mathcal{R}[\mathcal{E}][\bullet] \overset{!}{=} \mathrm{Tr}_B[U^\dagger(\bullet \otimes \beta')U]. \tag{2}$$

We may call this condition **tabletop time-reversibility.** Most notably, this is satisfied by Gibbs-preserving maps in **thermal operations** [2]. The question is where else does this hold? Put another way, "how special are thermal operations, with regard to reversibility?"

II. RESPONSES & RESULTS

In this work, we answer these three questions. Firstly, we adopt the perspective that the physically viable, universally applicable and axiomatically valid characterization of classical and quantum reversibility lies in **Bayes' rule** [11, 12]]

$$\hat{\varphi}_\gamma(a|a') = \varphi(a'|a)\frac{\gamma(a)}{\varphi[\gamma](a')}, \tag{3}$$

and the **Petz Recovery map** [13–15]

$$\hat{\mathcal{E}}_\alpha[\bullet] = \sqrt{\alpha}\,\mathcal{E}^\dagger\left[\frac{1}{\sqrt{\mathcal{E}[\alpha]}}\bullet\frac{1}{\sqrt{\mathcal{E}[\alpha]}}\right]\sqrt{\alpha}. \tag{4}$$

respectively, which has been fruitful in comparing reversal across regimes and the derivation of fluctuation relations [16, 17]. Noting that the Petz Map has been seen as the prime candidate for the quantum generalization of Bayes' rule [18–23].

Doing so, we show by using these Bayesian tools to define reverse processes, this approach

1. **Recovers the typical examples of reverse processes** (eg. bijections and reversible processes go to inversions, bistochastic and unital processes go to their transpose and adjoint respectively and so on). Furthermore, it gives insights to why these forward maps give reverse processes they do.

2. Shows that reversal and marginalization (in both classical and quantum regimes) *do commute* as long as one takes into propagated correlations formed between the ancillary system and the reference of the reversal. **In other words, the Bayesian and open system perspectives on irreversibility coincide.** This is proven through the decomposition of these forward maps

$$\varphi(a'|a) = \sum_{bb'}\Phi(a',b'|a,b)\beta(b), \qquad \varphi = \Sigma_B\circ\Phi\circ\hat{\Sigma}_{B,\square\otimes\beta} \tag{5}$$

$$\mathcal{E}[\bullet] = \mathrm{Tr}_B\left[U(\bullet\otimes\beta)U^\dagger\right] = \mathrm{Tr}_B\circ\mathcal{U}\circ\hat{\mathrm{Tr}}_{B,\square\otimes\beta}[\bullet], \tag{6}$$

in terms of *assignment maps*:

$$\hat{\Sigma}_{B,\Lambda}[\bullet_A] = \bullet_A\cdot\left(\frac{\Lambda}{\Sigma_B[\Lambda]}\right)_{B|A}, \tag{7}$$

$$\hat{\mathrm{Tr}}_{B,\Omega}[\bullet_A] = \sqrt{\Omega}\left[\left(\frac{1}{\sqrt{\mathrm{Tr}_B[\Omega]}}\bullet_A\frac{1}{\sqrt{\mathrm{Tr}_B[\Omega]}}\right)\otimes\mathbb{1}_B\right]\sqrt{\Omega} \tag{8}$$

The proofs, theorems and technical details can be found in the main text [1].

3. Finally, we show that **tabletop time-reversibility is a remarkably special condition**, identifying families of this condition for qubit channels and beyond. We also find physically insightful theorems [1] pertaining to a generalization of thermal operations, its relationship with correlations and its implications on energetics in the quantum regime.

III. IMPACT

Finally, we make some qualitative remarks on the impacts of this work.

1. It provides a practical benefit by identifying scenarios where reversal (and thus, information recovery) can be done with the same unitary that defines the dilation of the transformation. This is significant as it is well known that, in general, this is an extremely complex process to implement.

2. It gives a conceptual basis for the definition of reverse processes for quantum fluctuation theorems, giving a quantum informational perspective [8, 16, 17, 24].

3. It helps quantify how irreversibility can be seen as a function of the reverse process' dependence on reference prior. In other words, it gives a quantitative meaning to the connection of irreversibility (and entropy) to prior information. Something illustrated by famous physics puzzles like Landauer Erasure and even Laplace's and Maxwell's Demons.

[1] C. C. Aw, L. H. Zaw, M. Balanzó-Juandó, and V. Scarani, Role of dilations in reversing physical processes: Tabletop reversibility and generalized thermal operations, P R X Quantum **5**, 010332 (2024).

[2] J. W. Gibbs, On the equilibrium of heterogeneous substances, American Journal of Science **s3-16**, 441 (1878), https://www.ajsonline.org/content/s3-16/96/441.full.pdf.

[3] L. Onsager, Reciprocal relations in irreversible processes. ii., Physical review **38**, 2265 (1931).

[4] U. Seifert, Stochastic thermodynamics, fluctuation theorems and molecular machines, Reports on Progress in Physics **75**, 126001 (2012).

[5] F. Brandao, M. Horodecki, N. Ng, J. Oppenheim, and S. Wehner, The second laws of quantum thermodynamics, Proceedings of the National Academy of Sciences **112**, 3275 (2015).

[6] D. J. Evans and D. J. Searles, The fluctuation theorem, Advances in Physics **51**, 1529 (2002).

[7] G. E. Crooks, Quantum operation time reversal, Phys. Rev. A **77**, 034101 (2008).

[8] M. Campisi, P. Hänggi, and P. Talkner, Colloquium: Quantum fluctuation relations: Foundations and applications, Rev. Mod. Phys. **83**, 771 (2011).

[9] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).

[10] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (2002).

[11] S. Watanabe, Conditional probabilities in physics, Progr. Theor. Phys. Suppl. **E65**, 135 (1965).

[12] E. T. Jaynes, *Probability Theory: The Logic of Science* (Cambridge University Press, 2003).

[13] D. Petz, Sufficient subalgebras and the relative entropy of states of a von neumann algebra, Comm. Math. Phys. **105**, 123 (1986).

[14] D. Petz, Sufficiency of channels over von Neumann algebras, The Quarterly Journal of Mathematics **39**, 97 (1988).

[15] M. Wilde, Recoverability in quantum information theory, Proceedings of the Royal Society A **471**, 20150338 (2015).

[16] C. C. Aw, F. Buscemi, and V. Scarani, Fluctuation theorems with retrodiction rather than reverse processes, AVS Quantum Science **3**, 045601 (2021), https://doi.org/10.1116/5.0060893.

[17] F. Buscemi and V. Scarani, Fluctuation theorems from bayesian retrodiction, Phys. Rev. E **103**, 052111 (2021).

[18] M. S. Leifer and R. W. Spekkens, Towards a formulation of quantum theory as a causally neutral theory of bayesian inference, Phys. Rev. A **88**, 052130 (2013).

[19] A. J. Parzygnat and B. P. Russo, A non-commutative bayes' theorem, Linear Algebra and its Applications **644**, 28 (2022).

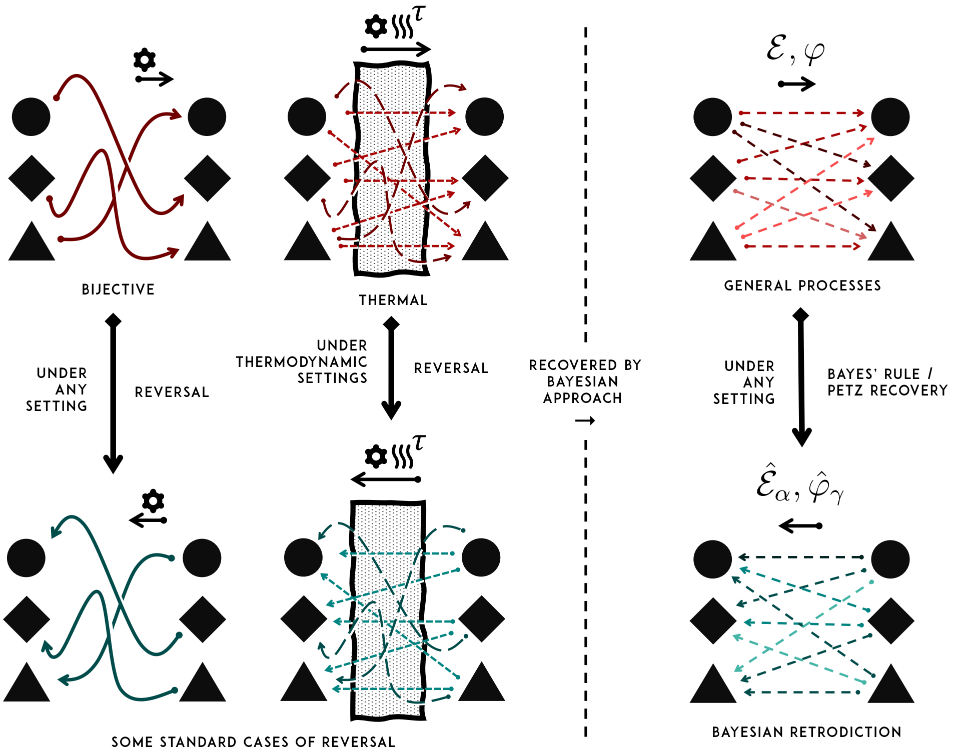
[20] A. J. Parzygnat and J. Fullwood, From time-reversal symmetry to quantum bayes' rules, PRX Quantum **4**, 020334 (2023).

[21] A. J. Parzygnat and F. Buscemi, Axioms for retrodiction: achieving time-reversal symmetry with a prior, Quantum **7**, 1013 (2023).

[22] J. Surace and M. Scandi, State retrieval beyond bayes' retrodiction, Quantum **7**, 990 (2023).

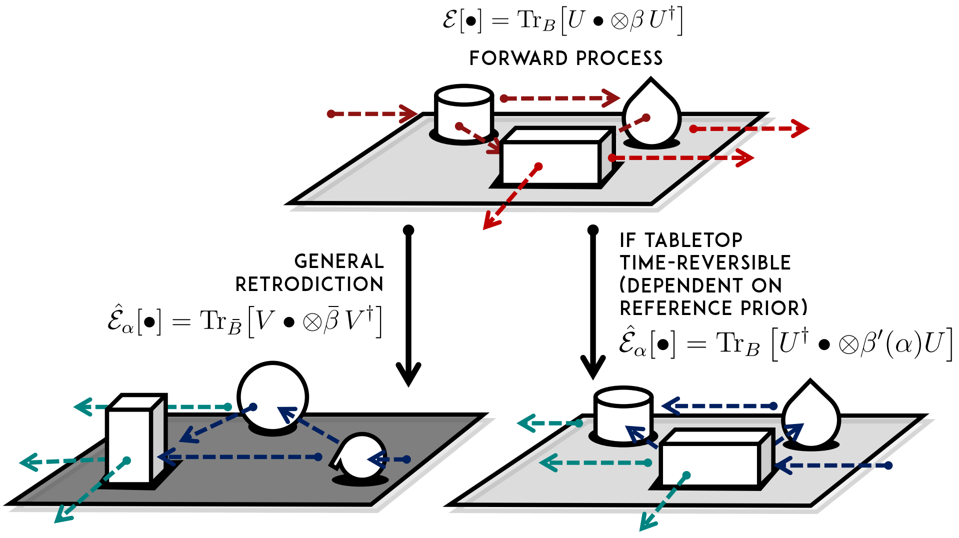
[23] C. C. Aw, K. Onggadinata, D. Kaszlikowski, and V. Scarani, Quantum bayesian inference in quasiprobability representations, PRX Quantum **4**, 020352 (2023).

[24] H. Kwon and M. S. Kim, Fluctuation theorems for a quantum channel, Phys. Rev. X **9**, 031029 (2019).



τ
BIJECTIVE
THERMAL
UNDER ANY SETTING
REVERSAL
UNDER THERMODYNAMIC SETTINGS
REVERSAL
τ
SOME STANDARD CASES OF REVERSAL
RECOVERED BY BAYESIAN APPROACH
→
$\mathcal{E}, \varphi$
GENERAL PROCESSES
UNDER ANY SETTING
BAYES' RULE / PETZ RECOVERY
$\hat{\mathcal{E}}_\alpha, \hat{\varphi}_\gamma$
BAYESIAN RETRODICTION

FIG. 1: Illustrations for standard examples of reversal. Bayesian inversion or "retrodiction" is a formal recipe that reproduce results of standard reverse processes for any characterized process, and any under setting as captured by a reference state.



$\mathcal{E}[\bullet] = \mathrm{Tr}_B\left[U \bullet \otimes \beta\, U^\dagger\right]$
FORWARD PROCESS
GENERAL RETRODICTION
$\hat{\mathcal{E}}_\alpha[\bullet] = \mathrm{Tr}_{\bar{B}}\left[V \bullet \otimes \bar{\beta}\, V^\dagger\right]$
IF TABLETOP TIME-REVERSIBLE (DEPENDENT ON REFERENCE PRIOR)
$\hat{\mathcal{E}}_\alpha[\bullet] = \mathrm{Tr}_B\left[U^\dagger \bullet \otimes \beta'(\alpha) U\right]$

FIG. 2: An illustration of tabletop time-reversibility. Any channel $\mathcal{E}$ can be dilated to on a global $\mathcal{U}$ and a bath. Bayesian retrodiction associates a reverse channel $\hat{\mathcal{E}}_\alpha$ to $\mathcal{E}$, which can itself be dilated into a larger unitary process $\mathcal{V}$. However, $\mathcal{V} \neq \mathcal{U}^\dagger$ is in general—informally speaking, such that "a different experimental setup" would be required to implement the forward and reverse channels. Tabletop reversible channels are when $\mathcal{V} = \mathcal{U}^\dagger$: informally, when we can "run the experimental setup backwards" to implement the reverse channel.

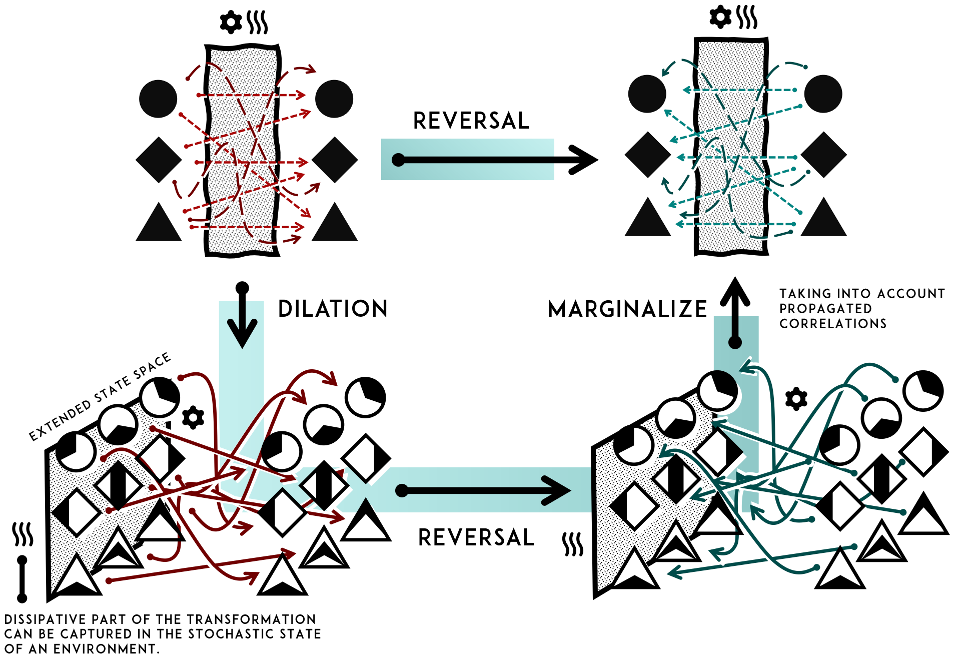

REVERSAL
DILATION
MARGINALIZE
TAKING INTO ACCOUNT PROPAGATED CORRELATIONS
EXTENDED STATE SPACE
REVERSAL
DISSIPATIVE PART OF THE TRANSFORMATION CAN BE CAPTURED IN THE STOCHASTIC STATE OF AN ENVIRONMENT.

FIG. 3: Two routes for Bayesian retrodiction illustrated. One can show that these two protocols always give the same reverse process, as long as the propagated correlations formed across the reference prior and the ancillary environment is accounted for. This is captured by the retrodictive assignment map (7).

Tsirelson's Precession Protocol: A Theory-independent Bound Saturated by Quantum Mechanics, and Other Generalisations

Lin Htoo Zaw[1] * Mirjam Weilenmann[2] Valerio Scarani[2] [3]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *Département de Physique Appliquée, Université de Genève, Genève, Switzerland*
[3] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Abstract. Tsirelson's precession protocol certifies the nonclassicality of a system by asking how often a uniformly-precessing variable is positive at one of three equally-spaced points in time [1]. It does not require simultaneous or sequential measurements like other nonclassicality tests, and has also been shown to be useful for detecting Wigner negativity and entanglement. Here, we present two recent results about the protocol. The first result is a theory-independent bound for systems with finitely many outcomes [2]. We show that, unlike Bell and noncontextuality inequalities, quantum theory saturates the general bound. As such, the precession protocol falsifies any general theory that does not also saturate this bound. The second result involves previously-proposed generalisations of the protocol. We characterise all such protocols with three probing times for the quantum harmonic oscillator. An open question about the maximum violation of these generalised protocols is partially answered, the exact relationship between violating states of different protocols is also found. This characterises the wider class of states whose Wigner negativity and entanglement can be detected by the precession protocol.

Keywords: harmonic oscillator, spin angular momentum, theory-independent bound, general probabilistic theories

Background and Motivation. The time evolution of uniformly-precessing variables $(A_x(t), A_y(t))$—like the position and momentum of the harmonic oscillator, or components of a vector rotating with a fixed angular momentum—is the same in both classical and quantum theory. Both the classical observables and the corresponding quantum operators in the Heisenberg representation satisfy

$$\begin{aligned} A_x(t) &= \cos(\tfrac{2\pi t}{T})A_x(0) + \sin(\tfrac{2\pi t}{T})A_y(0) \\ A_y(t) &= \cos(\tfrac{2\pi t}{T})A_y(0) - \sin(\tfrac{2\pi t}{T})A_x(0) \end{aligned} \tag{1}$$

for the period T. As the dynamics are the same in both classical and quantum theory, one does not expect to find quantumness in the dynamics of the harmonic oscillator.

Tsirelson showed that, on the contrary, the nonclassicality of a system can be certified by simply asking how often a uniformly-precessing variable is positive [1]. The precession protocol involves many rounds, where $A_x(t)$ is measured at a randomly-chosen time $t_k = kT/3$ for $k \in \{0, 1, 2\}$ in each round, and after many rounds, the score

$$P_3 := \frac{1}{3}\sum_{k=0}^{2}\left\{\Pr\left[A_x(\tfrac{kT}{3}) > 0\right] + \frac{1}{2}\Pr\left[A_x(\tfrac{kT}{3}) = 0\right]\right\} \tag{2}$$

is calculated. The nonclassicality of the system is certified if the observed value P_3 violates the classical bound $P_3 > 2/3 =: \mathbf{P}_3^c$ [1].

Violations of the classical bound have been shown for specific examples of quantum systems. The maximum quantum violation is $P_3 \approx 0.709$ for the quantum harmonic oscillator, and conjectured to be $P_3 = 0.75$ for spin systems [4]. An open question here is the maximum violation by quantum theory: is $P_3 = 0.75$ the best that quantum theory can do, or are there uniformly-precessing quantum variables that do better?

Since the first few works on Tsirelson's precession protocol, some generalisations have also been proposed. They include probing the system at $k\tilde{T}/3$ for some $\tilde{T} \neq T$ [5], which captures the situation where the period of the prcession is not precisely known, and studying the classical bound as a facet in a constrained conditional probability polytope [6], which gives rise to the so-called Type I inequality (nonclassical when $P_{\mathrm{I}} > 2/3$) and Type II inequality (nonclassical when $P_{\mathrm{II}} > 1/3$), where

$$\begin{aligned} P_{\mathrm{I}} &:= \frac{1}{3}\sum_{k=0}^{2}\left\{\Pr\left[A_x(\tfrac{2kT}{5}) > 0\right] + \frac{1}{2}\Pr\left[A_x(\tfrac{2kT}{5}) = 0\right]\right\} \\ P_{\mathrm{II}} &:= \frac{1}{3}\sum_{k=0}^{2}(-1)^k\left\{\Pr\left[A_x(\tfrac{kT}{5}) > 0\right] + \frac{1}{2}\Pr\left[A_x(\tfrac{kT}{5}) = 0\right]\right\}. \end{aligned} \tag{3}$$

An open question here is the maximum possible violation of these generalised protocols: unlike the original precession protocol, estimates of the maximum score have yet to be found for specific quantum systems, let alone quantum theory in general.

Practical Applications. The precession protocol bounds the Wigner negativity volume [4], which is a measure of the amount of non-Gaussian resource required for quantum information processing [7, 8]. As the protocol only requires quadrature measurements, it is straightforward to perform in optical systems with homodyne measurements and optomechanics with position measurements at different times. When applied to collective modes of coupled oscillators, it has also been shown to witness non-Gaussian entanglement between coupled os-

*htoo@zaw.li

cillators [9]. Finally, for spin ensembles, it solves an open problem about the detection of the genuine multipartite entanglement of GHZ states using only measurements of the total angular momentum of the system [10].

Foundational Applications. Unlike other nonclassicality tests like noncontextual or Leggett–Garg inequalities [11, 12], the precession protocol does not require simultaneous or sequential measurements. Furthermore, the precession protocol is not susceptible to the so-called "*clumsiness loophole*" [13]. As such, it offers a more straightforward experimental test of nonclassicality in situations where the measured variable is certain to be uniformly-precessing.

Contributions. There are several related open questions for the precession protocol: *What is the maximum possible violation of the original protocol (or its extensions) for a specific quantum system (or quantum theory in general)*? Our contributions answer one open question, and partially answer another.

Our first contribution is to derive a theory-independent bound for the original precession protocol for systems with a finitely many outcomes [2]. The derivation relies only on the linearity of the expectation value with respect to the observables, which is an assumption satisfied by all general probabilistic theories [14]. The derived general bound depends only on the spectrum of the measured observable, where spectrum is defined in a purely theory-independent manner as the set of all possible outcomes.

We then prove by construction that the general bound is saturated by quantum mechanics, which answers the question about the maximum possible violation of the original precession protocol by quantum theory. This means that no general theory can outperform quantum theory in the precession protocol. As the cat state of a spin-3/2 particle saturates this bound, and the cat state is commonly prepared for its metrological properties [15], this provides a simple test that can experimentally falsify general theories that do not also saturate this bound.

Our second contribution is to characterise the family of precession protocols with three probing times, which include the type I and type II inequalities [3]. For the quantum harmonic oscillator, we not only show how the maximum quantum violation for every such protocol is related to the violation of the original precession protocol, but also derive the exact unitary relationship between violating states of different protocols.

In particular, denoting $\mathbf{P}_3^\infty$, $\mathbf{P}_\mathrm{I}^\infty$, and $\mathbf{P}_\mathrm{II}^\infty$ as the maximum quantum score for the quantum harmonic oscillator with the original, type I, and type II inequalities respectively, we show that $\mathbf{P}_\mathrm{I}^\infty = \mathbf{P}_3^\infty$ and $\mathbf{P}_\mathrm{II}^\infty = \mathbf{P}_3^\infty - 1/3$. This partially answers the open question about the maximum quantum violation for generalisations of the precession protocol for the quantum harmonic oscillator.

In terms of applications, our results expand the class of states that can be detected by the family of precession protocols. From the derived relationship between the different protocols, we can show that if a state is detected by one protocol, a squeezed version of that state will be detected by another protocol. This is particularly useful when information is encoded in superpositions of coherent states, as is common in the field of continuous variable quantum information processing, where squeezing has been recently introduced as a technique to protect the encoded state against photon loss [16, 17]. As previous work has shown that the entanglement of the three-headed cat state can be detected by the original precession protocol [9], our results therefore imply that the same state, protected via squeezing, can be detected by other members of the family of precession protocols with three probing times.

References

[1] B. Tsirelson. How often is the coordinate of a harmonic oscillator positive? arXiv:quant-ph/0611147, 2006.

[2] L. H. Zaw, M. Weilenmann, V. Scarani. A theory-independent bound saturated by quantum mechanics. arXiv:2401.16147, 2024.

[3] L. H. Zaw, V. Scarani. *In Preparation.*

[4] L. H. Zaw, C. C. Aw, Z. Lasmar, V. Scarani. Detecting quantumness in uniform precessions. *Phys. Rev. A*, 106(3):032222, 2022.

[5] L. H. Zaw, V. Scarani. Dynamics-based quantumness certification of continuous variables with generic time-independent Hamiltonians. *Phys. Rev. A*, 108(2):022211, 2023.

[6] M. Plávala, T. Heinosaari, S. Nimmrichter, O. Gühne. Tsirelson Inequalities: Detecting Cheating and Quantumness in One Fell Swoop. arXiv:2309.00021, 2023.

[7] R. Takagi, Q. Zhuang. Convex resource theory of non-Gaussianity. *Phys. Rev. A*, 97(6):062337, 2018.

[8] F. Albarelli, M. G. Genoni, M. G. A. Paris, A. Ferraro. Resource theory of quantum non-Gaussianity and Wigner negativity. *Phys. Rev. A*, 98(5):052350, 2018.

[9] P. Jayachandran, L. H. Zaw, V. Scarani. Dynamics-Based Entanglement Witnesses for Non-Gaussian States of Harmonic Oscillators. *Phys. Rev. Lett.*, 130(16):160201, 2023.

[10] KN. Huynh-Vu, L. H. Zaw, V. Scarani. Certification of genuine multipartite entanglement in spin ensembles with measurements of total angular momentum. *Phys. Rev. A*, 109(4):042402, 2024.

[11] C. Budroni, A. Cabello, O. Gühne, M. Kleinmann, J. Larsson. Kochen-Specker contextuality. *Rev. Mod. Phys.*, 94(4):045007, 2022.

[12] A. J. Leggett, A. Garg. Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks? *Phys. Rev. Lett.*, 54(9):857–860, 1985.

[13] M. M. Wilde, A. Mizel. Addressing the Clumsiness Loophole in a Leggett-Garg Test of Macrorealism. *Found. Phys.*, 42(2):256–265, 2012.

[14] M. Plávala. General probabilistic theories: An introduction. *Phys. Rep.*, 1033:1–64, 2023.

[15] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, P. Treutlein. Quantum metrology with nonclassical states of atomic ensembles. *Rev. Mod. Phys.*, 90(3):035005, 2018.

[16] T. Hillmann, F. Quijandría Quantum error correction with dissipatively stabilized squeezed-cat qubits. *Phys. Rev. A*, 107(3):032423, 2023.

[17] Q. Xu, G. Zheng, YX. Wang, P. Zoller, A. A. Clerk, L. Jiang. Autonomous quantum error correction and fault-tolerant quantum computation with squeezed cat qubits. *npj Quantum Inf.*, 9:78, 2023.

Bridging magic and non-Gaussian resources via Gottesman-Kitaev-Preskill encoding

Oliver Hahn[1] * Giulia Ferrini[1] Ryuji Takagi[2] †

[1] *Wallenberg Centre for Quantum Technology, Department of Microtechnology and Nanoscience, Chalmers University of Technology, Sweden , SE-412 96 Göteborg, Sweden*
[2] *Department of Basic Science, University of Tokyo, Komaba, Meguro-ku, Tokyo 153-0041, Japan*

Abstract. Although the similarity between non-stabilizer states—also known as magic states—in discrete-variable systems and non-Gaussian states in continuous-variable systems has widely been recognized, the precise connections between these two notions have still been unclear. We establish a fundamental link between these two quantum resources via the Gottesman-Kitaev-Preskill (GKP) encoding. We show that the negativity of the continuous-variable Wigner function for an encoded GKP state coincides with a magic measure we introduce, which matches the negativity of the discrete Wigner function for odd dimensions. We also provide a continuous-variable representation of the stabilizer Rényi entropy—a recent proposal for a magic measure for multi-qubit states. With this in hand, we give a classical simulation algorithm with runtime scaling with the resource contents, quantified by our magic measures. We also employ our results to prove that implementing a multi-qubit logical non-Clifford operation in the GKP code subspace requires a non-Gaussian operation even at the limit of perfect encoding, despite the fact that the ideal GKP states already come with much non-Gaussianity.

Keywords: resource theories, magic states, non-Gaussianity, GKP encoding

1 Background and motivation

Quantum computing is predicted to give a computational speed-up compared to classical computation. It is still an open problem to find and pinpoint the origins of the speed-up or what manifestation would allow for such phenomena. This fact becomes even more important, as in reality every quantum information processing task will be restricted in a certain way given that they will be implemented in a physical system.

One of the promising platforms for quantum information processing is to utilize a quantum optical system, which is equipped with an infinite-dimensional Hilbert space accommodating continuous-variable systems. There, the non-Gaussian states have been identified as necessary resources for quantum computational advantages [1], as computation solely run by Gaussian resources can be efficiently simulated classically. The most prominent measure that quantifies non-Gaussian features [2–7] is the negativity of Wigner function [4, 8, 9] that also captures the hardness of classical simulability. Other natural platforms, such as superconducting and ion-trap-based architectures, assume discrete-variable systems, in which quantum information is encoded in finite-dimensional Hilbert spaces. Among many relevant quantum resources needed for efficient quantum information processing, one peculiar quantity necessary for quantum speedup is the non-stabilizerness, also known as quantum magic, as quantum circuits only consisting of stabilizer states and Clifford operations can be efficiently simulatable by classical computers. Interestingly, the magicness of discrete-variable states can also be studied by looking at a discrete version of the Wigner function [10, 11]. Indeed, the negativity of the discrete Wigner function [12] has been shown to be a valid magic measure when the underlying Hilbert space has odd dimensions.

Although it has been pointed out that there is a conceptual similarity between non-Gaussianity and magic in terms of necessary resources for universal quantum computation, the direct quantitative connection between these two resources has still been elusive. In particular, constructing a map between non-Gaussianity and magic will not only solidify the relation between two main operational frameworks that are important for quantum computing but also provide a novel approach where one resource could be analyzed by employing a tool developed for analyzing the other.

2 Bridging magic and non-Gaussianity

In this work, we accomplish this by finding a fundamental relation between the discrete and continuous-variable distributions via the Gottesman-Kitaev-Preskill (GKP) encoding [13], which is one of the standard error-correcting codes for continuous-variable systems. Our results therefore recover and significantly extend a recent finding of the relation between multi-qubit systems and continuous-variable systems [14]. We accomplish this by introducing a new operator basis for qudit systems. For $l, m \in \mathbb{Z}_{2d}$, let $O_{l,m}$ be an operator defined by

$$O_{l,m} = \omega_d^{-ml/2} M_l Z_d^m \tag{1}$$

*oliver.hahn@chalmers.se
†ryujitakagi.pat@gmail.com

where $M_l = \sum_{\substack{u,v\in\mathbb{Z}_d \\ u+v \mod d=l}} |u\rangle\langle v|$ and Z_d the d-dimensional Pauli Z operator. This can easily be extended to n-qudit systems, where we define $O_{\boldsymbol{l},\boldsymbol{m}} = \prod O_{l_i,m_i}$ for $\boldsymbol{l},\boldsymbol{m} \in \mathbb{Z}_{2d}^n$. The newly defined operators are hermitian and unitary operators that are orthogonal in the Hilbert-Schmidt inner product $\mathrm{Tr}\left(O_{l,m}O_{l',m'}\right) = \delta_{mm'}\delta_{ll'}d$. Let us now define the distribution

$$x_\rho(\boldsymbol{l},\boldsymbol{m}) := d^{-n}\,\mathrm{Tr}(O_{\boldsymbol{l},\boldsymbol{m}}\rho) \tag{2}$$

which corresponds to the coefficients for $O_{\boldsymbol{l},\boldsymbol{m}}$ when expanding the state ρ with this operator basis.

This distribution is inherently connected to GKP states, which form an error correction code for bosonic systems. The peculiar property of the Wigner function of GKP states is that it comes with an atomic form, where the Dirac distribution has disjoint support

$$W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}(\boldsymbol{r}) = \frac{\sqrt{d}^n}{\sqrt{8\pi}^n}\sum_{\boldsymbol{l},\boldsymbol{m}} c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m}) \times \delta\left(\boldsymbol{r_p} - \boldsymbol{m}\sqrt{\frac{\pi}{2d}}\right)\delta\left(\boldsymbol{r_q} - \boldsymbol{l}\sqrt{\frac{\pi}{2d}}\right) \tag{3}$$

where ρ_{GKP} refers to a GKP state that encodes a qudit state ρ, and $c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m})$ is a coefficient serving as a weight for each peak in the Wigner function of a GKP state ρ_{GKP}. We show that this coefficient exactly coincides with the distribution introduced above, i.e.,

$$c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m}) = x_\rho(\boldsymbol{l},\boldsymbol{m}). \tag{4}$$

Using this connection we can now state the first theorem. We will use the periodicity of the GKP Wigner function and only consider one unit cell of the lattice and are thus restricting to a hypercube $r_{q_i} \in [0,\sqrt{2d\pi}), r_{p_i} \in [0,\sqrt{2d\pi})$ in the phase space. This motivates us to consider an l_p-norm of a function f defined for a unit cell $\|f\|_{p,\mathrm{cell}} := \left(\int_{\mathrm{cell}} d\boldsymbol{r}|f(\boldsymbol{r})|^p\right)^{1/p}$ where $\int_{\mathrm{cell}}$ refers to the integral over the unit hypercube. We then obtain the following result that directly connects discrete- and continuous-variable quantum resources.

Theorem 1. *For an n-qudit state ρ on a d^n-dimensional space and for an arbitrary $p > 0$, it holds that*

$$d^{n(1-1/p)}\|x_\rho\|_p = \frac{\|W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}}{\|W_{\mathrm{STAB}_n,\mathrm{GKP}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}}, \tag{5}$$

where $\|W_{\mathrm{STAB}_n,\mathrm{GKP}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}$ is the quantity that takes the same value for every n-qudit pure stabilizer state ϕ. When d is odd, we further have

$$d^{n(1-1/p)}\|W_\rho^{\mathrm{DV}}\|_p = \frac{\|W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}}{\|W_{\mathrm{STAB}_n,\mathrm{GKP}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}}. \tag{6}$$

with W_ρ^{DV} being the discrete Wigner function.

Theorem 1 relates the l_p-norm of GKP states to the l_p-norm of x_ρ for a discrete-variable state ρ, which quantifies the magicness in ρ, and therefore establishes a direct connection between the Wigner negativity of a qudit encoded in GKP and a magic quantifier in finite dimensions. The case of $p = 1$, i.e.,

$$\|x_\rho\|_1 = \frac{\|W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}}{\|W_{\mathrm{STAB}_n,\mathrm{GKP}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}}, \tag{7}$$

is particularly insightful. In this case, the 1-norm of the continuous-variable Wigner function coincides with the continuous-variable Wigner negativity, which is known to be a valid measure of non-Gaussianity [4, 9]. The quantity in Theorem 1 is then the amount of non-Gaussianity renormalized by the negativity of the GKP states encoding stabilizer states. This renormalization is necessary, as even stabilizer states encoded in GKP have non-zero continuous Wigner negativity.

Its property as a magic quantifier depends on whether the dimension of the discrete-variable systems is odd or even. For odd dimensions, $\|x_\rho\|_1$ coincides with the discrete Wigner negativity [12]. On the other hand, for the case of even dimensions, $\|x_\rho\|_p$ does not reduce to known magic measures in general. However, for the special case of $d = 2$, it is equivalent to the stabilizer Rényi entropy [15], a recent proposal for computable magic measures for multi-qubit systems. We discuss further properties of this quantity in the technical manuscript.

In addition to the Wigner function, we also find that l_p-norm of the discrete-variable characteristic function χ_ρ^{DV} (which corresponds to the coefficients of the generalized Pauli operators) exactly corresponds to that of continuous-variable characteristic functions. This particularly provides a new interpretation of the stabilizer Rényi entropy—which is precisely defined by the l_p norm of the Pauli coefficients—in terms of GKP encoding, and naturally extends it to all dimensions.

Theorem 2. *Let ρ be an n-qudit state on a d^n-dimensional space. Then,*

$$d^{n(1-1/p)}\|\chi_\rho^{\mathrm{DV}}\|_p = \frac{\|\chi_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}}{\|\chi_{\mathrm{STAB},\mathrm{GKP}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}} \tag{8}$$

where $\chi_\rho^{\mathrm{DV,CV}}$ is the discrete- and continuous-variable characteristic functions, and $\|\chi_{\mathrm{STAB},\mathrm{GKP}}^{\mathrm{CV}}\|_{p,\mathrm{cell}}$ is the quantity that takes the same value for every pure stabilizer state ϕ.

This result particularly establishes an insightful relation between continuous characteristic functions and stabilizer Rényi entropies [15]

$$M_\alpha(\rho) = \frac{2\alpha}{1-\alpha}\log\frac{\|\chi_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{2\alpha,\mathrm{cell}}}{\|\chi_{\mathrm{STAB},\mathrm{GKP}}^{\mathrm{CV}}\|_{2\alpha,\mathrm{cell}}} - \frac{\alpha\, n\log d}{1-\alpha} \tag{9}$$

where $M_\alpha(\rho) := \alpha(1-\alpha)^{-1}\log\|\Xi(\rho)\|_\alpha - n\log d$ with $\Xi_P(\rho) = \frac{1}{d^n}\,\mathrm{Tr}\left(\rho P\right)^2$ is α-stabilizer Rényi entropy.

3 Applications

Simulation algorithms Employing our framework, we introduce a classical simulation algorithm that runs with the cost quantified by the magic quantifiers we introduce, extending the previous approaches of classical simulation based on quasiprobability distributions [16, 17] to all dimensions. See technical manuscript for details of the algorithm.

The simulation time scales with the amount of negativity in the entire circuit defined as

$$\mathcal{M}_{\rightarrow} = \|x_\rho\|_1 \prod_{t=1}^{T} \max_{\boldsymbol{\lambda_t}} \|x_{U_t}(\boldsymbol{\lambda_t})\|_1 \max_{\boldsymbol{\lambda_T}} |x_\Pi(\boldsymbol{\lambda_T})| \tag{10}$$

where the maximum is taken over all trajectories and

$$x_\rho(\lambda) = \mathrm{Tr}\left(\rho \frac{O_{\boldsymbol{\lambda}}}{d^n}\right) \tag{11}$$

$$x_U(\lambda', \lambda) = \mathrm{Tr}\left(\frac{O_{\boldsymbol{\lambda'}}}{d^n} U O_{\boldsymbol{\lambda}} U^\dagger\right) \tag{12}$$

$$x_\Pi(\lambda) = \mathrm{Tr}\left(\Pi O_{\boldsymbol{\lambda}}\right). \tag{13}$$

are the coefficients related to the input state ρ, the unitary evolution U and the measurement effect Π with $\lambda = (\boldsymbol{l}, \boldsymbol{m}) \in \mathbb{Z}_d^{2n}$. The number of samples K that achieves precision ϵ with a failure probability p_f is given by

$$K \geq 2\mathcal{M}_{\rightarrow}^2 \frac{1}{\epsilon^2} \ln\left(\frac{2}{p_f}\right). \tag{14}$$

This shows that the number of samples directly scales with the resourcefulness of the input state $\|x_\rho\|_1$ if we evolve using the free operations of our magic quantifiers like Clifford unitaries. This result gives a nice operational interpretation of the quantifiers discussed in this work, as already noted in the case for the discrete Wigner negativity [16].

Magic needs non-Gaussianity It has been known since the original GKP paper [13] that one can implement the logical T-gate and thus get an H-type magic state by using a cubic phase state or cubic interaction e^{icQ^3}. However, this is merely one possibility for implementing a non-Gaussian interaction, and this does not show the necessity of non-Gaussianity to implement a non-Clifford operation on the code subspace. This is a widely held belief based on the correspondence between a pair of Pauli and displacement operators and that of Clifford and Gaussian operations, where displacement operators and Pauli operators are both Heisenberg-Weyl operators. However, this "belief" has not been proven in general, beyond specific scenarios in qubit systems [18]. Indeed, GKP states have much Wigner negativity and thus *a priori* additional non-Gaussianity may not be required, making the necessity of non-Gaussian operation to implement a non-Clifford operation nontrivial.

Nevertheless, the results established above allow us to show that non-Gaussian operations are essential to implement non-stabilizer operations in the GKP code space. In fact, we find that the Gaussian *protocols* [9]—a class of quantum channels larger than Gaussian operations, which also admits feed-forwarded Gaussian operations conditioned on the outcomes of Gaussian measurements—are not able to implement non-stabilizer operations in the GKP code space. Importantly, Gaussian protocols include a gate teleportation circuit involving a Gaussian measurement and a feed-forwarded Gaussian unitary, which itself is not a Gaussian operation. An immediate consequence of this result is that a Gaussian protocol cannot implement non-Clifford unitary gates deterministically.

Theorem 3. *Let Λ be a quantum channel with n-qubit input and output systems. If there exists a pure stabilizer state ϕ and a pure non-stabilizer state ψ such that $\Lambda(\phi) = \psi$, Λ cannot be implemented in a GKP code space by a Gaussian protocol. Also, for a quantum channel Λ with n-qudit input and output systems with odd local dimensions, the condition can be relaxed to the existence of a (potentially mixed) stabilizer state σ and a state ρ with $\|W_\rho^{\mathrm{DV}}\|_1 > 1$ such that $\Lambda(\sigma) = \rho$.*

4 Conclusions

We established a fundamental quantitative relation between discrete- and continuous-variable systems via the GKP encoding. We introduced a magic measure for discrete-variable systems and showed that it corresponds to the non-Gaussianity measure defined by the continuous-variable Wigner function that encodes the same qudit states via GKP encoding. Our distributions allow for a magic quantifier for all dimensions and extend the discrete Wigner negativity defined for odd dimensions in a unified manner. Furthermore, we present an analogous relation for characteristic functions, providing a new representation of the stabilizer Rényi entropy in terms of continuous-variable characteristic function.

Employing our framework, we introduced a classical simulation algorithm, where the run time scales with the magic quantifiers we introduced. We utilized our findings to demonstrate that achieving a deterministic implementation of a logical non-Clifford operation, with identical input and output dimensions within the GKP code subspace, necessitates a non-Gaussian operation, even when operating at the theoretical limit of ideal GKP state input.

Our work suggests various interesting future directions, including the extension of our results to realistic GKP states with finite squeezing, as well as the application of our framework to other bosonic codes.

References

[1] A. Mari and J. Eisert. Positive wigner functions render classical simulation of quantum computation efficient. *Phys. Rev. Lett.*, 109:230503, Dec 2012.

[2] Marco G. Genoni, Matteo G. A. Paris, and Konrad Banaszek. Measure of the non-gaussian character of a quantum state. *Phys. Rev. A*, 76:042327, Oct 2007.

[3] Marco G. Genoni, Matteo G. A. Paris, and Konrad Banaszek. Quantifying the non-gaussian character of a quantum state by quantum relative entropy. *Phys. Rev. A*, 78:060303, Dec 2008.

[4] Francesco Albarelli, Marco G. Genoni, Matteo G. A. Paris, and Alessandro Ferraro. Resource theory of quantum non-gaussianity and wigner negativity. *Phys. Rev. A*, 98:052350, Nov 2018.

[5] Ulysse Chabaud, Damian Markham, and Frédéric Grosshans. Stellar representation of non-gaussian quantum states. *Phys. Rev. Lett.*, 124:063605, Feb 2020.

[6] Bartosz Regula, Ludovico Lami, Giovanni Ferrari, and Ryuji Takagi. Operational quantification of continuous-variable quantum resources. *Phys. Rev. Lett.*, 126:110403, Mar 2021.

[7] Ludovico Lami, Bartosz Regula, Ryuji Takagi, and Giovanni Ferrari. Framework for resource quantification in infinite-dimensional general probabilistic theories. *Phys. Rev. A*, 103:032424, Mar 2021.

[8] Anatole Kenfack and Karol Życzkowski. Negativity of the wigner function as an indicator of non-classicality. *J. Opt. B: Quantum Semiclass. Opt.*, 6(10):396, aug 2004.

[9] Ryuji Takagi and Quntao Zhuang. Convex resource theory of non-Gaussianity. *Phys. Rev. A*, 97(6):062337, jun 2018.

[10] David Gross. *Finite phase space methods in quantum information*. PhD thesis, Diploma Thesis, Potsdam, 2005.

[11] D. Gross. Hudson's theorem for finite-dimensional quantum systems. *J. Math. Phys.*, 47(12):122107, 12 2006.

[12] Victor Veitch, S A Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. The resource theory of stabilizer quantum computation. *New J. Phys.*, 16(1):013009, jan 2014.

[13] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A*, 64:012310, Jun 2001.

[14] Oliver Hahn, Alessandro Ferraro, Lina Hultquist, Giulia Ferrini, and Laura García-Álvarez. Quantifying qubit magic resource with gottesman-kitaev-preskill encoding. *Phys. Rev. Lett.*, 128:210502, May 2022.

[15] Lorenzo Leone, Salvatore F. E. Oliviero, and Alioscia Hamma. Stabilizer rényi entropy. *Phys. Rev. Lett.*, 128:050402, Feb 2022.

[16] Hakop Pashayan, Joel J. Wallman, and Stephen D. Bartlett. Estimating outcome probabilities of quantum circuits using quasiprobabilities. *Phys. Rev. Lett.*, 115:070501, Aug 2015.

[17] Patrick Rall, Daniel Liang, Jeremy Cook, and William Kretschmer. Simulation of qubit quantum circuits via pauli propagation. *Phys. Rev. A*, 99:062337, Jun 2019.

[18] Hayata Yamasaki, Takaya Matsuura, and Masato Koashi. Cost-reduced all-gaussian universality with the gottesman-kitaev-preskill code: Resource-theoretic approach to cost analysis. *Phys. Rev. Res.*, 2:023270, Jun 2020.

Bridging magic and non-Gaussian resources via Gottesman-Kitaev-Preskill encoding

Oliver Hahn,[1, *] Giulia Ferrini,[1] and Ryuji Takagi[2, †]

[1] *Wallenberg Centre for Quantum Technology, Department of Microtechnology and Nanoscience,*
Chalmers University of Technology, Sweden , SE-412 96 Göteborg, Sweden
[2] *Department of Basic Science, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo, 153-8902, Japan*

Although the similarity between non-stabilizer states—also known as magic states—in discrete-variable systems and non-Gaussian states in continuous-variable systems has widely been recognized, the precise connections between these two notions have still been unclear. We establish a fundamental link between these two quantum resources via the Gottesman-Kitaev-Preskill (GKP) encoding. We show that the negativity of the continuous-variable Wigner function for an encoded GKP state coincides with a magic measure we introduce, which matches the negativity of the discrete Wigner function for odd dimensions. We also provide a continuous-variable representation of the stabilizer Rényi entropy—a recent proposal for a magic measure for multi-qubit states. With this in hand, we give a classical simulation algorithm with runtime scaling with the resource contents, quantified by our magic measures. We also employ our results to prove that implementing a multi-qubit logical non-Clifford operation in the GKP code subspace requires a non-Gaussian operation even at the limit of perfect encoding, despite the fact that the ideal GKP states already come with much non-Gaussianity.

I. INTRODUCTION

The difference between what constitutes quantum and classical physics is often hard to grasp. The hope is to leverage quantum mechanics in order to get a computational speed-up when using quantum computing compared to classical computation. Finding and pinpointing the origins of the speed-up or what property allows for such a phenomenon is still an open problem. Aside from an academic interest, this undertaking would allow us to identify and quantify what resources are required to do a certain computational task. This fact becomes even more important, as in reality every quantum information processing task will be restricted in a certain way given that they will be implemented in a physical system.

One of the promising platforms for quantum information processing consists of quantum optical systems [1], which is equipped with an infinite-dimensional Hilbert space associated with observable possessing a continuous-variable spectrum. In such systems, non-Gaussian components have been identified as necessary resources for quantum computational advantages [2], as computation solely run by Gaussian resources can be efficiently simulated classically. Such non-Gaussian features in e.g. quantum states can be quantified by several measures of non-Gaussianity [3–9], among which the negativity of Wigner function [5, 6, 10] has been known as the computable measure that also captures the hardness of classical simulability [11].

The other paradigm for quantum information processing assumes discrete-variable systems, in which quantum information is encoded in finite-dimensional Hilbert spaces. Promising platforms implementing discrete-variables systems include superconducting [12] and ion-trap-based [13] architectures. Among many relevant quantum resources needed for efficient quantum information processing in discrete-variable systems, one peculiar quantity necessary for quantum speedup is the non-stabilizerness [14], also known as quantum magic, which stems from the fact that quantum circuits only consisting of stabilizer states and Clifford operations can be efficiently simulable by classical computers [15]. Interestingly, the magicness of discrete-variable states can also be studied by looking at a discrete version of the Wigner function [16, 17] analogously to the case of continuous-variable systems. Indeed, the negativity of the discrete Wigner function [18, 19] has been shown to be a valid magic measure when the underlying Hilbert space has odd dimensions. For even dimensions, one needs to consider other quantifiers [20–33], as there is no known quasiprobability distribution that easily connects to magic.

Although some conceptual similarities between non-Gaussianity and magic resources have been observed [17, 33–35], the direct quantitative connection between these two resources has still been elusive. In particular, constructing a map between magic and non-Gaussianity would strengthen the relation between two main operational frameworks that are important for quantum computing and provide a novel approach where one resource could be analyzed by employing a tool developed for analyzing the other.

In this work, we accomplish this mapping by finding a fundamental relation between the discrete and continuous-variable systems via the Gottesman-Kitaev-Preskill (GKP) encoding [36], which is one of the most promising error-correcting codes for continuous-variable systems. We introduce a family of distributions for discrete-variable systems and show that their l_p-norm exactly corresponds to that of the continuous-variable Wigner function for the GKP state encoding the original discrete-variable qudit. Specifically for odd dimension, the l_1 norm of the qudit distributions yields the negativity of the associated Wigner function for both discrete and continuous-variable settings. The connection is even stronger as the continuous Wigner function can be directly represented using the discrete Wigner function of the encoded state. On the other hand, our distributions yield a magic quantifier for all dimensions, which encompasses the negativity of the discrete Wigner function defined for odd dimensions and the stabilizer Rényi entropy [28] defined for multi-qubit sys-

[*] oliver.hahn@chalmers.se
[†] ryujitakagi.pat@gmail.com

tems in a unified manner. Our results, therefore, allow for recovering and significantly extending a recent finding of the relation between multi-qubit systems and continuous-variable systems [29].

In addition to the Wigner function, we also find that l_p-norm of the discrete-variable characteristic function (which corresponds to the coefficients of the generalized Pauli operators) exactly corresponds to the one of continuous-variable characteristic functions of GKP-encoded states. This provides a new interpretation of the stabilizer Rényi entropy—which is precisely defined by the l_p norm of the Pauli coefficients—in terms of GKP encoding, and naturally extends it to all dimensions.

Employing our framework, we introduce a classical simulation algorithm that runs with the cost quantified by the magic measure we introduce, extending the previous approaches of classical simulation based on quasiprobability distributions [37, 38] to all dimensions. We also apply our results to prove that the deterministic implementation of a logical non-Clifford operation with the same input and output systems in the GKP code subspace requires a non-Gaussian operation even at the limit of ideal GKP state input. Since ideal GKP states have unbounded non-Gaussianity, it is not a priori obvious that more non-Gaussianity is needed to apply a logical non-Clifford operation. Our result shows that this is actually the case in general, extending an observation for specific non-Clifford gates in multi-qubit systems [39] to the general class of non-Clifford gates on all dimensions.

II. PRELIMINARIES

Here we briefly review the relevant formalism for discrete- and continuous-variable quantum computing.

A. Discrete variables

Qubits are ubiquitous in quantum information processing and are $d = 2$ level systems. Qudits are an intuitive generalizations to d dimensions. A general pure qudit state is defined as

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \tag{1}$$

with normalization condition $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$ and $|i\rangle$ a computational basis state. The Pauli group can be defined for arbitrary dimensions in analogy to the qubit case as $\mathcal{P}_d = \{\omega_D^u X_d^v Z_d^w : v, w \in \mathbb{Z}_d, u \in \mathbb{Z}_D\}$ where $\omega_d = e^{2\pi i/d}$ is the dth root of unity and

$$D = \begin{cases} d: & \text{for } d \text{ odd} \\ 2d: & \text{for } d \text{ even} \end{cases} \tag{2}$$

with $\mathbb{Z}_d$ being the integers modulo d. The d dimensional Pauli operators Z_d, X_d, sometimes also called shift and clock operators, are a way to generalize the qubit Pauli operators Z_2, X_2 and are defined as

$$X_d = \sum_{j=0}^{d-1} |j+1\rangle \langle j| \tag{3}$$

$$Z_d = \sum_{j=0}^{d-1} \omega_d^j |j\rangle \langle j| \tag{4}$$

with the property $X_d^d = Z_d^d = \mathbb{1}$ [40].

We use the generalized Pauli operators X_d, Z_d to define the operators of the d-dimensional Heisenberg-Weyl group as [16, 17]

$$P_d(a,b) = \omega_d^{\frac{1}{2}ab} X_d^a Z_d^b \tag{5}$$

with $a, b \in \mathbb{Z}_d$. Then, the commutation relations are

$$P_d(a,b) P_d(c,d) = \omega_d^{(a,b)\Omega(c,d)^T} P_d(c,d) P_d(a,b), \tag{6}$$

where

$$\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{7}$$

is the symplectic form.

For n-qudit systems, the Heisenberg-Weyl operators are written by

$$P_d(\boldsymbol{u}) = \otimes_{i=1}^n P_d(a_i, b_i) \tag{8}$$

with $\boldsymbol{u} = (\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{Z}_d^{2n}$, which satisfy the orthogonality relation

$$\mathrm{Tr}\left[P_d(\boldsymbol{u}) P_d^\dagger(\boldsymbol{v})\right] = d^n \delta_{\boldsymbol{u},\boldsymbol{v}}. \tag{9}$$

The d dimensional n qudit Clifford group is generated by the following unitary operations

$$\begin{aligned} R &= \sum_{j,s=0}^{d-1} \omega_d^{js} |s\rangle \langle j| \\ P &= \sum_{j=0}^{d-1} \omega_d^{j^2/2} (\omega_D \omega_{2d}^{-1})^{-j} |j\rangle \langle j| \\ \mathrm{SUM} &= \sum_{i,j=0}^{d-1} |i\rangle \langle i| \otimes |i+j \mod d\rangle \langle j| . \end{aligned} \tag{10}$$

For $d = 2$, these operators reduce to the Hadamard, Phase, and CNOT gate [40] respectively. A Clifford unitary U_C acts on the Heisenberg-Weyl operator in a simple way

$$U_C P_d(\boldsymbol{u}) U_C^\dagger = P_d(S\boldsymbol{u}) \tag{11}$$

where $S \in \mathrm{SP}(2n, \mathbb{Z}_D)$ is a symplectic matrix [40] associated with the Clifford unitary U_C .

Using the discrete Heisenberg-Weyl operators, we define the characteristic function [17]

$$\chi_\rho^{\mathrm{DV}}(\boldsymbol{u}) = d^{-n}\, \mathrm{Tr}\left[\rho P_d(\boldsymbol{u})^\dagger\right]. \tag{12}$$

Odd-dimensional systems allow for a simple way to define the discrete Wigner function by the discrete symplectic Fourier transform of the characteristic function

$$W_\rho^{\mathrm{DV}}(\boldsymbol{u}) = d^{-n} \sum_{\boldsymbol{v}\in\mathbb{Z}_d^{2n}} \omega_d^{-\boldsymbol{u}\Omega_n\boldsymbol{v}^T} \chi_\rho^{\mathrm{DV}}(\boldsymbol{v}) \tag{13}$$

$$= d^{-n}\,\mathrm{Tr}\,[A(\boldsymbol{u})\rho], \tag{14}$$

where Ω_n now takes the form

$$\Omega = \begin{pmatrix} 0 & \mathbb{1}_n \\ -\mathbb{1}_n & 0 \end{pmatrix} \tag{15}$$

and $\mathbb{1}_n$ is the $n \times n$ identity matrix. The phase space point operator in (10) can be written by

$$A(\boldsymbol{u}) = d^{-n} \sum_{\boldsymbol{v}\in\mathbb{Z}_d^{2n}} \omega_d^{-\boldsymbol{u}\Omega_n\boldsymbol{v}^T} P_d(\boldsymbol{u})^\dagger. \tag{16}$$

The discrete Wigner function in odd dimensions has many useful properties. It is covariant under Clifford unitaries U_C meaning that

$$W^{\mathrm{DV}}_{U_C\rho U_C^\dagger}(\boldsymbol{u}) = W_\rho^{\mathrm{DV}}(S\boldsymbol{u}) \tag{17}$$

with $S \in \mathrm{Sp}(2n, \mathbb{Z}_d)$ being the symplectic matrix associated with Clifford unitary U_C. The discrete Wigner function $W_\rho(\boldsymbol{u})$ is a quasiprobability distribution and is thus not necessarily positive. Nevertheless, it constructs a valid probability distribution for an arbitrary stabilizer state. This property was utilized to introduce a magic measure— a quantifier for non-stabilizerness—given by

$$\|W_\rho^{\mathrm{DV}}\|_1 = \sum_{\boldsymbol{u}} \left|W_\rho^{\mathrm{DV}}(\boldsymbol{u})\right| \tag{18}$$

which is known as the negativity of the Wigner function [19]. This is a resource monotone under Clifford operations in the sense of resource theories [41], meaning that this does not increase under Clifford operations. The negativity of the Wigner function (18) can be considered as a l_1-norm of the function $W_\rho^{\mathrm{DV}} : \mathbb{Z}_d^{2n} \to \mathbb{R}$. In the following, we also consider the l_p-norm of a function $f : \mathbb{Z}_d^{2n} \to \mathbb{C}$ defined by

$$\|f\|_p = \left(\sum_{\boldsymbol{u}\in\mathbb{Z}_d^{2n}} |f(\boldsymbol{u})|^p \right)^{1/p} \tag{19}$$

for a real number $p > 0$.

B. Continuous variables

A related but inherently different paradigm in quantum information processing uses infinite dimensional systems. The central observables in these systems are commonly called position Q and momentum P operators that fulfill the canonical commutation relations

$$[Q, P] = i. \tag{20}$$

These operators have continuous spectra, which is why this type of quantum information processing is often called *continuous variables*, in contrast to *discrete-variable* systems described in the previous section. For a n-mode system, the infinite-dimensional Heisenberg-Weyl operators, also known as displacement operators, are defined by

$$D(\boldsymbol{r}) = \prod_{j=1}^{n} e^{-ir_{p_j}r_{q_j}/2} e^{-ir_{q_j}P_j} e^{ir_{p_j}Q_j} \tag{21}$$

where $\boldsymbol{r} = (r_{q_1}, ..., r_{q_n}, r_{p_1}, ..., r_{p_n}) = (\boldsymbol{r_q}, \boldsymbol{r_p})$ and Q_j, P_j are position and momentum operators for j th mode. Displacement operators fulfill the commutation relation

$$D(\boldsymbol{r})D(\boldsymbol{r'}) = e^{-i\boldsymbol{r}\Omega_n\boldsymbol{r'}^T} D(\boldsymbol{r'})D(\boldsymbol{r}). \tag{22}$$

Similarly to the discrete case, we can use the continuous Heisenberg-Weyl operators to define the characteristic function

$$\chi_\rho^{\mathrm{CV}}(\boldsymbol{r}) = \mathrm{Tr}\,[\rho D(-\boldsymbol{r})] \tag{23}$$

and the Wigner function as its symplectic Fourier transform

$$\begin{aligned} W_\rho^{\mathrm{CV}}(\boldsymbol{r}) &= \frac{1}{(2\pi)^n} \int \mathrm{d}\boldsymbol{r'} e^{i\boldsymbol{r}\Omega_n\boldsymbol{r'}} \chi_\rho(\boldsymbol{r'}) \\ &= \frac{1}{(2\pi)^n} \int_{-\infty}^{\infty} \mathrm{d}^n\boldsymbol{x} e^{i\boldsymbol{r_p}\boldsymbol{x}} \left\langle \boldsymbol{r_q} + \frac{\boldsymbol{x}}{2} \right| \rho \left| \boldsymbol{r_q} - \frac{\boldsymbol{x}}{2} \right\rangle_Q . \end{aligned} \tag{24}$$

The continuous Wigner function is a quasi-probability distribution and the Wigner negativity [10]

$$\|W_\rho^{\mathrm{CV}}\|_1 = \int \mathrm{d}\boldsymbol{r} \left|W_\rho^{\mathrm{CV}}(\boldsymbol{r})\right| \tag{25}$$

can be used as a valid quantifier for non-Gaussianity [5, 6]. Similarly to the case of discrete variables, we also consider a l_p-norm for a function $f : \mathbb{R}^{2n} \to \mathbb{C}$ defined by

$$\|f\|_p = \left(\int d\boldsymbol{r} |f(\boldsymbol{r})|^p \right)^{1/p}, \tag{26}$$

which gives back the Wigner negativity (25) as the l_1-norm of the Wigner function.

A family of states playing a major role in this work are the Gottesman-Kitaev-Preskill (GKP) states [36]. They were originally introduced as error correction codes for bosonic quantum systems. In this work, we employ this encoding as a platform to map magic and non-Gaussian resources, extending a prior attempt for multiqubit systems [29].

In the following, we use a subscript to denote a continuous-variable state that encodes a discrete-variable state. For instance, ρ_{GKP} refers to a continuous-variable state that encodes a qudit state ρ by the GKP encoding. The computational basis state $|j\rangle$ is encoded in the GKP code as an infinite superposition of position eigenstates as

$$|j\rangle_{\mathrm{GKP}} = \sum_{s=-\infty}^{\infty} |Q = \alpha(j + ds)\rangle\,, \tag{27}$$

which is equipped with a Wigner function

$$\begin{aligned} &W^{\mathrm{CV}}_{|j\rangle\langle j|_{\mathrm{GKP}}}(r_q, r_p) \\ &= \frac{1}{2\pi}\int_{-\infty}^{\infty} \mathrm{d}x e^{i r_p x}\psi^j\left(r_q + \frac{x}{2}\right)^* \psi^j\left(r_q - \frac{x}{2}\right) \\ &\propto \sum_{s,t=-\infty}^{\infty} (-1)^{st}\delta\left(r_p - \frac{\pi}{d\alpha}s\right)\delta\left(r_q - \alpha j - \frac{d\alpha}{2}t\right) \end{aligned} \tag{28}$$

with $\alpha = \sqrt{\frac{2\pi}{d}}$. A useful property of the GKP code is that all Clifford unitaries on the code subspace can be implemented using Gaussian unitaries.

As can be seen in (28), the Wigner function of a GKP state consists of a collection of delta functions. This comes with an unbounded negativity, which reflects the fact that an ideal GKP state is unnormalizable. Nevertheless, one can see that the delta peaks are periodically positioned with the unit cell of the size $\sqrt{2d\pi} \times \sqrt{2d\pi}$. This motivates us to consider an l_p-norm of a function f considered for a unit cell, defined by

$$\|f\|_{p,\mathrm{cell}} := \left(\int_{\mathrm{cell}} d\boldsymbol{r}|f(\boldsymbol{r})|^p\right)^{1/p} \tag{29}$$

where $\int_{\mathrm{cell}}$ refers to the integral over the domain restricted to a hypercube $r_{q_i} \in [0, \sqrt{2d\pi}), r_{p_i} \in [0, \sqrt{2d\pi})$ in the phase space.

We also note that there is a subtlety when we compute l_p-norm of a function that involves a delta function. We describe the procedure to perform such integrals in Appendix A.

III. BRIDGING MAGIC AND NON-GAUSSIANITY

In this section, we present our results that directly connect the resource content of the discrete-variable state with that of the continuous one, establishing a quantitative relation between magic and non-Gaussianity.

A. Via Wigner function

The first path to connect magic and non-Gaussianity uses the continuous Wigner function.

In order to make this connection, we start by introducing a new operator basis for qudit systems. For $l, m \in \mathbb{Z}_{2d}$, let $O_{l,m}$ be an operator defined by

$$O_{l,m} = \omega_d^{-ml/2} M_l Z_d^m \tag{30}$$

where

$$M_l = \sum_{\substack{u,v\in\mathbb{Z}_d \\ u+v \mod d=l}} |u\rangle\langle v| . \tag{31}$$

This can easily be extended to n-qudit systems, where we define $O_{\boldsymbol{l},\boldsymbol{m}} = \prod_{i=1}^n O_{l_i,m_i}$ for $\boldsymbol{l},\boldsymbol{m} \in \mathbb{Z}_{2d}^n$.

Let us now define the distribution

$$x_\rho(\boldsymbol{l},\boldsymbol{m}) := d^{-n}\,\mathrm{Tr}(O_{\boldsymbol{l},\boldsymbol{m}}\rho) \tag{32}$$

which corresponds to the coefficients for $O_{\boldsymbol{l},\boldsymbol{m}}$ when expanding the state ρ with this operator basis. Although $\boldsymbol{l},\boldsymbol{m}$ are elements of $\mathbb{Z}_{2d}$ in general, the operators $O_{\boldsymbol{l},\boldsymbol{m}}$, and correspondingly $x_\rho(\boldsymbol{l},\boldsymbol{m})$, can only gain a phase factor by a translation $l_i \to l_i + d$ and $m_i \to m_i + d$ for any $i = 1, \ldots, n$, and that the operators $\{O_{\boldsymbol{l},\boldsymbol{m}}\}_{l,m\in\mathbb{Z}_d^n}$ form an operator basis of a n-qudit system. We consider the l_p-norm for this distribution over the restricted domain $\boldsymbol{l},\boldsymbol{m} \in \mathbb{Z}_d^n$, i.e.,

$$\|x_\rho\|_p = \left(\sum_{\boldsymbol{l},\boldsymbol{m}\in\mathbb{Z}_d^n} |x_\rho(\boldsymbol{l},\boldsymbol{m})|^p\right)^{1/p} . \tag{33}$$

The following result connects the l_p-norm of the continuous Wigner function of a qudit encoded in GKP with the l_p norm of the distribution defined in (32).

Theorem 1. *For an n-qudit state ρ on a d^n-dimensional space and for an arbitrary real number $p > 0$, it holds that*

$$d^{n(1-1/p)}\|x_\rho\|_p = \frac{\|W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}\|_{p,\mathrm{cell}}}{\|W^{\mathrm{CV}}_{\mathrm{STAB}_n,\mathrm{GKP}}\|_{p,\mathrm{cell}}}, \tag{34}$$

where

$$\begin{aligned} \|W^{\mathrm{CV}}_{\mathrm{STAB}_n,\mathrm{GKP}}\|_{p,\mathrm{cell}} &:= \|W^{\mathrm{CV}}_{\phi_{\mathrm{GKP}}}\|_{p,\mathrm{cell}} \\ &= (4d)^{n/p}/(8\pi d)^{n/2} \end{aligned} \tag{35}$$

is a quantity that takes the same value for every n-qudit pure stabilizer state ϕ. When d is odd, an even stronger result holds

$$d^{n(1-1/p)}\|W^{\mathrm{DV}}_\rho\|_p = \frac{\|W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}\|_{p,\mathrm{cell}}}{\|W^{\mathrm{CV}}_{\mathrm{STAB}_n,\mathrm{GKP}}\|_{p,\mathrm{cell}}}. \tag{36}$$

We prove Theorem 1 later in this section using the following general relation between the discrete Wigner function of the corresponding encoded state and the continuous-variable Wigner function for GKP states, which may be of interest on its own. The peculiar property of the Wigner function of GKP states is that it comes with an atomic form, where the Dirac distribution has disjoint support

$$\begin{aligned} &W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r}) \\ &= \frac{\sqrt{d}^n}{\sqrt{8\pi}^n}\sum_{\boldsymbol{l},\boldsymbol{m}} c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m})\delta\left(\boldsymbol{r_p} - \boldsymbol{m}\sqrt{\frac{\pi}{2d}}\right)\delta\left(\boldsymbol{r_q} - \boldsymbol{l}\sqrt{\frac{\pi}{2d}}\right) \end{aligned} \tag{37}$$

where $c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m})$ is a coefficient serving as a weight for each peak in the Wigner function of a GKP state ρ_{GKP}. We show how to derive Eq. (37) from (28) in Appendix B. This Wigner function forms a lattice, so we restrict it to one unit cell and focus on $l_i, m_i \in [0, 2d-1]$ or equivalently $l_i, m_i \in \mathbb{Z}_{2d}$ for each $i = 1, \ldots, n$.

The following result shows that the weight $c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m})$ in the domain $\boldsymbol{l},\boldsymbol{m} \in \mathbb{Z}_d^n$ exactly coincides with the distribution defined in (32).

Proposition 2. *For $\boldsymbol{l}, \boldsymbol{m} \in \mathbb{Z}_{2d}^n$, it holds that*

$$c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l}, \boldsymbol{m}) = x_\rho(\boldsymbol{l}, \boldsymbol{m}). \tag{38}$$

The proof of Proposition 2 can be found in Appendix B. This establishes the fundamental relation between discrete-variable and continuous-variable representations of an arbitrary state ρ. As we will see later in this section, for odd dimensions Proposition 2 directly connects the discrete Wigner function of an arbitrary state ρ and the continuous Wigner function of the GKP state that encodes ρ.

Theorem 1 relates the l_p-norm of GKP states to the l_p-norm of x_ρ for a discrete-variable state ρ, which quantifies the magicness in ρ, and therefore establishes a direct connection between the Wigner negativity of a qudit encoded in GKP and a finite-dimensional magic measure. The case of $p = 1$ is particularly insightful. In this case, the 1-norm of the continuous-variable Wigner function coincides with the continuous-variable Wigner negativity, which is known to be a valid measure of non-Gaussianity [5, 6]. The quantity in Theorem 1 is then the amount of non-Gaussianity renormalized by the negativity of the GKP states encoding stabilizer states. This renormalization is necessary, as even stabilizer states encoded in GKP have non-zero continuous Wigner negativity.

Its property as a magic measure depends on whether the dimension of the discrete-variable systems is odd or even. For odd dimensions, $\|x_\rho\|_1$ coincides with the discrete Wigner negativity [17, 19]. This is a magic measure defined for general mixed states that is monotonically non-increasing under stabilizer protocols [19], which consists of (1) Clifford unitaries (2) composition with stabilizer states (3) Pauli measurements (4) partial trace (5) the above operations conditioned on the outcomes of Pauli measurements or classical randomness. Moreover, it is faithful for pure states, i.e., $\|x_\psi\|_1 = 1$ if and only if ψ is a stabilizer state for an arbitrary pure state ψ [17].

On the other hand, for the case of even dimensions, $\|x_\rho\|_p$ does not reduce to known magic measures in general—the definition of a discrete Wigner function in even dimensions is more challenging and involves expanding the set of phase-space point operators to an over-complete basis [42]. In addition, the phase space point operators always have a unit trace [17, 42], while it is not the case for $O_{l,m}$ in even dimensions, indicating the subtlety of connecting it to Wigner functions. However, for the special case of $d = 2$, it is evident by definition that $\|x_\rho\|_p$ is equivalent to the stabilizer Rényi entropy [28], as the operator $\{O_{l,m}\}_{l,m}$ reduces to the Pauli operators. Indeed, the core properties that motivate the stabilizer Rényi entropy as "magic measures" can also be extended to $\|x_\rho\|_1$ for all dimensions as follows.

1. Invariance under Clifford unitaries U_C: $\left\|x_{U_C \rho U_C^\dagger}\right\|_1 = \|x_\rho\|_1$
2. Multiplicativity: $\|x_{\rho\otimes\sigma}\|_1 = \|x_\rho\|_1 \|x_\sigma\|_1$
3. Stabilizer states achieve the minimum value: $\|x_\phi\|_1 = 1$ for every pure stabilizer state ϕ, and $\|x_\psi\|_1 \geq 1$ for every pure state ψ.

The first two properties directly follow from the properties of the continuous Wigner function together with Theorem 1, or equivalently from the properties of the newly defined operators $O_{\boldsymbol{l},\boldsymbol{m}}$. We show the third property in Appendix C.

In addition, for odd dimensions and multi-qubit systems, we have the following property.

4. Faithfulness: For a pure state ϕ, $\|x_\phi\|_1 = 1$ if and only if ϕ is a stabilizer state.

This follows from the discrete Hudson's theorem [17] for odd dimensions and the faithfulness of stabilizer Rényi entropy [28] for multi-qubit systems.

The operators $O_{\boldsymbol{l},\boldsymbol{m}}$ are involutions that are orthogonal in the Hilbert-Schmidt inner product and therefore form a basis. Furthermore, they are closed under Clifford unitaries. We will delve more into the properties of the operators $O_{\boldsymbol{l},\boldsymbol{m}}$ in the next subsection.

Evidently, the major dividing line between even and odd dimensions for the above magic measures is the question of monotonicity under Pauli measurement and the inclusion of mixed states. The magic measures for odd dimensions are non-increasing under Pauli measurements, and they are valid magic measures for general mixed states. On the other hand, for even dimensions, they are designed solely for pure states, and the monotonicity under Pauli measurements does not hold in general [43]. In particular, it is an important problem to find a computable magic measure for multi-qubit systems that is non-increasing even under Pauli measurements. One such measure is known as stabilizer nullity [26], but it is a highly discontinuous measure unstable under an infinitesimally small perturbation. Finding a continuous computable measure with full monotonicity will thus make an interesting future direction. This problem also generalizes to all even dimensions in an equivalent way.

1. *Properties of operator basis*

Since the operators $O_{\boldsymbol{l},\boldsymbol{m}}$ defined in Eq. 30 are of interest in their own way and play a central role in connecting the continuous-variable and discrete-variable worlds as can be seen in Theorem 1 and Proposition 2, let us investigate their properties. A proof of the properties outlined here can be found in Appendix D.

In general, $l, m \in \mathbb{Z}_{2d}$ are defined over $\mod 2d$. However, for most applications, one can restrict to $\mathbb{Z}_d$. For a value above d, the operators are periodic in d

$$M_l = M_{l+d} \tag{39}$$
$$Z_d^m = Z_D^{m+d} \tag{40}$$

but can have different phases

$$\begin{aligned} O_{l+d,m} &= (-1)^m O_{l,m} \\ O_{l,m+d} &= (-1)^l O_{l,m} \\ O_{l+d,m+d} &= (-1)^{l+m+d} O_{l,m} \end{aligned} \tag{41}$$

Therefore, if one is only interested in the operators independent of the sign, one can restrict the domain of l, m.

In general, $O_{l,m}$ and Z_d are unitary, and M_l is Hermitian. Thus, it holds that

$$O_{l,m}O_{l,m}^{\dagger} = \mathbb{1}. \tag{42}$$

The operator $O_{l,m}$ is also Hermitian $O = O^{\dagger}$ and thus

$$O_{l,m}O_{l,m} = \mathbb{1}, \tag{43}$$

implying that the spectrum is ± 1.

These operators are orthogonal in the sense of the Hilbert-Schmidt inner product

$$\operatorname{Tr}\left(O_{l,m}O_{l'm'}\right) = \delta_{mm'}\delta_{ll'}d. \tag{44}$$

Furthermore, the action of Clifford unitaries on the operators $O_{\boldsymbol{l},\boldsymbol{m}}$ is equivalent to a symplectic linear transformation on the coordinates $(\boldsymbol{l}, \boldsymbol{m})$ and constant shifts. We show this in Appendix D 2. For $d = 2$, one recovers the standard Pauli operators. Therefore, $O_{l,m}$ can be seen as a Hermitian generalization of the Pauli operators to arbitrary dimensions.

M_l contains d 1s for any dimension, but they behave differently for even and odd dimensions. Whether the operator is traceless for even dimensions depends on whether l is even or odd—M_l is traceless for odd l, while it has trace 2 for even l. For odd dimensions, the matrices M_l have trace 1.

Using the properties of M_l and the known properties of Z_d, we can now give a summary of the properties of $O_{l,m}$

$$\operatorname{Tr}[O_{l,m}] = \begin{cases} 1 + (-1)^m & d, l \text{ even} \\ (-1)^{ml} & d \text{ odd} \end{cases} \tag{45}$$

$$O_{l,m} = O_{l,m}^{\dagger} \tag{46}$$

$$O_{l,m}^2 = \mathbb{1} \tag{47}$$

$$\operatorname{Tr}\left(O_{l,m}O_{l'm'}\right) = \delta_{mm'}\delta_{ll'}d \tag{48}$$

As we have seen that the operators are orthogonal under the Hilbert-Schmidt norm and form a basis, we can expand operators in that basis. We restrict to $\boldsymbol{l}, \boldsymbol{m} \in \mathbb{Z}_d$, since the operators for other $\boldsymbol{l}, \boldsymbol{m}$ are the same modulo a potentially different sign that can be absorbed in the coefficients.

We can represent every quantum state in basis the operators $O_{\boldsymbol{l},\boldsymbol{m}}$ such that

$$\begin{aligned}\rho &= \sum_{\boldsymbol{m},\boldsymbol{l}} \operatorname{Tr}\left[\rho\frac{O_{\boldsymbol{l},\boldsymbol{m}}}{d^n}\right]O_{\boldsymbol{l},\boldsymbol{m}} \\ &= \sum_{\boldsymbol{l},\boldsymbol{m}} x_\rho(\boldsymbol{l},\boldsymbol{m})O_{\boldsymbol{l},\boldsymbol{m}}\end{aligned} \tag{49}$$

Given by the spectrum of $O_{\boldsymbol{l},\boldsymbol{m}}$, we can bound the value of the coefficients

$$-\frac{1}{d^n} \leq x_\rho(\boldsymbol{l},\boldsymbol{m}) \leq \frac{1}{d^n}. \tag{50}$$

We can further bound $x_\rho(\boldsymbol{l},\boldsymbol{m})$ using $\operatorname{Tr}(\rho) = 1$ as

$$\begin{aligned}\operatorname{Tr}(\rho) &= \sum_{\boldsymbol{l},\boldsymbol{m}} x_\rho(\boldsymbol{l},\boldsymbol{m}) \operatorname{Tr}\left(O_{\boldsymbol{l},\boldsymbol{m}}\right) \\ &= \begin{cases} \sum_{\boldsymbol{l},\boldsymbol{m}} (-1)^{\boldsymbol{l}\cdot\boldsymbol{m}} x_\rho(\boldsymbol{l},\boldsymbol{m}) = 1 & \text{odd} \\ \sum_{\boldsymbol{l},\boldsymbol{m}:\text{even}} 2^n x_\rho(\boldsymbol{l},\boldsymbol{m}) = 1 & \text{even} \end{cases}\end{aligned} \tag{51}$$

where $\boldsymbol{l}\cdot\boldsymbol{m} = \sum_{i=1}^n l_i m_i$.

Interestingly, we find the following characterization of pure stabilizer states, which we prove in Appendix D 3.

Proposition 3. *For an arbitrary pure stabilizer state ϕ, $x_\rho(\boldsymbol{l},\boldsymbol{m})$ have the same magnitude $|x_\rho(\boldsymbol{l},\boldsymbol{m})| = \frac{1}{d^n}$ with d^n non-zero coefficients over $\boldsymbol{l},\boldsymbol{m} \in \mathbb{Z}_d^n$.*

We note that, because of the property (41), the non-zero coefficients in the larger domain $\boldsymbol{m},\boldsymbol{l} \in \mathbb{Z}_{2d}^n$ for a pure stabilizer state still solely takes the value d^{-n}, and the number of non-zero coefficients increases to $(4d)^n$.

We see that $x_\rho(\boldsymbol{l},\boldsymbol{m})$ is not directly a quasi-probability distribution but can easily be modified to be one for odd dimensions. In the case of odd dimensions, we can show a direct connection between the operators $O_{l,m}$ and the phase space operators $A(a_1, a_2)$. The precise connection is

$$O_{2a_2,-2a_1} = A(a_1, a_2), \tag{52}$$

where now the index $2a_2, -2a_1 \in \mathbb{Z}_{2d}$ go over numbers $\bmod 2d$, to get the sign correct. We can make the connection even more explicit by correcting the trace of $O_{l,m}$ and remembering that otherwise the phase space operators and $O_{l,m}$ are reordered versions of each other

$$(-1)^{a_1 a_2} O_{a_1,a_2} = A(\sigma[a_1, a_2]^T) \tag{53}$$

where σ is some permutation matrix over $\mathbb{Z}_d^2$. This result directly connects the discrete Wigner function W_ρ^{DV} with the distribution x_ρ via

$$x_\rho(\boldsymbol{a_1},\boldsymbol{a_2}) = (-1)^{\boldsymbol{a_1}\cdot\boldsymbol{a_2}} W_\rho^{\text{DV}}(\sigma[\boldsymbol{a_1},\boldsymbol{a_2}]^T). \tag{54}$$

2. *Proof of Theorem 1*

We are now ready to show Theorem 1.

Proof of Theorem 1. Using Propositions 2 and 3, we get for an arbitrary pure stabilizer state ϕ that

$$\begin{aligned}\|W_{\phi_{\text{GKP}}}^{\text{CV}}\|_{p,\text{cell}} &= \left[(4d)^n\left\{\left(\frac{d}{8\pi}\right)^{n/2} d^{-n}\right\}^p\right]^{1/p} \\ &= \frac{(4d)^{n/p}}{(8\pi d)^{n/2}}.\end{aligned} \tag{55}$$

Proposition 2 gives

$$\begin{aligned}\|W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}\|_{p,\mathrm{cell}} &= \left[\sum_{\boldsymbol{l},\boldsymbol{m}\in\mathbb{Z}^n_{2d}}\left\{\left(\frac{d}{8\pi}\right)^{n/2}|x_\rho(\boldsymbol{l},\boldsymbol{m})|\right\}^p\right]^{1/p}\\ &= \left[4^n\sum_{\boldsymbol{l},\boldsymbol{m}\in\mathbb{Z}^n_{d}}\left\{\left(\frac{d}{8\pi}\right)^{n/2}|x_\rho(\boldsymbol{l},\boldsymbol{m})|\right\}^p\right]^{1/p}\\ &= 4^{n/p}\left(\frac{d}{8\pi}\right)^{n/2}\|x_\rho\|_p\\ &= d^{n(1-1/p)}\|W^{\mathrm{CV}}_{\phi_{\mathrm{GKP}}}\|_{p,\mathrm{cell}}\|x_\rho\|_p,\end{aligned} \tag{56}$$

which shows (34).

For odd-dimensional cases, we can employ (53) to get

$$\begin{aligned}\rho &= \sum_{\boldsymbol{a}_1,\boldsymbol{a}_2} W^{\mathrm{DV}}_\rho(\boldsymbol{a}_1,\boldsymbol{a}_2)A(\boldsymbol{a}_1,\boldsymbol{a}_2)\\ &= \sum_{\boldsymbol{a}_1,\boldsymbol{a}_2} x_\rho(\boldsymbol{a}_1,\boldsymbol{a}_2)O_{\boldsymbol{a}_1,\boldsymbol{a}_2}\\ &= \sum_{\boldsymbol{a}_1,\boldsymbol{a}_2} x_\rho(\boldsymbol{a}_1,\boldsymbol{a}_2)(-1)^{\boldsymbol{a}_1\cdot\boldsymbol{a}_2}A(\sigma[\boldsymbol{a}_1,\boldsymbol{a}_2]^T).\end{aligned} \tag{57}$$

This particularly gives

$$\begin{aligned}\left\|W^{\mathrm{DV}}_\rho\right\|_p &= \left(\sum_{\boldsymbol{a}_1,\boldsymbol{a}_2}\left|W^{\mathrm{DV}}_\rho(\boldsymbol{a}_1,\boldsymbol{a}_2)\right|^p\right)^{1/p}\\ &= \left(\sum_{\boldsymbol{l},\boldsymbol{m}}\left|(-1)^{\boldsymbol{l}\cdot\boldsymbol{m}}x_\rho(\boldsymbol{l},\boldsymbol{m})\right|^p\right)^{1/p}\\ &= \|x_\rho\|_p.\end{aligned} \tag{58}$$

This, together with (34), shows (36), completing the proof. □

This concludes the section on establishing a connection between magic and non-Gaussianity with Wigner functions.

B. Via characteristic function

In this section, we use the formalism of characteristic functions to establish a connection between magic and non-Gaussianity similar to the one found in the previous section.

The characteristic function of a qudit state $\rho = \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}^n_d}\rho_{\boldsymbol{u},\boldsymbol{v}}\left|\boldsymbol{u}\right\rangle\left\langle\boldsymbol{v}\right|$ encoded in GKP offers a striking connection to finite-dimensional systems as well. The characteristic function of a qudit encoded in GKP can then be written as

$$\begin{aligned}&\chi^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r})\\ &= \sqrt{\frac{2\pi}{d}}\sum_{l,m=-\infty}^{\infty}\gamma_{\rho_{\mathrm{GKP}}}(l,m)\delta\left(p-m\sqrt{\frac{2\pi}{d}}\right)\delta\left(q-l\sqrt{\frac{2\pi}{d}}\right).\end{aligned} \tag{59}$$

We show the derivation in Appendix E.

The following result establishes the fundamental connection between the discrete characteristic function and the continuous-variable characteristic function of GKP states that encodes the discrete-variable state.

Theorem 4. *Let ρ be an n-qudit state on a d^n-dimensional space. For $\boldsymbol{l},\boldsymbol{m}\in\mathbb{Z}^n_{2d}$, it holds that*

$$\gamma_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m}) = d^n\omega_d^{-\boldsymbol{l}\cdot\boldsymbol{m}/2}\omega_D^{-\boldsymbol{l}\cdot\boldsymbol{m}/2}\chi^{\mathrm{DV}}_\rho(\boldsymbol{l},\boldsymbol{m})^* \tag{60}$$

In particular,

$$d^{n(1-1/p)}\|\chi^{\mathrm{DV}}_\rho\|_p = \frac{\|\chi^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}\|_{p,\mathrm{cell}}}{\|\chi^{\mathrm{CV}}_{\mathrm{STAB,GKP}}\|_{p,\mathrm{cell}}} \tag{61}$$

where

$$\begin{aligned}\|\chi^{\mathrm{CV}}_{\mathrm{STAB,GKP}}\|_{p,\mathrm{cell}} &\coloneqq \|\chi^{\mathrm{CV}}_{\phi_{\mathrm{GKP}}}\|_{p,\mathrm{cell}}\\ &= \left(\frac{2\pi}{d}\right)^{n/2}(4d)^{n/p}\end{aligned} \tag{62}$$

is a quantity that takes the same value for every pure stabilizer state ϕ.

The proof can be found in Appendix E. This gives us a direct connection to the $\alpha-$stabilizer Rényi entropy defined for multi-qubits [28], which has recently been shown to be a magic monotone under stabilizer protocols for $\alpha \geq 2$ [44]. Our result also provides an immediate generalization to all dimensions. The natural extension of the $\alpha-$stabilizer Rényi entropy to n-qudit state is

$$\begin{aligned}&M_\alpha(\rho)\\ &= (1-\alpha)^{-1}\log\left(d^{-n\alpha}\sum_{P\in\mathcal{P}^*_n}\left|\mathrm{Tr}\left(\rho P\right)\right|^{2\alpha}\right) - n\log d\\ &= \alpha(1-\alpha)^{-1}\log\left\|\Xi(\rho)\right\|_\alpha - n\log d\end{aligned} \tag{63}$$

where $\mathcal{P}^*_n$ is the projective generalized Pauli (Heisenberg-Weyl) group which only contains $+1$ phase, $\Xi_P(\rho) = \frac{1}{d^n}\,\mathrm{Tr}\left(\rho P\right)^2$ forms a probability distribution when ρ is pure.

Thus, we see immediately by comparison that we can write all α-stabilizer Rényi entropies with the $l_{2\alpha}$-norm of the continuous-variable characteristic function for the qudit state that the GKP state encodes. Specifically, we have

$$\begin{aligned}M_\alpha(\rho) &= \frac{2\alpha}{1-\alpha}\log\|\chi^{\mathrm{DV}}_\rho\|_{2\alpha} - n\log d\\ &= \frac{2\alpha}{1-\alpha}\log\frac{\|\chi^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}\|_{2\alpha,\mathrm{cell}}}{\|\chi^{\mathrm{CV}}_{\mathrm{STAB,GKP}}\|_{2\alpha,\mathrm{cell}}} - \frac{\alpha\, n\log d}{1-\alpha}\end{aligned} \tag{64}$$

where in the second equality we used Theorem 4.

IV. SIMULATION ALGORITHMS

In this section, we provide simulation algorithms that use magic measures based on the connections we established with the Wigner and characteristic functions. We give the technical details in Appendix F.

A. Wigner function

The magic measures that were inspired by the continuous Wigner function allow for a nice operational interpretation of the simulation cost of a quantum circuit. Pashayan *et al.* [37] introduced a simulation algorithm for quasi-probability distributions that strictly resemble the discrete Wigner functions in odd dimensions. These ideas were used to adapt the simulator to multi-qubit cases by Rall *et al.* [38]. Using our unified approach that works for all dimensions, we can extend the simulator by Pashayan *et al.* to all dimensions and recover the simulator of Rall *et al.* for $d = 2$ (see Appendix F). The simulation time scales with the amount of negativity in the entire circuit defined as

$$\mathcal{M}_{\rightarrow} = \|x_\rho\|_1 \prod_{t=1}^{T} \max_{\boldsymbol{\lambda_t}} \|x_{U_t}(\boldsymbol{\lambda_t})\|_1 \max_{\boldsymbol{\lambda_T}} |x_\Pi(\boldsymbol{\lambda_T})| \tag{65}$$

where the maximum is taken over all trajectories and

$$x_\rho(\lambda) = \mathrm{Tr}\left(\rho \frac{O_{\boldsymbol{\lambda}}}{d^n}\right) \tag{66}$$

$$x_U(\lambda', \lambda) = \mathrm{Tr}\left(\frac{O_{\boldsymbol{\lambda'}}}{d^n} U O_{\boldsymbol{\lambda}} U^\dagger\right) \tag{67}$$

$$x_\Pi(\lambda) = \mathrm{Tr}\,(\Pi O_{\boldsymbol{\lambda}}). \tag{68}$$

are the coefficients related to the input state ρ, the unitary evolution U and the measurement effect Π with $\lambda = (\boldsymbol{l}, \boldsymbol{m}) \in \mathbb{Z}_d^{2n}$. The number of samples K that achieves precision ϵ with a failure probability p_f is given by

$$K \geq 2\mathcal{M}_{\rightarrow}^2 \frac{1}{\epsilon^2} \ln\left(\frac{2}{p_f}\right). \tag{69}$$

This shows that the number of samples directly scales with the resourcefulness of the input state $\|x_\rho\|_1$ if we evolve using the free operations of our magic quantifiers like Clifford unitaries. This result gives a nice operational interpretation of the quantifiers discussed in this work, as already noted in the case for the discrete Wigner negativity [37].

A few comments on the difference between even and odd dimensional systems are in order. For odd dimensional systems, it holds $\|x_\rho\|_1 \geq 1$, whereas it is possible for qubits that $\|x_\rho\|_1 \leq 1$ for specific states which reduce the number of samples needed. These qubit states are discussed in [38] and are called hyperoctahedral states. We show that this phenomenon exists in all even dimensions and call these states hyperpolyhedral states. See Appendix G for details. However, for pure states, it holds that $\|x_\rho\|_1 \geq 1$.

Another interesting difference between even and odd dimensions when Pauli measurements are involved is that the simulator is less competitive in even dimensions. The cost of measurements is taken into account via the term

$$\max_{\lambda_T} |x_\Pi(\lambda_T)|. \tag{70}$$

Since for odd-dimensional systems $O_{\boldsymbol{l},\boldsymbol{m}}$ has trace 1, computational basis measurements do not increase the simulation time. This is not the case for even dimensions. In this case, the measurements increase simulation time, as was noted by Rall *et al.* [38].

Let us assume that we would like to measure k-qudits of our n-qudit system in a computational basis state $|\boldsymbol{i}\rangle$. The measurement effect then is given as $\Pi = \mathbb{1}_{n-k} \otimes |\boldsymbol{i}\rangle\langle\boldsymbol{i}|$. Without loss of generality, assume the measurement of the state $|\boldsymbol{1}\rangle\langle\boldsymbol{1}|$, the state with all measured qudit in the 1 state. The expansion of a qudit in the operators $O_{l,m}$ is $|1\rangle\langle 1| = \frac{1}{d}\sum_{i=1}^{d-1} O_{2,i}$. The cost inferred from the measurement is then

$$\max_{\lambda_T} |x_\Pi(\lambda_T)| = \max_{\boldsymbol{l},\boldsymbol{m}} |\mathrm{Tr}\,[O_{\boldsymbol{l},\boldsymbol{m}} \mathbb{1}_{n-k} \otimes |\boldsymbol{1}\rangle\langle\boldsymbol{1}|]| \tag{71}$$

$$= \max_{\boldsymbol{l_{n-k}},\boldsymbol{m_{n-k}}} \left|\mathrm{Tr}\left[O_{\boldsymbol{l_{n-k}},\boldsymbol{m_{n-k}}}\right]\right| \max_{\boldsymbol{l_k},\boldsymbol{m_k}} |\mathrm{Tr}\,[O_{\boldsymbol{l_k},\boldsymbol{m_k}} |\boldsymbol{1}\rangle\langle\boldsymbol{1}|]| \tag{72}$$

The maximum trace $|\mathrm{Tr}\,[O_{\boldsymbol{l_k},\boldsymbol{m_k}} |\boldsymbol{1}\rangle\langle\boldsymbol{1}|]|$ is 1 for both even and odd dimensions. However, for the first term there is a big difference between even and odd dimensions. For odd dimensions the trace of $O_{\boldsymbol{l},\boldsymbol{m}}$ is ± 1, so unmeasured qudits do not add to the simulation cost in any way. This is not the case for even dimensions. In even dimensions the trace of a single qudit operator $O_{l,m}$ is either 0 or 2. Therefore, the maximum of the first term $\left|\mathrm{Tr}\left[O_{\boldsymbol{l_{n-k}},\boldsymbol{m_{n-k}}}\right]\right|$ is 2^{n-k}, and thus the number of unmeasured qudits increase the number of samples required exponentially.

B. Characteristic function

The same ideas can be used to construct a simulator that is based on characteristic functions. It will reduce to the simulator by Rall *et al.* [38] for $d = 2$. The simulation cost scales with a resource quantified using magic measures based on the connection of the characteristic functions.

Instead of representing the quantum state in the basis of $O_{\boldsymbol{l},\boldsymbol{m}}$, we use the Heisenberg-Weyl operators $P_d(\boldsymbol{l}, \boldsymbol{m})$ defined in (8) as our basis. Since they are unitary and traceless (with the exception of the identity operator) a few small modification are in order. A qudit state ρ and its characteristic function χ_ρ^{DV} can be written as

$$\rho = \frac{1}{d}\sum_{\boldsymbol{l},\boldsymbol{m}} \chi_\rho^{\mathrm{DV}}(\boldsymbol{l}, \boldsymbol{m}) P_d(\boldsymbol{l}, \boldsymbol{m}) \tag{73}$$

with $\chi_\rho^{\mathrm{DV}}(\boldsymbol{0}, \boldsymbol{0}) = 1$, since $P_d(\boldsymbol{0}, \boldsymbol{0}) = \mathbb{1}$. Furthermore, since the density operator is Hermitian, it holds that

$$\sum_{\boldsymbol{l},\boldsymbol{m}} \chi_\rho^{\mathrm{DV}}(\boldsymbol{l}, \boldsymbol{m}) P_d(\boldsymbol{l}, \boldsymbol{m}) = \sum_{\boldsymbol{l},\boldsymbol{m}} \left[\chi_\rho^{\mathrm{DV}}(\boldsymbol{l}, \boldsymbol{m})\right]^* P_d(\boldsymbol{l}, \boldsymbol{m})^\dagger. \tag{74}$$

Therefore, many coefficients in the decomposition are redundant. For Heisenberg-Weyl operators it holds that

$$P^\dagger(\boldsymbol{l}, \boldsymbol{m}) = \omega_D^{\boldsymbol{l}\cdot\boldsymbol{m}} P(-\boldsymbol{l}, -\boldsymbol{m}) \tag{75}$$

and therefore

$$\left[\chi_\rho^{\mathrm{DV}}(\boldsymbol{l}, \boldsymbol{m})\right]^* = \omega_D^{\boldsymbol{l}\cdot\boldsymbol{m}} \chi_\rho^{\mathrm{DV}}(-\boldsymbol{l}, -\boldsymbol{m}). \tag{76}$$

This implies that we have only $\frac{d^2-1}{2}$ independent coefficients in the decomposition. Thus, we can only sample from the independent coefficients, since they are pairwise dependent.

The rest of the algorithm works equivalently. The simulation times scale with the negativity of the entire circuit which is here re-expressed as

$$\mathcal{M}_{\rightarrow}^{\chi} = \left\|\chi_{\rho}^{\mathrm{DV}}\right\|_1 \prod_{t=1} \max_{\lambda_t} \left\|\chi_{U_t}^{\mathrm{DV}}(\lambda_t)\right\|_1 \max_{\lambda_T} \left|\chi_{\Pi}^{\mathrm{DV}}(\lambda_T)\right| \tag{77}$$

with

$$\chi_{\rho}^{\mathrm{DV}}(\lambda) = \mathrm{Tr}\left(\rho \frac{P^{\dagger}(\lambda)}{d^n}\right) \tag{78}$$

$$\chi_{U}^{\mathrm{DV}}(\lambda', \lambda) = \mathrm{Tr}\left(\frac{P^{\dagger}(\lambda')}{d^n} U P(\lambda) U^{\dagger}\right) \tag{79}$$

$$\chi_{\Pi}^{\mathrm{DV}}(\lambda') = \mathrm{Tr}\left(\Pi P(\lambda)\right). \tag{80}$$

The simulator behaves similarly to the previous one for even dimensions. The same simulation time increase happens for unmeasured qudits, and the operations that do not increase the runtime are quite limited.

V. MAGIC NEEDS NON-GAUSSIANITY

It has been known since the original GKP paper [36] that one can implement the logical T-gate and thus get an H-type magic state by using a cubic phase state or cubic interaction e^{icQ^3}. However, this is merely one possibility for implementing a non-Gaussian interaction, and this does not show the necessity of non-Gaussianity to implement a non-Clifford operation on the code subspace. This is a widely held belief based on the correspondence between a pair of Pauli and displacement operators and that of Clifford and Gaussian operations, where displacement operators and Pauli operators are both Heisenberg-Weyl operators. However, this "belief" has not been proven in general, beyond specific scenarios in qubit systems [39]. Indeed, GKP states have much Wigner negativity and thus *a priori* additional non-Gaussianity may not be required, making the necessity of non-Gaussian operation to implement a non-Clifford operation nontrivial.

Nevertheless, the results established above allow us to show that non-Gaussian operations are essential to implement non-stabilizer operations in the GKP code space. In fact, we find that the Gaussian *protocols* [5]—a class of quantum channels larger than Gaussian operations, which also admits feed-forwarded Gaussian operations conditioned on the outcomes of Gaussian measurements—are not able to implement non-stabilizer operations in the GKP code space. Importantly, Gaussian protocols include a gate teleportation circuit involving a Gaussian measurement and a feed-forwarded Gaussian unitary, which itself is not a Gaussian operation [45].

Theorem 5. *Let Λ be a quantum channel with n-qubit input and output. If there exists a pure stabilizer state ϕ and a pure non-stabilizer state ψ such that $\Lambda(\phi) = \psi$, Λ cannot be implemented in a GKP code space by a Gaussian protocol. Also, for a quantum channel Λ with n-qudit input and output systems with odd local dimensions, the condition can be relaxed to the existence of a (potentially mixed) stabilizer state σ and a state ρ with $\|W_{\rho}^{\mathrm{DV}}\|_1 > 1$ such that $\Lambda(\sigma) = \rho$.*

Proof. Suppose that Λ can be implemented in the GKP code space by a Gaussian protocol $\mathcal{G}$, i.e., $\mathcal{G}(\sigma_{\mathrm{GKP}}) = \rho_{\mathrm{GKP}}$ for qudit states σ and ρ such that $\Lambda(\sigma) = \rho$. Since $\|W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}$ does not increase under Gaussian protocols [5, 6, 29], we get

$$\|W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{1,\mathrm{cell}} = \|W_{\mathcal{G}(\sigma_{\mathrm{GKP}})}^{\mathrm{CV}}\|_{1,\mathrm{cell}} \leq \|W_{\sigma_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}. \tag{81}$$

Because of the assumption that ρ is also an n-qudit state, Theorem 1 and (81) imply that

$$\begin{aligned} \|x_{\sigma}\|_1 &= \frac{\|W_{\sigma_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}}{\|W_{\mathrm{STAB}_n,\mathrm{GKP}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}} \\ &\geq \frac{\|W_{\rho_{\mathrm{GKP}}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}}{\|W_{\mathrm{STAB}_n,\mathrm{GKP}}^{\mathrm{CV}}\|_{1,\mathrm{cell}}} \\ &= \|x_{\rho}\|_1. \end{aligned} \tag{82}$$

Suppose that the input state σ is a pure stabilizer state denoted by ϕ and the output state ρ is a pure non-stabilizer state ψ. Since $\|x_{\xi}\|_1$ is faithful for pure states as shown in Sec. III A, i.e., for a pure state ξ, $\|x_{\xi}\|_1 = 1$ if and only if ξ is a stabilizer state, we get $\|x_{\phi}\|_1 = 0$ and $\|x_{\psi}\|_1 > 0$. This is a contradiction with (82), showing that such a channel Λ cannot be implemented by a Gaussian protocol.

The statement for odd dimensions follows by the same argument using the relation (36).

□

An immediate consequence is that a Gaussian protocol cannot implement non-Clifford unitary gates deterministically. This does not contradict the protocol by Baragiola *et al.* [46], which requires many auxiliary GKP states—making the whole operation involving the preparation of such ancillary states highly non-Gaussian—to apply a single non-Clifford gate. In addition, their protocol is probabilistic and, therefore, does not directly fall into the scope of our result, which is pertinent to deterministic operations.

VI. CONCLUSION AND OUTLOOK

In this work, we established a fundamental relation between discrete- and continuous-variable systems via the Gottesman-Kitaev-Preskill encoding. We introduced a family of distributions for discrete-variable systems and showed that their l_p-norm exactly corresponds to that of the continuous Wigner function that encodes the same qudit states via GKP encoding. Notably, the discrete-variable distribution coincides with the discrete Wigner function for odd dimensions, allowing us to connect the negativity of Wigner functions of discrete and continuous variables for $p = 1$. More generally, our distributions allow for defining a magic quantifier for all dimensions and extend the discrete Wigner negativity defined for odd dimensions and the stabilizer Rényi entropy defined for multiqubit systems in a unified manner. Furthermore, we showed that the l_p-norm of the discrete-variable characteristic function corresponds to the characteristic function of a GKP state that encodes the same qudit state. This provides a new interpretation of the stabilizer Rényi entropy in terms of the GKP encoding and naturally extends it to all dimensions. Employing this framework, we introduced a classical simulation algorithm, where the run time scales with the magic measures we introduced. The first algorithm is based on the magic measures connected to the continuous Wigner function and recovers the simulator in Ref. [37], while the second one is based on the magic measures connected to the continuous characteristic function. Both algorithms give a strong operational interpretation to the magic measures we introduced. We utilized our findings to demonstrate that achieving a deterministic implementation of a logical non-Clifford operation, with identical input and output dimensions within the GKP code subspace, necessitates a non-Gaussian operation, even when operating at the theoretical limit of ideal GKP state input.

Our framework offers a novel approach to analyzing magic and non-Gaussian resources by employing tools developed for the other. This begs the question of whether we can investigate more properties of finite-dimensional systems using infinite-dimensional ones or vice versa. Furthermore, we have seen that the magic measures defined in this work behave differently for even and odd dimensions. An interesting future direction is to further investigate the origin of this behavior. Finally, being able to investigate and see the dependence of the dimensionality could shed new light on the source of quantum speed-ups.

Note added.—During the completion of this manuscript, a related independent work by Lingxuan Feng and Shunlong Luo [47] was brought to our attention, where the authors found a complementary relation between the description of a qudit state and continuous-variable Wigner function of the corresponding GKP state.

ACKNOWLEDGMENTS

We thank Kaifeng Bu and Ulysse Chabaud for helpful discussions. G.F. acknowledges support from the Swedish Research Council (Vetenskapsrådet) through the project grant DAIQUIRI, as well as from the HORIZON-EIC-2022-PATHFINDERCHALLENGES-01 programme under Grant Agreement Number 101114899 (Veriqub). G.F., O.H. acknowledge support from the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT). R.T. acknowledges the support of JSPS KAKENHI Grant Number JP23K19028, JP24K16975, JST, CREST Grant Number JPMJCR23I3, Japan, and MEXT KAKENHI Grant-in-Aid for Transformative Research Areas A “Extreme Universe” Grant Number JP24H00943.

Appendix A: l_p norm and renormalization

In this section, we formalize a way to compute the l_p norm of the characteristic function as well as the Wigner function of GKP states. Note here that the l_1 norm of the Wigner function is the Wigner negativity. The l_p norm is defined as

$$\|f\|_p = \left(\int \mathrm{d}\boldsymbol{x} |f(\boldsymbol{x})|^p\right)^{\frac{1}{p}}. \tag{A1}$$

We are interested in computing the l_p-norm of characteristic and Wigner functions of GKP states, so we deal with sums of Dirac distribution, where the distributions have disjoint support

$$\begin{aligned}&\left(\int_{-\infty}^{\infty} \mathrm{d}\boldsymbol{x} \left|\sum_i f_i(\boldsymbol{x})\delta(\boldsymbol{x}-\boldsymbol{x}_i)\right|^p\right)^{\frac{1}{p}} \\ &= \left(\sum_i |f_i(\boldsymbol{x}_i)|^p \delta(0)^{p-1}\right)^{\frac{1}{p}} = \left(\sum_i |f_i(\boldsymbol{x}_i)|^p\right)^{\frac{1}{p}} \delta(0)^{\frac{p-1}{p}}.\end{aligned} \tag{A2}$$

This integral evaluates to the same Dirac distribution $\delta(0)^{(p-1)/p}$ for all GKP states, which will be canceled by dividing it by the l_p-norm for another GKP state as in Theorems 1 and 4. Therefore, we will define the norm as

$$\begin{aligned}&\left(\int_{-\infty}^{\infty} \mathrm{d}\boldsymbol{x} \left|\sum_i f_i(\boldsymbol{x})\delta(\boldsymbol{x}-\boldsymbol{x}_i)\right|^p\right)^{\frac{1}{p}} \\ &= \left(\int_{-\infty}^{\infty} \mathrm{d}\boldsymbol{x} \left|\sum_i f_i(\boldsymbol{x})\right|^p \delta(\boldsymbol{x}-\boldsymbol{x}_i)\right)^{\frac{1}{p}} \\ &= \left(\sum_i |f_i(\boldsymbol{x}_i)|^p\right)^{\frac{1}{p}}\end{aligned} \tag{A3}$$

as a kind of regularization.

Appendix B: Proof of Proposition 2

In this section, we derive the atomic form of a n-qudit state encoded in the Gottesman-Kitaev-Preskill (GKP) code. We call the representation atomic if each Dirac distribution with different support appears only once in the summation, thus all Dirac distributions are distinct. We start deriving the atomic form for one qudit encoded in GKP and then generalize it to n-qudit systems.

1. One Qudit

For a single qudit, the Wigner function of a computational basis state $|j\rangle\langle j|$ encoded in GKP are

$$\begin{aligned}&W^{\mathrm{CV}}_{|j\rangle\langle j|_{\mathrm{GKP}}}(r_q, r_p) \\ &\propto \sum_{s,t=-\infty}^{\infty} (-1)^{st} \delta(r_p - \frac{\pi}{d\alpha} s)\delta(r_q - \alpha j - \frac{d\alpha}{2} t).\end{aligned} \tag{B1}$$

In order to derive the Wigner function of an arbitrary qudit state $\rho = \sum_{u,v\in\mathbb{Z}_d} \rho_{u,v} \left|u\right\rangle \left\langle v\right|$ encoded in the GKP code, we expand our state in the computational basis

$$W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(r_q,r_p) = \sum_{u,v\in\mathbb{Z}_d} \rho_{uv} \frac{1}{2\pi} \int_{-\infty}^{\infty} \mathrm{d}x\, e^{ir_p x} \left[\sum_{s=-\infty}^{\infty} \delta\left(r_q + \frac{x}{2} - \sqrt{\frac{2\pi}{d}}(u+ds)\right)\right] \left[\sum_{t=-\infty}^{\infty} \delta\left(r_q - \frac{x}{2} - \sqrt{\frac{2\pi}{d}}(v+dt)\right)\right]. \tag{B2}$$

We then use the linearity of the Wigner function and get cross terms between the computational basis states j and k

$$\begin{aligned}
W^{\mathrm{CV}}_{|j\rangle\langle k|_{\mathrm{GKP}}}(r_q,r_p) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \mathrm{d}x e^{ir_p x} \left[\sum_{s=-\infty}^{\infty} \delta\left(r_q + \frac{x}{2} - \sqrt{\frac{2\pi}{d}}(j+ds)\right)\right] \left[\sum_{t=-\infty}^{\infty} \delta\left(r_q - \frac{x}{2} - \sqrt{\frac{2\pi}{d}}(k+dt)\right)\right] \\
&= \frac{1}{2\cdot 2\pi} \sum_{s,t} e^{2ir_p(r_q - \sqrt{\frac{2\pi}{d}}(k+dt))} \delta\left(r_q - \sqrt{\frac{\pi}{2d}}[j+k+ds+dt]\right) \\
&= \frac{1}{2\cdot 2\pi} \sum_{s,t} e^{2ir_p(q - \sqrt{\frac{2\pi}{d}}(k+dt-ds))} \delta\left(r_q - \sqrt{\frac{\pi}{2d}}[j+k+dt]\right) \\
&= \frac{1}{2\cdot 2\pi} \sum_{s,t} e^{2ir_p\sqrt{\frac{2\pi}{d}}ds} e^{2ir_p(r_q - \sqrt{\frac{2\pi}{d}}(k+dt))} \delta\left(r_q - \sqrt{\frac{\pi}{2d}}(j+k+dt)\right) \\
&= \frac{1}{2\cdot 2\pi} \sum_{s,t} \delta\left(\sqrt{\frac{2d}{\pi}} r_p - s\right) \delta\left(r_q - \sqrt{\frac{\pi}{2d}}(j+k+dt)\right) e^{2ir_p(\sqrt{\frac{\pi}{2d}}(j+k+dt) - \sqrt{\frac{2\pi}{d}}(k+dt))} \\
&= \frac{1}{2\sqrt{2\pi d}} \sum_{s,t} \delta\left(r_p - s\sqrt{\frac{\pi}{2d}}\right) \delta\left(r_q - \sqrt{\frac{\pi}{2d}}(j+k+dt)\right) e^{ir_p\sqrt{\frac{2\pi}{d}}(j-k-dt)},
\end{aligned} \tag{B3}$$

where we used the Poisson resummation formula

$$\sum_{n=-\infty}^{\infty} e^{i2\pi nx} = \sum_{k=-\infty}^{\infty} \delta(x-k). \tag{B4}$$

We simplify (B2) by using (B3) and arrive at

$$W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(r_q,r_p) = \frac{1}{\sqrt{8\pi d}} \sum_{u,v=0}^{d-1} \rho_{u,v} \sum_{s,t} (-1)^{s(u-v-dt)/d} \delta\left(r_p - s\sqrt{\frac{\pi}{2d}}\right) \delta\left(r_q - \sqrt{\frac{\pi}{2d}}(u+v+dt)\right). \tag{B5}$$

We need to find the coefficients $c_{\rho_{\mathrm{GKP}}}(l,m)$ such that

$$\begin{aligned}
&W_{\rho_{\mathrm{GKP}}}(r_q,r_p) \\
&= \frac{\sqrt{d}}{\sqrt{8\pi}} \sum_{l,m} c_{\rho_{\mathrm{GKP}}}(l,m) \delta\left(r_p - m\sqrt{\frac{\pi}{2d}}\right) \delta\left(r_q - l\sqrt{\frac{\pi}{2d}}\right)
\end{aligned} \tag{B6}$$

only has disjoint support for each Dirac distribution in the summation.

By inspection of Eq. (B5), we immediately see that $\delta\big(r_p - s\sqrt{\frac{\pi}{2d}}\big)$ is already in the correct form and thus will only contribute a phase with $s = m$. Furthermore, we restrict the GKP state to one until the cell of length $\sqrt{2d\pi}$, so each m, l can have $2d$ values $m, l \in \{0, 1, ..., 2d-1\}$. For now, let us consider $s = m = 0$. Then we get the same Dirac distribution for q if $u + v + dt = l$. This requirement can be simplified if we remember that we consider only a unit cell and thus $u+v \mod d = l$. Consequently the matrix element $c_{\rho_{\mathrm{GKP}}}(l,0)$ will be a sum of $\rho_{u,v}$ with $u+v \mod d = l$. We can write this as

$$c_{\rho_{\mathrm{GKP}}}(l,0) = d^{-1}\operatorname{Tr}(\rho M_l) \tag{B7}$$

with

$$M_l = \sum_{\substack{u,v\in\mathbb{Z}_d\\ u+v \bmod d = l}} |u\rangle\langle v| \,. \tag{B8}$$

As an example, if we take qubits $d=2$

$$M_0 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad M_1 = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \tag{B9}$$

so we retrieve the identity and Pauli X. For qutrits $d=3$ we get

$$M_0 = \begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix} \; M_1 = \begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix} \; M_2 = \begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{pmatrix} \tag{B10}$$

We now consider the general case with $m \neq 0$. Recalling $l = u+v+dt$, the contribution for $m \neq 0$ is given by the phase factor

$$\begin{aligned}\sum_m (-1)^{m(u-v-dt)/d} &= \sum_m (-1)^{m(2u-l)/d}\\ &= \sum_m e^{i\pi m(2u-l)/d} = \omega_d^{-ml/2}\omega_d^{mu}\end{aligned} \tag{B11}$$

where $\omega_d = e^{2\pi i/d}$ is the d th root of unity. This allows us to obtain the general form of matrix elements in (B6) as

$$\begin{aligned} c_{\rho_{\mathrm{GKP}}}(l,m) &= d^{-1}\omega_d^{-ml/2}\operatorname{Tr}(M_l Z_d^m \rho) && \text{(B12)}\\ &= d^{-1}\operatorname{Tr}(O_\rho(l,m)\rho) && \text{(B13)}\\ &= x_\rho(l,m). && \text{(B14)}\end{aligned}$$

This shows Proposition 2 in the case of $n=1$.

2. n-Qudits

In this section, we will derive the multi-qudit atomic form of GKP states. The state of an arbitrary n-qudit state is given as $\rho = \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_d^n}\rho_{\boldsymbol{u},\boldsymbol{v}}|\boldsymbol{u}\rangle\langle\boldsymbol{v}|$. The Wigner function for the GKP state that encodes this n-qudit state is then

$$\begin{aligned} &W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r})\\ &= \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_d^n}\rho_{\boldsymbol{u},\boldsymbol{v}}\prod_{i=1}^n \frac{1}{2\pi}\int_{-\infty}^{\infty}\mathrm{d}r_{x_i}\, e^{ir_{p_i}r_{x_i}}\left[\sum_{s_i=-\infty}^{\infty}\delta\left(r_{q_i}+\frac{r_{x_i}}{2}-\sqrt{\frac{2\pi}{d}}(u_i+ds_i)\right)\right]\left[\sum_{t_i=-\infty}^{\infty}\delta\left(r_{q_i}-\frac{r_{x_i}}{2}-\sqrt{\frac{2\pi}{d}}(v_i+dt_i)\right)\right]\\ &= \frac{1}{(\sqrt{8\pi d})^n}\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_d^n}\rho_{\boldsymbol{u},\boldsymbol{v}}\prod_{i=1}^n\left[\sum_{s_i,t_i}(-1)^{\frac{s_i}{d}(u_i-v_i-dt_i)}\delta\left(r_{p_i}-\sqrt{\frac{\pi}{2d}}s_i\right)\delta\left(r_{q_i}-\sqrt{\frac{\pi}{2d}}(dt_i+u_i+v_i)\right)\right].\end{aligned} \tag{B15}$$

We are now ready to show Proposition 2 by confirming that

$$\begin{aligned} W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r}) = \frac{\sqrt{d}^n}{\sqrt{8\pi}^n}&\sum_{\boldsymbol{l},\boldsymbol{m}} c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m})\\ &\times\delta\left(\boldsymbol{r_p}-\boldsymbol{m}\sqrt{\frac{\pi}{2d}}\right)\delta\left(\boldsymbol{r_q}-\boldsymbol{l}\sqrt{\frac{\pi}{2d}}\right)\end{aligned} \tag{B16}$$

coincides with (B15) by taking $c_{\rho_{\mathrm{GKP}}}(\boldsymbol{l},\boldsymbol{m}) = x_\rho(\boldsymbol{l},\boldsymbol{m})$. We note that

$$\begin{aligned} &x_\rho(\boldsymbol{l},\boldsymbol{m})\\ &= d^{-n}\omega_d^{-\boldsymbol{m}\cdot\boldsymbol{l}/2}\operatorname{Tr}(M_{l_1}\otimes\ldots\otimes M_{l_n}Z_d^{m_1}\otimes\ldots\otimes Z_d^{m_n}\rho)\\ &= d^{-n}\omega_d^{-\boldsymbol{m}\cdot\boldsymbol{l}/2}\operatorname{Tr}(M_{\boldsymbol{l}}Z_d^{\boldsymbol{m}}\rho)\end{aligned} \tag{B17}$$

with

$$\begin{aligned} &\operatorname{Tr}(M_{\boldsymbol{l}}Z_d^{\boldsymbol{m}}\rho)\\ &\quad= \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_d^n}\rho_{\boldsymbol{u},\boldsymbol{v}}\langle\boldsymbol{v}|\,M_{l_1}\otimes\ldots\otimes M_{l_n}Z_d^{m_1}\otimes\ldots\otimes Z_d^{m_n}\,|\boldsymbol{u}\rangle\\ &\quad= \sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{Z}_d^n}\rho_{\boldsymbol{u},\boldsymbol{v}}\omega_d^{m_1u_1}\ldots\omega_d^{m_nu_n}\langle\boldsymbol{v}|\,M_{l_1}\otimes\ldots\otimes M_{l_n}\,|\boldsymbol{u}\rangle\,.\end{aligned} \tag{B18}$$

Note that $\langle\boldsymbol{v}|\,M_{l_1}\otimes\ldots\otimes M_{l_n}\,|\boldsymbol{u}\rangle = 1$ when

$$u_i+v_i+dt_i = l_i \tag{B19}$$

and $\langle\boldsymbol{v}|\,M_{l_1}\otimes\ldots\otimes M_{l_n}\,|\boldsymbol{u}\rangle = 0$ otherwise. Consequently, the Wigner function (B16) with the coefficients (B17) becomes

$$\begin{aligned}
W^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r}) &= \frac{\sqrt{d}^n}{\sqrt{8\pi}^n}\sum_{\boldsymbol{l},\boldsymbol{m}} x_\rho(\boldsymbol{l},\boldsymbol{m})\delta\Big(\boldsymbol{r_p}-\boldsymbol{m}\sqrt{\frac{\pi}{2d}}\Big)\delta\Big(\boldsymbol{r_q}-\boldsymbol{l}\sqrt{\frac{\pi}{2d}}\Big)\\
&= \frac{1}{\sqrt{8\pi d}^n}\sum_{\boldsymbol{l},\boldsymbol{m}}\sum_{u,v\in\mathbb{Z}_d^n}\rho_{uv}\omega_d^{-\boldsymbol{m}\cdot\boldsymbol{l}/2}\omega_d^{m_1u_1}...\omega_d^{m_nu_n}\,\langle v|\,M_{l_1}\otimes...\otimes M_{l_n}\,|u\rangle\,\Big(\boldsymbol{r_p}-\boldsymbol{m}\sqrt{\frac{\pi}{2d}}\Big)\delta\Big(\boldsymbol{r_q}-\boldsymbol{l}\sqrt{\frac{\pi}{2d}}\Big)\\
&= \frac{1}{\sqrt{8\pi d}^n}\sum_{u,v\in\mathbb{Z}_d^n}\rho_{uv}\prod_{i=1}^n\sum_{m_i,t_i}\omega_d^{-m_i(u_i+v_i+dt_i)/2}\omega_d^{m_iu_i}\Big(r_{p_i}-m_i\sqrt{\frac{\pi}{2d}}\Big)\delta\Big(r_{q_i}-\sqrt{\frac{\pi}{2d}}(u_i+v_i+dt_i)\Big)\\
&= \frac{1}{\sqrt{8\pi d}^n}\sum_{u,v\in\mathbb{Z}_d^n}\rho_{uv}\prod_{i=1}^n\sum_{m_i,t_i}(-1)^{m_i(u_i-v_i-dt_i)/d}\Big(r_{p_i}-m_i\sqrt{\frac{\pi}{2d}}\Big)\delta\Big(r_{q_i}-\sqrt{\frac{\pi}{2d}}(u_i+v_i+dt_i)\Big)
\end{aligned} \tag{B20}$$

which coincides with (B15). This completes the proof of Proposition 2.

Appendix C: Proof of Property 3 of $\|x_\rho\|_1$

In this section, we prove a property of $\|x_\rho\|_1$ among those listed in Sec. III, specifically that $\|x_\phi\|_1 = 1$ for every pure stabilizer state ϕ and $\|x_\psi\|_1 \geq 1$ for every pure state ψ.

We have the requirement for a pure state ψ that

$$\mathrm{Tr}(\psi^2) = \sum_{\boldsymbol{l},\boldsymbol{m}} x_\psi(\boldsymbol{l},\boldsymbol{m})^2 d^n = 1, \tag{C1}$$

which implies

$$\sum_{\boldsymbol{l},\boldsymbol{m}}\mathrm{Tr}(O_{\boldsymbol{l},\boldsymbol{m}}\psi)^2 = d^n. \tag{C2}$$

Recalling that $O_{\boldsymbol{l},\boldsymbol{m}}$ has eigenvalues ± 1, it holds that $|\,\mathrm{Tr}(O_{\boldsymbol{l},\boldsymbol{m}}\psi)| \leq 1,\ \forall \boldsymbol{l},\boldsymbol{m}$. This gives

$$\sum_{\boldsymbol{l},\boldsymbol{m}}|\,\mathrm{Tr}(O_{\boldsymbol{l},\boldsymbol{m}}\psi)| \geq \sum_{\boldsymbol{l},\boldsymbol{m}}\mathrm{Tr}(O_{\boldsymbol{l},\boldsymbol{m}}\psi)^2 = d^n, \tag{C3}$$

showing $\|x_\psi\|_1 \geq 1$ for every pure state ψ.

Let ϕ be an arbitrary pure stabilizer state. Proposition 3 ensures that $|x_\phi(\boldsymbol{l},\boldsymbol{m})| = 1/d^n$ for d^n elements, leading to

$$\|x_\phi\|_1 = \sum_{\boldsymbol{l},\boldsymbol{m}}|x_\phi(\boldsymbol{l},\boldsymbol{m})| = \frac{1}{d^n}\cdot d^n = 1, \tag{C4}$$

completing the proof.

Appendix D: Properties of the operator basis

1. Basic properties

In this section, we will show the properties of the operator

$$O_{l,m} = \omega_d^{-ml/2}M_lZ_d^m. \tag{D1}$$

As mentioned in the main text, the parameters are $l,m\in\mathbb{Z}_{2d}$. We will first show a property that involves all $l,m\in\mathbb{Z}_{2d}$. It holds that

$$\sum_{l,m\in\mathbb{Z}_{2d}} O_{l,m} = \sum_{l,m\in\mathbb{Z}_{2d}}\sum_{x=0}^{d-1}\omega_d^{-m(\frac{l}{2}-x)}\,|{-x}+l\rangle\langle x| \tag{D2}$$

$$= \sum_{l\in\mathbb{Z}_{2d}}\sum_{x=0}^{d-1}\sum_{m\in\mathbb{Z}_{2d}}\omega_d^{-m(\frac{l}{2}-x)}\,|{-x}+l\rangle\langle x| \tag{D3}$$

$$= \sum_{x=0}^{d-1}\sum_{l\in\mathbb{Z}_{2d}}\delta_{l,2x}\,|{-x}+l\rangle\langle x| \tag{D4}$$

$$= \mathbb{1}. \tag{D5}$$

Thus by summing over all $l,m\in\mathbb{Z}_{2d}$ we can resolve the identity using the operators $O_{l,m}$. Using the operators, however, as an operators basis we do not need all $l,m\in\mathbb{Z}_{2d}$. It suffices to restrict to $l,m\in\mathbb{Z}_d$. If we now have a value above d, we have

$$M_l = M_{l+d} \tag{D6}$$

$$Z_d^m = Z_d^{m+d}. \tag{D7}$$

However, the phases can be different

$$\begin{aligned}
O_{l+d,m} &= \omega_d^{-m(l+d)/2}M_lZ_d^m\\
&= (-1)^mO_{l,m}\\
O_{l,m+d} &= \omega_d^{-l(m+d)/2}M_lZ_d^m\\
&= (-1)^lO_{l,m}\\
O_{l+d,m+d} &= \omega_d^{-(l+d)(m+d)/2}M_lZ_d^m\\
&= (-1)^{l+m+d}O_{l,m}.
\end{aligned} \tag{D8}$$

So we get the same operators with a different sign.

It is easy to see that M_l is Hermitian. M_l is also an involution meaning $M_l^2 = \mathbb{1}$

$$M_lM_l = \sum_{\substack{u+v \bmod d=l\\ u'+v' \bmod d=l}} |u\rangle\,\langle v|u'\rangle\,\langle v'| \tag{D9}$$

$$= \sum_{\substack{u+v \bmod d=l \\ v+v' \bmod d=l}} |u\rangle\langle v'| \tag{D10}$$

$$= \sum_{u=v' \bmod d} |u\rangle\langle v'| \tag{D11}$$

$$= \sum_u |u\rangle\!\langle u|\,. \tag{D12}$$

Therefore,

$$\begin{aligned} O_{l,m}O_{l,m}^\dagger &= M_l Z_d^m \left(Z_d^m\right)^\dagger M_l^\dagger \\ &= M_l M_l \\ &= \mathbb{1}. \end{aligned} \tag{D13}$$

This confirms that $O_{l,m}$ is unitary. The operator $O_{l,m}$ is also Hermitian

$$\begin{aligned} O_{l,m}^\dagger &= \left[\omega_d^{-ml/2} M_l Z_d^m\right]^\dagger \\ &= \left[\omega_d^{-ml/2} \sum_{u+v \bmod d=l} \omega_d^{vm} |u\rangle\langle v|\right]^\dagger \\ &= \omega_d^{ml/2} \sum_{u+v \bmod d=l} \omega_d^{-vm} |v\rangle\langle u| \\ &= \omega_d^{-ml/2} \sum_{u+v \bmod d=l} \omega_d^{m(l-v)} |v\rangle\langle u| \\ &= \omega_d^{-ml/2} \sum_{u+v \bmod d=l} \omega_d^{um} |v\rangle\langle u| \\ &= O_{l,m} \end{aligned} \tag{D14}$$

and thus also an involution

$$O_{l,m}O_{l,m} = \mathbb{1} \tag{D15}$$

because of (D13). This implies that its eigenvalue is ±1.

The operators are orthogonal under the Hilbert-Schmidt inner product

$$\begin{aligned} \mathrm{Tr}\left(O_{l,m}O_{l',m'}\right) &= \omega_d^{-ml/2}\omega_d^{-m'l'/2}\,\mathrm{Tr}\left(M_l Z_d^m M_{l'} Z_d^{m'}\right) \\ &= \omega_d^{mv}\omega_d^{m'v'}\omega_d^{-ml/2}\omega_d^{-m'l'/2} \\ &\times \mathrm{Tr}\left(\sum_{\substack{u+v \bmod d=l \\ v'+v \bmod d=l'}} |u\rangle\langle v'|\right) \\ &= \sum_{\substack{u+v \bmod d=l \\ u+v \bmod d=l'}} \omega_d^{mv+m'u}\omega_d^{-ml/2}\omega_d^{-m'l'/2}. \end{aligned} \tag{D16}$$

This is 0 if $l \neq l'$ because $l, l' \in [0, d-1]$. Now assume $l = l'$, then we get

$$\begin{aligned} \mathrm{Tr}\left(O_{l,m}O_{l,m'}\right) &= \sum_{u+v \bmod d=l} \omega_d^{mv}\omega_d^{m'u}\omega_d^{-ml/2}\omega_d^{-m'l/2} \\ &= \sum_{u+v \bmod d=l} \omega_d^{(m-m')(v-u)/2} \\ &= \sum_{v\in\mathbb{Z}_d} \omega_d^{\tilde{m}v} e^{-i\pi\tilde{m}l/d} \\ &= e^{-i\pi\tilde{m}l/d} \sum_{v\in\mathbb{Z}_d} \omega_d^{\tilde{m}v} \end{aligned} \tag{D17}$$

where we set $\tilde{m} := m - m'$. This is 0 if $\tilde{m} \neq 0$, i.e., $m \neq m'$ because a sum over roots of unity is 0. On the other hand, when $l = l'$ and $m = m'$ we get

$$\mathrm{Tr}\left(O_{l,m}O_{l,m}\right) = \sum_{v\in\mathbb{Z}_d} 1 = d. \tag{D18}$$

In conclusion, we have

$$\mathrm{Tr}\left(O_{l,m}O_{l',m'}\right) = \delta_{mm'}\delta_{ll'}d. \tag{D19}$$

As we have seen earlier, $O_{l,m}$ are the standard Pauli operators for $d = 2$. So for $d > 2$ the operators $O_{l,m}$ are a generalization of the Pauli operators to arbitrary dimensions with the property of being an involution and Hermitian. In general, M_l and $O_{l,m}$ behave differently for even and odd dimensions, so we will separate the discussion.

a. *Odd dimensions*

In this section, we assume that the dimension d is odd. Then, the trace is

$$\mathrm{Tr}\left(O_{l,m}\right) = \sum_{2x \bmod d=l} \omega_d^{-ml/2}\omega_d^{mx}. \tag{D20}$$

When l is even, the solution for $2x \mod d = l$ is $x = l/2$ and gives $\mathrm{Tr}(O_{l,m}) = 1$. When l is odd, the solution for $2x \mod d = l$ is $x = (d+l)/2$, which gives $\mathrm{Tr}(O_{l,m}) = (-1)^m$. These can concisely be written as

$$\mathrm{Tr}\left(O_{l,m}\right) = (-1)^{ml}. \tag{D21}$$

The operator M_l has more structure, as seen in Eq. 31 which we report here for convenience

$$M_l = \sum_{u+v \bmod d=l} |u\rangle\langle v| \tag{D22}$$

There are d possibilities to fulfill this equation, so the matrix representation of M_l in computational basis will have d ones and the rest 0. Furthermore, the diagonal entries $2u \mod d = l$ have only one solution for every l. Therefore, the matrix M_l has one diagonal term 1 and is zero otherwise. Consequently $\mathrm{Tr}\left(M_l\right) = 1$.

Recall that we introduced the operators $O_{l,m}$ as the ones that connect the GKP state to the qudit state it encodes. Remarkably, we can establish a direct connection between this and the phase space point operators in odd dimensions, which a priori may not have anything to do with the operators $O_{l,m}$. The phase space point operators are defined as

$$\begin{aligned}A(a_1,a_2) &= d^{-1}\sum_{b_1,b_2=0}^{d-1} e^{-2i\frac{\pi}{d}(a_1,a_2)\Omega_d(b_1,b_2)^T} e^{i\frac{\pi}{d}b_1b_2} \\ &\quad\times \left(X_d^\dagger\right)^{b_2}\left(Z_d^\dagger\right)^{b_1} \\ &= d^{-1}\sum_{b_1,b_2}\omega_d^{a_2b_1}\omega_d^{b_2(\frac{1}{2}b_1-a_1)}\left(X_d^\dagger\right)^{b_2}\left(Z_d^\dagger\right)^{b_1}.\end{aligned} \tag{D23}$$

Using the expansion of Z_d and X_d in the computational basis

$$\begin{aligned}Z_d^b &= \sum_x \omega_d^{bx}|x\rangle\langle x| \\ Z_d^{b,\dagger} &= \sum_x \omega_d^{-bx}|x\rangle\langle x| = Z(-b) \\ X_d^b &= \sum_x |x+b\rangle\langle x| \\ X_d^{b\dagger} &= \sum_x |x\rangle\langle x+b| = X(-b)\end{aligned} \tag{D24}$$

we can write the phase space point operator as

$$\begin{aligned}A(a_1,a_2) &= d^{-1}\sum_x\sum_{b_1b_2}\omega_d^{b_1(a_2+\frac{1}{2}b_2)}\omega_d^{-a_1b_2}X_d^{-b_2}Z_d^{-b_1} \\ &= d^{-1}\sum_x\sum_{b_1b_2}\omega_d^{b_1(a_2-x+\frac{1}{2}b_2)}\omega_d^{-a_1b_2}|x-b_2\rangle\langle x|.\end{aligned} \tag{D25}$$

In order to further simplify, we need the discrete resummation formula

$$\frac{1}{d}\sum_{k=0}^{d-1}e^{2i\pi\frac{kn}{d}} = \delta_{0,n}. \tag{D26}$$

The phase space point operators can then be simplified to

$$\begin{aligned}&A(a_1,a_2) \\ &= d^{-1}\sum_x\sum_{b_1b_2}\omega_d^{b_1(a_2-x+\frac{1}{2}b_2)}\omega_d^{-a_1b_2}|x-b_2\rangle\langle x| \\ &= \sum_x\sum_{b_2}\delta_{0,a_2-x+\frac{1}{2}b_2}\omega_d^{-a_1b_2}|x-b_2\rangle\langle x| \\ &= \sum_x\sum_{b_2}\delta_{b_2,2(x-a_2)}\omega_d^{-a_1b_2}|x-b_2\rangle\langle x| \\ &= \sum_x\omega_d^{-2a_1(x-a_2)}|x-2(x-a_2)\rangle\langle x| \\ &= \sum_x\omega_d^{2a_1a_2}\omega_d^{-2a_1x}|-x+2a_2\rangle\langle x|.\end{aligned} \tag{D27}$$

Using the following substitutions

$$\begin{aligned}u &= -x+2a_2 \\ v &= x \\ u+v &= 2a_2 = l\end{aligned} \tag{D28}$$

we rewrite the phase space point operators as

$$\begin{aligned}A(a_1,l) &= \sum_{u+v \bmod d=l}\omega_d^{-a_1l}\omega_d^{-2a_1v}|u\rangle\langle v| \\ &= \sum_{u+v \bmod d=l}\omega_d^{a_1l}\omega_d^{-2a_1u}|u\rangle\langle v|.\end{aligned} \tag{D29}$$

By comparing this equation with the definition of $O_{l,m}$, we can identify $m = -2a_1$ and we get

$$A(a_1,a_2) = O_{2a_2,-2a_1}. \tag{D30}$$

This shows that the operator basis $\{O_{l,m}\}_{l,m\in\mathbb{Z}_d}$ is equivalent to the phase space point operators $\{A(a_1,a_2)\}_{a_1,a_2\in\mathbb{Z}_d}$ up to permutation and phase factors. Indeed, the oddness of d and (D8) ensure that there is a one-to-one correspondence between $a_1,a_2\in\mathbb{Z}_d$ and $l,m\in\mathbb{Z}_d$ such that $A(a_1,a_2) = O_{2a_2,-2a_1} \propto O_{l,m}$ up to phase, as $2a_2$ and $-2a_1$ respectively takes all values in $\mathbb{Z}_d$ by changing $a_1,a_2\in\mathbb{Z}_d$, and O_{l_1,m_1} and O_{l_2,m_2} coincide up to phase if $l_1 = l_2 \bmod d$ and $m_1 = m_2 \bmod d$.

b. Even dimensions

Now we investigate the operators $O_{l,m}$ for the case of even-dimensional systems. The trace is

$$\mathrm{Tr}\left(O_{l,m}\right) = \sum_x\omega^{-ml/2}\sum_{u+v \bmod d=l}\omega^{mu}\langle x|u\rangle\langle v|x\rangle \tag{D31}$$

$$= \sum_{2x \bmod d=l}\omega^{-ml/2}\omega^{mx}, \tag{D32}$$

which vanishes if l is odd. Suppose l is even and write $l = 2k$. Then we get

$$\mathrm{Tr}\left(O_{l,m}\right) = \sum_{2x \bmod d=l}\omega^{-ml/2}\omega^{mx} \tag{D33}$$

$$= \omega^{-mk}\left(\omega^{mk}+\omega^{m(k+\frac{d}{2})}\right) \tag{D34}$$

$$= 1+\omega^{m\frac{d}{2}} \tag{D35}$$

$$= 1+(-1)^m. \tag{D36}$$

We have the same behavior for the operators M_l. For odd dimensions the equation $u+v \mod d = l$ has d solutions. Therefore, the matrix representation in computational basis will have d 1's with the rest being 0. For odd l, the equation $2u \mod d = l$ has no solution, implying $\mathrm{Tr}\left(M_l\right) = 0$ for odd l. For even l, the equation $2u \bmod d = l$ has two solutions, $u = l/2$ and $u = l/2+d/2$. Therefore, we have $\mathrm{Tr}\left(M_l\right) = 2$.

We can make here an interesting observation. It is known that for odd dimensions the phase space point operator at the origin $A(0,0)$ acts as the parity operation

$$A(0,0)|x\rangle = |-x\rangle \tag{D37}$$

for a computational basis state x. The operators $O_{l,m}$ show the same behavior for even dimensions and thus for all dimensions

$$O_{0,0}\left|x\right\rangle = M_0\left|x\right\rangle = \left|-x\right\rangle. \tag{D38}$$

2. Clifford Covariance

This section investigates how the operators $O_{l,m}$ transform under Clifford unitaries. We will see that they behave almost equivalently to the Heisenberg-Weyl operators.

X_d, Z_d generate the $d-$dimensional Heisenberg-Weyl group and $R, P,$ SUM the $d-$dimensional Clifford unitaries. their action of computational basis state are [40]

$$X_d : \left|j\right\rangle \to \left|j+1\right\rangle \tag{D39}$$

$$Z_d : \left|j\right\rangle \to \omega_d^j \left|j\right\rangle \tag{D40}$$

$$R : \left|j\right\rangle \to \sum_{s=0}^{d-1} \omega_d^{js}\left|s\right\rangle \tag{D41}$$

$$P : \left|j\right\rangle \to \omega_d^{j^2/2}(\omega_D \omega_{2d}^{-1})^{-j}\left|j\right\rangle \tag{D42}$$

$$\text{SUM} : \left|i\right\rangle\left|j\right\rangle \to \left|i\right\rangle\left|i+j \mod d\right\rangle \tag{D43}$$

A Clifford unitary U_C maps the Heisenberg-Weyl operators

$$P_d(a,b) = \omega_d^{\frac{1}{2}ab} X_d^a Z_d^b \tag{D44}$$

in the following way

$$U_C P_d(u) U_C^\dagger = P_d(Su) \tag{D45}$$

where S is a $2n \times 2n$ matrix with entries over $\mathbb{Z}_D$ with $D = d$ for d odd and $D = 2d$ for d even. Heisenberg-Weyl operators have the following commutation relations

$$\left(X_d^a Z_d^b\right)\left(X_d^{a'} Z_d^{b'}\right) = \omega_d^{(a,b)\Omega(a',b')^T}\left(X_d^{a'} Z_d^{b'}\right)\left(X_d^a Z_d^b\right). \tag{D46}$$

We are now interested in how Clifford unitaries and Pauli operators transform

$$O_{l,m} = \sum_{x=0}^{d-1} \omega_d^{-m(\frac{l}{2}-x)}\left|-x+l\right\rangle\left\langle x\right| \tag{D47}$$

with $l, m \in [0, 2d-1]$ or equivalently $\mathbb{Z}_{2d}$. The values the computational basis states can have are $\mod d$ and the operators Z_d^m, M_l are repeating for $m, l \geq d$. The difference for $m, l \geq d$ is the phase factor $\omega_d^{-ml/2}$ that repeats after $2d$. This phase factor is important for the action of Clifford unitaries on the operators $O_{l,m}$, while it can be essentially neglected if we only want to use them as a basis. We expect by our construction through GKP that Clifford unitaries map $O_{\boldsymbol{l},\boldsymbol{m}}$ to another $O_{\boldsymbol{l'},\boldsymbol{m'}}$ and therefore keeps the negativity invariant.

The QFT gate R transforms the operator $O_{l,m}$ as

$$RO_{\boldsymbol{l},\boldsymbol{m}}R^\dagger = \sum_{x=0}^{d-1} \omega_d^{-m(\frac{l}{2}-x)} R\left|-x+l\right\rangle\left\langle x\right| R^\dagger \tag{D48}$$

$$= \sum_{s,s'} \omega_d^{-ml/2}\omega_d^{sl} \sum_x \omega_d^{x(m-s-s')}\left|s\right\rangle\left\langle s'\right| \tag{D49}$$

$$= \sum_{s,s'} \omega_d^{-ml/2}\omega_d^{sl}\delta_{s,m-s'}\left|s\right\rangle\left\langle s'\right| \tag{D50}$$

$$= \sum_{s'} \omega_d^{-ml/2}\omega_d^{ml}\omega_d^{-ls'}\left|m-s'\right\rangle\left\langle s'\right| \tag{D51}$$

$$= \sum_x \omega_d^{ml/2}\omega_d^{-lx}\left|m-x\right\rangle\left\langle x\right| \tag{D52}$$

and therefore transforms the coordinates like

$$m \to -l \tag{D53}$$

$$l \to m. \tag{D54}$$

The Phase gate P behaves differently for even and odd dimensions. For odd dimensions, we get

$$\begin{aligned} PO_{\boldsymbol{l},\boldsymbol{m}}P^\dagger &= \sum_x \omega_d^{-ml/2}\omega_d^{mx}\omega_d^{(-x+l)(-x+l-1)/2}\omega_d^{-x(x-1)/2} \\ &\quad \times\left|-x+l\right\rangle\left\langle x\right| \\ &= \sum_x \omega_d^{-ml/2}\omega_d^{mx}\omega_d^{(l^2-l)/2}\omega_d^{x(1-l)}\left|-x+l\right\rangle\left\langle x\right| \\ &= \sum_x \omega_d^{-l(m-l+1)/2}\omega_d^{x(m-l+1)}\left|-x+l\right\rangle\left\langle x\right| \end{aligned} \tag{D55}$$

with the coordinates transforming like

$$m \to m-l+1 \tag{D56}$$

$$l \to l. \tag{D57}$$

For even dimensions we nearly get the same result

$$PO_{\boldsymbol{l},\boldsymbol{m}}P^\dagger = \sum_x \omega_d^{-ml/2}\omega_d^{mx}\omega_d^{(-x+l)^2/2}\omega_d^{-x^2/2}\left|-x+l\right\rangle\left\langle x\right| \tag{D58}$$

$$= \sum_x \omega_d^{-ml/2}\omega_d^{mx}\omega_d^{(l^2)/2}\omega_d^{-xl}\left|-x+l\right\rangle\left\langle x\right| \tag{D59}$$

$$= \sum_x \omega_d^{-l(m-l)/2}\omega_d^{x(m-l)}\left|-x+l\right\rangle\left\langle x\right| \tag{D60}$$

and

$$m \to m-l \tag{D61}$$

$$l \to l. \tag{D62}$$

The action of Z_d transform $O_{l,m}$ as

$$Z_d O_{\boldsymbol{l},\boldsymbol{m}} Z_d^\dagger = \sum_x \omega_d^{-ml/2}\omega_d^{mx}\omega_d^{-x+l}\omega_d^{-x}\left|-x+l\right\rangle\left\langle x\right| \tag{D63}$$

$$= \sum_x \omega_d^{-l(m-2)/2}\omega_d^{x(m-2)}\left|-x+l\right\rangle\left\langle x\right| \tag{D64}$$

with the coordinates transforming as

$$m \to m-2 \tag{D65}$$

$$l \to l. \tag{D66}$$

Similarly for X_d we get

$$X_d O_{\boldsymbol{l},\boldsymbol{m}} X_d^\dagger = \sum_x \omega_d^{-ml/2} \omega_d^{mx} \left|-x+l+1\right\rangle \left\langle x+1\right| \tag{D67}$$

$$= \sum_x \omega_d^{-ml/2} \omega_d^{m(x-1)} \left|-x+l+2\right\rangle \left\langle x\right| \tag{D68}$$

$$= \sum_x \omega_d^{-m(l+2)/2} \omega_d^{mx} \left|-x+l+2\right\rangle \left\langle x\right| \tag{D69}$$

and

$$m \to m \tag{D70}$$

$$l \to l+2. \tag{D71}$$

The missing gate for the full Clifford group is the SUM gate

$$\mathrm{SUM} O_{\boldsymbol{l},\boldsymbol{m}} \otimes O_{\boldsymbol{l'},\boldsymbol{m'}} \mathrm{SUM}^\dagger = \sum_{x,y} \omega_d^{-ml/2} \omega_d^{-m'l'/2} \omega_d^{mx} \omega_d^{m'y} \left|-x+l,-y-x+l'\right\rangle \left\langle x,y+x\right| \tag{D72}$$

$$= \sum_{x,y'} \omega_d^{-ml/2} \omega_d^{-m'l'/2} \omega_d^{mx} \omega_d^{m'(y'-x)} \left|-x+l,-y'+l'+l\right\rangle \left\langle x,y'\right| \tag{D73}$$

$$= \sum_{x,y'} \omega_d^{-ml/2} \omega_d^{-m'l'/2} \omega_d^{x(m-m')} \omega_d^{m'y'} \left|-x+l,-y'+l'+l\right\rangle \left\langle x,y'\right| \tag{D74}$$

and

$$m \to m-m' \tag{D75}$$

$$l \to l \tag{D76}$$

$$m' \to m' \tag{D77}$$

$$l' \to l'+l. \tag{D78}$$

So we can write down the matrices that transform the coordinates under the action of Clifford unitaries $U_C O_{\boldsymbol{l},\boldsymbol{m}} U_C^\dagger = O_{M_{U_C}[l,l',m,m']^T}$. The matrices have the basis (l,m) or l,l',m,m', without the constant shifts and are given as

$$P : \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \tag{D79}$$

$$R : \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{D80}$$

$$\mathrm{SUM} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{D81}$$

These matrices are all symplectic and therefore they fulfill the relation

$$M^T \Omega M = \Omega \tag{D82}$$

$$\Omega = \begin{pmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0. \end{pmatrix} \tag{D83}$$

Interestingly, Clifford unitaries act on the Heisenberg-Weyl operators in a very similar way. The matrices S in the basis a,b and a_1,a_2,b_1,b_2 are given as [40]

$$P' : \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{D84}$$

$$R' : \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{D85}$$

$$\mathrm{SUM} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{D86}$$

where these matrices are over $\mathbb{Z}_D$ ($D = d$ for odd $D = 2d$ for even). It was shown that these matrices generate the symplectic group over $\mathbb{Z}_D$. We can connect our matrices (up to constant shifts) to these matrices

$$R^3 = R' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{D87}$$

$$P^{d-1} = P' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{D88}$$

while the SUM gate is already in the correct form. So the action of a Clifford unitary on $O_{\boldsymbol{l},\boldsymbol{m}}$ is a symplectic transformation over $\mathbb{Z}_{2d}$ of l,m. There is, however, a constant shift for P in the odd dimensional case.

3. Stabilizer states (Proof of Proposition 3)

This section shows that pure stabilizer states are flat when decomposing in the operators $O_{l,m}$ meaning all operators have the same weight modulo signs. We can write the zero state in all dimensions as

$$|0\rangle\!\langle 0| = |0\rangle\!\langle 0| + \frac{1}{d}\sum_{j}\sum_{\substack{u+v \mod d=0\\ v\neq 0}} w_d^{jv}\,|u\rangle\,\langle v| = \frac{1}{d}\sum_{j=0}^{d-1} O_{0,j} = \frac{1}{d}\sum_{j} M_0 Z_d^j = \frac{1}{d}\sum_{j}\sum_{u+v \mod d=0} \omega_d^{jv}\,|u\rangle\,\langle v| \tag{D89}$$

where we used that

$$\sum_{j=0}^{d-1}\omega_d^{jv} = 0 \tag{D90}$$

for $v \neq 0$. We see that all $O_{l,m}$ have the same weight. Using that the operators $O_{l,m}$ are covariant under Clifford unitaries as shown in Appendix D 2, we see that every pure stabilizer state has a flat weight.

Appendix E: Proof of Theorem 4

We compute the characteristic function for a qudit state ρ encoded in a GKP state. We need to use the following property of the displacement operator

$$D(\boldsymbol{r}) = \prod_{j=1}^{n} e^{ir_{q_j}r_{p_j}/2} e^{ir_{q_j}P_j} e^{-ir_{p_j}Q_j}; \tag{E1}$$

Then, the characteristic function of a qudit encoded in a GKP state is given as

$$\begin{aligned}
\chi^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r}) &= \mathrm{Tr}\left[\rho D(-\boldsymbol{r})\right]\\
&= \sum_{u,v\in\mathbb{Z}_d} \rho_{u,v}\,\langle u|\,D(-\boldsymbol{r})\,|v\rangle\\
&= \sum_{u,v\in\mathbb{Z}_d} \rho_{u,v} \sum_{s,t=-\infty}^{\infty} \left\langle \sqrt{\frac{2\pi}{d}}(u+ds)\middle| D(-\boldsymbol{r}) \middle| \sqrt{\frac{2\pi}{d}}(v+dt)\right\rangle_q\\
&= \sum_{u,v}\sum_{s,t} \rho_{u,v} e^{ir_q r_p/2} e^{ir_p\sqrt{\frac{2\pi}{d}}(v+dt)} \left\langle \sqrt{\frac{2\pi}{d}}(u+ds)\middle| \sqrt{\frac{2\pi}{d}}(v+dt)+r_q\right\rangle_q\\
&= \sum_{u,v}\sum_{s,t} \rho_{u,v} e^{ir_q r_p/2} e^{ir_p\sqrt{\frac{2\pi}{d}}(v+dt)} \delta\left(r_q - \sqrt{\frac{2\pi}{d}}(u-v-d(t-s))\right)\\
&= \sum_{u,v}\sum_{s,t} \rho_{u,v} e^{i2\pi s(r_p\sqrt{\frac{d}{2\pi}})} e^{i\frac{r_p}{2}(r_q+2\sqrt{\frac{2\pi}{d}}(v+dt))} \delta\left(r_q - \sqrt{\frac{2\pi}{d}}(u-v-dt)\right)\\
&= \sqrt{\frac{2\pi}{d}}\sum_{u,v}\sum_{s,t} \rho_{u,v}\,\delta\left(r_p - \sqrt{\frac{2\pi}{d}}s\right)\delta\left(r_q - \sqrt{\frac{2\pi}{d}}(u-v-dt)\right) e^{i\frac{r_p}{2}(r_q+2\sqrt{\frac{2\pi}{d}}(v+dt))}\\
&= \sqrt{\frac{2\pi}{d}}\sum_{u,v}\sum_{s,t} \rho_{u,v} e^{i\frac{\pi}{d}s(u+v+dt)} \delta\left(r_p - \sqrt{\frac{2\pi}{d}}s\right)\delta\left(r_q - \sqrt{\frac{2\pi}{d}}(u-v-dt)\right).
\end{aligned} \tag{E2}$$

With this expression, we aim at finding the coefficient $\gamma_{\rho_{\mathrm{GKP}}}(l,m)$ for $l,m \in \mathbb{Z}_d$ such that

$$\begin{aligned}
&\chi^{\mathrm{CV}}_{\rho_{\mathrm{GKP}}}(\boldsymbol{r})\\
&= \sqrt{\frac{2\pi}{d}}\sum_{l,m=-\infty}^{\infty} \gamma_{\rho_{\mathrm{GKP}}}(l,m)\\
&\quad\times \delta\left(r_p - m\sqrt{\frac{2\pi}{d}}\right)\delta\left(r_q - l\sqrt{\frac{2\pi}{d}}\right).
\end{aligned} \tag{E3}$$

Similarly to the case for the Wigner function, we restrict to one unit cell. Thus, the requirement for l is

$$u - v - dt = l \tag{E4}$$

$$u - v \mod d = l \tag{E5}$$

and therefore

$$\gamma_{\rho_{\rm GKP}}(l,0) = \sum_{u-v \mod d=l} \langle v|\,\rho\,|u\rangle = \operatorname{Tr}\left[X_d^l \rho\right]. \tag{E6}$$

By simplifying the phase factor

$$e^{i\frac{\pi}{d}s(v+u+dt)} = e^{i\frac{\pi}{d}s(-l+2u)} = \omega_d^{-sl/2}\omega_d^{su} \tag{E7}$$

we can write the coefficients as

$$\gamma_{\rho_{\rm GKP}}(l,m) = \omega_d^{-lm/2} \operatorname{Tr}\left[\rho X_d^l Z_d^m\right]. \tag{E8}$$

Therefore, the coefficients are given by the trace over the Pauli operators in d dimensions. This can be generalized to n qudits as

$$\begin{aligned}\gamma_{\rho_{\rm GKP}}(\boldsymbol{l},\boldsymbol{m}) &= \omega_d^{-\boldsymbol{l}\cdot\boldsymbol{m}/2} \operatorname{Tr}\left[\rho X^{\boldsymbol{l}} Z^{\boldsymbol{m}}\right] \\ &= d^n \omega_d^{-\boldsymbol{l}\cdot\boldsymbol{m}/2} \omega_D^{-\boldsymbol{l}\cdot\boldsymbol{m}/2} \chi_\rho^{\rm DV}(\boldsymbol{l},\boldsymbol{m})^*,\end{aligned} \tag{E9}$$

which shows (60).

Using (60) and the fact that $|\chi_\phi^{\rm DV}(\boldsymbol{l},\boldsymbol{m})| = d^{-n}$ for $(4d)^n$ elements in $\boldsymbol{l},\boldsymbol{m} \in \mathbb{Z}_{2d}^n$ and zero otherwise, we can get for a pure qudit state ϕ that

$$\|\chi_{\phi_{\rm GKP}}^{\rm CV}\|_{p,\rm cell} = (4d)^{n/p}\left(\frac{2\pi}{d}\right)^{n/2}. \tag{E10}$$

We then get, again by using (60), that

$$\begin{aligned}\|\chi_{\rho_{\rm GKP}}^{\rm CV}\|_{p,\rm cell} &= \left[\sum_{\boldsymbol{l},\boldsymbol{m}\in\mathbb{Z}_{2d}^n}\left\{\left(\frac{2\pi}{d}\right)^{n/2} d^n |\chi_\rho^{\rm DV}(\boldsymbol{l},\boldsymbol{m})|\right\}^p\right]^{1/p} \\ &= \left[4^n \sum_{\boldsymbol{l},\boldsymbol{m}\in\mathbb{Z}_{d}^n}\left\{(2\pi d)^{n/2}\,|\chi_\rho^{\rm DV}(\boldsymbol{l},\boldsymbol{m})|\right\}^p\right]^{1/p} \\ &= 4^{n/p}(2\pi d)^{n/2}\|\chi_\rho^{\rm DV}\|_p \\ &= d^{n(1-1/p)}\|\chi_\rho^{\rm DV}\|_p,\end{aligned} \tag{E11}$$

completing the proof.

Appendix F: Simulation algorithm

For the convenience of the reader we will use the frame notation from the works of [37]

$$F(\lambda) = \frac{O_\lambda}{d^n} \tag{F1}$$

$$G(\lambda) = O_\lambda \tag{F2}$$

$$\rho = \sum_\lambda \operatorname{Tr}\left(\rho\frac{O_\lambda}{d^n}\right)O_\lambda = \sum_\lambda G(\lambda)\operatorname{Tr}\left(\rho F(\lambda)\right). \tag{F3}$$

Unitary evolution of a state can be rewritten in this notation as

$$\begin{aligned}U\rho U^\dagger &= \sum_\lambda UG(\lambda)U^\dagger \operatorname{Tr}\left(\rho F(\lambda)\right) &\text{(F4)}\\ &= \sum_{\lambda,\lambda'} G(\lambda')\operatorname{Tr}\left(F(\lambda')UG(\lambda)U^\dagger\right)\operatorname{Tr}\left(\rho F(\lambda)\right) &\text{(F5)}\end{aligned}$$

and the output of a measurement Π is

$$\operatorname{Tr}\left(\Pi U\rho U^\dagger\right) = \sum_{\lambda,\lambda'} x_\Pi(\lambda')x_U(\lambda',\lambda)x_\rho(\lambda) \tag{F6}$$

with

$$x_\rho(\lambda) = \operatorname{Tr}\left(\rho F(\lambda)\right) \tag{F7}$$

$$x_U(\lambda',\lambda) = \operatorname{Tr}\left(F(\lambda')UG(\lambda)U^\dagger\right) \tag{F8}$$

$$x_\Pi(\lambda) = \operatorname{Tr}\left(\Pi G(\lambda)\right). \tag{F9}$$

Out of these quantities we can define the following probability distributions

$$P(\lambda|\rho) = \frac{|x_\rho(\lambda)|}{\|x_\rho\|_1} \tag{F10}$$

$$P(\lambda'|U,\lambda) = \frac{|x_U(\lambda',\lambda)|}{\|x_U(\lambda)\|_1} \tag{F11}$$

$$\|x_U(\lambda)\|_1 = \sum_{\lambda'}|x_U(\lambda',\lambda)| \tag{F12}$$

$$\|x_\rho\|_1 = \sum_\lambda |x_\rho(\lambda)| \tag{F13}$$

Thus we can rewrite the Born rule probability as

$$\begin{aligned}P(\Pi|U\rho U^\dagger) &= \sum_{\lambda,\lambda'} x_\Pi(\lambda')x_U(\lambda',\lambda)x_\rho(\lambda) &\text{(F14)}\\ &= \sum_{\lambda,\lambda'} M_{\lambda,\lambda'}P(\lambda'|U,\lambda)P(\lambda|\rho) &\text{(F15)}\end{aligned}$$

with $M_{\lambda,\lambda'} = \operatorname{sign}(x_\Pi(\lambda')x_U(\lambda',\lambda))x_\Pi(\lambda')\|x_U(\lambda)\|_1\|x_\rho\|_1$.

The simulation strategy is to sample λ from $P(\lambda|\rho)$ and then consider a possible transition to λ' from $P(\lambda'|U,\lambda)$. This can easily be generalized to a sequence of unitaries of length T as well. We then define a random variable as

$$\begin{aligned}M_{\vec{\lambda}} &= x_\Pi(\lambda_T)\operatorname{sign}(x_\rho(\lambda_0))\|x_\rho\|_1 &\text{(F16)}\\ &\times \prod_{t=1}^T \operatorname{sign}(x_{U_t}(\lambda_t,\lambda_{t-1}))\|x_{U_t}(\lambda_{t-1})\|_1. &\text{(F17)}\end{aligned}$$

The expectation value of this random variable is

$$\begin{aligned}\mathbb{E}(M_{\vec{\lambda}}) &= \sum_{\vec{\lambda}} P(\lambda_0|\rho)\prod_{t=1}^T P(\lambda_t|U_t,\lambda_{t-1})M_{\vec{\lambda}} &\text{(F18)}\\ &= \sum_{\vec{\lambda}} x_\Pi(\lambda_T)\prod_{t=1}^T x_{U_t}(\lambda_t,\lambda_{t-1})x_\rho(\lambda_0) &\text{(F19)}\end{aligned}$$

which is exactly the Born probability we want to estimate. The random variable output from our sampling algorithm is an unbiased estimator for the Born probability. The number of samples needed to achieve a given precision can be computed using the Hoeffding inequality Given a sequence of K *iid* random variables X_j bounded by $|X_j| \leq b$ and expected mean $\mathbb{E}(X)$, the probability that $\sum_{j=1}^{K} X_j/K$ deviated from the mean by more than ϵ is upper bounded by

$$P\left(\left|\mathbb{E}(X)-\sum_{j=1}^{K}\frac{X_j}{K}\right| \geq \epsilon\right) \leq 3\exp\left(-\frac{K\epsilon^2}{2b^2}\right) \tag{F20}$$

or equivalently we can achieve precision $\left|\mathbb{E}(X)-\sum_{j=1}^{K}\frac{X_j}{K}\right| \leq \epsilon$ with probability at least $(1-p_f)$ by setting the number of samples as

$$K = \left\lceil 2b^2\frac{1}{\epsilon^2}\ln\left(\frac{2}{p_f}\right)\right\rceil . \tag{F21}$$

We then define the negativity of the entire circuit as

$$\mathcal{M}_{\rightarrow} = \|x_\rho\|_1 \prod_{t=1} \max_{\lambda_t} \|x_{U_t}(\lambda_t)\|_1 \max_{\lambda_T} |x_\Pi(\lambda_T)| \tag{F22}$$

so it is the maximum negativity over all trajectories. This bounds the random variable from above, so we need at least

$$K \geq 2\mathcal{M}_{\rightarrow}^2\frac{1}{\epsilon^2}\ln\left(\frac{2}{p_f}\right) \tag{F23}$$

samples.

Appendix G: Hyperpolyhedral states

In this section, we investigate the phenomena of hyperpolyhedral states. In [38] the authors encounter hyperoctahedral states for qubit systems. They define these states as the states which have the stabilizer norm smaller than 1 or in our formulation $\sum_{\boldsymbol{l},\boldsymbol{m}} |x_{\boldsymbol{l},\boldsymbol{m}}| < 1$. For odd dimensional states these states are equivalent to Wigner positive states $\sum_{\boldsymbol{l},\boldsymbol{m}} |x_{\boldsymbol{l},\boldsymbol{m}}| = 1$. This set is strictly bigger than the set of stabilizer states.

For even dimensions, the question of a Wigner function is more difficult, especially related to computability, even though one can define such a quantity [42, 48, 49]. We define the Hyperpolyhedral states similarly to the qubit case for all even dimensions with $\sum_{\boldsymbol{l},\boldsymbol{m}} |x_{\boldsymbol{l},\boldsymbol{m}}| \leq 1$. Here we show that hyperpolyhedral states exist for all even dimensions and that they are not equivalent to stabilizer states.

The computational basis states can be expanded in the operators $O_{l,m}$ as

$$|0\rangle\langle 0| = \frac{1}{d}\sum_{i=0}^{d-1} O_{0,i} \tag{G1}$$

$$|1\rangle\langle 1| = X_d\,|0\rangle\langle 0|\,X_d^\dagger = \frac{1}{d}\sum_{i=0}^{d-1} O_{2,i} \tag{G2}$$

$$\dots \tag{G3}$$

$$\left|\frac{d}{2}\right\rangle\left\langle\frac{d}{2}\right| = X_d^{\frac{d}{2}}\,|0\rangle\langle 0|\,X_d^{\frac{d}{2}\dagger} \tag{G4}$$

$$= \frac{1}{d}\sum_{i=0}^{d-1} O(d,i) = \frac{1}{d}\sum_{i=0}^{d-1}(-1)^i O_{0,i} \tag{G5}$$

$$\dots \tag{G6}$$

$$|d-1\rangle\langle d-1| = X_d^{d-1}\,|0\rangle\langle 0|\,X_d^{d-1\dagger} \tag{G7}$$

$$= \frac{1}{d}\sum_{i=0}^{d-1}(-1)^i O_{d-1,i} \tag{G8}$$

Thus, we can reorder them to pairs in the following way

$$|0\rangle\langle 0| + \left|\frac{d}{2}\right\rangle\left\langle\frac{d}{2}\right| = \frac{1}{d}\sum_{i=0}^{d-1}(1+(-1)^i)O_{0,i} \tag{G9}$$

$$\dots \tag{G10}$$

$$|k\rangle\langle k| + \left|k+\frac{d}{2}\right\rangle\left\langle k+\frac{d}{2}\right| = \frac{1}{d}\sum_{i=0}^{d-1}(1+(-1)^i)O_{k,i} \tag{G11}$$

The maximally mixed state is $\frac{\mathbb{1}}{d} = \frac{1}{d}\sum_{i=0}^{d-1}|i\rangle\langle i|$. Therefore, if we compute

$$\sum_{l,m=0}^{d-1}\left|\mathrm{Tr}\left[\frac{\mathbb{1}}{d}O_{l,m}\right]\right| = \frac{1}{d}, \tag{G12}$$

we get a value that is smaller than the one for a pure stabilizer state. Therefore, one can "hide" magic in a product state of a magic state and the maximally mixed state or similarly including Clifford equivalent states. Since this quantity goes directly into the simulator cost, we see that the hyperpolyhedral states are easier to simulate than pure stabilizer states.

Appendix H: Decompositions of stabilizer states

In this section, we show how to obtain the decompositions of stabilizer states in the basis of $O_{\boldsymbol{l},\boldsymbol{m}}$ given their stabilizers.

Every stabilizer state with a d^n dimensional stabilizer group S fulfills the following eigenvalue equations [16]

$$\omega_d^{\boldsymbol{v}\Omega\boldsymbol{m}^T} P_d(\boldsymbol{m})\,|M_S, v\rangle = |M_S, v\rangle \tag{H1}$$

where M_S is the space of coordinates associated with the stabilizer group and $\boldsymbol{v}$ is the coordinate of one Heisenberg-Weyl operator. Note that $\boldsymbol{m} \in \mathbb{Z}_d^{2n}$ and that the phases are taken care of by the phase factor $\omega_d^{\boldsymbol{v}\Omega\boldsymbol{m}^T}$. This $\boldsymbol{v}$ takes care of the phase in front of the Heisenberg-Weyl operator. The stabilizer group S and in turn the set of coordinates are generated by n Heisenberg-Weyl operators $S = \langle S_1, ..., S_n\rangle$ or n coordinates $M_S = \langle \boldsymbol{s_1}, ..., \boldsymbol{s_n}\rangle$ respectively. The set M_S includes a linear combinations involving the n generators $\boldsymbol{s_i}$ with coefficients $k_i \in \mathbb{Z}_d$. The characteristic function of a stabilizer state $|\phi\rangle\langle\phi|$ can be represented as [17]

$$\chi^{\mathrm{DV}}_{|\phi\rangle\langle\phi|}(\boldsymbol{a}) = \frac{1}{d^n}\omega_d^{\boldsymbol{v}\Omega\boldsymbol{a}^T}\delta_{M_S}(\boldsymbol{a}) \tag{H2}$$

where $\delta_{M_S}(\boldsymbol{a})$ is the indicator function that $\delta_{M_S}(\boldsymbol{a}) = 1$, iff $\boldsymbol{a} \in M_S$ and 0 otherwise.

For odd dimensions, the phase space point operators $A(a_1, a_2)$ had a one-to-one correspondence with the operators $O_{l,m}$. Something similar holds for even dimensions as well. In that case, the operators $O_{l,m}$ are directly connected with operators $\tilde{A}(a_1, a_2)$ that are identically defined as the phase space point operators but do not fulfill the same set of properties.

In the proof to show the connection between the phase space point operators in odd dimensions and the operators $O_{l,m}$, we used the resummation formula

$$\frac{1}{d}\sum_{k=0}^{d-1} e^{2\pi i \frac{kn}{d}} = \delta_{0,n}. \tag{H3}$$

For even dimensions, the sums appear with $2d$ instead of just d and then

$$\frac{1}{d}\sum_{k=0}^{d-1} e^{2\pi i \frac{kn}{2d}} \neq \delta_{0,n}, \tag{H4}$$

so one cannot easily use the discrete resummation formula. However, the equation can be modified to hold in all dimensions. In even dimensions, it holds that

$$\frac{1}{2d}\sum_{k=0}^{2d-1} e^{2\pi i \frac{kn}{2d}} = \frac{1}{\tilde{d}}\sum_{k=0}^{\tilde{d}-1} e^{2\pi i \frac{kn}{d}} = \delta_{0,n}. \tag{H5}$$

We see that by doubling the domain of the sum, we recover the discrete resummation formula. So we can use the discrete resummation formula in all dimensions by considering

$$\frac{1}{D}\sum_{k=0}^{D-1} e^{2\pi i \frac{kn}{D}} = \delta_{0,n} \tag{H6}$$

and in consequence

$$\frac{1}{D^n}\sum_{\boldsymbol{x}\in\mathbb{Z}_D^{2n}} \omega_D^{-(\boldsymbol{u}+\boldsymbol{v})\Omega\boldsymbol{x}^T} = \delta_{0,\boldsymbol{u}+\boldsymbol{v}}. \tag{H7}$$

We define the symplectic Fourier transform as

$$(\mathcal{F}f)(\boldsymbol{a}) = \frac{1}{D^n}\sum_{\boldsymbol{b}\in\mathbb{Z}_D^{2n}} \omega_D^{-\boldsymbol{a}\Omega\boldsymbol{b}^T} f(\boldsymbol{b}). \tag{H8}$$

We see here again that the parameters $\boldsymbol{a}$ are not over $\mathbb{Z}_d^{2n}$ but over $\mathbb{Z}_D^{2n}$ as mentioned before. In order to differentiate between the phase-space point operators in odd dimensions $A(\boldsymbol{a}) = \frac{1}{d^n}\sum_{\boldsymbol{b}\in\mathbb{Z}_d^{2n}} \omega_d^{-\boldsymbol{a}\Omega\boldsymbol{b}^T} P_d^\dagger(\boldsymbol{b})$ with their intimate relation with the discrete Wigner function, we define the equivalently defined operator $\tilde{A}(\boldsymbol{a}) = \frac{1}{D^n}\sum_{\boldsymbol{b}\in\mathbb{Z}_D^{2n}} \omega_D^{-\boldsymbol{a}\Omega\boldsymbol{b}^T} P^\dagger(\boldsymbol{b})$ for even dimensions.

Then consequently for even dimension, we can rewrite $\tilde{A}(\boldsymbol{a})$ as

$$\tilde{A}(\boldsymbol{a}) = \frac{1}{D}\sum_{\boldsymbol{b}\in\mathbb{Z}_D^{2n}} \omega_D^{-\boldsymbol{a}\Omega\boldsymbol{b}^T} P_d^\dagger(\boldsymbol{b}) \tag{H9}$$

$$= \frac{1}{D}\sum_{\boldsymbol{b}\in\mathbb{Z}_D^{2n},\boldsymbol{x}\in\mathbb{Z}_d^n} \omega_d^{\boldsymbol{b_1}(\frac{\boldsymbol{a_2}}{2}+\frac{\boldsymbol{b_2}}{2}-\boldsymbol{x})}\omega_D^{-\boldsymbol{a_1}\boldsymbol{b_2}} \left|\boldsymbol{x}-\boldsymbol{b_2}\right\rangle\left\langle\boldsymbol{x}\right| \tag{H10}$$

$$= \frac{1}{D}\sum_{\boldsymbol{b_2}\in\mathbb{Z}_D^{2n},\boldsymbol{x}\in\mathbb{Z}_d^n} \delta_{\boldsymbol{b_2},2\boldsymbol{x}-\boldsymbol{a_2}}\omega_D^{-\boldsymbol{a_1}\boldsymbol{b_2}} \left|\boldsymbol{x}-\boldsymbol{b_2}\right\rangle\left\langle\boldsymbol{x}\right| \tag{H11}$$

$$= \frac{1}{D}\sum_{\boldsymbol{x}\in\mathbb{Z}_d^n} \omega_d^{\boldsymbol{a_1}\boldsymbol{a_2}/2}\omega_d^{-\boldsymbol{a_1}\boldsymbol{x}} \left|\boldsymbol{a_2}-\boldsymbol{x}\right\rangle\left\langle\boldsymbol{x}\right| \tag{H12}$$

which is equivalent to $O_{\boldsymbol{l},\boldsymbol{m}}$ for $\boldsymbol{l} = \boldsymbol{a_2}, \boldsymbol{m} = -\boldsymbol{a_1}$.

We transform the characteristic function to get the coefficients $x_{|\phi\rangle\langle\phi|}$ corresponding to the operators $O_{l,m}$ for a stabilizer state ϕ as

$$\mathcal{F}(\chi^{\mathrm{DV}}_{|\phi\rangle\langle\phi|})(\boldsymbol{a}) = \frac{1}{(2d)^n}\frac{1}{d^n}\sum_{\boldsymbol{b}\in\mathbb{Z}_{2d}^{2n}} \omega_{2d}^{-\boldsymbol{a}\Omega\boldsymbol{b}^T}\delta_{M_s}(\boldsymbol{b})\omega_d^{\boldsymbol{v}\Omega\boldsymbol{b}^T} \tag{H13}$$

$$= \frac{1}{(2d)^n}\frac{1}{d^n}\sum_{\boldsymbol{b}\in M_S\cup M_S+d} \omega_{2d}^{-(\boldsymbol{a}-\boldsymbol{2v})\Omega\boldsymbol{b}^T}. \tag{H14}$$

We used that M_S was defined on $\mathbb{Z}_d^{2n}$, but the sum goes over $\mathbb{Z}_{2d}^{2n}$ so we need to take this into account when dealing with the phase factors. We write $M_S \cup M_S + d$ as the extension from $\mathbb{Z}_d^{2n}$ to $\mathbb{Z}_{2d}^{2n}$. This set is generated by the same generators $\boldsymbol{s_i}$ but includes now lienar combinations with coefficients $k_i \in \mathbb{Z}_{2d}$. We can simplify the sum by using the generators of the coordinate space $M_S = \langle \boldsymbol{s_1}, ..., \boldsymbol{s_n}\rangle$ to

$$\mathcal{F}(\chi^{\mathrm{DV}}_{|\phi\rangle\langle\phi|})(\boldsymbol{a}) = \frac{1}{(2d)^n}\frac{1}{d^n}\sum_{\boldsymbol{b}\in M_S\cup M_S+d} \omega_{2d}^{-(\boldsymbol{a}-\boldsymbol{2v})\Omega\boldsymbol{b}^T} \tag{H15}$$

$$= \prod_{i=1}^{n}\left(\sum_{k_i=0}^{2d-1}\omega_{2d}^{-(\boldsymbol{a}-\boldsymbol{2v})\Omega[k_i\boldsymbol{s_i}]^T}\right) \tag{H16}$$

$$= \prod_{i=1}^{n}\left(\sum_{k_i=0}^{2d-1}\omega_{2d}^{-k_i(\boldsymbol{a}-\boldsymbol{2v})\Omega\boldsymbol{s_i}^T}\right) \tag{H17}$$

$$= \frac{1}{d^n}\delta_{M_S+2\boldsymbol{v}}(\boldsymbol{a}). \tag{H18}$$

From the first to the second line we decomposed the elements $\boldsymbol{b} \in M_S \cup M_S + d$ using the generators $M_S \cup M_S + d$. Each element $\boldsymbol{b}$ can be decomposed into a linear combination of the generators $\boldsymbol{s_i}$ and coefficients $k_i \in \mathbb{Z}_{2d}$. In the last line, we used the resummation formula (H7) and saw that the sum is 0 by using except in the case where $(\boldsymbol{a} - 2\boldsymbol{v})\Omega\boldsymbol{b}^T = 0$ and thus the Pauli operators in the stabilizer group commute with Pauli operators with coordinates $\boldsymbol{a} - 2\boldsymbol{v}$. This implies that $\boldsymbol{a} - 2\boldsymbol{v} \in M_S$ since S is a stabilizer group with the maximal number of commuting Pauli operators. As shown in (H12), the expression in Eq. (H18) coincides with $x_{|\phi\rangle\langle\phi|}(l = \boldsymbol{a_2}, m = -\boldsymbol{a_1})$. A few comments are in order. We have shown that we can write every pure stabilizer state using d^n operators $O_{\boldsymbol{l},\boldsymbol{m}}$ that all have the phase $+1$

$$|\phi\rangle\langle\phi| = \sum_{(\boldsymbol{l},\boldsymbol{m})\in\mathbb{Z}_{2d}^{2n}} x_{|\phi\rangle\langle\phi|}(\boldsymbol{l},\boldsymbol{m}) O_{\boldsymbol{l},\boldsymbol{m}} \tag{H19}$$

$$= \frac{1}{d^n} \sum_{(-\boldsymbol{m},\boldsymbol{l})\in M_s+2\boldsymbol{v}} O_{\boldsymbol{l},\boldsymbol{m}}. \tag{H20}$$

Note that the sums go over D and not d, which makes a difference in even dimensions. As we know, the operators $O_{\boldsymbol{l},\boldsymbol{m}}$ repeat with period d with the opposite sign. Let us take the example of qubits $Z_2 = O_{0,1}$ while $-Z_2 = O_{2,1}$. So if we constrain $(\boldsymbol{l},\boldsymbol{m}) \in \mathbb{Z}_d^{2n}$ we can get phases ±1, while if we allow for all $(\boldsymbol{l},\boldsymbol{m}) \in \mathbb{Z}_D^{2n}$ we get decompositions with only $+1$ signs.

[1] S. Konno, W. Asavanant, F. Hanamura, H. Nagayoshi, K. Fukui, A. Sakaguchi, R. Ide, F. China, M. Yabuno, S. Miki, H. Terai, K. Takase, M. Endo, P. Marek, R. Filip, P. van Loock, and A. Furusawa, *Logical states for fault-tolerant quantum computation with propagating light,* Science **383**, 289 (2024).

[2] A. Mari and J. Eisert, *Positive wigner functions render classical simulation of quantum computation efficient,* Phys. Rev. Lett. **109**, 230503 (2012).

[3] M. G. Genoni, M. G. A. Paris, and K. Banaszek, *Measure of the non-gaussian character of a quantum state,* Phys. Rev. A **76**, 042327 (2007).

[4] M. G. Genoni, M. G. A. Paris, and K. Banaszek, *Quantifying the non-gaussian character of a quantum state by quantum relative entropy,* Phys. Rev. A **78**, 060303 (2008).

[5] R. Takagi and Q. Zhuang, *Convex resource theory of non-Gaussianity,* Phys. Rev. A **97**, 062337 (2018).

[6] F. Albarelli, M. G. Genoni, M. G. A. Paris, and A. Ferraro, *Resource theory of quantum non-gaussianity and wigner negativity,* Phys. Rev. A **98**, 052350 (2018).

[7] U. Chabaud, D. Markham, and F. Grosshans, *Stellar representation of non-gaussian quantum states,* Phys. Rev. Lett. **124**, 063605 (2020).

[8] B. Regula, L. Lami, G. Ferrari, and R. Takagi, *Operational quantification of continuous-variable quantum resources,* Phys. Rev. Lett. **126**, 110403 (2021).

[9] L. Lami, B. Regula, R. Takagi, and G. Ferrari, *Framework for resource quantification in infinite-dimensional general probabilistic theories,* Phys. Rev. A **103**, 032424 (2021).

[10] A. Kenfack and K. Życzkowski, *Negativity of the wigner function as an indicator of non-classicality,* J. Opt. B: Quantum Semiclass. Opt. **6**, 396 (2004).

[11] V. Veitch, N. Wiebe, C. Ferrie, and J. Emerson, *Efficient simulation scheme for a class of quantum optics experiments with non-negative wigner representation,* New Journal of Physics **15**, 013037 (2013).

[12] S. Krinner, N. Lacroix, A. Remm, A. Di Paolo, E. Genois, C. Leroux, C. Hellings, S. Lazar, F. Swiadek, J. Herrmann, G. J. Norris, C. K. Andersen, M. Müller, A. Blais, C. Eichler, and A. Wallraff, *Realizing repeated quantum error correction in a distance-three surface code,* Nature **605**, 669 (2022).

[13] V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, A. Miano, B. Brock, A. Ding, L. Frunzio, *et al.*, *Real-time quantum error correction beyond break-even,* Nature **616**, 50 (2023).

[14] S. Bravyi and A. Kitaev, *Universal quantum computation with ideal clifford gates and noisy ancillas,* Phys. Rev. A **71**, 022316 (2005).

[15] D. Gottesman, *The Heisenberg Representation of Quantum Computers,* arXiv:quant-ph/9807006 (1998).

[16] D. Gross, *Finite phase space methods in quantum information*, PhD thesis, Diploma Thesis, Potsdam (2005).

[17] D. Gross, *Hudson's theorem for finite-dimensional quantum systems,* J. Math. Phys. **47**, 122107 (2006).

[18] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, *Negative quasi-probability as a resource for quantum computation,* New J. Phys. **14**, 113011 (2012).

[19] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, *The resource theory of stabilizer quantum computation,* New J. Phys. **16**, 013009 (2014).

[20] M. Howard and E. Campbell, *Application of a resource theory for magic states to fault-tolerant quantum computing,* Phys. Rev. Lett. **118**, 090501 (2017).

[21] S. Bravyi and D. Gosset, *Improved classical simulation of quantum circuits dominated by clifford gates,* Phys. Rev. Lett. **116**, 250501 (2016).

[22] S. Bravyi, G. Smith, and J. A. Smolin, *Trading classical and quantum computational resources,* Phys. Rev. X **6**, 021043 (2016).

[23] B. Regula, *Convex geometry of quantum resource quantification,* J. Phys. A: Math. Theor. **51**, 045303 (2017).

[24] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, *Simulation of quantum circuits by low-rank stabilizer decompositions,* Quantum **3**, 181 (2019).

[25] K. Bu and D. E. Koh, *Efficient classical simulation of clifford circuits with nonstabilizer input states,* Phys. Rev. Lett. **123**, 170502 (2019).

[26] M. Beverland, E. Campbell, M. Howard, and V. Kliuchnikov, *Lower bounds on the non-clifford resources for quantum computations,* Quantum Science and Technology **5**, 035009 (2020).

[27] J. R. Seddon, B. Regula, H. Pashayan, Y. Ouyang, and E. T. Campbell, *Quantifying quantum speedups: Improved classical simulation from tighter magic monotones,* PRX Quantum **2**, 010345 (2021).

[28] L. Leone, S. F. E. Oliviero, and A. Hamma, *Stabilizer rényi entropy,* Phys. Rev. Lett. **128**, 050402 (2022).

[29] O. Hahn, A. Ferraro, L. Hultquist, G. Ferrini, and L. García-Álvarez, *Quantifying qubit magic resource with gottesman-kitaev-preskill encoding,* Phys. Rev. Lett. **128**, 210502 (2022).

[30] T. Haug and M. Kim, *Scalable measures of magic resource for quantum computers,* PRX Quantum **4**, 010301 (2023).

[31] K. Bu, W. Gu, and A. Jaffe, *Stabilizer Testing and Magic Entropy,* arXiv:2306.09292 (2023).

[32] T. Haug, S. Lee, and M. S. Kim, *Efficient stabilizer entropies for quantum computers,* arXiv:2305.19152 (2023).

[33] K. Bu, W. Gu, and A. Jaffe, *Entropic Quantum Central Limit Theorem and Quantum Inverse Sumset Theorem,* arXiv:2401.14385 (2024).

[34] K. Bu, W. Gu, and A. Jaffe, *Quantum entropy and central limit theorem,* Proc. Natl. Acad. Sci. U.S.A. **120**, e2304589120 (2023).

[35] K. Bu, W. Gu, and A. Jaffe, *Discrete Quantum Gaussians and Central Limit Theorem,* arXiv:2302.08423 (2023).

[36] D. Gottesman, A. Kitaev, and J. Preskill, *Encoding a qubit in an oscillator,* Phys. Rev. A **64**, 012310 (2001).

[37] H. Pashayan, J. J. Wallman, and S. D. Bartlett, *Estimating outcome probabilities of quantum circuits using quasiprobabilities,* Phys. Rev. Lett. **115**, 070501 (2015).

[38] P. Rall, D. Liang, J. Cook, and W. Kretschmer, *Simulation of qubit quantum circuits via pauli propagation,* Phys. Rev. A **99**, 062337 (2019).

[39] H. Yamasaki, T. Matsuura, and M. Koashi, *Cost-reduced all-gaussian universality with the gottesman-kitaev-preskill code: Resource-theoretic approach to cost analysis,* Phys. Rev. Res. **2**, 023270 (2020).

[40] J. M. Farinholt, *An ideal characterization of the clifford operators,* J. Phys. A: Math. Theor. **47**, 305303 (2014).

[41] E. Chitambar and G. Gour, *Quantum resource theories,* Rev. Mod. Phys. **91**, 025001 (2019).

[42] R. Raussendorf, J. Bermejo-Vega, E. Tyhurst, C. Okay, and M. Zurel, *Phase-space-simulation method for quantum computation with magic states on qubits,* Phys. Rev. A **101**, 012350 (2020).

[43] T. Haug and L. Piroli, *Stabilizer entropies and nonstabilizerness monotones,* Quantum **7**, 1092 (2023).

[44] L. Leone and L. Bittel, *Stabilizer entropies are monotones for magic-state resource theory,* arXiv:2404.11652 (2024), 10.48550/arXiv.2404.11652.

[45] Here, we follow the standard definition where Gaussian operations are quantum channels that map Gaussian states to Gaussian states.

[46] B. Q. Baragiola, G. Pantaleoni, R. N. Alexander, A. Karanjai, and N. C. Menicucci, *All-gaussian universality and fault tolerance with the gottesman-kitaev-preskill code,* Phys. Rev. Lett. **123**, 200502 (2019).

[47] L. Feng and S. Luo, *Connecting Continuous and Discrete Wigner Functions Via GKP Encoding,* Int. J. Theor. Phys. **63**, 40 (2024).

[48] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega, *Contextuality and wigner-function negativity in qubit quantum computation,* Phys. Rev. A **95**, 052334 (2017).

[49] J. Bermejo-Vega, N. Delfosse, D. E. Browne, C. Okay, and R. Raussendorf, *Contextuality as a resource for models of quantum computation with qubits,* Phys. Rev. Lett. **119**, 120505 (2017).

The search for a unique measure of entanglement: A story of entropy, reversibility, and hypothesis testing

Bartosz Regula[1] *

[1] *RIKEN Center for Quantum Computing, Japan*

Abstract. The methods to characterise quantum resources such as entanglement are often based on our understanding of thermodynamics. Such connections hinted at the possibility of a unique measure of entanglement emerging in a suitable regime, which would exactly mirror the role that entropy plays in the second law of thermodynamics. This conjecture turned out to be deeply related to an important problem in quantum hypothesis testing of entangled states, whose seminal solution in 2010 inspired a large body of work in the study of quantum resources. However, 12 years later, this claimed solution was found to be incorrect, casting doubt on the whole supposed parallel between entanglement and thermodynamics, and reopening the search for a unique measure of entanglement.

In this talk, I will overview the motivations for these fundamental conjectures, the recent developments surrounding the problems, and the remaining open questions. In particular, I will discuss how a 'second law of entanglement' — if at all possible — must be fundamentally different from the second law of thermodynamics, and how the conjectured unique measure of entanglement can indeed be proven to be true when certain relaxed assumptions are taken.

References

[1] S. Popescu and D. Rohrlich, *Thermodynamics and the measure of entanglement*, Phys. Rev. A 56, R3319(R) (1997)

[2] V. Vedral and E Kashefi, *Uniqueness of the Entanglement Measure for Bipartite Pure States and Thermodynamics*, Phys. Rev. Lett. 89, 037903 (2002)

[3] F. G. S. L. Brandão and M. B. Plenio, *A Reversible Theory of Entanglement and its Relation to the Second Law*, Commun. Math. Phys. 295, 829 (2010).

[4] L. Lami and B. Regula, *No second law of entanglement manipulation after all,* Nat. Phys. 19, 184-189 (2023).

[5] M. Berta, F. G. S. L. Brandão, G. Gour, L. Lami, M. B. Plenio, B. Regula, and M. Tomamichel, *On a gap in the proof of the generalised quantum Stein's lemma and its consequences for the reversibility of quantum resources*, Quantum 7, 1103 (2023).

[6] M. Berta, F. G. S. L. Brandão, G. Gour, L. Lami, M. B. Plenio, B. Regula, and M. Tomamichel, *The tangled state of quantum hypothesis testing*, Nat. Phys. 20, 172-175 (2024).

[7] B. Regula and L. Lami, *Reversibility of quantum resources through probabilistic protocols*, Nat. Commun. 15, 3096 (2024).

*bartosz.regula@gmail.com

Learning quantum states and unitaries of bounded gate complexity

Haimeng Zhao⋆[1] [2] * Laura Lewis⋆[1] [3] † Ishaan Kannan⋆[1] ‡ Yihui Quek[4] [5] §
Hsin-Yuan Huang[1] [3] [5] ¶ Matthias C. Caro[1] [6] ‖

[1] *Institute for Quantum Information and Matter, Caltech, Pasadena, CA, USA*
[2] *Tsinghua University, Beijing, China*
[3] *Google Quantum AI, Venice, CA, USA*
[4] *Harvard University, 17 Oxford Street, Cambridge, MA, USA*
[5] *Massachusetts Institute of Technology, Cambridge, MA, USA*
[6] *Freie Universität Berlin, Berlin, Germany*

Abstract. While quantum state tomography is notoriously hard, most states hold little interest to practically-minded tomographers, as those appearing in Nature have bounded gate complexity. In this work, we prove that to learn a state/unitary with gate complexity G to a small trace/average-case distance, the optimal sample complexity scales linearly in G. In contrast, the computational complexity must scale exponentially in G under cryptographic conjectures. These results establish fundamental limitations on quantum machine learning models and provide new perspectives on no-free-lunch theorems. Together, our results relate the complexity of learning quantum states and unitaries to that of creating them.

Keywords: quantum learning theory, state tomography, unitary tomography, sample complexity, computational complexity

The tasks of general *state* and *process tomography* – that is, determining an unknown quantum state/unitary from copies of it/queries to it – are practically ubiquitous [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13] but exponentially costly [14, 15, 16]. Despite this theoretical obstacle, there is hope that efficient tomography remains within reach, since the vast majority of states and unitaries are not of immediate physical interest [17, 18, 19]. Indeed, practitioners may be able to leverage *prior knowledge* about the unknown state or process. Previous works have demonstrated efficient learning if the unknown state is known to be a stabilizer [20, 21, 22, 23], of limited T-gate count [24, 25, 26, 27], or the output of a shallow circuit [28]; or if the unknown process is a local Pauli noise channel [29].

Our work centers around a prior that is fundamental in physics and timely to the current state of quantum technology, albeit underexplored in tomography: gate complexity. While the vast majority of many-body states and unitaries have exponential gate complexity, those that can even be prepared "in Nature" [17, 18, 19] are likely to have at most polynomial gate complexity. This raises the following question:

What is the complexity of learning states/unitaries with bounded gate complexity?

We first study the *sample/query complexity* of learning an n-qubit state/unitary implemented by G two-qubit gates: the number of samples collected from the system or queries to the process required to output an ϵ-accurate classical description of the unknown object. Previously, [30] showed that the state learning task can be accomplished with sample complexity $\tilde{\mathcal{O}}(nG^2/\epsilon^4)$. However, it is not known if this is the optimal sample complexity for the state learning task. In this work, we fully resolve this problem by proving a matching upper and lower bound (up to log factors) of $\tilde{\Theta}(G/\epsilon^2)$ for learning n-qubit states generated by G gates to trace distance ϵ. For learning unitaries, we establish a query complexity scaling linear in the gate complexity G and independent of the system size n, which is optimal in the scaling of G (up to log factors). Turning to the question of *computational complexity*, we demonstrate that any quantum learning algorithm requires computational time scaling exponentially in G.

Our results pose fresh implications in other subfields of quantum information. Firstly, the Brown-Susskind conjecture [31, 32, 33, 34, 35, 36] states that the complexity of a generic local quantum circuit grows linearly with the number of gates for an exponentially long time, holographically dual to the steady growth of a wormhole's volume in the bulk theory. This conjecture has recently been confirmed [37, 38] with "complexity" understood as (exact) "circuit complexity" [35]. Our work suggests that this conjecture may also be true for an alternative notion of complexity – that of learning the quantum circuit. Secondly, our work completely characterizes the complexity of inferring a classical circuit description of a quantum circuit from limited copies of its output state: yet such a description holds the key to computing arbitrarily many more properties of this state (via classical simulation algorithms) than would have been possible by using the limited state copies directly. We thus expect our results to shed light on the link between classical simulability and learnability of quantum states [39, 40]. They also provide a *learning* perspective on the celebrated recent notion of state complexity classes [41, 42], which ask what

*haimengzhao@icloud.com
†llewis@alumni.caltech.edu
‡ikannan@caltech.edu
§yquek@mit.edu
¶hsinyuan@caltech.edu
‖matthias.caro@fu-berlin.de

⋆These authors contributed equally to this work.

states can be synthesized by polynomial-space quantum circuits.

1 Learning quantum states and unitaries

Learning quantum states. First, we consider learning quantum states of bounded complexity. Let $|\psi\rangle = U|0\rangle^{\otimes n}$ be an n-qubit pure state generated by a unitary U consisting of G two-qubit gates. Given N copies of $\rho \triangleq |\psi\rangle\!\langle\psi|$, we aim to learn a classical circuit description $\hat{\rho}$ of ρ that is ϵ-close to ρ in trace distance: $\mathrm{d}_{\mathrm{tr}}(\hat{\rho}, \rho) = \|\hat{\rho} - \rho\|_1/2 < \epsilon$. We fully characterize the sample complexity in the following theorem.

Theorem 1 (State learning) $N = \tilde{\Theta}\left(G/\epsilon^2\right)$ *copies of an n-qubit pure state with circuit complexity G are necessary and sufficient to learn it to within ϵ trace distance with high probability.*

This result also resolves an open question from [43] and improves [30] to achieve the optimal scaling. In the regime where $G = \mathcal{O}(\mathsf{poly}(n))$, our algorithm improves substantially over the sample complexity $N = \mathcal{O}(2^n)$ of the sample-optimal result for arbitrary pure quantum states [14, 15]. Note that we do not need to have access to the unitary U which generates the unknown state $|\psi\rangle$.

While our algorithm to learn the unknown quantum state $|\psi\rangle$ is sample-efficient and sample-optimal, it is computationally inefficient. We prove that this cannot be avoided in general: any quantum algorithm that learns $|\psi\rangle$ given access to copies of this state must use time exponential-in-G, under the commonly-believed cryptographic assumption that $\mathsf{RingLWE}$ [44] cannot be solved by a quantum computer in sub-exponential time. This imposes strong computational complexity limitations on learning even comparatively simple states, in stark contrast with our sample complexity results. Meanwhile, we show that the learning task is computationally-efficiently solvable for $G = \mathcal{O}(\log n)$, implying a transition point of computational efficiency. Previous work [45, 46] arrives at related hardness results for $G = \mathrm{poly}(n)$, but our detailed analysis allows us to sharpen the computational lower bound and obtain this transition point.

Theorem 2 (Computational hardness; States) *Any quantum algorithm that learns an n-qubit state with circuit complexity G to within ϵ trace distance requires* $\exp(\Omega(\min(G, n)))$ *time, assuming the quantum sub-exponential hardness of* $\mathsf{RingLWE}$*. Meanwhile, for* $G = \mathcal{O}(\log n)$*, an efficient learning algorithm exists.*

Learning quantum unitaries. Next, we consider learning unitaries of bounded complexity. Let U be a unitary consisting of G two-qubit gates. Given query access to U, we aim to learn a classical circuit description $\hat{U}$ of U that is ϵ-close to U. A natural distance metric analogous to the trace distance for states is the diamond distance $\mathrm{d}_{\diamond}(U, V) = \max_{\rho} \|(U \otimes I)\rho(U \otimes I)^{\dagger} - (V \otimes I)\rho(V \otimes I)^{\dagger}\|_1$. We find that in this worst-case learning task, a number of queries exponential in G is necessary.

Theorem 3 (Worst-case unitary learning) *Any quantum algorithm learning an n-qubit unitary with circuit complexity G in diamond distance with high probability must use at least* $\Omega\left(2^{\min\{G/(2C), n/2\}}/\epsilon\right)$ *queries, where* $C > 0$ *is a universal constant. Meanwhile, there exists such an algorithm using* $\tilde{\mathcal{O}}(2^n G/\epsilon)$ *queries.*

Having established this no-go theorem for worst-case learning, we turn to a more realistic average-case learning alternative. Here, the accuracy is measured using the average-case metric, $\mathrm{d}_{\mathrm{avg}}(U, V) = \sqrt{\mathbb{E}_{|\psi\rangle}[\mathrm{d}_{\mathrm{tr}}(U|\psi\rangle, V|\psi\rangle)^2]}$. This metric characterizes the average error when testing the learned unitary on Haar-random inputs. We find that, similarly to the state learning task, linear-in-G many queries is optimal.

Theorem 4 (Average-case unitary learning) $N = \tilde{\mathcal{O}}\left(G \min\{1/\epsilon^2, \sqrt{2^n}/\epsilon\}\right)$ *queries are sufficient to learn an n-qubit unitary with circuit complexity G to ϵ root mean squared trace distance with high probability. Meanwhile, at least* $\Omega\left(G/\epsilon\right)$ *queries to the unitary, its inverse, or the controlled versions are necessary.*

The similar linear-in-G sample/query complexity in Theorems 1 and 4 hints at a common underlying source of complexity. However, in contrast to state learning, unitary learning comes with two natural such sources: (1) to readout input and output states, and (2) to learn the mapping from inputs to outputs. Our results suggest that the former may encapsulate the central difficulty whereas the latter may be easy. This seemingly contradicts recent quantum no free lunch theorems [47, 48], which state that $\Omega(2^n)$ samples are required to learn a generic unitary even from classically described input-output state pairs. To resolve this, we reformulate the quantum no free lunch theorem from an information-theoretic perspective.

Theorem 5 (Learning with classical descriptions) $\mathcal{O}(2^n/r)$ *classically described samples with mixed (entangled) input states of (Schmidt) rank r are sufficient to learn any n-qubit unitary to any accuracy with high probability. Moreover, any such algorithm that is robust to noise needs at least* $\Omega(2^n/r)$ *samples.*

Similarly to state learning, our average-case unitary learning algorithm is not computationally efficient. This is again inevitable, and the same is true for worst-case unitary learning. Moreover, the hard instances we construct are implementable with Clifford+T circuits with $\tilde{\omega}(\log n)$ T gates [24], so, together with Theorem 2, this gives a negative answer to an open question (the fifth question) in the survey [39].

Theorem 6 (Computational hardness; Unitaries) *Any quantum algorithm that learns an n-qubit unitary with circuit complexity G requires* $\exp(\Omega(\min(G, n)))$ *time, assuming the quantum sub-exponential hardness of* $\mathsf{RingLWE}$*. Meanwhile, for* $G = \mathcal{O}(\log n)$*, an efficient learning algorithm exists.*

Apart from learning quantum states and dynamics themselves, a more classically minded learner may care more about learning classical functions resulting from quantum processes. We define these *physical functions* $f(x) : [0, 1]^{\nu} \to \mathbb{R}$ in three steps: (1) a fixed state preparation procedure that can depend on x; (2) a unitary evolution consisting of G tunable two-qubit gates and arbitrary fixed unitaries that can depend on x, arranged in a circuit structure; (3) the measurement of a fixed observable, whose expectation is the function output. Despite the generality of this setup, we find that certain well-behaved functions are actually not physical: they cannot be efficiently approximated or learned via physical functions. This reveals a fundamental limitation on the functional expressivity of both nature and practical quantum machine learning models [49, 50, 51, 52].

Theorem 7 (Learning physical functions) *At least $G \geq \tilde{\Omega}(1/\epsilon^{\nu/2})$ gates and $N \geq \Omega(1/\epsilon^{\nu})$ samples are needed to approximate and learn arbitrary 1-bounded and 1-Lipschitz $\mathbb{R}$-valued functions on $[0,1]^{\nu}$ to accuracy ϵ in $\|\cdot\|_{\infty}$ with high probability using physical functions.*

2 Proof ideas

Sample complexity upper bounds. We prove the upper bounds in Theorems 1 and 4 by explicitly constructing learning algorithms using a hypothesis selection protocol [53] based on classical shadow tomography [54]. Specifically, we construct a covering net $\mathcal{N}$ over the set of states/unitaries with gate complexity G such that for any such state/unitary, there exists a candidate in $\mathcal{N}$ that is ϵ-close in trace/average case distance to it, respectively. To select the candidate closest to our unknown object, we utilize classical shadows with random Clifford measurements to estimate all distances simultaneously to ϵ error using $\mathcal{O}(\log|\mathcal{N}|/\epsilon^2) \leq \tilde{\mathcal{O}}(G/\epsilon^2)$ copies/queries. The last inequality follows because we are able to prove that $|\mathcal{N}| \leq e^{\tilde{\mathcal{O}}(G)}$. Finally, we output the closest candidate.

The above strategy leads to a sample complexity that depends logarithmically on n, which is undesirable when G is smaller than $n/2$ (i.e., when some qubits are untouched by the circuit). We improved upon this by first performing a junta learning step [55] to identify which qubits are acted upon non-trivially. After identifying the non-trivial qubits, we perform a measure-and-postselect step. This allows us to construct a covering net only over the qubits acted upon non-trivially, whose cardinality no longer depends on n. Proceeding as before, we can remove the n dependence in the sample complexity.

Furthermore, for unitary learning, we improve the ϵ dependence to the Heisenberg scaling $\tilde{\mathcal{O}}(1/\epsilon)$ via a bootstrap method [16], using the above learner as a subroutine. We iteratively refine our learning outcome $\hat{U}$ by performing hypothesis selection over a covering net of $(U\hat{U}^{\dagger})^p$, with p increasing exponentially as the iteration proceeds. Although the circuit complexity of $(U\hat{U}^{\dagger})^p$ grows with p, a covering net with p-independent cardinality can be constructed based on the one-to-one correspondence with U. However, unlike the diamond distance learner in [16], which has fine control over every eigenvalue of the unitaries, our average-case learner only has average control over eigenvalues. Thus for the bootstrap to work (i.e., for the learning error to decrease with increasing p), the average-case learner has to work in an exponentially small error regime, which results in a dimensional factor in the final sample complexity $\tilde{\mathcal{O}}(\sqrt{2^n}G/\epsilon)$.

Sample complexity lower bounds. We prove the lower bounds in Theorems 1 and 4 by reduction to a distinguishing task: if we can approximately learn states/unitaries, then we can use this learning algorithm to distinguish a set of states/unitaries that are far apart from each other. Hence a lower bound on the sample complexity of distinguishing states/unitaries in a packing net implies a lower bound for learning.

For state learning, we construct a packing net $\mathcal{M}$ of the set of $(\log_2 G)$-qubit states. These states have circuit complexity $\sim G$ because $\mathcal{O}(2^k)$ two-qubit gates can implement any pure k-qubit states [56]. We prove that $|\mathcal{M}| \geq e^{\Omega(G)}$, which means that to distinguish these states, one has to gather $\Omega(\log|\mathcal{M}|) \geq \Omega(G)$ bits of information. Meanwhile, Holevo's theorem [57] asserts that the amount of information carried by each sample is upper bounded by $\tilde{\mathcal{O}}(\epsilon^2)$ [58]. Hence, we need at least $\tilde{\Omega}(G/\epsilon^2)$ copies of the unknown state.

Similarly, for unitary learning, we construct a packing net by stacking all the gates into $\log_4 G$ qubits, using the fact that $\mathcal{O}(4^k)$ two-qubit gates can implement any k-qubit unitaries [59]. Lacking an analog of Holevo's theorem for unitary queries, we turn to a recently established bound on the success probability of unitary discrimination [60] and obtain an $\Omega(G)$ sample complexity lower bound for constant ϵ. To incorporate the ϵ dependence, we follow [16] and map the problem into a fractional query problem. We show that with N queries, we can use the learning algorithm to simulate [61, 62] an $\mathcal{O}(\epsilon N)$ query algorithm that solves the above constant-error distinguishing problem. This gives us the desired $\Omega(G/\epsilon)$ lower bound.

Computational hardness. We prove the computational complexity lower bounds in Theorems 2 and 6 by reduction to the task of distinguishing pseudorandom states/functions [63, 64] from truly random states/functions. The hardness of this task relies on the computational assumption that Ring Learning with Errors ($\mathsf{RingLWE}$) cannot be solved efficiently with a quantum computer [65]. In particular, if we consider learning a pseudorandom state or a unitary implementing a pseudorandom function, then an efficient learner implies an efficient distinguisher from Haar-random states or truly random functions, thus contradicting the pseudorandomness assumption. The circuit complexity at which this computational hardness kicks in is the complexity of the circuit required to implement pseudorandom states/functions. Indeed, we show that the pseudorandom functions constructed in [65] based on the hardness of $\mathsf{RingLWE}$ can be implemented with $G = \mathcal{O}(\mathsf{poly}(n))$ gates and depth $\mathcal{O}(\mathsf{polylog}(n))$, Then, we can also construct pseudorandom quantum states from these pseudorandom functions [66], which can be implemented with $G = \mathcal{O}(\mathsf{poly}(n))$ gates and depth $\mathcal{O}(\mathsf{polylog}(n))$. We can boost this to our exponential computational complexity lower bound by assuming the sub-exponential hardness of $\mathsf{RingLWE}$ rather than just polynomial hardness. The efficient learning algorithm at $G = \mathcal{O}(\log n)$ follows by junta learning [55] and standard tomography methods.

References

[1] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.

[2] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222–229, 2011.

[3] Christian Kokail, Rick van Bijnen, Andreas Elben, Benoît Vermersch, and Peter Zoller. Entanglement Hamiltonian tomography in quantum simulation. *Nature Physics*, 17(8):936–942, 2021.

[4] Jose Carrasco, Andreas Elben, Christian Kokail, Barbara Kraus, and Peter Zoller. Theoretical and experimental perspectives of quantum verification. *PRX Quantum*, 2(1):010102, 2021.

[5] Masoud Mohseni, Ali T Rezakhani, and Daniel A Lidar. Quantum-process tomography: Resource analysis of different strategies. *Physical Review A*, 77(3):032322, 2008.

[6] Jeremy L O'Brien, Geoff J Pryde, Alexei Gilchrist, Daniel FV James, Nathan K Langford, Timothy C Ralph, and Andrew G White. Quantum process tomography of a controlled-not gate. *Physical review letters*, 93(8):080502, 2004.

[7] Andrew James Scott. Optimizing quantum process tomography with unitary 2-designs. *Journal of Physics A: Mathematical and Theoretical*, 41(5):055308, 2008.

[8] Isaac L Chuang and Michael A Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.

[9] Ryan Levy, Di Luo, and Bryan K Clark. Classical shadows for quantum process tomography on near-term quantum computers. *arXiv preprint arXiv:2110.02965*, 2021.

[10] Seth T Merkel, Jay M Gambetta, John A Smolin, Stefano Poletto, Antonio D Córcoles, Blake R Johnson, Colm A Ryan, and Matthias Steffen. Self-consistent quantum process tomography. *Physical Review A*, 87(6):062119, 2013.

[11] Robin Blume-Kohout, John King Gamble, Erik Nielsen, Kenneth Rudinger, Jonathan Mizrahi, Kevin Fortier, and Peter Maunz. Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography. *Nature communications*, 8(1):14485, 2017.

[12] Hsin-Yuan Huang, Steven T Flammia, and John Preskill. Foundations for learning from noisy quantum experiments. *arXiv preprint arXiv:2204.13691*, 2022.

[13] Zhenyu Cai, Ryan Babbush, Simon C Benjamin, Suguru Endo, William J Huggins, Ying Li, Jarrod R McClean, and Thomas E O'Brien. Quantum error mitigation. *arXiv preprint arXiv:2210.00921*, 2022.

[14] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. *IEEE Transactions on Information Theory*, 63(9):5628–5641, 2017.

[15] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 899–912, 2016.

[16] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. Query-optimal estimation of unitary channels in diamond distance. *arXiv preprint arXiv:2302.14066*, 2023.

[17] David Poulin, Angie Qarry, Rolando Somma, and Frank Verstraete. Quantum simulation of time-dependent Hamiltonians and the convenient illusion of Hilbert space. *Physical review letters*, 106(17):170501, 2011.

[18] Fernando GSL Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. Models of quantum complexity growth. *PRX Quantum*, 2(3):030316, 2021.

[19] Thomas Barthel and Jianfeng Lu. Fundamental limitations for measurements in quantum many-body systems. *Physical Review Letters*, 121(8):080406, 2018.

[20] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70(5):052328, 2004.

[21] Ashley Montanaro. Learning stabilizer states by bell sampling. *arXiv preprint arXiv:1707.04012*, 2017.

[22] Richard A Low. Learning and testing algorithms for the clifford group. *Physical Review A*, 80(5):052314, 2009.

[23] Andrea Rocchetto. Stabiliser states are efficiently pac-learnable. *Quantum Info. Comput.*, 18(7–8):541–552, June 2018.

[24] Ching-Yi Lai and Hao-Chung Cheng. Learning quantum circuits of some t gates. *IEEE Transactions on Information Theory*, 68(6):3951–3964, 2022.

[25] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Efficient learning of quantum states prepared with few non-clifford gates. *arXiv preprint arXiv:2305.13409*, 2023.

[26] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Efficient learning of quantum states prepared with few non-clifford gates

ii: Single-copy measurements. *arXiv preprint arXiv:2308.07175*, 2023.

[27] Dominik Hangleiter and Michael J Gullans. Bell sampling from quantum circuits. *arXiv preprint arXiv:2306.00083*, 2023.

[28] Cambyse Rouzé and Daniel Stilck França. Learning quantum many-body systems from a few copies. *arXiv preprint arXiv:2107.03333*, 2021.

[29] Cambyse Rouzé and Daniel Stilck França. Efficient learning of the structure and parameters of local pauli noise channels. *arXiv preprint arXiv:2307.02959*, 2023.

[30] Scott Aaronson. Shadow tomography of quantum states. In *STOC*, pages 325–338, 2018.

[31] Adam R Brown and Leonard Susskind. Second law of quantum complexity. *Physical Review D*, 97(8):086015, 2018.

[32] Leonard Susskind. Black holes and complexity classes. *arXiv preprint arXiv:1802.02175*, 2018.

[33] Leonard Susskind. Computational complexity and black hole horizons. *Fortschritte der Physik*, 64(1):24–43, 2016.

[34] Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational pseudorandomness, the wormhole growth paradox, and constraints on the ads/cft duality. *arXiv preprint arXiv:1910.14646*, 2019.

[35] Douglas Stanford and Leonard Susskind. Complexity and shock wave geometries. *Physical Review D*, 90(12):126007, 2014.

[36] Adam R Brown, Daniel A Roberts, Leonard Susskind, Brian Swingle, and Ying Zhao. Complexity, action, and black holes. *Physical Review D*, 93(8):086006, 2016.

[37] Jonas Haferkamp, Philippe Faist, Naga BT Kothakonda, Jens Eisert, and Nicole Yunger Halpern. Linear growth of quantum circuit complexity. *Nature Physics*, 18(5):528–532, 2022.

[38] Zhi Li. Short proofs of linear growth of quantum circuit complexity. *arXiv preprint arXiv:2205.05668*, 2022.

[39] Anurag Anshu and Srinivasan Arunachalam. A survey on the complexity of learning quantum states. *arXiv preprint arXiv:2305.20069*, 2023.

[40] M. Hinsche, M. Ioannou, A. Nietner, J. Haferkamp, Y. Quek, D. Hangleiter, J.-P. Seifert, J. Eisert, and R. Sweke. One t gate makes distribution learning hard. *Phys. Rev. Lett.*, 130:240602, Jun 2023.

[41] Gregory Rosenthal and Henry Yuen. Interactive proofs for synthesizing quantum states and unitaries. *CoRR*, abs/2108.07192, 2021.

[42] Tony Metger and Henry Yuen. stateqip = statepspace, 2023.

[43] Nengkun Yu and Tzu-Chieh Wei. Learning marginals suffices! *arXiv preprint arXiv:2303.08938*, 2023.

[44] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pages 1–23. Springer, 2010.

[45] Lisa Yang and Netta Engelhardt. The complexity of learning (pseudo) random dynamics of black holes and other chaotic systems. *arXiv preprint arXiv:2302.11013*, 2023.

[46] Amira Abbas, Robbie King, Hsin-Yuan Huang, William J Huggins, Ramis Movassagh, Dar Gilboa, and Jarrod R McClean. On quantum backpropagation, information reuse, and cheating measurement collapse. *arXiv preprint arXiv:2305.13362*, 2023.

[47] Kyle Poland, Kerstin Beer, and Tobias J Osborne. No free lunch for quantum machine learning. *arXiv preprint arXiv:2003.14103*, 2020.

[48] Kunal Sharma, Marco Cerezo, Zoë Holmes, Lukasz Cincio, Andrew Sornborger, and Patrick J Coles. Reformulation of the no-free-lunch theorem for entangled datasets. *Physical Review Letters*, 128(7):070501, 2022.

[49] Lukas Gonon and Antoine Jacquier. Universal approximation theorem and error bounds for quantum neural networks and quantum reservoirs. *arXiv preprint arXiv:2307.12904*, 2023.

[50] Adrián Pérez-Salinas, David López-Núñez, Artur García-Sáez, Pol Forn-Díaz, and José I Latorre. One qubit as a universal approximant. *Physical Review A*, 104(1):012405, 2021.

[51] Maria Schuld, Ryan Sweke, and Johannes Jakob Meyer. Effect of data encoding on the expressive power of variational quantum-machine-learning models. *Physical Review A*, 103(3):032430, 2021.

[52] Alberto Manzano, David Dechant, Jordi Tura, and Vedran Dunjko. Parametrized quantum circuits and their approximation capacities in the context of quantum machine learning. *arXiv preprint arXiv:2307.14792*, 2023.

[53] Costin Bădescu and Ryan O'Donnell. Improved quantum data analysis. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1398–1411, 2021.

[54] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020.

[55] Thomas Chen, Shivam Nadimpalli, and Henry Yuen. Testing and learning quantum juntas nearly optimally. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1163–1185. SIAM, 2023.

[56] Vivek V Shende, Stephen S Bullock, and Igor L Markov. Synthesis of quantum logic circuits. In *Proceedings of the 2005 Asia and South Pacific Design Automation Conference*, pages 272–275, 2005.

[57] A. S. Holevo. Some estimates of the information transmitted by quantum communication channels. *Probl. Inf. Transm.*, 9(3):177–183, 1973.

[58] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 913–925, 2016.

[59] Juha J Vartiainen, Mikko Möttönen, and Martti M Salomaa. Efficient decomposition of quantum gates. *Physical review letters*, 92(17):177902, 2004.

[60] Jessica Bavaresco, Mio Murao, and Marco Túlio Quintino. Unitary channel discrimination beyond group structures: Advantages of sequential and indefinite-causal-order strategies. *Journal of Mathematical Physics*, 63(4), 2022.

[61] Dominic W Berry, Andrew M Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 792–809. IEEE, 2015.

[62] Richard Cleve, Daniel Gottesman, Michele Mosca, Rolando D Somma, and David Yonge-Mallo. Efficient discrete-time simulations of continuous-time quantum query algorithms. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 409–416, 2009.

[63] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[64] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

[65] Srinivasan Arunachalam, Alex Bredariol Grilo, and Aarthi Sundaram. Quantum hardness of learning shallow classical circuits. *SIAM Journal on Computing*, 50(3):972–1013, 2021.

[66] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019.

Learning quantum states and unitaries of bounded gate complexity

Haimeng Zhao⋆,[1, 2, *] Laura Lewis⋆,[1, 3, †] Ishaan Kannan⋆,[1, ‡]
Yihui Quek,[4, 5, §] Hsin-Yuan Huang,[1, 3, 5, ¶] and Matthias C. Caro[1, 6, **]

[1] *Institute for Quantum Information and Matter, Caltech, Pasadena, CA, USA*
[2] *Tsinghua University, Beijing, China*
[3] *Google Quantum AI, Venice, CA, USA*
[4] *Harvard University, 17 Oxford Street, Cambridge, MA, USA*
[5] *Massachusetts Institute of Technology, Cambridge, MA, USA*
[6] *Freie Universität Berlin, Berlin, Germany*

While quantum state tomography is notoriously hard, most states hold little interest to practically-minded tomographers. Given that states and unitaries appearing in Nature are of bounded gate complexity, it is natural to ask if efficient learning becomes possible. In this work, we prove that to learn a state generated by a quantum circuit with G two-qubit gates to a small trace distance, a sample complexity scaling linearly in G is necessary and sufficient. We also prove that the optimal query complexity to learn a unitary generated by G gates to a small average-case error scales linearly in G. While sample-efficient learning can be achieved, we show that under reasonable cryptographic conjectures, the computational complexity for learning states and unitaries of gate complexity G must scale exponentially in G. We illustrate how these results establish fundamental limitations on the expressivity of quantum machine learning models and provide new perspectives on no-free-lunch theorems in unitary learning. Together, our results answer how the complexity of learning quantum states and unitaries relate to the complexity of creating these states and unitaries.

I. INTRODUCTION

A central problem in quantum physics is to characterize a quantum system by constructing a full classical description of its state or its unitary evolution based on data from experiments. These two tasks, named *quantum state tomography* [1–4] and *quantum process tomography* [5–9], are (in)famous for being ubiquitous yet highly expensive. The applications of tomography include quantum metrology [10, 11], verification [12, 13], benchmarking [5–8, 14–17], and error mitigation [18]. Yet tomography provably requires exponentially many (in the system size n) copies of the unknown state [19, 20] or runs of the unknown process [21]. This intuitively arises from the exponential scaling of the number of parameters needed to describe an *arbitrary* quantum system.

But the situation is less dire than it theoretically appears. In practice, tools for analyzing many-body systems often exploit *known structures* cleverly to predict their phenomenology or classically simulate them. Notable examples include the BCS theory for superconductivity [22], tensor networks [23, 24], and neural network [25–27] Ansätze. Indeed, while *most* of the states or unitaries may have exponential gate complexity [28], such objects are also unphysical: an exponentially-complex state or unitary cannot be produced in Nature with a reasonable amount of time [29]. In particular, [29] shows that quantum states/unitaries with bounded gate complexity are precisely those that can be produced by bounded-time evolution of time-dependent local Hamiltonians.

In this work, we study if tomography, too, can benefit from the observation that Nature can only produce states and unitaries with bounded complexity. This gives rise to the following main question.

Can we efficiently learn states/unitaries of bounded gate complexity?

In particular, we consider the following two tasks:

1. Given copies (samples) of a pure quantum state $|\psi\rangle$ generated by G two-qubit gates, learn $|\psi\rangle$ to within ϵ trace distance; see Figure 1(a).
2. Given uses (queries) of a unitary U composed of G two-qubit gates, learn U to within ϵ root mean squared trace distance between output states (average-case learning); see Figure 1(b).

Note that the G quantum gates can act on arbitrary pairs of qubits without any geometric locality constraint. By allowing general gates beyond discrete gate sets, this setting encompasses continuous time-dependent Hamiltonian dynamics via Trotterization [29] and thus analog quantum simulation [30]. It also includes states heavily studied in condensed matter such as symmetry-protected topologically

[⋆] These authors contributed equally to this work.
[*] haimengzhao@icloud.com
[†] llewis@alumni.caltech.edu
[‡] ikannan@caltech.edu
[§] yquek@mit.edu
[¶] hsinyuan@caltech.edu
[**] matthias.caro@fu-berlin.de

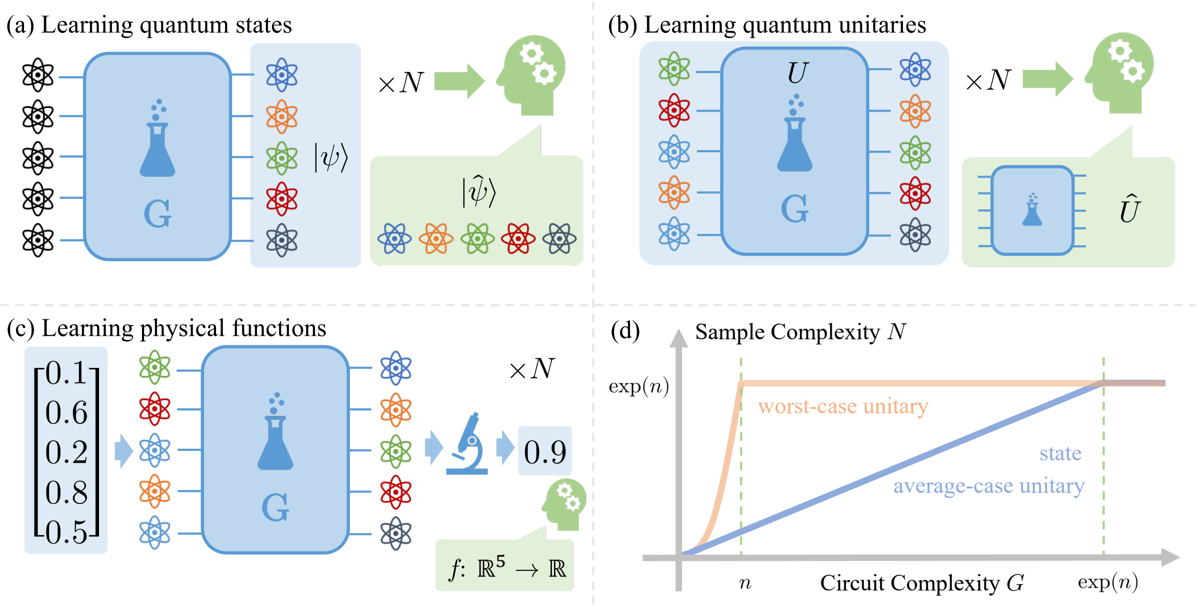


Figure 1. (a)-(c) Schematic overview of the learning models in this work. (a) Learning quantum states with bounded circuit complexity G. (b) Learning unitaries with bounded circuit complexity G. (c) Learning classical functions from quantum experiments with bounded circuit complexity G. (d) Sample complexity of learning states in trace distance and unitaries in average-case distance scales linearly with circuit complexity, while that of learning unitaries in worst-case distance scales exponentially.

ordered states [31–33] and tensor network states [34–36]. Previously, [37] showed that Task 1 can be accomplished with a sample complexity of $\tilde{\mathcal{O}}(nG^2/\epsilon^4)$. In our work, we present algorithms for both of these tasks that use a number of samples/queries linear in the circuit complexity G up to logarithmic factors. Moreover, the sample complexity is independent of system size. Thus, for G scaling polynomially with the number of qubits, our learning procedures improve upon previous work [37] and have significantly lower sample/query complexities than required for general tomography, answering our central question affirmatively. We also prove matching lower bounds (up to logarithmic factors), showing that our algorithms are effectively optimal. Moreover, we show that the focus on average-case learning is crucial in the case of unitaries: unitary tomography up to error ϵ in diamond distance (a worst-case metric over input states) requires a number of queries scaling exponentially in G, establishing an exponential separation between average and worst case.

While our learning algorithms for bounded-complexity states and unitaries are efficient in terms of sample/query complexity, they are not computationally efficient. We prove that this is unavoidable. Assuming the quantum subexponential hardness of Ring Learning with Errors (RingLWE) [38–43], any quantum algorithm that learns arbitrary states/unitaries with $\tilde{\mathcal{O}}(G)$ gates requires computational time scaling exponentially in G. This result highlights a significant computational complexity limitation on learning even comparatively simple states and unitaries. This result also answers an open question in [44]. Meanwhile, we show that poly(n)-time algorithms are possible for $G = \mathcal{O}(\log n)$. Together, this establishes a crossover in computational hardness at $G \sim \log n$, kicking in far before the sample complexity becomes exponential (at $G = \exp(n)$). This means that relatively few samples/queries already contain enough information for the learning task, but it is hard to retrieve the information.

Finally, we study two variations of unitary learning which deepen our insights about the problem. The first variation utilizes classical (not quantum) descriptions of input and output pairs, and explains why both learning states and unitaries display a linear-in-G sample complexity: The underlying source of complexity in learning unitaries is, in fact, the readout of input and output quantum states, rather than learning the mapping. We generalize recent quantum no-free lunch theorems [45, 46] to reach this conclusion. For the second variation we study quantum machine learning (QML) models. We focus on learning classical functions that map variables controlling the input states and the evolution to some experimentally observed property of the outputs (Figure 1(c)). Surprisingly, we find that certain well-behaved many-variable functions can in fact not (even approximately) be implemented by quantum experiments with bounded complexity. This highlights a fundamental limitation on the functional expressivity of both Nature and practical QML models.

Sample complexity	State	Unitary (average-case)	Unitary (worst-case)
Upper bound	$\tilde{\mathcal{O}}\left(G/\epsilon^2\right)$	$\tilde{\mathcal{O}}\left(G \min\left\{1/\epsilon^2, \sqrt{2^n}/\epsilon\right\}\right)$	$\tilde{\mathcal{O}}\left(2^n G/\epsilon\right)$
Lower bound	$\tilde{\Omega}\left(G/\epsilon^2\right)$	$\Omega\left(G/\epsilon\right)$	$\Omega\left(2^{\min\{G/(2C), n/2\}}/\epsilon\right)$

Table I. **Sample complexity of learning n-qubit states and unitaries with circuit complexity G.** The learning accuracy ϵ is measured in trace distance for states, root mean squared trace distance for average case unitary learning, and diamond distance for worst case. Here, $C > 0$ is some universal constant. Throughout the manuscript, $\tilde{\mathcal{O}}, \tilde{\Theta}$ and $\tilde{\Omega}$ denote that we are suppressing non-leading logarithmic factors.

II. RESULTS

In this section, we discuss our rigorous guarantees for learning quantum states and unitaries with circuit complexity G. Our sample complexity results are summarized in Table I and Figure 1(d).

We also present computational complexity results, where we establish the exponential-in-G growth of computational complexity, implying that $\log n$ gate complexity is a transition point at which learning becomes computationally inefficient. In particular, we prove that for circuit complexity $\tilde{\mathcal{O}}(G)$, any quantum algorithm for learning states in trace distance or unitaries in average-case distance must use time exponential in G, under the conjecture that RingLWE cannot be solved by a quantum computer in sub-exponential time. Hence, for a number G of gates that scales slightly higher than $\log n$, the learning tasks cannot be solved by any polynomial-time quantum algorithm under the same conjecture. Meanwhile, for $G = \mathcal{O}(\log n)$, both learning tasks can be solved efficiently in polynomial time.

A. Learning quantum states

We consider the task of learning quantum states of bounded circuit complexity. Let $|\psi\rangle = U|0\rangle^{\otimes n}$ be an n-qubit pure state generated by a unitary U consisting of G two-qubit gates acting on the zero state. Throughout this section, we denote $\rho \triangleq |\psi\rangle\!\langle\psi|$. Given N identically prepared copies of ρ, the goal is to output a classical circuit description of a quantum state $\hat{\rho}$ that is ϵ-close to ρ in trace distance: $\mathrm{d}_{\mathrm{tr}}(\hat{\rho}, \rho) = \|\hat{\rho} - \rho\|_1/2 < \epsilon$. We establish the following theorem, which states that linear-in-G many samples (up to logarithmic factors) are both necessary and sufficient to learn the unknown quantum state $|\psi\rangle$ within a small trace distance.

Theorem 1 (State learning)**.** *Suppose we are given N copies of an n-qubit pure state $\rho = |\psi\rangle\!\langle\psi|$, where $|\psi\rangle = U|0\rangle^{\otimes n}$ is generated by a unitary U consisting of G two-qubit gates. Then, $N = \tilde{\Theta}\left(G/\epsilon^2\right)$ copies are necessary and sufficient to learn the state within ϵ-trace distance d_{tr} with high probability.*

Previous work [37] obtained a sample complexity of $\tilde{\mathcal{O}}(nG^2/\epsilon^4)$ for this task, which we show to be sub-optimal. Notably, our result achieves the optimal scaling in both G and ϵ up to logarithmic factors and is independent of the system size n. Thus, we completely characterize the sample complexity, resolving an open question from [47]. We prove the upper bound in Appendix B 1, utilizing covering nets [48] and quantum hypothesis selection [49]. Our proposed algorithm first creates a covering net over the space of all unitaries consisting of G two-qubit gates. This can easily be transformed into a covering net over the space of all quantum states generated by G two-qubit gates by applying each element of the unitary covering net to the zero state. Thus, any quantum state generated by G two-qubit gates is close (in trace distance) to some element of the covering net. We can then apply quantum hypothesis selection [49] to the covering net, which allows us to identify the element in the covering net that is close to the unknown target state $|\psi\rangle$ and achieve the optimal ϵ dependence. We also note that our algorithm for learning quantum states does not require knowledge of or access to the unitary U which generates the unknown state $|\psi\rangle$. Only the condition that some unitary U consisting of G gates generates $|\psi\rangle$ is needed. The lower bound is proven in Appendix B 2 by using an information-theoretic argument via reduction to distinguishing a packing net over G-gate states [19].

Our algorithm to learn the unknown quantum state $|\psi\rangle$ is computationally inefficient, as it requires a search over a covering net whose cardinality is exponential in G. We show that for circuits of size $\tilde{\mathcal{O}}(G)$, any quantum algorithm that can learn $|\psi\rangle$ to within a small trace distance given access to copies of this state must use time exponential in G, under commonly-believed cryptographic assumptions [38–43]. Meanwhile, the learning task is computationally-efficiently solvable for $G = \mathcal{O}(\log n)$ via junta learning [50] and standard tomography methods. This implies a transition point of computational efficiency at $\log n$ circuit complexity. Previous work [51, 52] arrives at similar hardness results for polynomial circuit complexity, but our detailed analysis allows us to sharpen the computational lower bound and obtain this transition point. [53] also proves computational complexity lower bounds for distribution learning that are similar in spirit.

Theorem 2 (State learning computational complexity)**.** *Suppose we are given N copies of an unknown n-qubit pure state $|\psi\rangle = U|0\rangle^{\otimes n}$ generated by an arbitrary unknown unitary U consisting of $\tilde{\mathcal{O}}(G)$ two-qubit gates. Suppose that* RingLWE *cannot be solved by a quantum computer in sub-exponential time. Then, any quantum algorithm that learns the state to within ϵ trace distance d_{tr} must use $\exp(\Omega(\min\{G,n\}))$ time. Meanwhile, for $G = \mathcal{O}(\log n)$, the learning task can be solved in polynomial time.*

B. Learning quantum unitaries

For learning unitaries, a natural distance metric analogous to the trace distance for states is the diamond distance $\mathrm{d}_\diamond(U,V) = \max_\rho \|(U\otimes I)\rho(U\otimes I)^\dagger - (V\otimes I)\rho(V\otimes I)^\dagger\|_1$, where ρ is over any arbitrarily extended Hilbert space. It characterizes the optimal success probability for discriminating between two unitary channels. Moreover, it can be reinterpreted in terms of the largest distance between $U|\psi\rangle$ and $V|\psi\rangle$ over all input states $|\psi\rangle$, and thus represents the error we make in the worst case over input states. We find that in this worst-case learning task, a number of queries exponential in G is necessary to learn the unitary.

Theorem 3 (Worst-case unitary learning)**.** *To learn an n-qubit unitary composed of G two-qubit gates to accuracy ϵ in diamond distance $\mathrm{d}_\diamond$ with high probability, any quantum algorithm must use at least $\Omega\left(2^{\min\{G/(2C),n/2\}}/\epsilon\right)$ queries to the unknown unitary, where $C > 0$ is a universal constant. Meanwhile, there exists such an algorithm using $\tilde{\mathcal{O}}(2^n G/\epsilon)$ queries.*

The complete proof is given in Appendix C 1 and relies on the adversary method [54–57]. We construct a set of unitaries that a worst-case learning algorithm can successfully distinguish, but that only make minor differences when acting on states so that a minimal number of queries have to be made in order to distinguish them. The upper bound is achieved by the average-case learning algorithm in Theorem 4 below when applied in the regime of exponentially small error.

Having established this no-go theorem for worst-case learning, we turn to a more realistic average-case learning alternative. Here, the accuracy is measured using the root mean squared trace distance between output states over Haar-random inputs, $\mathrm{d}_{\mathrm{avg}}(U,V) = \sqrt{\mathbb{E}_{|\psi\rangle}[\mathrm{d}_{\mathrm{tr}}(U|\psi\rangle, V|\psi\rangle)^2]}$. This metric characterizes the average error when testing the learned unitary on randomly chosen input states.

We find that, similarly to the state learning task, linear-in-G many queries are both necessary and sufficient to learn a unitary in the average case.

Theorem 4 (Average-case unitary learning)**.** *There exists an algorithm that learns an n-qubit unitary composed of G two-qubit gates to accuracy ϵ in root mean squared trace distance $\mathrm{d}_{\mathrm{avg}}$ with high probability using $\tilde{\mathcal{O}}\left(G\min\{1/\epsilon^2, \sqrt{2^n}/\epsilon\}\right)$ queries to the unknown unitary. Meanwhile, $\Omega\left(G/\epsilon\right)$ queries to the unitary or its inverse or the controlled versions are necessary for any such algorithm.*

We show the upper bound in Appendix C 2 by combining a covering net with quantum hypothesis selection similarly to the upper bound in Theorem 1. Our algorithm achieving the query complexity $\tilde{\mathcal{O}}(G/\epsilon^2)$ uses maximally entangled states and the Choi–Jamiołkowski duality [58–60]. With a bootstrap method similar to quantum phase estimation [21], we improve the ϵ-dependence to the Heisenberg scaling $\tilde{\mathcal{O}}(1/\epsilon)$, albeit at the cost of a dimensional factor. Without auxiliary systems, we prove a query complexity bound of $\tilde{\mathcal{O}}(G\min\{1/\epsilon^4, (\sqrt{2^n})^3/\epsilon\})$. The lower bound is proven in Appendix C 3 by mapping to a fractional query problem [21, 61, 62] and making use of a recent upper bound on the success probability in unitary distinguishing tasks [63]. In the case of learning generic unitaries, our result yields a $\Omega(4^n/\epsilon)$ lower bound, improving upon the $\Omega(4^n/n^2)$ bound from the recent work [51], which studies the hardness of learning Haar-(pseudo)random unitaries.

As Haar-random states are hard to generate in practice, we also discuss other input state ensembles of physical interest. Relying on the equivalence of root mean squared trace distances over different locally scrambled ensembles [64, 65], recently established in [66], our algorithm achieves the same average-case guarantee over any such ensemble. Notable examples of locally scrambled ensembles include products of Haar-random single-qubit states or of random single-qubit stabilizer states, 2-designs on n-qubit states, and output states of random local quantum circuits with any fixed architecture.

The similar linear-in-G sample/query complexity scaling in Theorems 1 and 4 hints at a common underlying source of complexity. However, in contrast to state learning, unitary learning comes with two natural such sources: (1) to readout input and output states, and (2) to learn the mapping from inputs to outputs. The similarity between learning states and unitaries in terms of complexities suggests that the former may encapsulate the central difficulty in unitary learning whereas the latter may be easy. This seemingly contradicts recent quantum no-free-lunch theorems [45, 46, 67], which state $\Omega(2^n)$ samples are required to learn a generic unitary even from classical descriptions of input-output state pairs, highlighting the difficulty of (2).

To resolve this apparent contradiction, we reformulate the quantum no-free-lunch theorem (Theorem 17) from a unifying information-theoretic perspective in Appendix C 4. We highlight that enlarging the space for the classically described data allows to systematically reduce the sample complexity until a single sample suffices to learn a general unitary. Therefore, the difficulty of learning the mapping, as indicated by quantum no-free-lunch theorems, vanishes when we allow auxiliary systems and query access to the unitary. Inspired by this observation, we give two ways of enlarging the representation space with auxiliary systems. The first is fundamentally quantum, making use of entangled input states [46]. The other is purely classical, relying on mixed state inputs [68].

Theorem 5 (Learning with classical descriptions)**.** *There exists an algorithm that learns a generic n-qubit unitary with any non-trivial accuracy and with high success probability using $\mathcal{O}(2^n/r)$ classically described input-output pairs with mixed (entangled) input states of (Schmidt) rank r. Moreover, any such algorithm that is robust to noise needs at least $\Omega(2^n/r)$ samples.*

Similarly to the case for state learning, our average-case unitary learning algorithm is not computationally efficient. We show that this cannot be avoided. Under commonly-believed cryptographic assumptions [38–43], any quantum algorithm that can learn unknown unitaries with circuit size $\tilde{\mathcal{O}}(G)$ to a small error in average-case distance from queries must have a computational time exponential in G. This implies the same computational hardness for worst-case unitary learning, and a $\log n$ transition point of computational efficiency. Note that the hard instances we construct are implementable with a similar number of Clifford and T gates [69]. Therefore, together with Theorem 2, this implies that there is no polynomial time quantum algorithms for learning Clifford+T circuits with $\tilde{\omega}(\log n)$ T gates, answering an open question (the fifth question) in the survey [44] negatively.

Theorem 6 (Unitary learning computational complexity)**.** *Suppose we are given N queries to an arbitrary unknown n-qubit unitary U consisting of $\tilde{\mathcal{O}}(G)$ two-qubit gates. Assume that $\mathsf{RingLWE}$ cannot be solved by a quantum computer in sub-exponential time. Then, any quantum algorithm that learns the unitary to within ϵ average-case distance $\mathrm{d}_{\mathrm{avg}}$ must use $\exp(\Omega(\min\{G,n\}))$ time. Meanwhile, for $G = \mathcal{O}(\log n)$, the learning task can be solved in polynomial time.*

C. Learning physical functions

Apart from learning quantum states and dynamics themselves, a more classically minded learner may care more about learning classical functions resulting from quantum processes. We define these *physical functions* in Appendix D as functions $f(x, \{U_i\}_{i=1}^G, a)$ mapping $x \in [0,1]^\nu$ to $\mathbb{R}$ resulting from a physical experiment consisting of three steps: (1) a fixed state preparation procedure that can depend on x; (2) a unitary evolution consisting of G tunable two-qubit gates $\{U_i\}_{i=1}^G$ and arbitrary fixed unitaries that can depend on x, arranged in a circuit architecture a; (3) the measurement of a fixed observable, whose expectation is the function output. By tuning the local gates $\{U_i\}_{i=1}^G$ and potentially changing architecture a, we obtain a resulting class of functions that can be implemented in this general experimental setting. Despite the generality of this setup, we find that certain well-behaved functions are actually not physical in this sense: they cannot be efficiently approximated or learned via physical functions.

Theorem 7 (Approximating and learning with physical functions)**.** *To approximate and learn arbitrary 1-bounded and 1-Lipschitz $\mathbb{R}$-valued functions on $[0,1]^\nu$ to accuracy ϵ in $\|\cdot\|_\infty$ with high probability, using physical functions with G gates and variable circuit structures, we must use $G \geq \tilde{\Omega}(1/\epsilon^{\nu/2})$ gates and collect at least $\Omega(1/\epsilon^\nu)$ samples.*

We prove this in Appendix D by noting that to approximate arbitrary 1-bounded and 1-Lipschitz functions well, the complexity of experimentally implementable functions cannot be too small, as measured by pseudo-dimension [70] or fat-shattering dimension [71]. Then the gate complexity lower bound follows because the function class complexity is limited by the circuit complexity [72], and we can appeal to results in classical learning theory [73] to obtain our sample complexity lower bound.

It has been established that a classical neural network can learn to approximate any 1-bounded and 1-Lipschitz functions to accuracy ϵ in $\|\cdot\|_\infty$ with $\tilde{\Theta}(1/\epsilon^\nu)$ parameters, exponential in the number of variables ν, known as the curse of dimensionality [74]. Our results show that quantum neural networks can do no better. This result not only is relevant to the practical implementation of quantum machine learning, complementing existing results on the universal approximation of quantum neural networks [75–78], but also has deep implications to the physicality of the function class at consideration. It means that there are some many-variable 1-bounded and 1-Lipschitz functions that cannot be implemented in Nature efficiently. On the other hand, certain more restricted function classes can be approximated using only $\mathcal{O}(1/\epsilon^2)$ parameters with both classical [74] and quantum neural networks [75], independent of the number of variables. This reveals a fundamental limitation on the functional expressivity of Nature, practical QML models, and quantum signal processing algorithms [79, 80].

III. DISCUSSION

Our work provides a new, more fine-grained perspective on the fundamental problems of state and process tomography by analyzing them for the broad and physically relevant class of bounded-complexity states and unitaries. It complements existing literature on learning restricted classes of states/unitaries or their properties. Examples include stabilizer circuits and states [81–84], Clifford circuits with few non-Clifford T gates and their output states [69, 85–88], matrix product operators [24] and states [89–91], phase states [82, 92–94], permutationally invariant states [95–97], outputs of shallow quantum circuits [98], PAC learning quantum states [99], shadow tomography [37], classical shadow formalism [14, 100–102], and property prediction of the outputs of quantum processes [103–105]. It also raises many interesting questions for future research.

Firstly, to account for decoherence and imperfections in realistic experiments, it is natural to generalize our results to mixed states and channels. As our learning algorithms based on hypothesis selection and classical shadows rely on the purity/unitarity of the unknown state/process, it seems that different algorithmic approaches would be needed to go beyond states of constant rank. Moreover, while our results show that learners using only single-copy measurements and no coherent quantum processing can achieve optimal sample/query complexity (in G) for pure state/unitary learning (in line with the state tomography protocol in [20], which uses at most $\mathrm{rank}(\rho)$ copies at a time for the tomography of general state ρ), quantum-enhanced learners, using multi-copy measurements and coherent processing, may have an advantage in the case of mixed states and channels. Such a quantum advantage is known for general mixed state tomography [106, 107] and in certain channel learning scenarios [103, 105, 108–112], however, to our knowledge not yet under assumptions of bounded complexity.

Secondly, there are several regimes of interest in which our results may be further extended. For instance, while we establish computational efficiency transition for state and unitary learning at logarithmic circuit complexity, we leave open the question of computationally efficient learning with constraints beyond circuit complexity (e.g., constant-depth circuits where the gates are spread out). Another potential improvement related to the computational complexity is in regards to average-case computational hardness. While our computational lower bounds hold in the worst-case, this does not tell us if most states/unitaries of bounded gate complexity are computationally hard to learn. Are there a worst-case to average-case reduction for this problem? Or perhaps is there an average-case notion of pseudorandomness that one could leverage here? An additional regime where our work can be extended is as follows. Our adaptation of the bootstrap strategy from [21] to average-case unitary learning achieves Heisenberg scaling only at the cost of a dimension-dependent factor. Given recent work in state shadow tomography [113–115], it may not be possible to find a learner free from this dimensional factor while achieving the ϵ^{-1} scaling. Finding such a learner or disproving its existence could serve as an important contribution to recent progress on Heisenberg-limited learning in different scenarios [116–118].

Thirdly, can we make learning even more efficient if the circuit structure is fixed and known in advance? Our upper bound already implies an algorithm with $\tilde{\mathcal{O}}(G)$ sample complexity for fixed circuit structure, but the lower bound proof crucially relies on the ability to place gates freely in the construction of the packing net. A particular fixed circuit structure of physical relevance is the brickwork circuit [119]. In Appendix E, we give preliminary results showing that if an n-qubit G-gate brickwork circuit suffices to implement an approximate unitary t-design [120], then the metric entropy of this unitary class with respect to $\mathrm{d}_{\mathrm{avg}}$ is lower bounded by $\Omega(tn)$. Considering the known lower bound of $G \geq \tilde{\Omega}(tn)$ on the size of brickwork circuits implementing t-designs [120], whose tightness is still an open problem [121], this may hint at a similar $\tilde{\Theta}(G)$ sample complexity of learning brickwork circuits.

Lastly, we outline a potential connection to the Brown-Susskind conjecture [122, 123] originating from the wormhole-growth paradox in holographic duality [124–127]. Informally, the conjecture states that the complexity of a generic local quantum circuit grows linearly with the number of 2-qubit gates for an exponentially long time, dual to the steady growth of a wormhole's volume in the bulk theory. With "complexity" understood as "circuit complexity" [126], this conjecture has recently been confirmed for exact circuit complexity [128, 129] while the case of approximate circuit complexity is only partially resolved [130, 131]. Our work suggests an alternative approach to the Brown-Susskind conjecture. Namely, we have demonstrated that the complexity of learning quantum circuits grows linearly with the number of local gates in the worst case. If our bounds were extended to hold with high probability over random circuits with G gates, this would yield a sample complexity version of the Brown-Susskind conjecture, suggesting the complexity of learning as a dual of the wormhole volume.

Via these open questions, tomography problems dating back to the early days of quantum computation and information connect closely to different avenues of current research in the field. Consequently, answering these questions will shed new light on fundamental quantum physics as well as on the frontiers of quantum complexity and quantum learning.

IV. METHODS

In this section, we discuss the main ideas behind the proof of our results on the sample complexity of learning states (Theorem 1) and unitaries (Theorem 4), along with the computational complexity (Theorems 2 and 6).

A. Sample complexity upper bounds

We prove the upper bounds in Theorems 1 and 4 using a hypothesis selection protocol similar to [49], but now based on classical shadow tomography [100] that enables a linear-in-G scaling.

a. State learning For state learning, we first take a minimal covering net $\mathcal{N}$ over the set of states with bounded circuit complexity G such that for any such state $|\psi\rangle$, there exists a state in the covering net that is ϵ-close to $|\psi\rangle$ in trace distance. This net then serves as a set of candidate states from which the learning algorithm will select one. Importantly, we prove that the cardinality of $\mathcal{N}$ can be upper bounded by $|\mathcal{N}| \leq e^{\tilde{\mathcal{O}}(G)}$. Here, note that the tilde hides a logarithmic factor in terms of system size, which we remove using a more detailed analysis with ideas from junta learning [50].

Next, we use classical shadows created via random Clifford measurements [100] to estimate the trace distance between the unknown state and each of the candidates in $\mathcal{N}$. This is achieved by estimating the expectation value of the Helstrom measurement [132], which is closely related to the trace distance between two states. As the rank of Helstrom measurements between pure states is at most 2, Clifford classical shadows can efficiently estimate all $\binom{|\mathcal{N}|}{2}$ of them simultaneously to ϵ error using $\mathcal{O}(\log|\mathcal{N}|/\epsilon^2) \leq \tilde{\mathcal{O}}(G/\epsilon^2)$ copies of $|\psi\rangle$. Then we select the candidate that has the smallest trace distance from $|\psi\rangle$ as the output.

The above strategy leads to a sample complexity upper bound that depends logarithmically on the number of qubits n. This is undesirable when the circuit complexity G is smaller than $n/2$ (i.e., when some of the qubits are in fact never influenced by the circuit). We improve our algorithm in this small-size regime by first performing a junta learning step [50] to identify which of the qubits are acted on non-trivially. After that, we enhance our protocol with a measure-and-postselect step. This allows us to construct a covering net only over the qubits acted upon non-trivially whose cardinality no longer depends on n. We then perform the hypothesis selection as before. In this way, we are able to achieve a sample complexity independent of system size.

b. Unitary learning The algorithm for unitary learning is similar to the state learning protocol. When allowing the use of an auxiliary system, we utilize the fact that the average-case distance between unitaries is equivalent to the trace distance between their Choi states. This way, we can reduce the problem to state learning of the Choi states and achieve the $\tilde{\mathcal{O}}(G/\epsilon^2)$ sample complexity. Without auxiliary systems, we can sample random input states and perform one-shot Clifford shadows on the outputs to estimate the squared average-case distance, resulting in an $\tilde{\mathcal{O}}(G/\epsilon^4)$ sample complexity with a sub-optimal ϵ-dependence.

Furthermore, we improve the ϵ dependence in unitary learning to the Heisenberg scaling $\tilde{\mathcal{O}}(1/\epsilon)$ via a bootstrap method similar to [21], using the above learning algorithm as a sub-routine. Specifically, we iteratively refine our learning outcome $\hat{U}$ by performing hypothesis selection over a covering net of $(U\hat{U}^\dagger)^p$, with p increasing exponentially as the iteration proceeds. Although the circuit complexity of $(U\hat{U}^\dagger)^p$ grows with p, a covering net with p-independent cardinality can be constructed based on the one-to-one correspondence to U. However, unlike the diamond distance learner considered in [21], which has fine control over every eigenvalue of the unitaries, our average-case learner only has control over the average of the eigenvalues. Thus for the bootstrap to work (i.e., for the learning error to decrease with increasing p), the average-case learner has to work in an exponentially small error regime, which results in a dimensional factor in the final sample complexity $\tilde{\mathcal{O}}(\sqrt{2^n}G/\epsilon)$.

B. Sample complexity lower bounds

We prove the sample complexity lower bounds in Theorems 1 and 4 by reduction to distinguishing tasks. Specifically, if we can learn the state/unitary to within ϵ error, then we can use this learning algorithm to distinguish a set of states/unitaries that are 3ϵ far apart from each other. Hence a lower bound on the sample complexity of distinguishing states/unitaries from a packing net implies a lower bound for the learning task.

a. State learning For state learning, we construct a packing net $\mathcal{M}$ of the set of $(\log_2 G)$-qubit states, which we later tensor product with zero states on the remaining qubits. These states have circuit complexity $\sim G$ because $\mathcal{O}(2^k)$ two-qubit gates can implement any pure k-qubit states [133]. We prove that the cardinality of $\mathcal{M}$ can be lower bounded by $e^{\Omega(G)}$. This means that to distinguish the states in $\mathcal{M}$, one has to gather $\Omega(\log|\mathcal{M}|) \geq \Omega(G)$ bits of information. Meanwhile, Holevo's theorem [134] asserts that the amount of information carried by each sample is upper bounded by $\tilde{\mathcal{O}}(\epsilon^2)$ [135]. Hence, we need at least $\tilde{\Omega}(G/\epsilon^2)$ copies of the unknown state.

b. Unitary learning Similarly, for unitary learning, we construct a packing net by stacking all the gates into $\log_4 G$ qubits, using the fact that $\mathcal{O}(4^k)$ two-qubit gates suffice to implement any k-qubit unitaries [136]. Lacking an analogue of Holevo's theorem for unitary queries, we turn to a recently established bound on the success probability of unitary discrimination [63] and obtain an $\Omega(G)$ sample complexity lower bound for constant ϵ. To incorporate the ϵ dependence, we follow [21] and map the problem into a fractional query problem. We show that with N queries, we can use the learning algorithm to simulate [61, 62] an $\mathcal{O}(\epsilon N)$ query algorithm that solves the above constant-accuracy distinguishing problem. This gives us the desired $N \geq \Omega(G/\epsilon)$ lower bound.

C. Computational hardness

We prove the computational complexity lower bounds in Theorems 2 and 6 again by reduction to distinguishing tasks, whose hardness relies on cryptographic primitives in this case. In particular, we show that if we can learn the state/unitary in polynomial time, then we can use this learning algorithm to efficiently distinguish between pseudorandom states/functions [137, 138] and truly random states/functions. We note that similar ideas have been used to establish a cryptographic no-cloning theorem [137] for PRS, but without gate complexity dependence and the unitary counterpart. The RingLWE hardness assumption here may also be relaxed to the existence of appropriate quantum-secure PRS/PRF constructions that have the same gate complexity discussed below.

Our proofs rely on the construction of quantum-secure pseudorandom functions (PRFs) that can be implemented using TC^0 circuits, subject to the assumption that Ring Learning with Errors (RingLWE) cannot be solved by a quantum computer in sub-exponential time [40]. We show that the circuit construction of [40] can be implemented quantumly using $G = \mathcal{O}(n\mathsf{polylog}(n))$ gates by converting this TC^0 circuit into a quantum circuit that computes the same function. With this construction, we can prove the computational hardness of learning when $G = \mathcal{O}(n\mathsf{polylog}(n))$ as follows.

a. State learning For state learning, we utilize these quantum-secure PRFs to construct pseudorandom quantum states (PRS), in particular binary phase states from [137, 139], with $G = \mathcal{O}(n\mathsf{polylog}(n))$ gates. Given copies of some unknown quantum state that is promised to either be a PRS or a Haar-random state, we design a procedure that can distinguish these two cases. The distinguisher uses our algorithm for learning states along with the SWAP test applied to the learned state and the given state [140, 141]. Thus, we show that if our learning algorithm was able to computationally efficiently learn PRS, then we would have an efficient distinguisher between PRS and Haar-random states, contradicting the definition of a PRS [137].

b. Unitary learning The proof idea in the unitary setting is similar. In this case, we consider PRFs directly rather than the PRS construction. Given query access to some unknown unitary that is promised to be the unitary oracle of either a PRF or a uniformly random Boolean function, we design a procedure that can distinguish these two cases. The distinguisher uses our algorithm for learning unitaries along with the SWAP test [140, 141]. Here, we query the given/learned unitaries on a random tensor product of single-qubit stabilizer states and conduct the SWAP test between the output states. This way, we show that if our learning algorithm was able to computationally efficiently learn a unitary implementing a PRF, then we would have an efficient distinguisher between PRFs and uniformly random functions, which contradicts the definition of a PRF [138].

We then go one step further and show computational hardness for circuit size $\tilde{\mathcal{O}}(G)$. To do this we rely critically on the assumption that RingLWE is hard not just to polynomial-time quantum algorithms, but even to quantum algorithms that run for longer (sub-exponential) time. This allows us to take a much smaller input size to the PRS/PRF in our previous constructions (i.e., over $\mathcal{O}(G)$ qubits which can be implemented with $\tilde{\mathcal{O}}(G)$ gates). The sub-exponential computational hardness of $\mathsf{RingLWE}$ then implies that solving the learning tasks requires time exponential in G.

Meanwhile, for $G = \mathcal{O}(\log n)$, the learning tasks can be solved efficiently by junta learning and standard tomography methods. This establishes $\log n$ circuit complexity as a transition point of computational efficiency. This also implies that the circuit complexity of the PRS/PRF constructions in [40, 139] is optimal up to logarithmic factors, otherwise it would contradict efficient tomography of $\mathcal{O}(\log n)$-complexity states/unitaries. Finally, we note that the PRS/PRF we consider can be implemented with a similar number of Clifford and T gates, extending our results to Clifford+T circuits.

ACKNOWLEDGMENTS

The authors thank John Preskill for valuable feedback and continuous support throughout this project. The authors also thank Ryan Babbush, Yiyi Cai, Charles Cao, Alexandru Gheorghiu, András Gilyén, Alex B. Grilo, Jerry Huang, Nadine Meister, Chris Pattison, Alexander Poremba, Xiao-Liang Qi, Ruohan Shen, Mehdi Soleimanifar, Yu Tong, Tzu-Chieh Wei, Tai-Hsuan Yang, Nengkun Yu for fruitful discussions. Finally, the authors thank Antonio Anna Mele and the anonymous reviewers at QIP 2024 for feedback on an earlier version of this paper. HZ was supported by a Caltech Summer Undergraduate Research Fellowship (SURF). LL was supported by a Mellon Mays Undergraduate Fellowship. HH was supported by a Google PhD fellowship and a MediaTek Research Young Scholarship. HH acknowledges the visiting associate position at the Massachusetts Institute of Technology. MCC was supported by a DAAD PRIME fellowship. This work was done (in part) while a subset of the authors were visiting the Simons Institute for the Theory of Computing. The Institute for Quantum Information and Matter is an NSF Physics Frontiers Center.

DATA AVAILABILITY

No data are generated or analyzed in this theoretical work.

AUTHOR CONTRIBUTIONS

Y.Q., H.H., and M.C.C. conceived the project. H.Z., L.L., and I.K. led the development of the theory and the analytic calculations. All authors contributed to the mathematical aspects of this work. H.Z. and L.L. wrote the manuscript with input from all authors.

COMPETING INTERESTS

The authors declare no competing interests.

[1] Konrad Banaszek, Marcus Cramer, and David Gross. Focus on quantum tomography. *New Journal of Physics*, 15(12):125020, 2013.

[2] Robin Blume-Kohout. Optimal, reliable estimation of quantum states. *New Journal of Physics*, 12(4):043034, 2010.

[3] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. Quantum state tomography via compressed sensing. *Physical review letters*, 105(15):150401, 2010.

[4] Zdenek Hradil. Quantum-state estimation. *Physical Review A*, 55(3):R1561, 1997.

[5] Masoud Mohseni, Ali T Rezakhani, and Daniel A Lidar. Quantum-process tomography: Resource analysis of different strategies. *Physical Review A*, 77(3):032322, 2008.

[6] Jeremy L O'Brien, Geoff J Pryde, Alexei Gilchrist, Daniel FV James, Nathan K Langford, Timothy C Ralph, and Andrew G White. Quantum process tomography of a controlled-not gate. *Physical review letters*, 93(8):080502, 2004.

[7] Andrew James Scott. Optimizing quantum process tomography with unitary 2-designs. *Journal of Physics A: Mathematical and Theoretical*, 41(5):055308, 2008.

[8] Isaac L Chuang and Michael A Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.

[9] GM D'Ariano and P Lo Presti. Quantum tomography for measuring experimentally the matrix elements of an arbitrary quantum operation. *Physical review letters*, 86(19):4195, 2001.

[10] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.

[11] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222–229, 2011.

[12] Christian Kokail, Rick van Bijnen, Andreas Elben, Benoît Vermersch, and Peter Zoller. Entanglement Hamiltonian tomography in quantum simulation. *Nature Physics*, 17(8):936–942, 2021.

[13] Jose Carrasco, Andreas Elben, Christian Kokail, Barbara Kraus, and Peter Zoller. Theoretical and experimental perspectives of quantum verification. *PRX Quantum*, 2(1):010102, 2021.

[14] Ryan Levy, Di Luo, and Bryan K Clark. Classical shadows for quantum process tomography on near-term quantum computers. *arXiv preprint arXiv:2110.02965*, 2021.

[15] Seth T Merkel, Jay M Gambetta, John A Smolin, Stefano Poletto, Antonio D Córcoles, Blake R Johnson, Colm A Ryan, and Matthias Steffen. Self-consistent quantum process tomography. *Physical Review A*, 87(6):062119, 2013.

[16] Robin Blume-Kohout, John King Gamble, Erik Nielsen, Kenneth Rudinger, Jonathan Mizrahi, Kevin Fortier, and Peter Maunz. Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography. *Nature communications*, 8(1):14485, 2017.

[17] Hsin-Yuan Huang, Steven T Flammia, and John Preskill. Foundations for learning from noisy quantum experiments. *arXiv preprint arXiv:2204.13691*, 2022.

[18] Zhenyu Cai, Ryan Babbush, Simon C Benjamin, Suguru Endo, William J Huggins, Ying Li, Jarrod R McClean, and Thomas E O'Brien. Quantum error mitigation. *arXiv preprint arXiv:2210.00921*, 2022.

[19] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. *IEEE Transactions on Information Theory*, 63(9):5628–5641, 2017.

[20] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 899–912, 2016.

[21] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. Query-optimal estimation of unitary channels in diamond distance. *arXiv preprint arXiv:2302.14066*, 2023.

[22] John Bardeen, Leon N Cooper, and John Robert Schrieffer. Theory of superconductivity. *Physical review*, 108(5):1175, 1957.

[23] Román Orús. A practical introduction to tensor networks: Matrix product states and projected entangled pair states. *Annals of physics*, 349:117–158, 2014.

[24] Giacomo Torlai, Christopher J Wood, Atithi Acharya, Giuseppe Carleo, Juan Carrasquilla, and Leandro Aolita. Quantum process tomography with unsupervised learning and tensor networks. *Nature Communications*, 14(1):2858, 2023.

[25] Giuseppe Carleo and Matthias Troyer. Solving the quantum many-body problem with artificial neural networks. *Science*, 355(6325):602–606, 2017.

[26] Giacomo Torlai, Guglielmo Mazzola, Juan Carrasquilla, Matthias Troyer, Roger Melko, and Giuseppe Carleo. Neural-network quantum state tomography. *Nat. Phys.*, 14(5):447, 2018.

[27] Haimeng Zhao, Giuseppe Carleo, and Filippo Vicentini. Empirical sample complexity of neural network mixed state reconstruction. *arXiv preprint arXiv:2307.01840*, 2023.

[28] Fernando GSL Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. Models of quantum complexity growth. *PRX Quantum*, 2(3):030316, 2021.

[29] David Poulin, Angie Qarry, Rolando Somma, and Frank Verstraete. Quantum simulation of time-dependent Hamiltonians and the convenient illusion of Hilbert space. *Physical review letters*, 106(17):170501, 2011.

[30] Iulia M Georgescu, Sahel Ashhab, and Franco Nori. Quantum simulation. *Reviews of Modern Physics*, 86(1):153, 2014.

[31] Bei Zeng, Xie Chen, Duan-Lu Zhou, and Xiao-Gang Wen. *Quantum information meets quantum matter.* Springer, 2019.

[32] Daniel Malz, Georgios Styliaris, Zhi-Yuan Wei, and J Ignacio Cirac. Preparation of matrix product states with log-depth quantum circuits. *Physical Review Letters*, 132(4):040404, 2024.

[33] David T Stephen, Arpit Dua, Ali Lavasani, and Rahul Nandkishore. Nonlocal finite-depth circuits for constructing symmetry-protected topological states and quantum cellular automata. *PRX Quantum*, 5(1):010304, 2024.

[34] Michael Foss-Feig, David Hayes, Joan M Dreiling, Caroline Figgatt, John P Gaebler, Steven A Moses, Juan M Pino, and Andrew C Potter. Holographic quantum algorithms for simulating correlated spin systems. *Physical Review Research*, 3(3):033002, 2021.

[35] Christian Schön, Enrique Solano, Frank Verstraete, J Ignacio Cirac, and Michael M Wolf. Sequential generation of entangled multiqubit states. *Physical review letters*, 95(11):110503, 2005.

[36] Yichen Huang, Xie Chen, et al. Quantum circuit complexity of one-dimensional topological phases. *Physical Review B*, 91(19):195143, 2015.

[37] Scott Aaronson. Shadow tomography of quantum states. In *STOC*, pages 325–338, 2018.

[38] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pages 1–23. Springer, 2010.

[39] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[40] Srinivasan Arunachalam, Alex Bredariol Grilo, and Aarthi Sundaram. Quantum hardness of learning shallow classical circuits. *SIAM Journal on Computing*, 50(3):972–1013, 2021.

[41] Ilias Diakonikolas, Daniel Kane, Pasin Manurangsi, and Lisheng Ren. Cryptographic hardness of learning halfspaces with massart noise. *Advances in Neural Information Processing Systems*, 35:3624–3636, 2022.

[42] Divesh Aggarwal, Huck Bennett, Zvika Brakerski, Alexander Golovnev, Rajendra Kumar, Zeyong Li, Spencer Peters, Noah Stephens-Davidowitz, and Vinod Vaikuntanathan. Lattice problems beyond polynomial time. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1516–1526, 2023.

[43] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In *Theory of Cryptography Conference*, pages 93–122. Springer, 2023.

[44] Anurag Anshu and Srinivasan Arunachalam. A survey on the complexity of learning quantum states. *arXiv preprint arXiv:2305.20069*, 2023.

[45] Kyle Poland, Kerstin Beer, and Tobias J Osborne. No free lunch for quantum machine learning. *arXiv preprint arXiv:2003.14103*, 2020.

[46] Kunal Sharma, Marco Cerezo, Zoë Holmes, Lukasz Cincio, Andrew Sornborger, and Patrick J Coles. Reformulation of the no-free-lunch theorem for entangled datasets. *Physical Review Letters*, 128(7):070501, 2022.

[47] Nengkun Yu and Tzu-Chieh Wei. Learning marginals suffices! *arXiv preprint arXiv:2303.08938*, 2023.

[48] Roman Vershynin. *High-dimensional probability*, volume 47 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, 2018.

[49] Costin Bădescu and Ryan O'Donnell. Improved quantum data analysis. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1398–1411, 2021.

[50] Thomas Chen, Shivam Nadimpalli, and Henry Yuen. Testing and learning quantum juntas nearly optimally. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1163–1185. SIAM, 2023.

[51] Lisa Yang and Netta Engelhardt. The complexity of learning (pseudo) random dynamics of black holes and other chaotic systems. *arXiv preprint arXiv:2302.11013*, 2023.

[52] Amira Abbas, Robbie King, Hsin-Yuan Huang, William J Huggins, Ramis Movassagh, Dar Gilboa, and Jarrod R McClean. On quantum backpropagation, information reuse, and cheating measurement collapse. *arXiv preprint arXiv:2305.13362*, 2023.

[53] M Hinsche, M Ioannou, A Nietner, J Haferkamp, Y Quek, D Hangleiter, J-P Seifert, J Eisert, and R Sweke. One t gate makes distribution learning hard. *Physical Review Letters*, 130(24):240602, 2023.

[54] Joran van Apeldoorn. *A quantum view on convex optimization.* PhD thesis, University of Amsterdam, 2019.

[55] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 636–643, 2000.

[56] Aleksandrs Belovs. Variations on quantum adversary. *arXiv preprint arXiv:1504.06943*, 2015.

[57] Peter Hoyer, Troy Lee, and Robert Spalek. Negative weights make adversaries stronger. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 526–535, 2007.

[58] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[59] Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

[60] Min Jiang, Shunlong Luo, and Shuangshuang Fu. Channel-state duality. *Physical Review A*, 87(2):022310, 2013.

[61] Dominic W Berry, Andrew M Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 792–809. IEEE, 2015.

[62] Richard Cleve, Daniel Gottesman, Michele Mosca, Rolando D Somma, and David Yonge-Mallo. Efficient discrete-time simulations of continuous-time quantum query algorithms. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 409–416, 2009.

[63] Jessica Bavaresco, Mio Murao, and Marco Túlio Quintino. Unitary channel discrimination beyond group structures: Advantages of sequential and indefinite-causal-order strategies. *Journal of Mathematical Physics*, 63(4), 2022.

[64] Wei-Ting Kuo, AA Akhtar, Daniel P Arovas, and Yi-Zhuang You. Markovian entanglement dynamics under locally scrambled quantum evolution. *Physical Review B*, 101(22):224202, 2020.

[65] Hong-Ye Hu, Soonwon Choi, and Yi-Zhuang You. Classical shadow tomography with locally scrambled quantum dynamics. *Physical Review Research*, 5(2):023027, 2023.

[66] Matthias C. Caro, Hsin-Yuan Huang, Nicholas Ezzell, Joe Gibbs, Andrew T. Sornborger, Lukasz Cincio, Patrick J. Coles, and Zoë Holmes. Out-of-distribution generalization for learning quantum dynamics. *Nature Communications*, 14, 2023.

[67] Xinbiao Wang, Yuxuan Du, Zhuozhuo Tu, Yong Luo, Xiao Yuan, and Dacheng Tao. Transition role of entangled data in quantum machine learning. *arXiv preprint arXiv:2306.03481*, 2023.

[68] Zhan Yu, Xuanqiang Zhao, Benchi Zhao, and Xin Wang. Optimal quantum dataset for learning a unitary transformation. *Physical Review Applied*, 19(3):034017, 2023.

[69] Ching-Yi Lai and Hao-Chung Cheng. Learning quantum circuits of some t gates. *IEEE Transactions on Information Theory*, 68(6):3951–3964, 2022.

[70] David Pollard. Convergence of stochastic processes. *Springer Series in Statistics*, 1984.

[71] Michael J Kearns and Robert E Schapire. Efficient distribution-free learning of probabilistic concepts. *Journal of Computer and System Sciences*, 48(3):464–497, 1994.

[72] Matthias C Caro and Ishaun Datta. Pseudo-dimension of quantum circuits. *Quantum Machine Intelligence*, 2(2):14, 2020.

[73] Martin Anthony, Peter L Bartlett, Peter L Bartlett, et al. *Neural network learning: Theoretical foundations.* Cambridge University Press, 1999.

[74] Philipp Grohs and Gitta Kutyniok. *Mathematical aspects of deep learning.* Cambridge University Press, 2022.

[75] Lukas Gonon and Antoine Jacquier. Universal approximation theorem and error bounds for quantum neural networks and quantum reservoirs. *arXiv preprint arXiv:2307.12904*, 2023.

[76] Adrián Pérez-Salinas, David López-Núñez, Artur García-Sáez, Pol Forn-Díaz, and José I Latorre. One qubit as a universal approximant. *Physical Review A*, 104(1):012405, 2021.

[77] Maria Schuld, Ryan Sweke, and Johannes Jakob Meyer. Effect of data encoding on the expressive power of variational quantum-machine-learning models. *Physical Review A*, 103(3):032430, 2021.

[78] Alberto Manzano, David Dechant, Jordi Tura, and Vedran Dunjko. Parametrized quantum circuits and their approximation capacities in the context of quantum machine learning. *arXiv preprint arXiv:2307.14792*, 2023.

[79] John M Martyn, Zane M Rossi, Andrew K Tan, and Isaac L Chuang. Grand unification of quantum algorithms. *PRX quantum*, 2(4):040203, 2021.

[80] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, 2019.

[81] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70(5):052328, 2004.

[82] Ashley Montanaro. Learning stabilizer states by bell sampling. *arXiv preprint arXiv:1707.04012*, 2017.

[83] Richard A Low. Learning and testing algorithms for the clifford group. *Physical Review A*, 80(5):052314, 2009.

[84] Andrea Rocchetto. Stabiliser states are efficiently pac-learnable. *Quantum Info. Comput.*, 18(7–8):541–552, June 2018.

[85] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Efficient learning of quantum states prepared with few non-clifford gates. *arXiv preprint arXiv:2305.13409*, 2023.

[86] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Efficient learning of quantum states prepared with few non-clifford gates ii: Single-copy measurements. *arXiv preprint arXiv:2308.07175*, 2023.

[87] Dominik Hangleiter and Michael J Gullans. Bell sampling from quantum circuits. *arXiv preprint arXiv:2306.00083*, 2023.

[88] Lorenzo Leone, Salvatore FE Oliviero, Seth Lloyd, and Alioscia Hamma. Learning efficient decoders for quasi-chaotic quantum scramblers. *arXiv preprint arXiv:2212.11338*, 2022.

[89] Marcus Cramer, Martin B Plenio, Steven T Flammia, Rolando Somma, David Gross, Stephen D Bartlett, Olivier Landon-Cardinal, David Poulin, and Yi-Kai Liu. Efficient quantum state tomography. *Nature communications*, 1(1):149, 2010.

[90] Olivier Landon-Cardinal, Yi-Kai Liu, and David Poulin. Efficient direct tomography for matrix product states. *arXiv preprint arXiv:1002.4632*, 2010.

[91] Yuchen Guo and Shuo Yang. Scalable quantum state tomography with locally purified density operators

and local measurements. *arXiv preprint arXiv:2307.16381*, 2023.

[92] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20, 1993.

[93] Martin Rötteler. Quantum algorithms to solve the hidden shift problem for quadratics and for functions of large gowers norm. In *International Symposium on Mathematical Foundations of Computer Science*, pages 663–674. Springer, 2009.

[94] Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. Optimal Algorithms for Learning Quantum Phase States. In Omar Fawzi and Michael Walter, editors, *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*, volume 266 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3:1–3:24, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[95] Géza Tóth, Witlef Wieczorek, David Gross, Roland Krischek, Christian Schwemmer, and Harald Weinfurter. Permutationally invariant quantum tomography. *Physical review letters*, 105(25):250403, 2010.

[96] Tobias Moroder, Philipp Hyllus, Géza Tóth, Christian Schwemmer, Alexander Niggebaum, Stefanie Gaile, Otfried Gühne, and Harald Weinfurter. Permutationally invariant state reconstruction. *New Journal of Physics*, 14(10):105001, 2012.

[97] Christian Schwemmer, Géza Tóth, Alexander Niggebaum, Tobias Moroder, David Gross, Otfried Gühne, and Harald Weinfurter. Experimental comparison of efficient tomography schemes for a six-qubit state. *Physical review letters*, 113(4):040503, 2014.

[98] Cambyse Rouzé and Daniel Stilck França. Learning quantum many-body systems from a few copies. *arXiv preprint arXiv:2107.03333*, 2021.

[99] Scott Aaronson. The learnability of quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 463(2088):3089–3114, 2007.

[100] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020.

[101] Andreas Elben, Steven T Flammia, Hsin-Yuan Huang, Richard Kueng, John Preskill, Benoît Vermersch, and Peter Zoller. The randomized measurement toolbox. *Nature Review Physics*, 2022.

[102] Jonathan Kunjummen, Minh C Tran, Daniel Carney, and Jacob M Taylor. Shadow process tomography of quantum channels. *Physical Review A*, 107(4):042403, 2023.

[103] Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, et al. Quantum advantage in learning from experiments. *Science*, 376(6598):1182–1186, 2022.

[104] Hsin-Yuan Huang, Sitan Chen, and John Preskill. Learning to predict arbitrary quantum processes. *arXiv preprint arXiv:2210.14894*, 2022.

[105] Matthias C Caro. Learning quantum processes and hamiltonians via the pauli transfer matrix. *arXiv preprint arXiv:2212.04471*, 2022.

[106] Sitan Chen, Jerry Li, Brice Huang, and Allen Liu. Tight bounds for quantum state certification with incoherent measurements. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1205–1213. IEEE, 2022.

[107] Sitan Chen, Brice Huang, Jerry Li, Allen Liu, and Mark Sellke. When does adaptivity help for quantum state learning?, 2023.

[108] Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. Exponential separations between learning with and without quantum memory. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 574–585. IEEE, 2022.

[109] Kean Chen, Qisheng Wang, Peixun Long, and Mingsheng Ying. Unitarity estimation for quantum channels. *IEEE Transactions on Information Theory*, 69(8):5116–5134, 2023.

[110] Omar Fawzi, Aadil Oufkir, and Daniel Stilck França. Lower bounds on learning pauli channels. *arXiv preprint arXiv:2301.09192*, 2023.

[111] Omar Fawzi, Nicolas Flammarion, Aurélien Garivier, and Aadil Oufkir. Quantum channel certification with incoherent measurements. In Gergely Neu and Lorenzo Rosasco, editors, *Proceedings of Thirty Sixth Conference on Learning Theory*, volume 195 of *Proceedings of Machine Learning Research*, pages 1822–1884. PMLR, 12–15 Jul 2023.

[112] Aadil Oufkir. Sample-optimal quantum process tomography with non-adaptive incoherent measurements. *arXiv preprint arXiv:2301.12925*, 2023.

[113] Joran van Apeldoorn. Quantum probability oracles & multidimensional amplitude estimation. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[114] William J Huggins, Kianna Wan, Jarrod McClean, Thomas E O'Brien, Nathan Wiebe, and Ryan Babbush. Nearly optimal quantum algorithm for estimating multiple expectation values. *Physical Review Letters*, 129(24):240501, 2022.

[115] Joran van Apeldoorn, Arjan Cornelissen, András Gilyén, and Giacomo Nannicini. Quantum tomography using state-preparation unitaries. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1265–1318. SIAM, 2023.

[116] Hsin-Yuan Huang, Yu Tong, Di Fang, and Yuan Su. Learning many-body hamiltonians with heisenberg-limited scaling. *Physical Review Letters*, 130(20):200403, 2023.

[117] Alicja Dutkiewicz, Thomas E O'Brien, and Thomas Schuster. The advantage of quantum control in many-

body Hamiltonian learning. *arXiv preprint arXiv:2304.07172*, 2023.

[118] Haoya Li, Yu Tong, Hongkang Ni, Tuvia Gefen, and Lexing Ying. Heisenberg-limited Hamiltonian learning for interacting bosons. *arXiv preprint arXiv:2307.04690*, 2023.

[119] Matthew PA Fisher, Vedika Khemani, Adam Nahum, and Sagar Vijay. Random quantum circuits. *Annual Review of Condensed Matter Physics*, 14:335–379, 2023.

[120] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346:397–434, 2016.

[121] Jonas Haferkamp. Random quantum circuits are approximate unitary t-designs in depth $O\left(nt^{5+o(1)}\right)$. *Quantum*, 6:795, 2022.

[122] Adam R Brown and Leonard Susskind. Second law of quantum complexity. *Physical Review D*, 97(8):086015, 2018.

[123] Leonard Susskind. Black holes and complexity classes. *arXiv preprint arXiv:1802.02175*, 2018.

[124] Leonard Susskind. Computational complexity and black hole horizons. *Fortschritte der Physik*, 64(1):24–43, 2016.

[125] Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational pseudorandomness, the wormhole growth paradox, and constraints on the ads/cft duality. *arXiv preprint arXiv:1910.14646*, 2019.

[126] Douglas Stanford and Leonard Susskind. Complexity and shock wave geometries. *Physical Review D*, 90(12):126007, 2014.

[127] Adam R Brown, Daniel A Roberts, Leonard Susskind, Brian Swingle, and Ying Zhao. Complexity, action, and black holes. *Physical Review D*, 93(8):086006, 2016.

[128] Jonas Haferkamp, Philippe Faist, Naga BT Kothakonda, Jens Eisert, and Nicole Yunger Halpern. Linear growth of quantum circuit complexity. *Nature Physics*, 18(5):528–532, 2022.

[129] Zhi Li. Short proofs of linear growth of quantum circuit complexity. *arXiv preprint arXiv:2205.05668*, 2022.

[130] Michał Oszmaniec, Michał Horodecki, and Nicholas Hunter-Jones. Saturation and recurrence of quantum complexity in random quantum circuits. *arXiv preprint arXiv:2205.09734*, 2022.

[131] Jonas Haferkamp. On the moments of random quantum circuits and robust quantum complexity. *arXiv preprint arXiv:2303.16944*, 2023.

[132] Carl W. Helstrom. Quantum detection and estimation theory. *J. Statist. Phys.*, 1:231–252, 1969.

[133] Vivek V Shende, Stephen S Bullock, and Igor L Markov. Synthesis of quantum logic circuits. In *Proceedings of the 2005 Asia and South Pacific Design Automation Conference*, pages 272–275, 2005.

[134] A. S. Holevo. Some estimates of the information transmitted by quantum communication channels. *Probl. Inf. Transm.*, 9(3):177–183, 1973.

[135] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 913–925, 2016.

[136] Juha J Vartiainen, Mikko Möttönen, and Martti M Salomaa. Efficient decomposition of quantum gates. *Physical review letters*, 92(17):177902, 2004.

[137] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[138] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

[139] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019.

[140] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, 1997.

[141] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[142] Matthias C Caro, Hsin-Yuan Huang, Marco Cerezo, Kunal Sharma, Andrew Sornborger, Lukasz Cincio, and Patrick J Coles. Generalization in quantum machine learning from few training data. *Nature Communications*, 13, 2022.

[143] Mark M. Wilde. *Quantum Information Theory.* Cambridge University Press, Cambridge, 2nd edition, 2013.

[144] John Watrous. *The Theory of Quantum Information.* Cambridge University Press, 2018.

[145] Antonio Anna Mele. Introduction to haar measure tools in quantum information: A beginner's tutorial. *arXiv preprint arXiv:2307.08956*, 2023.

[146] Thomas Barthel and Jianfeng Lu. Fundamental limitations for measurements in quantum many-body systems. *Physical Review Letters*, 121(8):080406, 2018.

[147] Stanislaw J Szarek. Nets of Grassmann manifold and orthogonal group. In *Proceedings of research workshop on Banach space theory (Iowa City, Iowa, 1981)*, page 169. University of Iowa Iowa City, IA, 1982.

[148] Costin Bădescu and Ryan O'Donnell. Improved quantum data analysis. *arXiv preprint arXiv:2011.10908*, 2020.

[149] VN Vapnik and A Ya Chervonenkis. On the uniform convergence of relative frequencies of events to their probabilities. *Theory of Probability and its Applications*, 16(2):264, 1971.

[150] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 719–737.

Springer, 2012.

[151] Moni Naor and Omer Reingold. Synthesizers and their application to the parallel construction of pseudo-random functions. *Journal of Computer and System Sciences*, 58(2):336–375, 1999.

[152] Yasuhiro Takahashi, Seiichiro Tani, and Noboru Kunihiro. Quantum addition circuits and unbounded fan-out. *Quantum Info. Comput.*, 10(9):872–890, sep 2010.

[153] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Five two-qubit gates are necessary for implementing the toffoli gate. *Physical Review A*, 88(1):010304, 2013.

[154] Paul W Beame, Stephen A Cook, and H James Hoover. Log depth circuits for division and related problems. *SIAM Journal on Computing*, 15(4):994–1003, 1986.

[155] Gregory Rosenthal. Query and depth upper bounds for quantum unitaries via grover search. *arXiv preprint arXiv:2111.07992*, 2021.

[156] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Annual International Cryptology Conference*, pages 208–236. Springer, 2022.

[157] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1589–1602, 2023.

[158] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Annual International Cryptology Conference*, pages 269–295. Springer, 2022.

[159] William Kretschmer. Quantum Pseudorandomness and Classical Complexity. In Min-Hsiu Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:20, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[160] Michael Kearns, Yishay Mansour, Dana Ron, Ronitt Rubinfeld, Robert E. Schapire, and Linda Sellie. On the learnability of discrete distributions. In *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '94, page 273–282, New York, NY, USA, 1994. Association for Computing Machinery.

[161] Gregory Rosenthal. Efficient quantum state synthesis with one query. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2508–2534. SIAM, 2024.

[162] Henry Yuen. An improved sample complexity lower bound for (fidelity) quantum state tomography. *Quantum*, 7:890, 2023.

[163] A. S. Holevo. Statistical decision theory for quantum systems. *J. Multivariate Anal.*, 3:337–394, 1973.

[164] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998.

[165] Craig Gidney. Constructing large controlled nots, 2015. https://algassert.com/circuits/2015/06/05/Constructing-Large-Controlled-Nots.html. Accessed: 2023-08-20.

[166] Mark M Wilde. *Quantum information theory*. Cambridge university press, 2013.

[167] Michael M. Wolf. Quantum channels and operations - guided tour, 7 2012.

[168] John Wright. *How to learn a quantum state*. PhD thesis, Carnegie Mellon University, 2016.

[169] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Information-theoretic bounds on quantum advantage in machine learning. *Physical Review Letters*, 126(19):190505, 2021.

[170] H. Flanders. On Spaces of Linear Transformations with Bounded Rank. *Journal of the London Mathematical Society*, s1-37(1):10–16, 01 1962.

[171] Alexandros Eskenazis, Paata Ivanisvili, and Lauritz Streck. Low-degree learning and the metric entropy of polynomials. *arXiv preprint arXiv:2203.09659*, 2022.

[172] Gyora M Benedek and Alon Itai. Learnability with respect to fixed distributions. *Theoretical Computer Science*, 86(2):377–389, 1991.

[173] Thomas M Cover and Joy A. Thomas. *Elements of information theory*. John Wiley & Sons, 1999.

[174] Peter L Bartlett, Philip M Long, and Robert C Williamson. Fat-shattering and the learnability of real-valued functions. In *Proceedings of the seventh annual conference on Computational learning theory*, pages 299–310, 1994.

[175] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum random access memory. *Physical review letters*, 100(16):160501, 2008.

[176] Adrián Pérez-Salinas, Alba Cervera-Lierta, Elies Gil-Fuster, and José I Latorre. Data re-uploading for a universal quantum classifier. *Quantum*, 4:226, 2020.

[177] Matthias C. Caro, Elies Gil-Fuster, Johannes Jakob Meyer, Jens Eisert, and Ryan Sweke. Encoding-dependent generalization bounds for parametrized quantum circuits. *Quantum*, 5, 2021.

[178] Mehryar Mohri, Afshin Rostamizadeh, and Ameet Talwalkar. *Foundations of machine learning*. The MIT Press, 2018.

[179] Michael M Wolf. Mathematical foundations of machine learning, 2018.

[180] Paul W Goldberg and Mark R Jerrum. Bounding the Vapnik-Chervonenkis dimension of concept classes parameterized by real numbers. *Machine Learning*, 18(2-3):131–148, 1995.

[181] Hugh E. Warren. Lower bounds for approximation by nonlinear manifolds. *Transactions of the American Mathematical Society*, 133(1):167–178, 1968.

[182] Dmitry Yarotsky. Error bounds for approximations with deep relu networks. *Neural Networks*, 94:103–114, 2017.

Appendices

CONTENTS

Appendix A: Preliminaries

Throughout the appendices, we use $d = 2^n$ to denote the dimension of the n-qubit Hilbert space unless otherwise stated.

1. Distance metrics

Here we review some distance metrics and their properties used throughout our proofs. In the main text we have already introduced the trace distance

$$\mathrm{d_{tr}}(|\psi\rangle, |\phi\rangle) = \frac{1}{2}\| \, |\psi\rangle\!\langle\psi| - |\phi\rangle\!\langle\phi| \, \|_1 \, , \tag{A.1}$$

which is analogously defined for density matrices as $\mathrm{d_{tr}}(\rho, \sigma) = \|\rho - \sigma\|_1/2$, the diamond distance

$$\mathrm{d}_\diamond(U, V) = \max_\rho \|(U \otimes I)\rho(U \otimes I)^\dagger - (V \otimes I)\rho(V \otimes I)^\dagger\|_1 \, , \tag{A.2}$$

and the root mean squared trace distance

$$\mathrm{d_{avg}}(U, V) = \sqrt{\mathop{\mathbb{E}}_{|\psi\rangle}[\mathrm{d_{tr}}(U|\psi\rangle, V|\psi\rangle)^2]} \tag{A.3}$$

where the expectation is taken over Haar measure[2].

Apart from these, we also use the following auxiliary distance metrics. We define the quotient spectral distance

$$d_2'(U,V) = \min_{e^{i\phi}\in U(1)} \|U - e^{i\phi}V\| \tag{A.4}$$

to be the spectral distance $d_2(U,V) = \|U - V\|$ up to a global phase. Similarly, we define the quotient normalized Frobenius distance

$$d_F'(U,V) = \min_{e^{i\phi}\in U(1)} \frac{1}{\sqrt{d}}\|U - e^{i\phi}V\|_F \tag{A.5}$$

as the normalized Frobenius norm distance $d_F(U,V) = \frac{1}{\sqrt{d}}\|U - V\|_F$ up to a global phase.

The following lemma shows that (quotient) spectral distance and diamond distance are equivalent.

Lemma 1 (Spectral and diamond distance of unitaries, variant of [142, Lemma B.5])**.** *For any two d-dimensional unitaries U and V, we have*

$$\frac{1}{\sqrt{2}} d_2'(U,V) \le \frac{1}{2}\,\mathrm{d}_\diamond(U,V) \le d_2'(U,V) \le \|U - V\|. \tag{A.6}$$

Proof. Since stabilization is not necessary for computing the diamond distance of two unitary channels [143], we have

$$\begin{aligned}
\frac{1}{2}\,\mathrm{d}_\diamond(U,V) &= \max_{|\psi\rangle} \frac{1}{2}\|U|\psi\rangle\langle\psi|U^\dagger - V|\psi\rangle\langle\psi|V^\dagger\|_1 = \max_{|\psi\rangle}\sqrt{1 - |\langle\psi|U^\dagger V|\psi\rangle|^2}\\
&= \max_{|\psi\rangle}\sqrt{(1 + |\langle\psi|U^\dagger V|\psi\rangle|)(1 - |\langle\psi|U^\dagger V|\psi\rangle|)} \ge \max_{|\psi\rangle}\frac{1}{\sqrt{2}}\sqrt{2(1 - |\langle\psi|U^\dagger V|\psi\rangle|)}\\
&= \frac{1}{\sqrt{2}}\min_{e^{i\phi}\in U(1)}\max_{|\psi\rangle}\|U|\psi\rangle - e^{i\phi}V|\psi\rangle\|_2 = \frac{1}{\sqrt{2}}\min_{e^{i\phi}\in U(1)}\|U - e^{i\phi}V\| = \frac{1}{\sqrt{2}}d_2'(U,V),
\end{aligned} \tag{A.7}$$

where we have used $\left|\langle\psi|U^\dagger V|\psi\rangle\right| \ge 0$ and the standard conversion between trace distance and fidelity. This proves the first inequality. Similarly, we have

$$\begin{aligned}
\frac{1}{2}\,\mathrm{d}_\diamond(U,V) &= \max_{|\psi\rangle} \frac{1}{2}\|U|\psi\rangle\langle\psi|U^\dagger - V|\psi\rangle\langle\psi|V^\dagger\|_1 = \max_{|\psi\rangle}\sqrt{1 - |\langle\psi|U^\dagger V|\psi\rangle|^2}\\
&= \max_{|\psi\rangle}\sqrt{(1 + |\langle\psi|U^\dagger V|\psi\rangle|)(1 - |\langle\psi|U^\dagger V|\psi\rangle|)} \le \max_{|\psi\rangle}\sqrt{2(1 - |\langle\psi|U^\dagger V|\psi\rangle|)}\\
&= \min_{e^{i\phi}\in U(1)}\max_{|\psi\rangle}\|U|\psi\rangle - e^{i\phi}V|\psi\rangle\|_2 = \min_{e^{i\phi}\in U(1)}\|U - e^{i\phi}V\| = d_2'(U,V),
\end{aligned} \tag{A.8}$$

where we have used $\left|\langle\psi|U^\dagger V|\psi\rangle\right| \le 1$, proving the second inequality. The third inequality follows immediately from $d_2'(U,V) = \min_{e^{i\phi}\in U(1)}\|U - e^{i\phi}V\| \le \|U - V\|$. □

We will also utilize the subadditivity of the diamond distance.

Lemma 2 (Subadditivity of diamond distance [144, Prop. 3.48])**.** *For any d-dimensional unitaries U_1, U_2, V_1, V_2, we have the following inequality:*

$$\mathrm{d}_\diamond(U_2U_1, V_2V_1) \le \mathrm{d}_\diamond(U_2, V_2) + \mathrm{d}_\diamond(U_1, V_1). \tag{A.9}$$

From the standard relationship between different p-norms, we have the following relation between d_2' and d_F'.

Lemma 3 (Norm conversion between quotient spectral and normalized Frobenius distance)**.** *For any two d-dimensional unitaries U and V, we have*

$$\frac{1}{\sqrt{d}} d_2'(U,V) \le d_F'(U,V) \le d_2'(U,V). \tag{A.10}$$

[2] Due to the concentration of Lipschitz functions on inputs drawn from the Haar measure, controlling this root mean squared distance also leads to error bounds that hold with high probability over random input states.

Proof. For any $e^{i\phi} \in U(1)$, the standard relation between matrix norms gives us

$$\|U - Ve^{i\phi}\| \leq \|U - Ve^{i\phi}\|_F \leq \sqrt{d}\|U - Ve^{i\phi}\|. \tag{A.11}$$

Taking the minimum of $\|U - Ve^{i\phi}\|_F$ over $e^{i\phi}$ in the first inequality and dividing by $\sqrt{d}$, we obtain

$$\frac{1}{\sqrt{d}} d_2'(U,V) \leq \frac{1}{\sqrt{d}}\|U - Ve^{i\phi}\| \leq d_F'(U,V). \tag{A.12}$$

Similarly, taking the minimum of $\|U - Ve^{i\phi}\|$ over $e^{i\phi}$ in the second inequality and dividing by $\sqrt{d}$ yields

$$d_F'(U,V) \leq \frac{1}{\sqrt{d}}\|U - Ve^{i\phi}\|_F \leq d_2'(U,V). \tag{A.13}$$

Thus we have the desired results. □

The following lemma collects some useful properties of d_F' and in particular shows that d_F' and $\mathrm{d_{avg}}$ are equivalent.

Lemma 4 (Properties of quotient normalized Frobenius distance)**.** *For any two d-dimensional unitaries U and V, we have:*

1. $\frac{1}{2}d_F'(U,V) \leq \mathrm{d_{avg}}(U,V) \leq d_F'(U,V)$.
2. *For any integer $p \geq 1$, $d_F'(U^p, V^p) \leq p d_F'(U,V)$.*
3. *For any integer $p \geq 1$, if $d_F'(U,I), d_F'(V,I) \leq \frac{4/(25\pi)}{\sqrt{d}}$, then $d_F'(U^{1/p}, V^{1/p}) \leq \frac{2}{p} d_F'(U,V)$.*

Item 3 can be viewed as a version of [21, Lemma 3.1].

Proof. Item 1: From properties of the Haar integral (see e.g., [145, Example 50]), we have

$$\mathrm{d_{avg}}(U,V)^2 = 1 - \frac{d + |\operatorname{tr}(U^\dagger V)|^2}{d(d+1)}. \tag{A.14}$$

On the other hand, we have

$$d_F'^2(U,V) = \min_{e^{i\phi}\in U(1)} \frac{1}{d}\|U - Ve^{i\phi}\|_F^2 = \min_{e^{i\phi}\in U(1)} 2 - \frac{2}{d}\mathrm{Re}[\operatorname{tr}(U^\dagger V e^{i\phi})] = 2 - \frac{2}{d}|\operatorname{tr}(U^\dagger V)|. \tag{A.15}$$

Combining them, we get

$$\mathrm{d_{avg}}(U,V)^2 = \frac{d}{d+1} d_F'^2(U,V)\left(1 - \frac{d_F'^2(U,V)}{4}\right) \in \left[\frac{1}{4}d_F'^2(U,V), d_F'^2(U,V)\right], \tag{A.16}$$

because $d_F'^2(U,V) \in [0,2]$. Thus we have established Item 1.

Item 2: From triangle inequality, we have

$$d_F'(U^p, V^p) \leq \sum_{k=1}^p d_F'(U^{p+1-k}V^{k-1}, U^{p-k}V^k) = \sum_{k=1}^p d_F'(U,V) = p d_F'(U,V), \tag{A.17}$$

where we have used the unitary invariance of d_F'. This proves Item 2.

Item 3: We first prove the following modified version without the global phase: "If $d_F(U,I), d_F(V,I) \leq \frac{4/(5\pi)}{\sqrt{d}}$, then $d_F(U^{1/p}, V^{1/p}) \leq \frac{2}{p} d_F(U,V)$." Let $U = e^X, V = e^Y$ with $\|X\|, \|Y\| \leq \pi$. We can refine the bound on $\|X\|, \|Y\|$ by noting the following

$$\|X\| \leq \frac{\pi}{2}\|e^X - I\| \leq \frac{\pi}{2}\|U - I\|_F = \frac{\pi\sqrt{d}}{2} d_F(U,I) \leq \frac{2}{5}, \tag{A.18}$$

where the first inequality can be seen from eigenvalue analysis as follows: Let $i\theta_k$ be the eigenvalues of X with $|\theta_k| \leq \pi$. Then we have

$$\|X\| = \max_k |\theta_k| \leq \pi \max_k \left|\sin\frac{\theta_k}{2}\right| = \frac{\pi}{2}\max_k \left|e^{i\theta_k} - 1\right| = \frac{\pi}{2}\|e^X - I\|. \tag{A.19}$$

Similarly, we have $\|Y\| \le 2/5$.

Next, we prove the following inequality when $\|X\|, \|Y\| \le 2/5$ (similar to [146, Appendix D]):

$$\frac{1}{2}\|X-Y\|_F \le \|e^X - e^Y\|_F \le \|X-Y\|_F. \tag{A.20}$$

For the upper bound, we use the triangle inequality and a telescoping sum representation: For any $m \in \mathbb{N}$,

$$\|e^X - e^Y\|_F \le \sum_{k=1}^{m} \|e^{(k-1)X/m}(e^{X/m} - e^{Y/m})e^{(m-k)Y/m}\|_F = m\|e^{X/m} - e^{Y/m}\|_F\,, \tag{A.21}$$

and by taking $m \to \infty$ we arrive at the upper bound. For the lower bound, note that by triangle inequality, we have

$$\|e^X - e^Y\|_F = \left\|\sum_{k=1}^{\infty}\frac{1}{k!}(X^k - Y^k)\right\|_F \ge \|X-Y\|_F - \left\|\sum_{k=2}^{\infty}\frac{1}{k!}(X^k - Y^k)\right\|_F. \tag{A.22}$$

The second term can be upper bounded by

$$\begin{aligned}\left\|\sum_{k=2}^{\infty}\frac{1}{k!}(X^k - Y^k)\right\|_F &= \left\|\sum_{k=2}^{\infty}\sum_{l=1}^{k}\frac{1}{k!}X^{l-1}(X-Y)Y^{k-l}\right\|_F\\ &\le \sum_{k=2}^{\infty}\frac{k}{k!}\left(\frac{2}{5}\right)^k \|X-Y\|_F\\ &= (e^{2/5}-1)\|X-Y\|_F\,,\end{aligned} \tag{A.23}$$

where we have used $\|AB\|_F \le \|A\| \cdot \|B\|_F$ and $\|X\|, \|Y\| \le 2/5$. Plugging this bound back in, we arrive at the lower bound

$$\|e^X - e^Y\|_F \ge (2 - e^{2/5})\|X-Y\|_F \ge \frac{1}{2}\|X-Y\|_F. \tag{A.24}$$

Equation (A.20) in particular implies

$$d_F(U^{1/p}, V^{1/p}) \le \frac{1}{p\sqrt{d}}\|X-Y\|_F \le \frac{2}{p}d_F(U,V)\,, \tag{A.25}$$

and thus the modified version of our claim.

Finally, we deal with the global phase and prove the d'_F version, where we assume $d'_F(U,I), d'_F(V,I) \le \frac{4/(25\pi)}{\sqrt{d}}$. Let $e^{i\phi_U}, e^{i\phi_V}, e^{i\phi} \in U(1)$ denote the global phases that minimize $d_F(U, Ie^{i\phi_U}), d_F(V, Ie^{i\phi_V})$ and $d_F(Ue^{-i\phi_U}, Ve^{-i\phi_V}e^{i\phi})$, respectively. Then $d_F(U, Ie^{i\phi_U}), d_F(V, Ie^{i\phi_V}) \le \frac{4/(25\pi)}{\sqrt{d}}$ by assumption, and $d_F(Ue^{-i\phi_U}, Ve^{-i\phi_V}) \le d_F(U, Ie^{i\phi_U}) + d_F(V, Ie^{i\phi_V}) \le \frac{8/(25\pi)}{\sqrt{d}}$. Therefore,

$$\begin{aligned}d_F(e^{i\phi}, I) &\le d_F(e^{i\phi}, (Ve^{-i\phi_V})^\dagger(Ue^{-i\phi_U})) + d_F((Ve^{-i\phi_V})^\dagger(Ue^{-i\phi_U}), I)\\ &= d_F(Ue^{-i\phi_U}, Ve^{-i\phi_V}e^{i\phi}) + d_F(Ue^{-i\phi_U}, Ve^{-i\phi_V})\\ &\le 2d_F(Ue^{-i\phi_U}, Ve^{-i\phi_V})\\ &\le \frac{16/(25\pi)}{\sqrt{d}}.\end{aligned} \tag{A.26}$$

This means that $d_F(Ue^{-i\phi_U}e^{-i\phi}, I) \le d_F(U, Ie^{i\phi_U}) + d_F(e^{i\phi}, I) \le \frac{(4+16)/(25\pi)}{\sqrt{d}} = \frac{4/(5\pi)}{\sqrt{d}}$. We also know that $d_F(Ve^{-i\phi_V}, I) \le \frac{4/(25\pi)}{\sqrt{d}} \le \frac{4/(5\pi)}{\sqrt{d}}$. Thus the two matrices $Ue^{-i\phi_U}e^{-i\phi}$ and $Ve^{-i\phi_V}$ satisfy the condition of the modified version without global phase, and we thus have

$$\begin{aligned}d'_F(U^{1/p}, V^{1/p}) &\le d'_F(U^{1/p}, V^{1/p}(e^{-i\phi_V})^{1/p}(e^{i\phi_U})^{1/p}(e^{i\phi})^{1/p})\\ &= d_F((Ue^{-i\phi_U}e^{-i\phi})^{1/p}, (Ve^{-i\phi_V})^{1/p})\\ &\le \frac{2}{p}d_F(Ue^{-i\phi_U}e^{-i\phi}, Ve^{-i\phi_V}) = d'_F(U,V).\end{aligned} \tag{A.27}$$

This concludes the proof of Item 3. □

Haar-random states are in general hard to generate. One may want to use other ensembles of input states and the associated distance metric for average-case learning. A class of ensembles of physical interest is that of locally scrambled ensembles [64, 65] defined as follows:

Definition 1 (Locally scrambled ensembles up to the second moment)**.** *An ensemble $\mathcal{S}$ of (i.e., a distribution over) n-qubit states is called a locally scrambled ensemble up to the second moment if it is of the form $\mathcal{S} = \mathcal{U}\left|0\right\rangle^{\otimes n}$, where $\mathcal{U}$ is an ensemble of unitaries that is locally scrambled up to the second moment. That is, there exists another unitary ensemble $\mathcal{U}'$, such that: (1) for any U' randomly sampled from $\mathcal{U}'$ and for any tensor product of single-qubit unitaries $\otimes_{i=1}^{n} U_i$, $U' \otimes_{i=1}^{n} U_i$ follows the same distribution of $\mathcal{U}'$; and (2) for any $2n$-qubit density matrices ρ, we have $\mathbb{E}_{U\sim\mathcal{U}}[U^{\otimes 2}\rho(U^\dagger)^{\otimes 2}] = \mathbb{E}_{U'\sim\mathcal{U}'}[U'^{\otimes 2}\rho(U'^\dagger)^{\otimes 2}]$. We use $\mathbb{S}_{\mathrm{LS}}^{(2)}$ to denote the set of all such state ensembles.*

Notable examples of these ensembles include n-qubit Haar-random states, products of Haar-random single-qubit states, products of random single-qubit stabilizer states, 2-designs on n-qubit states, and output states of random local quantum circuits with any fixed architecture. The following lemma from the study of out-of-distribution generalization [66] shows that these ensembles lead to mutually equivalent average-case distance metrics.

Lemma 5 (Equivalence of locally scrambled average-case distances [66, Theorem 1])**.** *We denote by $d_P(U,V) = \sqrt{\mathbb{E}_{\left|\psi\right\rangle\sim P}[\mathrm{d_{tr}}(U\left|\psi\right\rangle, V\left|\psi\right\rangle)^2]}$ the root mean squared trace distance with respect to an ensemble P. For any $P, Q \in \mathbb{S}_{\mathrm{LS}}^{(2)}$ and for any unitaries U, V, we have*

$$\frac{1}{\sqrt{2}} d_Q(U,V) \leq d_P(U,V) \leq \sqrt{2} d_Q(U,V). \tag{A.28}$$

The following lemma shows that the triangle inequality holds for d_P (and in particular, $\mathrm{d_{avg}}$).

Lemma 6 (Triangle inequality for average-case distance)**.** *Let $d_P(U,V) = \sqrt{\mathbb{E}_{\left|\psi\right\rangle\sim P}[\mathrm{d_{tr}}(U\left|\psi\right\rangle, V\left|\psi\right\rangle)^2]}$ be the root mean squared trace distance with respect to an ensemble P. For any three unitaries U, V and W, we have the triangle inequality*

$$d_P(U,V) \leq d_P(U,W) + d_P(W,V). \tag{A.29}$$

Proof. Note that

$$\begin{aligned}
d_P^2(U,V) &= \mathbb{E}_{\left|\psi\right\rangle\sim P}[\mathrm{d_{tr}}(U\left|\psi\right\rangle, V\left|\psi\right\rangle)^2] \leq \mathbb{E}_{\left|\psi\right\rangle\sim P}[(\mathrm{d_{tr}}(U\left|\psi\right\rangle, W\left|\psi\right\rangle) + \mathrm{d_{tr}}(W\left|\psi\right\rangle, V\left|\psi\right\rangle))^2] \\
&= d_P^2(U,W) + d_P^2(W,V) + 2\mathbb{E}_{\left|\psi\right\rangle\sim P}[\mathrm{d_{tr}}(U\left|\psi\right\rangle, W\left|\psi\right\rangle)\,\mathrm{d_{tr}}(W\left|\psi\right\rangle, V\left|\psi\right\rangle)] \\
&\leq d_P^2(U,W) + d_P^2(W,V) + 2\sqrt{\mathbb{E}_{\left|\psi\right\rangle\sim P}[\mathrm{d_{tr}}(U\left|\psi\right\rangle, W\left|\psi\right\rangle)^2]} \cdot \sqrt{\mathbb{E}_{\left|\psi\right\rangle\sim P}[\mathrm{d_{tr}}(W\left|\psi\right\rangle, V\left|\psi\right\rangle)^2]} \\
&= \left(d_P(U,W) + d_P(W,V)\right)^2,
\end{aligned} \tag{A.30}$$

where we have used the triangle inequality for $\mathrm{d_{tr}}$ and the Cauchy-Schwartz inequality. Taking the square root gives us the desired result. □

2. Covering and packing nets

Our results in state and unitary learning utilize a tool from high-dimensional probability theory, namely covering and packing nets. We employ covering nets in our proofs of the sample complexity upper bounds and packing nets in our proofs of sample complexity lower bounds. Intuitively, covering and packing nets characterize the complexity of a space by discretizing it with small balls of a given resolution. We formally define these concepts below.

Definition 2 (Covering net/number and metric entropy)**.** *Let (X, d) be a metric space. Let $K \subseteq X$ be a subset and $\epsilon > 0$. Then, define the following.*

- *$N \subseteq K$ is an* ϵ-covering net *of K if for any $x \in K$, there exists a $y \in N$ such that $d(x,y) \leq \epsilon$.*
- *The* covering number *$\mathcal{N}(K, d, \epsilon)$ of K is the smallest possible cardinality of an ϵ-covering net of K.*
- *The* metric entropy *is $\log \mathcal{N}(K, d, \epsilon)$.*

We can similarly define a packing net.

Definition 3 (Packing net/number). *Let (X, d) be a metric space. Let $K \subseteq X$ be a subset and $\epsilon > 0$. Then, define the following.*

- *$N \subseteq K$ is an ϵ-*packing net *of K if for any $x, y \in N$, $d(x, y) > \epsilon$.*
- *The* packing number *$\mathcal{M}(K, d, \epsilon)$ of K is the largest possible cardinality of an ϵ-packing net of K.*

The following equivalence between covering and packing numbers is often useful.

Lemma 7 (Covering and packing are equivalent, [48, Section 4.2]). *Let (X, d) be a metric space. Let $K \subseteq X$ and $\epsilon > 0$. We have*

$$\mathcal{N}(K, d, \epsilon/2) \geq \mathcal{M}(K, d, \epsilon) \geq \mathcal{N}(K, d, \epsilon). \tag{A.31}$$

Covering numbers also have the following monotonicity property.

Lemma 8 (Monotonicity of covering number, [48, Section 4.2]). *Let (K, d) be a metric space. If $L \subseteq K$, then $\mathcal{N}(L, d, \epsilon) \leq \mathcal{N}(K, d, \epsilon/2)$.*

For our purposes, we need the following upper and lower bounds on the covering number of the unitary group. Since the states that we consider can be generated by unitaries applied to a fixed input state, a covering number upper bound for unitaries with respect to the diamond distance implies a corresponding covering number upper bound for states with respect to the trace distance.

Lemma 9 (Covering number of the unitary group, [147, Proposition 7], [146, Lemma 1] and [142, Lemma C.1]). *Let $\|\cdot\|'$ be any unitarily invariant norm. there exist universal constants $c_1, c_2 > 0$ such that for any $\epsilon \in (0, 2]$, the covering number of the d-dimensional unitary group $U(d)$ with respect to the norm $\|\cdot\|'$ satisfies:*

$$\left(\frac{c_1}{\epsilon}\right)^{d^2} \leq \mathcal{N}(U(d), \|\cdot\|', \|I\|'\epsilon) \leq \left(\frac{c_2}{\epsilon}\right)^{d^2}. \tag{A.32}$$

In particular, for the spectral norm $\|\cdot\|$, we have the upper bound $\mathcal{N}(U(d), \|\cdot\|, \epsilon) \leq (6/\epsilon)^{2d^2}$. For the Frobenius norm $\|\cdot\|_F$, we have $(c_1/\epsilon)^{d^2} \leq \mathcal{N}(U(d), \|\cdot\|_F, \sqrt{d}\epsilon) \leq (c_2/\epsilon)^{d^2}$.

We can use this result to bound the covering number for n-qubit unitaries consisting of G two-qubit gates.

Theorem 8 (Covering number of G-gate unitaries). *Let $U^G \subseteq U(2^n)$ be the set of n-qubit unitaries that can be implemented by G two-qubit gates. Then for any $\epsilon \in (0, 1]$, there exist universal constants $c_1, c_2, C > 0$ such that for $1 \leq G/C \leq 4^{n+1}$, the metric entropy of U^G with respect to the normalized Frobenius distance d_F can be bounded as*

$$\frac{G}{4C}\log\left(\frac{c_1}{\epsilon}\right) \leq \log\mathcal{N}(U^G, d_F, \epsilon) \leq 16G\log\left(\frac{c_2 G}{\epsilon}\right) + 2G\log n. \tag{A.33}$$

Moreover, the metric entropy with respect to diamond distance $\mathrm{d}_\diamond$ can be explicitly upper bounded by

$$\log\mathcal{N}(U^G, \mathrm{d}_\diamond, \epsilon) \leq 32G\log\left(\frac{12G}{\epsilon}\right) + 2G\log n. \tag{A.34}$$

Proof. The proof of the upper bounds is similar to the proof of Theorem C.1 in [142]. We first prove the upper bound for diamond distance.

Let $\epsilon \in (0, 1]$, and define $\epsilon' = \epsilon/2G$. Then by Lemma 9, there exists an ϵ'-covering net $\tilde{\mathcal{N}}_{\epsilon'}$ of the set of two-qubit unitaries $U(2^2)$ with respect to the spectral norm $\|\cdot\|$ of size

$$|\tilde{\mathcal{N}}_{\epsilon'}| \leq \left(\frac{6}{\epsilon'}\right)^{32} = \left(\frac{12G}{\epsilon}\right)^{32}. \tag{A.35}$$

This bound applies when the two-qubit unitary acts on a fixed set of two qubits. We can consider two-qubit unitaries that act on any of the n qubits. Let $U^{2q} \subset U(2^n)$ denote this set of two-qubit unitaries that can act on any pair of the n qubits of the system. Because there are $\binom{n}{2}$ pairs of qubits that the unitary could act on, the size of the covering net $\tilde{\mathcal{N}}_{\epsilon',n}$ of U^{2q} is bounded by

$$|\tilde{\mathcal{N}}_{\epsilon',n}| \leq \binom{n}{2}\left(\frac{12G}{\epsilon}\right)^{32}. \tag{A.36}$$

Recall that we want to find a covering net for the set U^G of n-qubit unitaries consisting of G two-qubit gates. Any unitary $U \in U^G$ can be written as $U_G U_{G-1}...U_1$ for $U_i \in U^{2q}$, where we suppress the tensor product with identity for readability. We consider the set of unitaries obtained by multiplying elements of the covering net $\tilde{\mathcal{N}}_{\epsilon',n}$ of U^{2q}. Namely, we define

$$\mathcal{N}_\epsilon \triangleq \{U_G U_{G-1}...U_1 | U_i \in \tilde{\mathcal{N}}_{\epsilon',n}, 1 \leq i \leq G\}. \tag{A.37}$$

Let $U \in U^G$ be any arbitrary unitary that can be implemented by G two-qubit gates, i.e., it can be written as $U = U_G U_{G-1}...U_1$ for $U_i \in U^{2q}$. As $\tilde{\mathcal{N}}_{\epsilon',n}$ is an ϵ'-covering net of the set U^{2q} of two-qubit unitaries, for each U_i comprising the circuit U, we can find a $\tilde{U}_i \in \tilde{\mathcal{N}}_{\epsilon',n}$ such that $\|U_i - \tilde{U}_i\| \leq \epsilon'$ for all $1 \leq i \leq G$, where $\|\cdot\|$ denotes the spectral norm. Then, the unitary $\tilde{U} \triangleq \tilde{U}_G \tilde{U}_{G-1}...\tilde{U}_1 \in \mathcal{N}_{\epsilon_1}$ satisfies

$$\mathrm{d}_\diamondsuit(U, \tilde{U}) \leq \sum_{i=1}^{G} \mathrm{d}_\diamondsuit(U_i, \tilde{U}_i) \leq 2\sum_{i=1}^{G} \left\| U_i - \tilde{U}_i \right\| \leq 2G\epsilon' = \epsilon, \tag{A.38}$$

where we have employed the subadditivity of the diamond distance (Lemma 2) in the first inequality and then used the relationship between the diamond norm and spectral norm in the second inequality (Lemma 1). In the last inequality, we used that $\left\|U_i - \tilde{U}_i\right\| \leq \epsilon'$ and $\epsilon' = \epsilon/2G$.

Thus, $\mathcal{N}_\epsilon$ is an ϵ-covering net of the set U^G of n-qubit unitaries that can be implemented by G two-qubit gates with respect to the diamond distance. By definition of $\mathcal{N}_\epsilon$, we have $|\mathcal{N}_\epsilon| = |\tilde{\mathcal{N}}_{\epsilon',n}|^G$, since each unitary in the length G strings of unitaries comprising elements of $\mathcal{N}_\epsilon$ are chosen from $\tilde{\mathcal{N}}_{\epsilon',n}$. Then

$$|\mathcal{N}_\epsilon| \leq \binom{n}{2}^G \left(\frac{12G}{\epsilon}\right)^{32G} \leq n^{2G}\left(\frac{12G}{\epsilon}\right)^{32G}. \tag{A.39}$$

Taking the logarithm gives the desired result for diamond distance.

We can argue similarly for the normalized Frobenius distance d_F. Specifically, we make use of the subadditivity of $\|\cdot\|_F$: $\forall U_1, V_1, U_2, V_2 \in U(2^n)$, we have

$$\|U_2U_1 - V_2V_1\|_F \leq \|U_2U_1 - U_2V_1\|_F + \|U_2V_1 - V_2V_1\|_F = \|U_1 - V_1\|_F + \|U_2 - V_2\|_F, \tag{A.40}$$

where we have used triangle inequality and $\|\cdot\|_F$ being unitary invariant.

Consider any $U \in U^G, U = U_G \cdots U_1$, where $U_i, 1 \leq i \leq T$ are 2-qubit unitaries acting on some pair of qubits. Take $\epsilon' = \epsilon/G$ and let $\mathcal{N}_{\epsilon'}$ be an ϵ'-covering net of $U(2^2)$ with respect to $\|\cdot\|_F$. Then there exist $V_i \in \mathcal{N}, 1 \leq i \leq G$, such that $\|U_i - V_i\| \leq \epsilon/G$ when the V_i are placed on the corresponding qubits. Let $V = V_G \cdots V_1$. By sub-additivity, we have

$$\|U - V\|_F \leq \sum_{i=1}^{G} \sqrt{2^{n-2}}\|U_i - V_i\|_F \leq \sqrt{2^{n-2}}G\epsilon' = \sqrt{2^{n-2}}\epsilon, \tag{A.41}$$

where we have used the facts that the Frobenius norm is multiplicative w.r.t. tensor products and that an $(n-2)$-qubit identity has Frobenius norm equal to $\sqrt{2^{n-2}}$. Therefore, the set of $V = V_G \cdots V_1$, where $V_i \in U(2^2)$ and acting on all possible pair of qubits is a $(2^{n-2}\epsilon)$-covering net of U^G. Since the number of choices for qubits to act on is $\binom{n}{2}$ for each V_i, we have

$$\mathcal{N}(U^G, \|\cdot\|_F, \sqrt{2^{n-2}}\epsilon) \leq \left[\binom{n}{2}\mathcal{N}(U(2^2), \|\cdot\|_F, \epsilon/G)\right]^G \leq n^{2G}\left(\frac{c_2 G\sqrt{2^2}}{\epsilon}\right)^{16G}, \tag{A.42}$$

where we have used Lemma 9. Redefining ϵ to be $\epsilon/\sqrt{2^2}$ and switching to the normalized d_F, we obtain

$$\log \mathcal{N}(U^G, d_F, \epsilon) \leq 16G \log\left(\frac{c_2 G}{\epsilon}\right) + 2G\log n. \tag{A.43}$$

Finally, we prove the lower bound. For this, we consider a particular set of circuit structures where all the G gates are placed on the first $k \leq n$ qubits. The set of unitaries that can be implemented by such circuits is denoted by $U_G^{\leq k} \subseteq U^G$. From the theory of universal quantum gates (see [136]), we know that to implement an arbitrary k-qubit unitary, we only need $G_k = \mathcal{O}(4^k)$ two-qubit gates that can implement single-qubit gates and CNOT. That is, there exists a universal constant $C > 0$, such that $C4^k \geq G_k$. Therefore, for any integer $k \leq n$ satisfying $C4^k \leq G$, we have $G \geq G_k$. Then all possible k-qubit unitaries can be implemented with these G gates: $U^n(2^k) = \{U \otimes I_{2^{n-k}} : U \in U(2^k)\} \subseteq U_G^{\leq k} \subseteq U^G$, where $U^n(2^k)$ denotes the set obtained by embedding the k-qubit unitaries into the n-qubit unitaries via tensor-multiplication with the identity. Thus $\mathcal{N}(U^G, \|\cdot\|_F, \epsilon) \geq \mathcal{N}(U^n(2^k), \|\cdot\|_F, 2\epsilon)$ by monotonicity.

Next, we prove that $\mathcal{N}(U^n(2^k), \|\cdot\|_F, 2\epsilon) \geq \mathcal{N}(U(2^k), \|\cdot\|_F, 2\epsilon/\sqrt{2^{n-k}})$. To do this, we take a minimal 2ϵ-covering net $\mathcal{N}$ of $U^n(2^k)$ with $|\mathcal{N}| = \mathcal{N}(U^n(2^k), \|\cdot\|_F, 2\epsilon)$. Hence $\forall U \in U(2^k)$, $U \otimes I_{2^{n-k}} \in U^n(2^k)$, $\exists V \otimes I_{2^{n-k}} \in \mathcal{N}$, such that $\|U - V\|_F = \|U \otimes I_{2^{n-k}} - V \otimes I_{2^{n-k}}\|_F/\sqrt{2^{n-k}} \leq 2\epsilon/\sqrt{2^{n-k}}$. Therefore, $\{V : V \otimes I_{2^{n-k}} \in \mathcal{N}\}$ forms a $2\epsilon/\sqrt{2^{n-k}}$-covering net of $U(2^k)$, and we have $\mathcal{N}(U^n(2^k), \|\cdot\|_F, 2\epsilon) \geq \mathcal{N}(U(2^k), \|\cdot\|_F, 2\epsilon/\sqrt{2^{n-k}})$.

Combining the above inequalities, we have

$$\log \mathcal{N}(U^G, \|\cdot\|_F, \epsilon) \geq \log \mathcal{N}(U^n(2^k), \|\cdot\|_F, 2\epsilon) \geq \log \mathcal{N}(U(2^k), \|\cdot\|_F, 2\epsilon/\sqrt{2^{n-k}}) \geq 2^{2k} \log \frac{c_1\sqrt{2^n}}{2\epsilon}, \quad \text{(A.44)}$$

where the last inequalities follow from Lemma 9. The largest possible k is given by $k = \lfloor \log_4(G/C) \rfloor \geq \log_4 G/(4C)$. Thus, by redefining ϵ to be $\epsilon/\sqrt{2^n}$ and switching to d_F, we arrive at

$$\log \mathcal{N}(U^G, d_F, \epsilon) \geq \frac{G}{4C} \log \frac{c_1}{2\epsilon}. \quad \text{(A.45)}$$

This completes the proof of Theorem 8. □

The d_F covering number bounds in Theorem 8 do not yet properly take into account the global $U(1)$ phase. To obtain covering number for the average-case distance d_{avg}, which is equivalent to the quotient normalized Frobenius distance d'_F (Lemma 4 Item 1), we need to quotient out the global phase. This is formalized in the following lemma.

Lemma 10 (Packing number of quotient distance metric, variant of [146, Lemma 4])**.** *For any d-dimensional unitaries U and V, let $d_F(U,V) = \|U - V\|_F/\sqrt{d}$ be the normalized Frobenius distance, and $d'_F(U,V) = \min_{W \in U(1)} d_F(U, VW)$ be the corresponding quotient distance. Then there exists a universal constant $c_2 > 0$ such that the packing number of any set $\mathcal{U} \subseteq U(d)$ with respect to d_F and d'_F satisfies*

$$\log \mathcal{M}(\mathcal{U}, d_F, 4\epsilon) - \log(c_2/\epsilon) \leq \log \mathcal{M}(\mathcal{U}, d'_F, \epsilon) \leq \log \mathcal{M}(\mathcal{U}, d_F, \epsilon). \quad \text{(A.46)}$$

Proof. We focus on the lower bound first. Take a minimal ϵ-covering $\mathcal{N}_1$ of $\mathcal{U}$ with respect to d'_F and a minimal ϵ-covering $\mathcal{N}_2$ of $U(1)$ with respect to the absolute value distance $d_A(e^{i\phi}, e^{-i\phi'}) = |e^{i\phi} - e^{-i\phi'}|$. Then, for any $U \in \mathcal{U}$, there exists $V \in \mathcal{N}_1$ such that $d'_F(U,V) \leq \epsilon$. Let $e^{i\phi^\star} = \arg\min_{e^{i\phi}} d_F(U, Ve^{i\phi})$. Then $d_F(U, Ve^{i\phi^\star}) \leq \epsilon$, and there exists $e^{i\phi'} \in \mathcal{N}_2$ such that $d_A(e^{i\phi^\star}, e^{i\phi'}) \leq \epsilon$. Therefore,

$$d_F(U, Ve^{i\phi'}) \leq d_F(U, Ve^{i\phi^\star}) + d_F(Ve^{i\phi^\star}, Ve^{i\phi'}) = d_F(U, Ve^{i\phi^\star}) + d_F(Ie^{i\phi^\star}, Ie^{i\phi'}) \leq 2\epsilon, \quad \text{(A.47)}$$

where we have used the triangle inequality, d_F being unitary invariant, and $d_F(Ie^{i\phi^\star}, Ie^{i\phi'}) = \frac{1}{\sqrt{d}}\|Ie^{i\phi^\star} - Ie^{i\phi'}\|_F = \frac{\|I\|_F}{\sqrt{d}}|e^{i\phi^\star} - e^{i\phi'}| = d_A(e^{i\phi^\star}, e^{i\phi'}) \leq \epsilon$. Hence, the set $\{Ve^{i\phi'} : V \in \mathcal{N}_1, e^{i\phi'} \in \mathcal{N}_2\}$ is a (2ϵ)-covering of $\mathcal{U}$ with respect to d_F. Then

$$\mathcal{N}(\mathcal{U}, d_F, 2\epsilon) \leq \mathcal{N}(\mathcal{U}, d'_F, \epsilon)\mathcal{N}(U(1), d_A, \epsilon). \quad \text{(A.48)}$$

Therefore, using the equivalence of covering and packing (Lemma 7) and the covering number bound for $U(1)$ (Lemma 9), we arrive at

$$\log \mathcal{M}(\mathcal{U}, d'_F, \epsilon) \geq \log \mathcal{M}(\mathcal{U}, d'_F, 4\epsilon) - \log(c_2/\epsilon). \quad \text{(A.49)}$$

For the upper bound, note that $\forall U, V \in \mathcal{U}$, we have

$$d'_F(U,V) = \min_{e^{i\phi} \in U(1)} d_F(U, Ve^{i\phi}) \leq d_F(U,V). \quad \text{(A.50)}$$

Therefore, a maximal ϵ-packing net with respect to d'_F is an ϵ-packing net with respect to d_F. Therefore,

$$\mathcal{M}(\mathcal{U}, d'_F, \epsilon) \leq \mathcal{M}(\mathcal{U}, d_F, \epsilon). \quad \text{(A.51)}$$

This concludes the proof of Lemma 10. □

With Lemma 10, we can obtain the covering number of G-gate unitaries with respect to the average-case distance.

Corollary 1 (Covering number with average-case distance)**.** *Let $U^G \subseteq U(2^n)$ be the set of n-qubit unitaries that can be implemented by G two-qubit gates. Then for any $\epsilon \in (0,1]$, there exist universal constants $c_1, c_2, C > 0$ such that for $1 \leq G/C \leq 4^{n+1}$, the metric entropy of U^G with respect to the average-case distance $\mathrm{d}_{\mathrm{avg}}(U,V) = \sqrt{\mathbb{E}_{|\psi\rangle}[\mathrm{d}_{\mathrm{tr}}(U|\psi\rangle, V|\psi\rangle)^2]}$, where the expectation value is over Haar measure, can be bounded as*

$$\frac{G}{4C}\log\left(\frac{c_1}{8\epsilon}\right) - \log\left(\frac{c_2}{2\epsilon}\right) \leq \log \mathcal{N}(U^G, \mathrm{d}_{\mathrm{avg}}, \epsilon) \leq 16G\log\left(\frac{c_2 G}{\epsilon}\right) + 2G\log n. \tag{A.52}$$

Proof. The corollary follows directly from Theorem 8, Lemma 10, and the equivalence of d'_F and $\mathrm{d}_{\mathrm{avg}}$ (Lemma 4 Item 1). □

3. Classical shadows and hypothesis selection

Our proofs of the sample complexity upper bounds crucially rely on a known algorithm for quantum hypothesis selection [148]. The high-level idea is to find a covering net over all unitaries consisting of only G two-qubit gates and to then use quantum hypothesis selection to identify a candidate in the covering net close to the unknown target state/unitary. A similar idea has previously appeared in [103]. In this section, we discuss the quantum hypothesis selection algorithm from [148] and prove a performance guarantee when basing it on classical shadow tomography [100].

The quantum hypothesis selection algorithm takes as input (classical descriptions of) a set of hypothesis states $\sigma_1, \ldots, \sigma_m$ and quantum copies of an unknown state ρ. Using these copies, the algorithm identifies a hypothesis state σ_k that is close to the unknown state ρ in trace distance. Importantly, quantum hypothesis selection black-box reduces to shadow tomography [37], i.e., one can use the shadow tomography protocol as a black-box to solve quantum hypothesis selection. To obtain a better sample complexity scaling, we instead utilize classical shadow tomography [100].

Recall that a classical shadow is a succinct classical description of a quantum state that allows us to predict many expectation values accurately. One can construct this classical shadow description by applying a random unitary to the quantum state and measuring in the computational basis. The most prevalent examples are random Clifford measurements, where the random unitary is chosen to be a random Clifford circuit, or random Pauli measurements, where the random unitary is chosen to be a tensor product of random Pauli gates. Moreover, we have the following rigorous guarantee for using classical shadows to predict expectation values.

Theorem 9 (Theorem 1 in [100])**.** *Let $O_1, \ldots, O_M$ be Hermitian $2^n \times 2^n$ matrices, and let $\epsilon, \delta \in [0,1]$. Then,*

$$N = \mathcal{O}\left(\frac{\log(M/\delta)}{\epsilon^2} \max_{1\leq i \leq M} \left\| O_i - \frac{\mathrm{tr}(O_i)}{2^n}\mathbb{I} \right\|_{\mathrm{shadow}}^2\right) \tag{A.53}$$

copies of an unknown quantum state ρ suffice to predict $\hat{o}_i$ such that

$$|\hat{o}_i - \mathrm{tr}(O_i\rho)| \leq \epsilon \tag{A.54}$$

for all $1 \leq i \leq M$, with probability at least $1-\delta$.

Here, $\|\cdot\|_{\mathrm{shadow}}$ denotes the shadow norm, which depends on the ensemble of unitary transformations used to create the classical shadow. For instance, in the case of random Cliffords, the shadow norm can be controlled via the (unnormalized) Frobenius norm, compare [100, Proposition S1].

Now, we can prove a new guarantee for the quantum hypothesis selection by replacing shadow tomography with classical shadow in the proof in [148].

Proposition 1 (Proposition 5.3 in [148]; Classical Shadow Version)**.** *Let $0 < \epsilon, \delta < 1/2$. Given access to unentangled copies of a pure quantum state ρ and classical descriptions of m fixed pure hypothesis states $\sigma_1, \ldots, \sigma_m$, there exists a quantum algorithm that selects σ_k such that $\mathrm{d}_{\mathrm{tr}}(\rho, \sigma_k) \leq 3\eta + \epsilon$ with probability at least $1-\delta$, where $\eta = \min_i \mathrm{d}_{\mathrm{tr}}(\rho, \sigma_i)$. Moreover, this algorithm uses*

$$N = \mathcal{O}\left(\frac{\log(m/\delta)}{\epsilon^2}\right) \tag{A.55}$$

copies of the quantum state ρ.

In [148], they prove the guarantee on the quantum hypothesis selection algorithm using Helstrom's Theorem. We follow a similar proof. Thus, we first state Helstrom's Theorem and recall a corollary of it, which will be useful in the proof of Prop. 1.

Theorem 10 (Helstrom's Theorem [132])**.** *Consider two d-dimensional quantum states ρ and σ. Then, the trace distance between ρ and σ can be written as*

$$\frac{1}{2}\|\rho-\sigma\|_1 = \max_{\|O\|_\infty \leq 1} |\operatorname{tr}(O\rho) - \operatorname{tr}(O\sigma)|, \tag{A.56}$$

where the maximum is taken over all observables $O \in \mathbb{C}^{d\times d}$.

Corollary 2. *Consider two d-dimensional quantum states ρ and σ. Then, there exists an observable A achieving the maximum such that*

$$\operatorname{tr}(A\rho) - \operatorname{tr}(A\sigma) = \frac{1}{2}\|\rho-\sigma\|_1. \tag{A.57}$$

Proof of Corollary 2. We will construct an observable A that maximizes $\operatorname{tr}(O(\rho-\sigma))$ over all observables O with $\|O\|_\infty \leq 1$. Choose a representation of $\rho-\sigma$ in terms of eigenstates $|v\rangle$. Suppose the eigenvalues are discrete:

$$(\rho-\sigma)\,|v\rangle = \lambda_v\,|v\rangle\,. \tag{A.58}$$

Then, we can write the quantity we wish to maximize as

$$\operatorname{tr}(O(\rho-\sigma)) = \sum_v \lambda_v \,\langle v|O|v\rangle\,. \tag{A.59}$$

We can maximize this by choosing A such that

$$\langle v|A|v\rangle = \begin{cases} 1 & \text{if } \lambda_v > 0 \\ 0 & \text{if } \lambda_v \leq 0. \end{cases} \tag{A.60}$$

In this way, we can write A as a sum of projectors

$$A = \sum_{v:\lambda_v>0} |v\rangle\!\langle v|\,. \tag{A.61}$$

This maximizes $\operatorname{tr}(O(\rho-\sigma))$, so the corollary has been proven. □

With this, we can now prove Prop. 1.

Proof of Prop. 1. The proof of Proposition 5.3 in [148] uses shadow tomography as a black box. We follow the same strategy but use classical shadow tomography [100] instead of shadow tomography. Recall that in [148], they run the shadow tomography algorithm from [37] with observables given by Helstrom's Theorem [132]. This is the key step that uses samples of the unknown quantum state ρ, so we need to analyze it when using classical shadow instead of shadow tomography. In our setting, Corollary 2 states that for any $i \neq j$, there exists an observable A_{ij} such that

$$\operatorname{tr}(A_{ij}\sigma_i) - \operatorname{tr}(A_{ij}\sigma_j) = \frac{1}{2}\|\sigma_i - \sigma_j\|_1. \tag{A.62}$$

Thus, the algorithm in [148] uses $M = \binom{m}{2} = \mathcal{O}(m^2)$ observables $\{A_{ij}\}$ to select the hypothesis state, where m is the size of the hypothesis set. Using classical shadow instead of shadow tomography requires

$$N = \tilde{\mathcal{O}}\left(\frac{\log(M/\delta)}{\epsilon^2}\max_{i,j}\left\|A_{ij} - \frac{\operatorname{tr}(A_{ij})}{2^n}\mathbb{I}\right\|^2_{\text{shadow}}\right) \tag{A.63}$$

copies of ρ by Theorem 9, where M is the number of observables A_{ij} that we want to predict. Here, $M = \mathcal{O}(m^2)$ so that we require

$$N = \tilde{\mathcal{O}}\left(\frac{\log(m/\delta)}{\epsilon^2}\max_{i,j}\left\|A_{ij} - \frac{\operatorname{tr}(A_{ij})}{2^n}\mathbb{I}\right\|^2_{\text{shadow}}\right) \tag{A.64}$$

copies of ρ. We claim that

$$\max_{i,j} \left\| A_{ij} - \frac{\operatorname{tr}(A_{ij})}{2^n}\mathbb{I} \right\|_{\text{shadow}}^2 = \mathcal{O}(1). \tag{A.65}$$

The lemma then follows from this claim. We can prove this bound on the shadow norm using the construction of the observables A_{ij} from Helstrom's Theorem, as seen in Corollary 2. In our case, the states σ_i are pure, and hence of rank 1. Thus, the rank of $\sigma_i - \sigma_j$ is at most 2 so that A_{ij} is a projector of rank at most 2. Thus, the Frobenius norm of every A_{ij} is $\mathcal{O}(1)$ and, by [100, Proposition S1], the same holds for the shadow norm of the centered version of A_{ij}. □

4. Characterizing the complexity of function classes

In the proof of Theorem 7 (in Appendix D), we will need to characterize the complexity of certain function classes. The following definitions will be useful. Throughout the work, we use $\mathcal{Y}^{\mathcal{X}}$ to denote the set of functions from $\mathcal{X}$ to $\mathcal{Y}$.

Definition 4 (Growth function, [149]). *Let $\mathcal{F} \subseteq \mathcal{Y}^{\mathcal{X}}$ be a class of functions with finite target space $\mathcal{Y}$. For every subset $\Xi \subseteq X$, define the restriction of $\mathcal{F}$ to Ξ as $\mathcal{F}|_{\Xi} = \{f \in \mathcal{Y}^{\Xi} : \exists F \in \mathcal{F}, \forall x \in \Xi, f(x) = F(x)\}$. We define the growth function Γ of $\mathcal{F}$ as*

$$\Gamma(\mu) = \max_{\Xi \subseteq \mathcal{X} : |\Xi| \leq \mu} |\mathcal{F}|_{\Xi}| \tag{A.66}$$

for any $\mu \in \mathbb{N}$.

The growth function characterizes the size of $\mathcal{F}$ when restricted to a domain of μ points. With growth function, we can define the VC dimension that characterizes the complexity of binary functions.

Definition 5 (VC dimension, [149]). *The Vapnik-Chervonenkis (VC) dimension of a function class $\mathcal{F} \subseteq \{0,1\}^{\mathcal{X}}$ is defined as*

$$\operatorname{VCdim}(\mathcal{F}) = \max\{\mu \in \mathbb{N} : \Gamma(\mu) = 2^\mu\}, \tag{A.67}$$

or ∞ if the maximum does not exist. Here $\Gamma(\mu)$ is the growth function of $\mathcal{F}$. Or equivalently, $\operatorname{VCdim}(\mathcal{F})$ *is the largest $D \in \mathbb{N} \cup \{\infty\}$ such that there exists a set of points $\{x_i\}_{i=1}^D \subseteq \mathcal{X}$ that for all $C \subseteq [D]$, there is a function $f \in \mathcal{F}$ satisfying*

$$f(x_i) = 1 \iff i \in C. \tag{A.68}$$

These points are said to be shattered by $\mathcal{F}$.

To go beyond binary functions, we can use pseudo dimension defined below.

Definition 6 (Pseudo dimension, [70]). *The pseudo dimension of a real-valued function class $\mathcal{F} \subseteq \mathbb{R}^{\mathcal{X}}$ is defined as*

$$\operatorname{Pdim}(\mathcal{F}) = \operatorname{VCdim}(\{\mathcal{X} \times \mathbb{R} \ni (x,y) \to \operatorname{sgn}[f(x) - y] : f \in \mathcal{F}\}). \tag{A.69}$$

Or equivalently, $\operatorname{Pdim}(\mathcal{F})$ *is the largest $D \in \mathbb{N} \cup \{\infty\}$ such that there exists a set of points $\{(x_i, y_i)\}_{i=1}^D \subseteq \mathcal{X} \times \mathbb{R}$ that for all $C \subseteq [D]$, there is a function $f \in \mathcal{F}$ satisfying*

$$f(x_i) \geq y_i \iff i \in C. \tag{A.70}$$

These points are said to be pseudo-shattered by $\mathcal{F}$.

We will also use the fat-shattering dimension, a scale-sensitive variant of the pseudo-dimension.

Definition 7 (Fat-shattering dimension, [71]). *Let $\alpha > 0$. The α-fat-shattering dimension* $\operatorname{fat}(\mathcal{F}, \alpha)$ *of a real-valued function class $\mathcal{F} \subseteq \mathbb{R}^{\mathcal{X}}$ is defined as the largest $D \in \mathbb{N} \cup \{\infty\}$ such that there exists a set of points $\{(x_i, y_i)\}_{i=1}^D \subseteq \mathcal{X} \times \mathbb{R}$ that for all $C \subseteq [D]$, there is a function $f \in \mathcal{F}$ satisfying*

$$\begin{aligned} f(x_i) &\geq y_i + \alpha \quad \text{if} \quad i \in C, \\ f(x_i) &\leq y_i - \alpha \quad \text{if} \quad i \notin C. \end{aligned} \tag{A.71}$$

Such a set of points is said to be α-fat-shattered by $\mathcal{F}$.

5. Cryptography

Our computational complexity lower bounds rely on cryptographic primitives such as pseudorandom functions [138] and pseudorandom quantum states [137, 139]. A family of pseudorandom functions is a set of functions such that sampling from this family is indistinguishable from a uniformly random function. We present the formal definition below, following the presentation in [40].

Definition 8 (Pseudorandom functions (PRFs) [138])**.** *Let λ denote the security parameter. Let $\mathcal{K} = \{\mathcal{K}_\lambda\}_{\lambda\in\mathbb{N}}$ be an efficiently sampleable key space. Let $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda\in\mathbb{N}}, \{\mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ be collections of finite sets. Let $\mathcal{F} = \{f_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of efficiently-computable keyed functions $f_\lambda : \mathcal{K}_\lambda \times \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$. $\mathcal{F}$ is a* pseudorandom function *if for every polynomial-time probabilistic algorithm* Adv*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for every security parameter $\lambda \in \mathbb{N}$*

$$\left| \Pr_{\mathbf{k}\leftarrow\mathcal{K}_\lambda}[\mathsf{Adv}^{f(\mathbf{k},\cdot)}(\cdot) = 1] - \Pr_{g\in\mathcal{U}_\lambda}[\mathsf{Adv}^{g}(\cdot) = 1] \right| \le \mathsf{negl}(\lambda), \tag{A.72}$$

where the key $\mathbf{k}$ is picked uniformly at random from the key space $\mathcal{K}_\lambda$ and g is picked uniformly at random from $\mathcal{U}_\lambda$, the set of all functions from $\mathcal{X}_\lambda$ to $\mathcal{Y}_\lambda$. Here, $\mathsf{negl}(\lambda)$ *denotes a negligible function, i.e., a function that grows more slowly than any inverse polynomial in λ.*

Concretely, it is common to take the input and output spaces to be $\mathcal{X}_\lambda = \{0,1\}^m$ and $\mathcal{Y}_\lambda = \{0,1\}$ for some input length $m = m(\lambda)$ that depends on the security parameter λ. We consider this setting throughout the work.

Definition 9 (Quantum secure PRFs [40])**.** *Let λ denote the security parameter. A pseudorandom function is* quantum secure against $t(\lambda)$ adversaries *if it satisfies Definition 8 where* Adv *is a $t(\lambda)$-time quantum algorithm with quantum query access to $f_{\mathbf{k}}$ and g. When $t(\lambda) = \mathsf{poly}(\lambda)$, we say that the PRF is* quantum secure*.*

There are several constructions for implementing PRFs with low-depth circuits [40, 150, 151]. We will focus on the construction of [40], which relies on the assumption that the Ring Learning with Errors ($\mathsf{RingLWE}$) problem [38] is hard even for quantum computers. Specifically, we assume that $\mathsf{RingLWE}$ cannot be solved by a quantum computer in sub-exponential time, which is a commonly believed cryptographic assumption [39–43]. Here, $\mathsf{RingLWE}$ is a variant of the more well-known Learning with Errors problem [39] over polynomial rings. The $\mathsf{RingLWE}$ problem is to find a secret ring element $s \in R_q \triangleq \mathbb{Z}_q[x]/\langle x^\lambda - 1\rangle$ given pairs $(a, a\cdot s + e \bmod R_q)$, where λ denotes the security parameter, e is some error, q is a parameter of the problem. We only state this informally here and refer the reader to [38] for a formal definition and discussion. In [40], assuming that $\mathsf{RingLWE}$ cannot be solved by quantum computers in $t(\lambda)$ time, their construction produces a PRF secure against $\mathcal{O}(t(\lambda))$ quantum adversaries that is implementable by constant-depth, polynomial-size circuits. We state the precise result below.

Theorem 11 (Lemmas 3.15 and 3.16 in [40])**.** *Let λ denote the security parameter. Let the input size be $m = m(\lambda) = \omega(\log\lambda)$ and set the parameter $q = \lambda^{\omega(1)}$ to be a power of two such that $\log(q) \le \mathcal{O}(\mathsf{poly}(\lambda))$. Let $\mathcal{K} = \{\mathcal{K}_\lambda\}_{\lambda\in\mathbb{N}}$, where $\mathcal{K}_\lambda = R_q^{m+1}$. There exists a PRF $\mathcal{RF} = \{f_\lambda\}_{\lambda\in\mathbb{N}}$, where $f_\lambda : R_q^{m+1} \times \{0,1\}^m \to \{0,1\}$, satisfying the following two properties.*

1. *Every $f_\lambda(\mathbf{k},\cdot) \in \mathcal{RF}$ with $\mathbf{k} \in \mathcal{K}_\lambda$ can be computed by a TC^0 circuit.*
2. *Suppose there exists a distinguisher $\mathcal{D}$ for $\mathcal{RF}$, i.e., there exists an $\mathcal{O}(t(\lambda))$-time quantum algorithm $\mathcal{D}$ that satisfies*

$$\left| \Pr_{\mathbf{k}\leftarrow\mathcal{K}_\lambda}[\mathcal{D}^{|f_\lambda(\mathbf{k},\cdot)\rangle}(\cdot) = 1] - \Pr_{g\in\mathcal{U}}[\mathcal{D}^{|g\rangle}(\cdot) = 1] \right| > \mathsf{negl}(\lambda), \tag{A.73}$$

where the key $\mathbf{k}$ is picked uniformly at random from the key space $\mathcal{K}_\lambda$, g is picked uniformly at random from $\mathcal{U}$, the set of all functions from $\mathcal{X}_\lambda$ to $\mathcal{Y}_\lambda$, and $\mathcal{D}^{|f_\lambda(\mathbf{k},\cdot)\rangle}$ indicates that $\mathcal{D}$ has quantum oracle access to the function $f_\lambda(\mathbf{k},\cdot)$. Then, there exists a $t(\lambda)$-time quantum algorithm that solves $\mathsf{RingLWE}$.

In Property 2, this is equivalent to saying that the PRF is quantum secure against $\mathcal{O}(t(\lambda))$ adversaries, assuming that $\mathsf{RingLWE}$ cannot be solved by a $t(\lambda)$-time quantum algorithm. Also, note that in Property 1, TC^0 circuits refer to constant-depth, polynomial-size circuits with unbounded fan-in AND, OR, NOT, and $\mathsf{MAJORITY}$ gates. We claim that every TC^0 circuit has a quantum circuit computing the same function with poly-logarithmic overhead in depth.

Proposition 2 (Quantum circuits for TC^0)**.** *Let C be a TC^0 circuit on m inputs computing some Boolean function $f : \{0,1\}^m \to \{0,1\}$. Then, there exists a quantum circuit C' on $n = \mathcal{O}(\mathsf{poly}(m))$ qubits of size $\mathcal{O}(n\mathsf{polylog}(n))$ and depth $\mathcal{O}(\mathsf{polylog}(n))$ that implements f.*

Here, when we say that C' implements the function f, we mean that $C' |x\rangle |z\rangle = C' |x\rangle |z \oplus f(x)\rangle$.

Proof. Note that the number of qubits is $n = \mathcal{O}(\mathsf{poly}(m))$ because after each gate in the classical circuit C, we must store the result in an ancilla qubit to maintain unitarity. Recall that TC^0 circuits are constant-depth, polynomial-size circuits with unbounded fan-in AND, OR, NOT, and MAJORITY gates. Thus, it suffices to find the depth of implementing each of these gates quantumly. The size then follows because a circuit of depth d on n qubits can have at most nd gates. NOT gates can clearly be implemented in constant depth since this is just an X gate. An AND gate with m inputs can be completed in logarithmic depth by computing AND pairwise with CNOT. Similarly, we can compute an OR gate with the same logarithmic depth. It remains to analyze the depth needed for computing a MAJORITY gate. Recall that the MAJORITY gate is defined as

$$\mathsf{MAJ}(x_1, \ldots, x_m) = \left\lfloor \frac{1}{2} + \frac{(\sum_{i=1}^m x_i) - 1/2}{m} \right\rfloor = \left\lfloor \frac{1}{2} + \frac{\sum_{i=1}^m x_i}{m} - \frac{1}{2m} \right\rfloor. \tag{A.74}$$

Here, addition is done over the integers and $x_i \in \{0,1\}$. We first analyze the depth/size required for the addition $\sum_{i=1}^m x_i$. Note that the maximum value of this sum is m, which can be stored in $\mathcal{O}(\log m)$ bits. Thus, we can write each of the x_i in binary using $\log m$ bits by padding with zeros and perform addition in this way. We can perform the addition of the m inputs pairwise, parallelized to $\mathcal{O}(\log m)$ depth and requiring $\mathcal{O}(m)$ addition operations. Moreover, one can perform these addition operations using quantum circuits of size and depth $\mathcal{O}(\log m)$ [152]. The construction in [152] uses Toffoli gates, but these can be decomposed into two-qubit gates with constant overhead [153]. In total, we have that $\sum_{i=1}^m x_i$ can be implemented by a quantum circuit of depth $\mathcal{O}(\log^2 m)$.

To divide this sum by m, note that there exist classical Boolean circuits for integer division of depth $\mathcal{O}(\log\log m)$ since our inputs can be represented in binary using $\log m$ bits [154]. These Boolean circuits use only standard AND, OR, and NOT gates. As explained previously, these can be implemented quantumly, and for fan-in-2 AND and OR gates, this can be done with constant overhead. Thus, this division step requires depth $\mathcal{O}(\log\log m)$ in total.

Finally, we need to compute the remaining addition/subtraction and floor operations. The addition/-subtraction can be ignored since they only occur once so that the depth is dominated by the other additions. For the floor, because the quantity inside can only be less than or equal to 1, then this is the same as deciding whether the quantity inside is less than 1 or not. This can be done in a constant number of operations.

Putting everything together, we see that the circuit depth for implementing a MAJORITY gate is dominated by $\mathcal{O}(\log^2 m)$.

Recall again that TC^0 describes constant-depth, polynomial-size circuits with unbounded fan-in AND, OR, NOT, and MAJORITY gates. We just analyzed the depth for each of these gates individually. In summary, we computed that $\mathcal{O}(\log m)$ quantum depth is sufficient for AND and OR. Constant $\mathcal{O}(1)$ depth is sufficient for NOT. Finally, $\mathcal{O}(\log^2 m)$ depth is sufficient for MAJORITY. In the overall circuit, this totals to $\mathcal{O}(\mathsf{polylog}(m))$ depth. Because a circuit of depth d on n qubits can have at most nd gates, then the size of this circuit is $\mathcal{O}(n\mathsf{polylog}(m))$ gates. Then, because $n = \mathcal{O}(\mathsf{poly}(m))$, we obtain the claim. □

Alternatively, we note that one can obtain a similar result using [155]. As a simple corollary of this along with Theorem 11, we can bound the depth/size of a quantum circuit for computing a PRF.

Corollary 3. *Let $\lambda = n$ denote the security parameter. Assuming that $\mathsf{RingLWE}$ cannot be solved in $t(n)$ time by a quantum computer, there exists a PRF $\mathcal{F} = \{f_\lambda\}_{\lambda\in\mathbb{N}}$ that is secure against $\mathcal{O}(t(n))$ quantum adversaries such that for keys $\mathbf{k} \in \mathcal{K}_\lambda$ (for the same key space as in Theorem 11), $f_\lambda(\mathbf{k}, \cdot) : \{0,1\}^m \to \{0,1\}$ is computable by an n-qubit quantum circuit of size $\mathcal{O}(n\mathsf{polylog}(n))$ and depth $\mathcal{O}(\mathsf{polylog}(n))$.*

Note here that by the above analysis, we have $m = \omega(\log(\lambda))$. Since $\mathcal{O}(\mathsf{poly}(m))$ qubits suffice to implement these PRFs, we can take $n = \lambda$, similar to [139].

Our proofs also require the notion of pseudorandom quantum states. Informally, pseudorandom quantum states are ensembles of quantum states that are indistinguishable from Haar-random states to any efficient (quantum) algorithm. Moreover, it is known how to construct these states using efficient quantum circuits. Recently, pseudorandom quantum states have been of great interest in quantum cryptography [156–158] and complexity theory [159]. We define them formally below, following the presentation in [137, 139].

Definition 10 (Pseudorandom quantum states (PRS) [137])**.** *Let $\lambda = n$ denote the security parameter. Let $\mathcal{K} = \{\mathcal{K}_\lambda\}_{\lambda \in \mathbb{N}}$ be the key space. A keyed family of pure quantum states $\{|\phi_k\rangle\}_{k \in \mathcal{K}_\lambda}$ is* pseudorandom against $t(n)$ adversaries *if the following two conditions hold:*

1. *(Efficient generation). There is a polynomial-time quantum algorithm* Gen *that generates state $|\phi_k\rangle$ on input k. That is, for all $\lambda \in \mathbb{N}$ and for all $k \in \mathcal{K}_\lambda$, $\mathsf{Gen}(1^\lambda, k) = |\phi_k\rangle$.*
2. *(Pseudorandomness). Any polynomially many copies of $|\phi_k\rangle$ with the same random $k \in \mathcal{K}_\lambda$ are computationally indistinguishable from the same number of copies of a Haar-random state. More precisely, for any $t(n)$-time quantum algorithm $\mathcal{D}$ and any $N = \mathsf{poly}(\lambda)$, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for all $\lambda \in \mathbb{N}$,*

$$\left| \Pr_{k \leftarrow \mathcal{K}_\lambda} \left[\mathcal{D}\left(|\phi_k\rangle^{\otimes N} \right) = 1 \right] - \Pr_{|\psi\rangle \leftarrow \mu} \left[\mathcal{D}\left(|\psi\rangle^{\otimes N} \right) = 1 \right] \right| \leq \mathrm{negl}(\lambda), \tag{A.75}$$

where μ is the Haar measure over pure states on n qubits.

When $t(n) = \mathsf{poly}(n)$, we simply say that the states are pseudorandom*.*

There exist efficient procedures to generate pseudorandom quantum states under standard cryptographic assumptions. In particular, we consider the construction by [139], which assumes the existence of quantum-secure pseudorandom functions.

Proposition 3 (Corollary of Claims 3 and 4 in [139])**.** *Let $\lambda = n$ denote the security parameter and $t(n) \geq \mathsf{poly}(n)$. Assuming that* $\mathsf{RingLWE}$ *cannot be solved by a quantum computer in $t(n)$ time, pseudorandom quantum states secure against $\mathcal{O}(t(n))$ adversaries with key space $\mathcal{K}$ (for the same key space as in Theorem 11) can be prepared using n-qubit quantum circuits of depth $\mathcal{O}(\mathsf{polylog}(n))$ and size $\mathcal{O}(n\mathsf{polylog}(n))$.*

Proof. Note that using the PRF from [40] and tracing through the proof of Claim 3 in [139], one can clearly see that security holds for $\mathcal{O}(t(n))$ adversaries rather than only efficient adversaries. We need to prove that the size and depth are as stated for the construction of pseudorandom quantum states in [139] using the PRF from [40]. To obtain the depth and size bounds, we analyze the construction in [139]. In Claim 3 of [139], they show that their constructed states can be prepared by applying a single layer of Hadamard gates followed by applying a quantum-secure PRF. First, the layer of Hadamards has depth 1 and size n. Using the construction from Corollary 3, applying the PRF can then be implemented in $\mathcal{O}(\mathsf{polylog}(n))$ depth and $\mathcal{O}(n\mathsf{polylog}(n))$ size. Thus, overall, the depth and size are dominated by the cost of evaluating the PRF. Moreover, in Claim 4 of [139], they prove that this is indeed constructs a pseudorandom quantum state. □

Note again that the number of qubits n in the quantum circuit depends on the security parameter λ. In fact, due to the construction used, the n depends on λ in the same way as for the PRF construction. Also note that the above constructions of PRF/PRS can be implemented using a number of Clifford and T gates of the same order. This is because the TC^0 circuits in the PRF constructions are classical circuits which can be implemented exactly by Toffoli gates, and Toffoli gates can be constructed using a constant number of Clifford and T gates. Also in the PRS construction, the remaining gates are Hadamard gates which are Clifford gates. Therefore, the computational hardness results in Appendices B 3 and C 5 also apply to Clifford+T circuits of the same gate complexity.

Appendix B: Learning quantum states

Recall that, given copies of a pure state of bounded circuit complexity, we wish to find a classical description for a quantum circuit that approximately implements this state. It is natural to require the learner to output a circuit description since this ensures that the output of the learner can indeed be used to prepare (approximate) copies of the unknown state. This model is similar-in-spirit to learning an (approximate) generator for an unknown classical probability distribution [160]. Nevertheless, our sample complexity results hold for learning classical descriptions beyond circuit descriptions, and our computational complexity results immediately extend to learners that output classical descriptions from which a circuit description can be derived efficiently (e.g., matrix product states/operators with constant bond dimension [34, 35], stabilizer descriptions, etc.).

Specifically, let $|\psi\rangle = U|0\rangle^{\otimes n}$, where U is a unitary consisting of G two-qubit gates. Throughout this section, we denote $\rho \triangleq |\psi\rangle\langle\psi|$. Suppose we are given N identically prepared copies of ρ. The goal is to learn a classical circuit description of a quantum state $\hat{\rho}$ that is ϵ-close to ρ in trace distance, i.e., $\mathrm{d}_{\mathrm{tr}}(\hat{\rho}, \rho) = \|\hat{\rho} - \rho\|_1/2 \leq \epsilon$.

In this appendix, we provide a proof of Theorem 1, which characterizes the sample complexity for this task. We restate the theorem below.

Theorem 12 (State learning, detailed restatement of Theorem 1)**.** *Let $\epsilon, \delta > 0$. Suppose we are given N copies of a pure n-qubit state density matrix $\rho = |\psi\rangle\!\langle\psi|$, where $|\psi\rangle = U|0\rangle^{\otimes n}$ is generated by a unitary U consisting of G two-qubit gates. Then, any algorithm that can output $\hat{\rho}$ such that $\mathrm{d}_{\mathrm{tr}}(\hat{\rho}, \rho) \leq \epsilon$ with probability at least $1-\delta$ requires at least*

$$N = \Omega\left(\min\left(\frac{2^n}{\epsilon^2}, \frac{G(1-\delta)}{\epsilon^2 \log(G/\epsilon)}\right) + \frac{\log(1/\delta)}{\epsilon^2}\right). \tag{B.1}$$

Meanwhile, there exists such an algorithm using

$$N = \mathcal{O}\left(\min\left(\frac{2^n \log(1/\delta)}{\epsilon^2}, \frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^2}\right)\right). \tag{B.2}$$

Here, the minimum with $2^n/\epsilon^2$ corresponds to the sample-optimal approaches for full quantum state tomography [19, 20]. The theorem in the main text corresponds to $\delta = \mathcal{O}(1)$ so that the upper and lower bounds are equal up to logarithmic factors.

In Appendix B 1 we prove the sample complexity upper bound, and in Appendix B 2, we show the sample complexity lower bound. Moreover, in Appendix B 3, we prove Theorem 2, which gives a lower bound on the computational complexity required for this task.

1. Sample complexity upper bound

In this section, we prove the sample complexity upper bound for Theorem 12. We provide an algorithm for learning the unknown quantum state within trace distance ϵ by constructing a covering net over the space of all unitaries consisting of G two-qubit gates. We can then obtain a covering net over all pure quantum states generated by G two-qubit gates by applying each element of the unitary covering net to the zero state. With this covering net, we can use quantum hypothesis selection [148] based on classical shadows [100] (discussed in Appendix A 3) to identify a state in the covering net that is close to the unknown target state. We note that this strategy may be adapted to other restricted state/unitary classes as long as we can construct a covering net with bounded cardinality.

Proposition 4 (State learning upper bound)**.** *Let $\epsilon, \delta > 0$. Suppose we are given N copies of a pure n-qubit state density matrix $\rho = |\psi\rangle\!\langle\psi|$, where $|\psi\rangle = U|0\rangle^{\otimes n}$ is generated by a unitary U consisting of G two-qubit gates. Then, there exists an algorithm that can output $\hat{\rho}$ such that $\mathrm{d}_{\mathrm{tr}}(\hat{\rho}, \rho) \leq \epsilon$ with probability at least $1-\delta$ using*

$$N = \mathcal{O}\left(\min\left(\frac{2^n \log(1/\delta)}{\epsilon^2}, \frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^2}\right)\right) \tag{B.3}$$

samples of $|\psi\rangle$.

Here, we take the minimum with $2^n/\epsilon^2$, as this is the upper bound achieved for full quantum state tomography on an arbitrary n-qubit pure state [19, 20]. Thus, we focus on proving the second term in the minimum. We prove this upper bound by considering two cases: (1) $G \geq n/2$ and (2) $G < n/2$. The upper bounds for each case agree and are given by Equation (B.3). We first prove the proposition for Case (1) and indicate what changes for Case (2).

Proof of Case (1). As previously described, this follows by first creating a covering net over all unitaries consisting of G two-qubit gates and then using quantum hypothesis selection [148].

By Theorem 8, we know that there exists an $(\epsilon/6)$-covering net $\mathcal{N}_{\epsilon/6}$ of the space of unitaries implemeted by G two-qubits gates with respect to the diamond distance $\mathrm{d}_\diamond$ with metric entropy bounded by

$$\log(|\mathcal{N}_{\epsilon/6}|) \leq 32G\log\left(\frac{72G}{\epsilon}\right) + 2G\log(n). \tag{B.4}$$

Applying each unitary $V' \in \mathcal{N}_{\epsilon/6}$ to the zero state, we obtain a new covering net

$$\mathcal{N}'_{\epsilon/6} = \{V' \, |0\rangle\langle 0|^{\otimes n} \, V'^{\dagger} : V' \in \mathcal{N}_{\epsilon/6}\} \tag{B.5}$$

for the set of pure quantum states generated by G two-qubit gates with respect to trace distance. We argue that this is true as follows. Any pure quantum state generated by G two-qubit gates can be written as $|\phi\rangle = V\,|0\rangle^{\otimes n}$ for some unitary V implemented by G two-qubit gates and let $\sigma = |\phi\rangle\langle\phi|$. Using the definition of the covering net $\mathcal{N}_{\epsilon/6}$, there exists a unitary $V' \in \mathcal{N}_{\epsilon/6}$ such that $\mathrm{d}_{\diamondsuit}(V, V') < \epsilon/6$. Consider $|\phi'\rangle = V'\,|0\rangle^{\otimes n}$ and let $\sigma' = |\phi'\rangle\langle\phi'| \in \mathcal{N}'_{\epsilon/6}$. By the definition of the diamond distance in terms of a worst case over input states, we also have $\mathrm{d}_{\mathrm{tr}}(\sigma, \sigma') \leq \mathrm{d}_{\diamondsuit}(V, V') \leq \epsilon/12 < \epsilon/6$. Thus, $\mathcal{N}'_{\epsilon/6}$ satisfies the definition of a covering net over the pure quantum states generated by G two-qubit gates with respect to trace distance d_{tr}. Moreover, we clearly see that $|\mathcal{N}'_{\epsilon/6}| \leq |\mathcal{N}_{\epsilon/6}|$.

We can consider this covering net $\mathcal{N}'_{\epsilon/6}$ as the set of hypothesis states in Proposition 1. Let $\rho = |\psi\rangle\langle\psi|$ be the unknown quantum state that we have copies of. By Proposition 1, there exists an algorithm to learn $\tilde{\rho}$ such that

$$\mathrm{d}_{\mathrm{tr}}(\rho, \tilde{\rho}) \leq 3 \cdot \frac{\epsilon}{6} + \frac{\epsilon}{2} = \epsilon \tag{B.6}$$

with probability at least $1 - \delta$. Here, note that we used $\eta = \epsilon/6$ in Proposition 1 by definition of an $(\epsilon/6)$-covering net. Furthermore, we may choose $\epsilon_2 = \epsilon/2$ and $\delta_1 = \delta/2$. In this way, we obtain $\tilde{\rho}$ such that $\mathrm{d}_{\mathrm{tr}}(\rho, \tilde{\rho}) \leq \epsilon$ with probability at least $1 - \delta$. Moreover, by Proposition 1, this algorithm to find $\tilde{\rho}$ requires at most

$$N = \mathcal{O}\left(\frac{\log\left(|\mathcal{N}'_{\epsilon/6}|/\delta\right)}{\epsilon^2}\right) = \mathcal{O}\left(\frac{G\log(G/\epsilon) + G\log(n) + \log(1/\delta)}{\epsilon^2}\right) \tag{B.7}$$

copies of ρ, where the second equality follows from Eq. (B.4). Because we are considering $G \geq n/2$ in this case, then we have

$$N = \mathcal{O}\left(\frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^2}\right), \tag{B.8}$$

as claimed. □

Notice in the above proof that we used $G \geq n/2$ in the last step to remove the extra $\log(n)$ factor. However, in Case (2), we can no longer execute this step and must consider a more careful strategy to remove the dependence on system size n. The key observation is that if $G < n/2$, some qubits in the system will be left in the zero state because no gate has acted upon them (for G two-qubit gates, at most $2G < n$ qubits are acted upon nontrivially). Notice that we only need to learn the quantum state on these $2G$ qubits rather than the whole system, since we can simply tensor product with the zero state for the remaining qubits. Thus, we require the ability to discern which qubits have been acted upon by the G two-qubit gates. Once we find this set of qubits, the idea is to consider a covering net for the set of pure quantum states generated by G two-qubit gates *on this restricted system*. Then, we can follow a similar argument to the above proof of Case (1).

We prove Case (2) of Proposition 4 in the following sections. For the rest of this section, let $\rho = |\psi\rangle\langle\psi|$. In Appendix B 1 a, we discuss an algorithm that identifies the qubits acted on nontrivially by the G two-qubit gates with high probability and show that restricting to these identified qubits does not cause much error. In Appendix B 1 b, we resolve a technical issue for defining the covering net on the restricted system, which stems from the algorithm possibly not identifying all qubits. Finally, in Appendix B 1 c, we combine these pieces to provide the full proof of Case (2).

a. *Postselection*

First, we present an algorithm to determine which qubits of the unknown quantum state $\rho = |\psi\rangle\langle\psi|$ have been acted upon nontrivially by the G two-qubit gates. We then prove a guarantee about the number of samples of ρ needed to determine these qubits with high probability. We also show that considering ρ to be the zero state on the rest of the qubits does not incur much error.

Suppose that the true set of qubits acted upon by the G two-qubit gates is denoted as A. To determine which qubits are in the set A, consider the procedure given in Algorithm 1. The idea behind this algorithm

Algorithm 1: Identify qubits acted upon nontrivially (state version)

```
Input: Copies of unknown $n$-qubit quantum state $\rho$.
Output: List $\hat{A} \subseteq [n]$ of qubits.
1 Initialize $\hat{A} = \emptyset$.
2 Repeat the following $N = \mathcal{O}\left(\frac{G+\log(1/\delta_1)}{\epsilon_1}\right)$ times:
    (a) Measure all qubits of the unknown state $\rho$ in the computational basis.
    (b) Given the measurement outcome $|x\rangle$, set $\hat{A} \leftarrow \hat{A} \cup \mathrm{supp}(x)$, where $\mathrm{supp}(x) = \{i \in [n] : x_i \neq 0\}$.
```

is simple. If we measure a qubit in the computational basis and receive a nonzero measurement outcome, then it must have been acted upon by one of the G two-qubit gates because the quantum state is assumed to have been initialized in the zero state. We prove that $\mathcal{O}\left(\frac{G+\log(1/\delta_1)}{\epsilon_1}\right)$ copies of ρ suffice to obtain, with high probability $1-\delta_1$, the desired property that measuring the qubits in $\hat{B} \triangleq [n] \setminus \hat{A}$ of ρ yields the all zero bit string with high probability $1-\epsilon_1$.

Lemma 11. *Let $\epsilon_1, \delta_1 > 0$. Suppose we are given copies of a pure n-qubit quantum state $\rho = |\psi\rangle\langle\psi|$ generated by G two-qubit gates acting on a subset of the qubits $A \subseteq [n]$. Then, Algorithm 1 uses $N = \mathcal{O}\left(\frac{G+\log(1/\delta_1)}{\epsilon_1}\right)$ copies of ρ and outputs with probability at least $1-\delta_1$ a list $\hat{A} \subset [n]$ such that*

$$\left\langle 0_{\hat{B}} \middle| \rho_{\hat{B}} \middle| 0_{\hat{B}} \right\rangle \geq 1 - \epsilon_1, \tag{B.9}$$

where $\rho_{\hat{B}}$ denotes the reduced density matrix of ρ when tracing out all qubits other than those in the set $\hat{B} = [n] \setminus \hat{A}$ and $\left|0_{\hat{B}}\right\rangle$ denotes the zero state on all qubits in $\hat{B}$.

Proof. Let A' be any possible set that could be output by Algorithm 1. Let $B' \triangleq [n] \setminus A'$. We first define some random variables to state our claim more precisely. Let $E_{i,A'}$ be the event that round i of measurement of the qubits in $B' = [n] \setminus A'$ in Algorithm 1 yields the all zero bitstring. Let $X_{i,A'}$ be the indicator random variable corresponding to the event $E_{i,A'}$. Then, we have that $\bar{X}_{A'} \triangleq \frac{1}{N}\sum_{i=1}^{N} X_{i,A'}$ is the number of times the qubits in B' are all measured to be zero divided by the total number of measurements. In other words, $\bar{X}_{A'}$ is an empirical estimate for the overlap that the state $\rho_{B'}$ on qubits in B' has with the all zero state. Moreover, we have

$$\mathbb{E}[X_{A'}] \triangleq \mathbb{E}[X_{i,A'}] = \langle 0_{B'}|\rho_{B'}|0_{B'}\rangle \tag{B.10}$$

for all A'. Note that the first definition makes sense because for any i, the $X_{i,A'}$ are identically distributed. This says that the true expectation of our random variables is the true overlap of the state $\rho_{B'}$ with the all zero state.

We claim that for any A', if the true overlap is less than $1-\epsilon_1$, then the estimated overlap is less than $1-\epsilon_1/2$ with high probability. Formally, in terms of our random variables, this is the following statement:

Claim 1. *For any set A' that could be output by Algorithm 1, if $\mathbb{E}[X_{A'}] < 1-\epsilon_1$, then $\bar{X}_{A'} < 1-\epsilon_1/2$ with probability at least $1-\delta_1$.*

Thus, we have reduced our task to a concentration problem. Note that it suffices to prove this because the set $\hat{A}$ actually identified by Algorithm 1 has $\bar{X}_{\hat{A}} = 1$. This is true because a qubit is only added to the set $\hat{A}$ in the algorithm if it measured and observed a nonzero outcome. Thus, all qubits in $\hat{B} = [n] \setminus \hat{A}$ must have given zero when measured throughout all rounds of measurement. By definition, this gives us that $\bar{X}_{\hat{A}} = 1$. Then, by the contrapositive of Claim 1, we see that $\mathbb{E}[X_{\hat{A}}] = \left\langle 0_{\hat{B}} \middle| \rho_{\hat{B}} \middle| 0_{\hat{B}} \right\rangle \geq 1-\epsilon_1$, with probability at least $1-\delta_1$. We now prove this claim using classical concentration inequalities.

Proof of Claim 1. First, fix some set A' that could be output by Algorithm 1. Suppose

$$\mathbb{E}[X_{A'}] \triangleq 1 - a < 1 - \epsilon_1, \tag{B.11}$$

where $a > \epsilon_1$. Recall the Bhatia-Davis Inequality, which states that for $X \in [b,d]$ that

$$\mathrm{Var}(X) \leq (d - \mathbb{E}[X])(\mathbb{E}[X] - b). \tag{B.12}$$

In our case, we have $X_{A'} \in [0,1]$ since they are indicator random variables so that the inequality gives us

$$\mathrm{Var}(X_{A'}) \leq (1 - \mathbb{E}[X])\mathbb{E}[X] \leq 1 - \mathbb{E}[X] = a. \tag{B.13}$$

Now, recall Bernstein's Inequality, which states that for independent random variables X_i with $|X_i| \leq c$ and $\sigma^2 = \frac{1}{N}\sum_{i=1}^N \mathrm{Var}(X_i)$, we have for any $t > 0$,

$$\Pr\left(\frac{1}{N}\sum_{i=1}^N X_i - \mathbb{E}[X] > t\right) \leq \exp\left(-\frac{Nt^2}{2\sigma^2 + 2ct/3}\right). \tag{B.14}$$

In our case, $c = 1, \sigma^2 \leq a$, and $t = a/2$. Then, Bernstein's Inequality results in

$$\Pr\left(\bar{X}_{A'} - \mathbb{E}[X] > \frac{a}{2}\right) \leq \exp\left(-\frac{Na^2/4}{2a + a/3}\right). \tag{B.15}$$

Plugging in $\mathbb{E}[X] = 1 - a$ and simplifying, we have

$$\Pr\left(\bar{X}_{A'} > 1 - \frac{a}{2}\right) \leq \exp\left(-\frac{3Na}{28}\right) \leq \exp\left(-\frac{3N\epsilon_1}{28}\right). \tag{B.16}$$

Since $a > \epsilon_1$, then $1 - a/2 < 1 - \epsilon_1/2$ so that we have

$$\Pr\left(\bar{X}_{A'} > 1 - \frac{\epsilon_1}{2}\right) \leq \exp\left(-\frac{3N\epsilon_1}{28}\right). \tag{B.17}$$

Plugging in $N = \frac{28\log\left(2^{2G}/\delta_1\right)}{3\epsilon_1}$, we have

$$\Pr\left(\bar{X}_{A'} > 1 - \frac{\epsilon_1}{2}\right) \leq \frac{\delta_1}{2^{2G}}. \tag{B.18}$$

Recall that this inequality was for a single fixed set A', but we want our claim to hold for any set A'. Thus, we need to union bound overall possible sets A' output by Algorithm 1.

We claim that the number of such sets is at most 2^{2G}. This is clear because if A' is output by the algorithm, then $A' \subseteq A$, where A is the true set of qubits that the G gates act nontrivially on. This is true by construction because in order for a qubit to be added to the set output by Algorithm 1, its result upon measurement must have yielded a nonzero outcome so that a gate must have acted upon this qubit. Hence $A' \subseteq A$, and because $|A| \leq 2G$, the number of possible subsets A' of A is at most 2^{2G}.

Thus, applying a union bound to Eq. (B.18), we see that the probability that, for any A', $\bar{X}_{A'}$ is greater than $1 - \epsilon_1/2$ is at most δ_1. In other words, $\bar{X}_{A'}$ is less than $1 - \epsilon_1/2$ with probability at least $1 - \delta_1$. Moreover, here we used

$$N = \frac{28\log\left(2^{2G}/\delta_1\right)}{3\epsilon_1} = \mathcal{O}\left(\frac{G + \log(1/\delta_1)}{\epsilon_1}\right). \tag{B.19}$$

This concludes the proof of the claim, which gives the result in Lemma 11 as explained previously. □

□

With this, we know that measuring qubits in $\hat{B} = [n] \setminus \hat{A}$ of ρ yields the all zero bistring with high probability. We want to show that, in fact, we can consider $\rho_{\hat{B}}$ as being the zero state without incurring much error. In particular, we want to show the following lemma.

Lemma 12. *Let $\epsilon, \delta_1 > 0$. Suppose we are given $N = \mathcal{O}\left(\frac{G+\log(1/\delta_1)}{\epsilon^2}\right)$ copies of an n-qubit quantum state ρ generated by G gates. Let $\hat{A} \subset [n]$ be as in Algorithm 1 and $\hat{B} = [n] \setminus \hat{A}$. Then, for $\Lambda = |0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}}$ (where $|0_{\hat{B}}\rangle$ denotes the zero state on all qubits in $\hat{B}$) and for the post-measurement state*

$$\rho' \triangleq \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{Tr}(\Lambda\rho)}, \tag{B.20}$$

we have

$$\mathrm{d_{tr}}(\rho, \rho') \leq \frac{\epsilon}{24} \tag{B.21}$$

with probability at least $1 - \delta_1$.

In other words, we want to show that our original state ρ is not far in trace distance from the new state ρ', where ρ' is the state ρ with the qubits in $\hat{B}$ projected to the zero state. In this way, we can effectively only consider the system on qubits in $\hat{A}$ when defining the covering net and using hypothesis selection. This turns out to be a bit more nuanced, but this is the general idea. To show this, we will use the Gentle Measurement Lemma, following the presentation in [143].

Lemma 13 (Lemma 9.4.1 in [143])**.** *Consider a density operator ρ and a measurement operator Λ, where $0 \leq \Lambda \leq I$. The measurement operator could be an element of a POVM. Suppose that the measurement operator Λ has a high probability of detecting the state ρ:*

$$\mathrm{Tr}(\Lambda\rho) \geq 1 - \epsilon, \tag{B.22}$$

where $\epsilon \in [0, 1]$ (the probability of detection is high if ϵ is close to zero). Then the post-measurement state

$$\rho' \triangleq \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{Tr}(\Lambda\rho)} \tag{B.23}$$

is $\sqrt{\epsilon}$-close to the original state ρ in trace distance:

$$\mathrm{d}_{\mathrm{tr}}(\rho, \rho') \leq \sqrt{\epsilon}. \tag{B.24}$$

Thus, the measurement does not disturb the state ρ by much if ϵ is small.

With this, we can now prove Lemma 12.

Proof of Lemma 12. As stated above, let $\hat{A} \subset [n]$ be as in Algorithm 1, and let $A \subset [n]$ be true the set of qubits acted non-trivially on by the G gates. Let $\hat{B} \triangleq [n] \setminus \hat{A}$ and let $B \triangleq [n] \setminus A$.

In order to apply the Gentle Measurement Lemma, we need to show that

$$\mathrm{Tr}(\Lambda\rho) \geq 1 - \left(\frac{\epsilon}{24}\right)^2. \tag{B.25}$$

Since $\Lambda = |0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}}$, where $|0_{\hat{B}}\rangle$ denotes the zero state on all qubits in $\hat{B}$, we have

$$\mathrm{Tr}(\Lambda\rho) = \mathrm{Tr}\big((|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}})\rho\big) = \mathrm{Tr}\big(|0_{\hat{B}}\rangle\langle 0_{\hat{B}}|\, \rho_{\hat{B}}\big) = \langle 0_{\hat{B}}|\rho_{\hat{B}}|0_{\hat{B}}\rangle, \tag{B.26}$$

where $\rho_{\hat{B}}$ denotes the reduced density matrix obtained by tracing out all qubits in $[n] \setminus \hat{B}$. Thus, it suffices to show that

$$\langle 0_{\hat{B}}|\rho_{\hat{B}}|0_{\hat{B}}\rangle \geq 1 - \left(\frac{\epsilon}{24}\right)^2. \tag{B.27}$$

Intuitively, this makes sense because in Algorithm 1, we identified the qubits in $\hat{B}$ as those being close to the zero state. Indeed, this holds by Lemma 11 when choosing $\epsilon_1 = (\epsilon/24)^2$. Thus, the result follows. □

b. *Permutation*

Before we can prove Proposition 4, we must resolve a technical issue. Namely, ideally, we would like to consider a covering net on the subsystem of qubits in the set A (the true set of qubits that the G gates generating the unknown state ρ act nontrivially on). In this way, because $\hat{A} \subseteq A$, where $\hat{A}$ is the set of qubits identified by Algorithm 1, then our postselected state ρ' from Lemma 12 should be close to some state in this covering net on the subsystem. This nearby state in the covering net can then be identified via quantum hypothesis selection [49]. By Lemma 12, this state from hypothesis selection is also close to the original unknown state ρ.

However, the problem with the above is that we do not know the true set of qubits A; we only know the identified set of qubits $\hat{A}$. Moreover, it is possible that $\hat{A} \subsetneq A$, i.e., Algorithm 1 may not have been able to detect certain qubits as having been acted upon nontrivially by the G gates. For example, suppose that when preparing the unknown state ρ, certain qubits are used as workspace ancillas and are reset to the zero state at the end of the computation.

In order to define a covering net on a system on which the G gates act (the setting of Lemma 9), we need to somehow identify the qubits in $A \setminus \hat{A}$ that are undetected by the algorithm. To do so, we argue that we can permute the qubits outside of the set $\hat{A}$ and not deviate much from the original state ρ. In this way, without loss of generality, we can permute the qubits such that those in $A \setminus \hat{A}$ are grouped together in some fixed set of qubits. Then, we can define a covering net on the system of qubits defined by this fixed set containing the qubits in $A \setminus \hat{A}$ and our identified set $\hat{A}$. By construction, we know that the G gates act on this subset of qubits, so this is the correct setting of Lemma 9. We note that the permutations used in the proof are a mathematical tool for the analysis, but the learner has to neither know nor perform these permutations.

To formalize this, we first define a permutation and claim that permuting the qubits outside of the set $\hat{A}$ does not change the post selected state ρ'.

Definition 11 (Permutation). *A unitary $W \in \mathrm{U}(2^n)$ is a* permutation unitary *if it satisfies the following property: W corresponds to a permutation $\sigma_W \in S_n$ of order 2, where S_n is the symmetric group of size n, and W acts as*

$$W |x_1 \dots x_n\rangle = |x_{\sigma_W(1)} \cdots x_{\sigma_W(n)}\rangle , \tag{B.28}$$

where $x = x_1 \cdots x_n \in \{0,1\}^n$. Moreover, we use W_S for a set $S \subseteq \{1, \dots, n\}$ to denote a permutation unitary where the corresponding permutation σ_{W_S} is such that $\sigma_{W_S}|_{\overline{S}} = \mathrm{id}$, where $\overline{S} = [n] \setminus S$. In other words, σ_{W_S} only permutes the elements in S.

It is easy to see here that because the corresponding permutation is of order 2, W is Hermitian. Our next lemma shows that such permutations when acting only on $\hat{B}$ do not change our post selected state.

Lemma 14. *Let ρ' be as in Lemma 12. Explicitly, let $\hat{A} \subset [n]$ be as in Algorithm 1 and $\hat{B} = [n] \setminus \hat{A}$. Then, for $\Lambda = |0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}}$ (where $|0_{\hat{B}}\rangle$ denotes the zero state on all qubits in $\hat{B}$), define*

$$\rho' = \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{Tr}(\Lambda\rho)}. \tag{B.29}$$

Then, we have

$$\rho'' \triangleq W_{\hat{B}}\rho' W_{\hat{B}} = \rho', \tag{B.30}$$

where $W_{\hat{B}}$ is any permutation unitary which only permutes qubits in $\hat{B}$.

Proof. To see the claim, we can simply expand the expression for ρ'':

$$\begin{aligned}
\rho'' &= W_{\hat{B}}\rho' W_{\hat{B}} && \text{(B.31)}\\
&= W_{\hat{B}} \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{Tr}(\Lambda\rho)} W_{\hat{B}} && \text{(B.32)}\\
&= W_{\hat{B}} \frac{\Lambda\rho\Lambda}{\mathrm{Tr}(\Lambda\rho)} W_{\hat{B}} && \text{(B.33)}\\
&= \frac{W_{\hat{B}}(|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I)\rho(|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I)W_{\hat{B}}}{\mathrm{Tr}(\Lambda\rho)} && \text{(B.34)}\\
&= \frac{(|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I)\rho(|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I)}{\mathrm{Tr}(\Lambda\rho)} && \text{(B.35)}\\
&= \rho', && \text{(B.36)}
\end{aligned}$$

where in the third line we used that Λ is a projector so that $\sqrt{\Lambda} = \Lambda$, and in the fifth line, we used the $W_{\hat{B}}$ only permutes the qubits in $\hat{B}$, which does not have any effect because here all qubits in $\hat{B}$ are in the zero state. □

Lemma 15. *Let $\epsilon, \delta_2 > 0$. The trace distance between ρ and the permuted state $\tilde{\rho} = W_{\hat{B}}\rho W_{\hat{B}}$, where $W_{\hat{B}}$ is any permutation unitary which only permutes qubits in $\hat{B}$, is less than $\epsilon/24$:*

$$\mathrm{d}_{\mathrm{tr}}(\rho, \tilde{\rho}) \leq \frac{\epsilon}{12} \tag{B.37}$$

with probability at least $1 - \delta_2$.

Proof. This proof combines Lemmas 12 and 14. The idea is the following. We know from Lemma 12 that ρ and the post selected state ρ' are close in trace distance. Moreover, by Lemma 14, we know that the post selected state ρ' and the permuted post selected state ρ'' are the equal (without error). We can also show similarly to Lemma 12 that the permuted state $\tilde{\rho}$ is close to the post selected state $\tilde{\rho}'$, where this postselection is done in the same way as Lemma 12 by replacing ρ with $\tilde{\rho}$. Moreover, we can see that $\rho'' = \tilde{\rho}'$, so the claim then follows by triangle inequality.

Now, let us formalize this. By Lemma 12, we have

$$\mathrm{d_{tr}}(\rho, \rho') \leq \frac{\epsilon}{24}, \tag{B.38}$$

with probability at least $1 - \delta_2/2$ (choosing $\delta_1 = \delta_2/2$) where

$$\rho' = \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{Tr}(\Lambda\rho)} \tag{B.39}$$

for $\Lambda = |0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}}$. By Lemma 14, we know that

$$\rho'' \triangleq W_{\hat{B}}\rho' W_{\hat{B}} = \rho', \tag{B.40}$$

where $W_{\hat{B}}$ is a permutation that only affects qubits in $\hat{B}$. Now, consider the permuted state $\tilde{\rho} = W_{\hat{B}}\rho W_{\hat{B}}$. Recall that in the proof of Lemma 12, to obtain Eq. (B.38), it sufficed to show that $\mathrm{Tr}(\Lambda\rho) \geq 1-(\epsilon/24)^2$, and the result followed by the Gentle Measurement Lemma (Lemma 13). Thus, by the same proof, as long as $\mathrm{Tr}(\Lambda\tilde{\rho}) \geq 1 - (\epsilon/24)^2$, then we also have

$$\mathrm{d_{tr}}(\tilde{\rho}, \tilde{\rho}') \leq \frac{\epsilon}{24}, \tag{B.41}$$

with probability at least $1 - \delta_2/2$, where

$$\tilde{\rho}' \triangleq \frac{\sqrt{\Lambda}\tilde{\rho}\sqrt{\Lambda}}{\mathrm{Tr}(\Lambda\tilde{\rho})}. \tag{B.42}$$

We can clearly see that this condition holds:

$$\mathrm{Tr}(\Lambda\tilde{\rho}) = \mathrm{Tr}\big((|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}})W_{\hat{B}}\rho W_{\hat{B}}\big) = \mathrm{Tr}\big((|0_{\hat{B}}\rangle\langle 0_{\hat{B}}| \otimes I_{\hat{A}})\rho\big) = \mathrm{Tr}(\Lambda\rho) \geq 1 - (\epsilon/24)^2, \tag{B.43}$$

where the second equality follows because $W_{\hat{B}}$ only permutes qubits in $\hat{B}$, which (rearranging with the trace) does not have any effect on $|0_{\hat{B}}\rangle\langle 0_{\hat{B}}|$ because all qubits in $\hat{B}$ are in the zero state. Thus, Eq. (B.41) holds.

We also claim that $\rho'' = \tilde{\rho}'$. This follows by effectively the same proof as Lemma 14.

Putting everything together, we have that $\rho' = \rho'' = \tilde{\rho}'$. Thus, by Eq. (B.38),

$$\mathrm{d_{tr}}(\rho, \tilde{\rho}') \leq \frac{\epsilon}{24} \tag{B.44}$$

with probability at least $1 - \delta_2/2$. By triangle equality with Eq. (B.41), we then obtain the claim:

$$\mathrm{d_{tr}}(\rho, \tilde{\rho}) \leq \frac{\epsilon}{12} \tag{B.45}$$

with probability at least $1 - \delta_2$. □

c. Proof of Case (2) of Proposition 4

With this, we can prove Case (2) of Proposition 4. Recall that in Case (2), we require that $G < n/2$. We provided a sketch of the argument throughout the previous sections, so we put everything together here.

Proof of Case (2) of Proposition 4. Let $\epsilon, \delta > 0$. Consider $G < n/2$. Because G is small compared to n, there exist some qubits that have not been acted upon by the G gates used to generate the state $\rho = |\psi\rangle\langle\psi|$. Thus, since we assume that the unknown quantum state ρ is constructed by applying a unitary to the all zero state, then these qubits not acted upon by the G gates remain in the zero state.

Using the techniques in Appendix B 1 a, we can find the qubits that are acted on nontrivially by the G gates. Then, we want to consider the covering net on only this set of qubits. However, because our algorithm does not necessarily find *all* qubits acted on nontrivially by the G gates, we argue in Appendix B 1 b that we can permute the qubits in the system without significantly affecting the original state ρ. In this way, we can consider a permutation which gathers those qubits acted upon nontrivially that our algorithm did not find into some fixed set. We can then define the covering net on the subsystem consisting of this fixed set along with the identified set of qubits.

Let us now formalize these ideas. Let $\hat{A}$ be the set of qubits identified by Algorithm 1, and let A be the true set of qubits acted on nontrivially by the G gates. Let $W_{\hat{B}}$ be a permutation only affecting the qubits in $\hat{B} \triangleq [n] \setminus A$ (Definition 11) which gathers the qubits in $A \setminus \hat{A}$ into some fixed set of qubits C. Since $|C| + |\hat{A}| = |A \setminus \hat{A}| + |\hat{A}| = |A| \leq 2G$, then $C \cup \hat{A}$ has at most $2G$ qubits and these qubits are acted upon by G gates.

By Theorem 8 we know that there exists an $(\epsilon/12)$-covering net $\mathcal{N}_{\epsilon/12}$ of the space of unitaries implemented by G two-qubit gates on the permuted system consisting of only qubits in $C \cup \hat{A}$ with respect to the diamond distance $\mathrm{d}_{\diamondsuit} = \max_\rho \left\| (U \otimes I)\rho(U \otimes I)^\dagger - (V \otimes I)\rho(V \otimes I)^\dagger \right\|_1$. Moreover, this covering net has metric entropy bounded by

$$\log\left(|\mathcal{N}_{\epsilon/12}|\right) \leq 32G \log\left(\frac{144G}{\epsilon}\right) + 2G\log(2G) = \mathcal{O}\left(G\log(G/\epsilon)\right). \tag{B.46}$$

We can instead consider

$$\mathcal{N}'_{\epsilon/12} = \{V' \left|0_{C\cup\hat{A}}\middle\rangle\!\middle\langle 0_{C\cup\hat{A}}\right| V'^\dagger : V' \in \mathcal{N}_{\epsilon/12}\}, \tag{B.47}$$

where $\left|0_{C\cup\hat{A}}\right\rangle$ denotes the zero state on all qubits in our subsystem $C \cup \hat{A}$. By the same argument as in Case (1), $\mathcal{N}'_{\epsilon/12}$ defines a covering net over the set of pure quantum states on the subsystem $C \cup \hat{A}$ generated by G two-qubit gates with respect to trace distance. Moreover, $|\mathcal{N}'_{\epsilon/12}| \leq |\mathcal{N}_{\epsilon/12}|$.

Since this covering net $\mathcal{N}'_{\epsilon/12}$ is only for states on at most $2G$ qubits, let $\mathcal{N}''_{\epsilon/12}$ be the set of states where each state in $\mathcal{N}'_{\epsilon/12}$ is tensored with the zero state for qubits in $[n] \setminus (C \cup \hat{A})$. Let $\tilde{\rho} = W_{\hat{B}}\rho W_{\hat{B}}$ be the original state on this permuted system. By definition of a covering net, we know that there exists some $\sigma_i \in \mathcal{N}''_{\epsilon/12}$ such that

$$\mathrm{d}_{\mathrm{tr}}(\tilde{\rho}, \sigma_i) \leq \frac{\epsilon}{12}. \tag{B.48}$$

We justify this further in the following. By definition, the only qubits in the state $\tilde{\rho}$ that are acted on nontrivially by the G gates are those in $C \cup \hat{A}$. Since no gates act on qubits outside of $C \cup \hat{A}$, then the other qubits in $\tilde{\rho}$ must be in the zero state. Hence, we can write $\tilde{\rho} = \tilde{\rho}_{C\cup\hat{A}} \otimes |0\rangle\!\langle 0|^{\otimes(n-|C\cup\hat{A}|)}$, where $\tilde{\rho}_{C\cup\hat{A}}$ denotes the state of the qubits in $C \cup \hat{A}$ which are acted upon by the G gates. Moreover, by definition of a covering net, then there exists some $\sigma_{i,C\cup\hat{A}} \in \mathcal{N}'_{\epsilon/12}$ such that

$$\mathrm{d}_{\mathrm{tr}}(\tilde{\rho}_{C\cup\hat{A}}, \sigma_{i,C\cup\hat{A}}) \leq \frac{\epsilon}{12}, \tag{B.49}$$

where similarly $\sigma_{i,C\cup\hat{A}}$ is a state on the qubits in $C \cup \hat{A}$ which are acted upon by G gates. Taking the tensor product with the zero state on the remaining qubits does not affect the trace distance. Thus, we can write $\sigma_i = \sigma_{i,C\cup\hat{A}} \otimes |0\rangle\!\langle 0|^{\otimes(n-|C\cup\hat{A}|)} \in \mathcal{N}''_{\epsilon/12}$, where this satisfies

$$\mathrm{d}_{\mathrm{tr}}(\tilde{\rho}, \sigma_i) = \mathrm{d}_{\mathrm{tr}}(\tilde{\rho}_{C\cup\hat{A}}, \sigma_{i,C\cup\hat{A}}) \leq \frac{\epsilon}{12}, \tag{B.50}$$

as claimed. Moreover, by Lemma 15, choosing $\delta_2 = \delta/2$, we know that

$$\mathrm{d}_{\mathrm{tr}}(\rho, \tilde{\rho}) \leq \frac{\epsilon}{12} \tag{B.51}$$

with probability at least $1 - \delta/2$. Recall that this approximation requires only

$$N_1 = \mathcal{O}\left(\frac{G + \log(1/\delta)}{\epsilon^2}\right) \tag{B.52}$$

copies of ρ (from Lemma 12) for identifying the set $\hat{A}$. By triangle inequality, we have that there exists some $\sigma_i \in \mathcal{N}''_{\epsilon/12}$ such that

$$\mathrm{d_{tr}}(\rho, \sigma_i) \leq \frac{\epsilon}{6} \tag{B.53}$$

with probability at least $1 - \delta/2$.

Using hypothesis selection on the covering net $\mathcal{N}''_{\epsilon/12}$ and the unknown state ρ, by Proposition 1, there exists an algorithm to learn σ such that

$$\mathrm{d_{tr}}(\rho, \sigma) \leq \epsilon \tag{B.54}$$

with probability at least $1 - \delta$, where we chose $\eta = \epsilon/6$ and $\epsilon/2, \delta/2$ for the parameters in Proposition 1. Moreover, by Proposition 1 and Equation (B.46), this algorithm requires only

$$N_2 = \mathcal{O}\left(\frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^2}\right) \tag{B.55}$$

copies of ρ. Putting everything together, we have that

$$\mathrm{d_{tr}}(\rho, \sigma) \leq \epsilon \tag{B.56}$$

with probability at least $1 - \delta$, where our algorithm to find σ requires only

$$N = N_1 + N_2 = \mathcal{O}\left(\frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^2}\right). \tag{B.57}$$

This matches our upper bound for Case (1) and thus concludes the proof of Proposition 4. □

2. Sample complexity lower bound

In this section, we prove the sample complexity lower bound for Theorem 12.

Proposition 5 (State learning lower bound)**.** *Let $\epsilon, \delta > 0$. Suppose we are given N copies of an n-qubit pure state density matrix $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = U|0\rangle^{\otimes n}$ is generated by a unitary U consisting of G two-qubit gates. Then, any algorithm that can output $\hat{\rho}$ such that $\mathrm{d_{tr}}(\hat{\rho}, \rho) \leq \epsilon$ with probability at least $1 - \delta$ requires at least*

$$N = \Omega\left(\min\left(\frac{2^n}{\epsilon^2}, \frac{G(1-\delta)}{\epsilon^2\log(G/\epsilon)}\right) + \frac{\log(1/\delta)}{\epsilon^2}\right) \tag{B.58}$$

samples of $|\psi\rangle$.

Here, similarly to the upper bound, we take the minimum with $\Omega(2^n/\epsilon^2)$, as this is the lower bound achieved for full quantum state tomography [19, 20]. We thus focus on the second term in the minimum. We first consider the number of samples required to learn n-qubit pure quantum states generated by G gates *applied only to the first $\lfloor\log_2(G/C)\rfloor$ qubits* (for some constant C specified later) of the $n \geq \lfloor\log_2(G/C)\rfloor$ qubits in total. Denote this set of states as S_1. Note that if $n \leq \lfloor\log_2(G/C)\rfloor$, then we can simply import the lower bound for full quantum state tomography [19, 20]. We later reduce the general case, where the G gates can be applied on any of the qubits, to this case. Namely, we prove the following proposition.

Proposition 6. *Let $\epsilon, \delta > 0$. Suppose we are given N copies of an n-qubit pure state density matrix $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = (U \otimes I)|0\rangle^{\otimes n} \in S_1$ is generated by a unitary U consisting of G two-qubit gates applied only to the first $\lfloor\log_2(G/C)\rfloor$ qubits for some constant C. Then, any algorithm that can output $\hat{\rho}$ such that $\mathrm{d_{tr}}(\hat{\rho}, \rho) \leq \epsilon$ with probability at least $1 - \delta$ requires at least*

$$N = \Omega\left(\min\left(\frac{2^n}{\epsilon^2}, \frac{G(1-\delta)}{\epsilon^2\log(G/\epsilon)}\right) + \frac{\log(1/\delta)}{\epsilon^2}\right) \tag{B.59}$$

samples of $|\psi\rangle$.

We note that for constant error ϵ, the $\Omega(G/\log G)$ lower bound can be improved to $\Omega(G)$ using [161, 162]. We prove Proposition 6 by combining results from [19, 133]. Namely, the lower bound in [19] works by lower bounding the sample complexity of learning any rank r, d-dimensional quantum state in terms of the packing number of this space of states. We apply their results to our setting, where the space of states that the packing net is defined over is S_1 instead. We first recall important results from [19, 133] that we use throughout the proof. [19] lower bounded the sample complexity of learning a d-dimensional pure state as follows.

Theorem 13 (In Proof of Theorem 3 in [19]). *Let $\epsilon \in (0,1)$ and $\delta \in (0,1)$. Suppose there exists a POVM $\{M_\sigma d\sigma\}$ on $(\mathbb{C}^d)^{\otimes N}$ such that for a pure quantum state $\rho \in \mathbb{C}^{d\times d}$,*

$$\int_{\mathrm{d_{tr}}(\sigma,\rho)\leq\epsilon} d\sigma \, \mathrm{Tr}\big[M_\sigma \rho^{\otimes N}\big] \geq 1-\delta. \tag{B.60}$$

Then

$$N \geq \frac{(1-\delta)\ln m - \ln 2}{\chi_0}, \tag{B.61}$$

where m is the size of an (2ϵ)-packing net of the space of d-dimensional pure state density matrices, and

$$\chi_0 \triangleq S(\mathbb{E}_U[U\rho_x U]) - S(\rho_x) \tag{B.62}$$

is the Holevo information, where ρ_x is any element of the (2ϵ)-packing net, S is the von Neumann entropy, and the expectation is taken over the Haar measure.

This states that any measurement procedure which can identify a state ρ up to ϵ-trace distance requires at least N copies of ρ, where N is given by Equation (B.61) and depends on the size of an (2ϵ)-packing net of the space of d-dimensional pure state density matrices. Moreover, [19] bounded the size of such a packing net.

Lemma 16 (Lemma 5 in [19]). *There exists an ϵ-packing net $\{\rho_1,\dots,\rho_m\}$ of the space of d-dimensional pure state density matrices satisfying*

$$c\ln m \geq d, \tag{B.63}$$

for c a sufficiently large constant and $d > 3$. This packing net also satisfies

$$\frac{\chi_0}{c} \leq \epsilon^2 \ln\left(\frac{d}{\epsilon}\right) \tag{B.64}$$

for a sufficiently large constant $c > 0$, where χ_0 is given by Equation (B.62).

Finally, the last result we will need gives a bound on the number of gates needed to generate an arbitrary n-qubit pure state.

Lemma 17 (Section 4 of [133]). *Any n-qubit pure quantum state can be recursively defined as the result of a quantum circuit implemented by $\mathcal{O}(2^n)$ two-qubit gates applied to the $|0\rangle^{\otimes n}$ state. Explicitly, this quantum circuit has at most $C\cdot 2^n$ two-qubit gates for some constant C.*

With these results, we can prove Proposition 6. The idea is that using Lemma 17, any pure state on the first $k \sim \log_2 G$ qubits can be generated by G gates. Then, we can use the same packing net construction as [19] from Lemma 16. Plugging into Theorem 13 then gives our lower bound. We also add an additional term to account for expected asymptotic δ behavior.

Proof of Proposition 6. We wish to construct a (2ϵ)-packing net over the space S_1 of n-qubit pure quantum states generated by applying G gates to the first $k = \lfloor \log_2(G/C)\rfloor$ qubits, where C is taken to be the same constant as in Lemma 17. First, consider only the subsystem consisting of the first k qubits. Notice that by Lemma 17, any k-qubit pure state can be generated by at most G gates. Thus, the space of k-qubit pure states is the same as the space of k-qubit pure states generated by at most G gates. In this way, we can construct a packing net for our subsystem of only the first k qubits by constructing a packing net for all k-qubit pure states. By Theorem 13, there exists an (2ϵ)-packing net $\mathcal{M}_{2\epsilon} = \{\sigma_1,\dots,\sigma_m\}$ of the space of k-qubit pure state density matrices satisfying

$$\ln m \geq \frac{2^k}{c}, \quad \chi_0 \leq 4c\epsilon^2 \ln\left(\frac{2^{k-1}}{\epsilon}\right). \tag{B.65}$$

From this, we can construct a packing net for our entire n-qubit system as follows.

$$\mathcal{M}'_{2\epsilon} \triangleq \{\sigma_i \otimes |0\rangle\langle 0|^{\otimes(n-k)} : \sigma_i \in \mathcal{M}_{2\epsilon}\}; \tag{B.66}$$

We claim that this is indeed a (2ϵ)-packing net of S_1. Let $|\psi\rangle = (U \otimes I)\,|0\rangle^{\otimes n} \in S_1$ and let $\rho = |\psi\rangle\langle\psi|$. Because U only acts on the first k qubits, then we can write $\rho = \rho_k \otimes |0\rangle\langle 0|^{\otimes(n-k)}$, where $\rho_k = U\,|0\rangle\langle 0|^{\otimes k}\,U$. Thus, we can see that $\mathcal{M}'_{2\epsilon} \subseteq S_1$. Importantly, all elements of $\mathcal{M}'_{2\epsilon}$ are n-qubit pure states generated by G gates on the first k qubits. Moreover, for any $\sigma'_i, \sigma'_j \in \mathcal{M}'_{2\epsilon}$, we have

$$\mathrm{d}_{\mathrm{tr}}(\sigma'_i, \sigma'_j) = \mathrm{d}_{\mathrm{tr}}(\sigma_i \otimes |0\rangle\langle 0|^{\otimes(n-k)}, \sigma_j \otimes |0\rangle\langle 0|^{\otimes(n-k)}) = \mathrm{d}_{\mathrm{tr}}(\sigma_i, \sigma_j) > 2\epsilon, \tag{B.67}$$

where the first equality follows by definition of $\mathcal{M}'_{2\epsilon}$ and the last inequality follows because $\sigma_i, \sigma_j \in \mathcal{M}_{2\epsilon}$.

Hence, $\mathcal{M}'_{2\epsilon}$ is indeed a (2ϵ)-packing net of S_1, which is the set of states we wish to learn. Moreover, it is of the same size as $\mathcal{M}_{2\epsilon}$, which had cardinality m satisfying Equation (B.65). Plugging Equation (B.65) into Theorem 13, we have that in order to learn ρ up to ϵ-trace distance, we require

$$N_1 \geq \frac{(1-\delta)\frac{2^k}{c} - \ln 2}{4c\epsilon^2 \ln(2^{k-1}/\epsilon)} \geq C_1 \frac{(1-\delta)G - C_2}{\epsilon^2 \ln(G/(2\epsilon))} = \Omega\left(\frac{G(1-\delta)}{\epsilon^2 \log(G/\epsilon)}\right), \tag{B.68}$$

where in the second inequality, C_1 and C_2 are constants, where C_1 depends on c.

This concludes the proof for the second term in the minimum in Proposition 6. Again, for $n < \lfloor \log_2(G/C) \rfloor$, we can appeal to the full quantum state tomography lower bound of [19, 20]. Thus, we obtain the lower bound

$$N_1 = \Omega\left(\min\left(\frac{2^n}{\epsilon^2}, \frac{G(1-\delta)}{\epsilon^2 \log(G/\epsilon)}\right)\right). \tag{B.69}$$

Notice, however, that in the limit as $\delta \to 0$ one should find $N \to \infty$. This behavior is not captured in Theorem 13 due to the use of the classical Fano's inequality, which treats the measurement procedure as a classical random variable. This behavior is also not present in lower bounds from [19, 20], where they assume that $\delta = \Theta(1)$. In order to recover the dependence on δ, we prove the following lemma.

Lemma 18. *Let $|\psi_0\rangle, |\psi_1\rangle$ be any two n-qubit pure quantum states. Suppose that $|\psi_0\rangle$ and $|\psi_1\rangle$ satisfy $\mathrm{d}_{\mathrm{tr}}(|\psi_0\rangle, |\psi_1\rangle) \geq \epsilon$. Then, for $\delta \in (0,1]$,*

$$N_2 = \Omega\left(\frac{\log(1/\delta)}{\epsilon^2}\right) \tag{B.70}$$

copies of $|\psi\rangle \in \{|\psi_0\rangle, |\psi_1\rangle\}$ are needed to distinguish whether $|\psi\rangle = |\psi_0\rangle$ or $|\psi\rangle = |\psi_1\rangle$ with probability at least $1-\delta$.

Proof. For pure states, we know that the relationship between fidelity and trace distance is given by

$$\mathrm{d}_{\mathrm{tr}}(|\alpha\rangle, |\beta\rangle) = \sqrt{1 - |\langle\alpha|\beta\rangle|^2}. \tag{B.71}$$

In our case, because $\mathrm{d}_{\mathrm{tr}}(|\psi_0\rangle, |\psi_1\rangle) \geq \epsilon$, then we have

$$|\langle\psi_0|\psi_1\rangle|^2 \leq 1 - \epsilon^2. \tag{B.72}$$

Using the Holevo-Helstrom Theorem [132, 163], in order to distinguish $|\psi_0\rangle$ from $|\psi_1\rangle$ with probability at least $1-\delta$, one requires at least N_2 copies of $|\psi\rangle \in \{|\psi_0\rangle, |\psi_1\rangle\}$ satisfying

$$1 - \delta \leq \frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_0|\psi_1\rangle|^{2N_2}} \tag{B.73}$$

Rearranging this inequality, we have

$$N_2 \geq \frac{\log(4\delta(1-\delta))}{\log(|\langle\psi_0|\psi_1\rangle|^2)} = \frac{\log\left(\frac{1}{4\delta(1-\delta)}\right)}{\log\left(\frac{1}{|\langle\psi_0|\psi_1\rangle|^2}\right)} \tag{B.74}$$

By Equation (B.72), this in particular requires

$$N_2 \geq \frac{\log\left(\frac{1}{4\delta(1-\delta)}\right)}{\log\left(\frac{1}{1-\epsilon^2}\right)} = \Omega\left(\frac{\log(1/\delta)}{\epsilon^2}\right). \tag{B.75}$$

□

In our case, note that the conditions of Lemma 18 hold by the existence of the packing net in Equation (B.66), where $|\psi_0\rangle, |\psi_1\rangle$ can be any two states in the packing net. Moreover, because approximating the unknown $|\psi\rangle$ to $(\epsilon/3)$-trace distance suffices to solve the distinguishing task in Lemma 18, then this lower bound also applies for the task of learning a state $|\psi\rangle$. Thus, combining Lemma 18 with Equation (B.69), we have

$$N = \Omega\left(\max\left(N_1, \frac{\log(1/\delta)}{\epsilon^2}\right)\right) = \Omega\left(\min\left(\frac{2^n}{\epsilon^2}, \frac{G(1-\delta)}{\epsilon^2\log(G/\epsilon)}\right) + \frac{\log(1/\delta)}{\epsilon^2}\right), \tag{B.76}$$

as claimed. □

This concludes the proof of Proposition 6. Recall that we are seeking a sample complexity lower bound for states for which we allow our G gates to act on any pair of the n qubits rather than only the first $\lfloor\log_2(G/C)\rfloor$ qubits. We complete the proof of Proposition 5 by reducing to the case of Proposition 6.

Proof of Proposition 5. As before, denote the set of n-qubit quantum states generated by G gates applied to only the first $\lfloor\log_2(G/C)\rfloor$ qubits as S_1. Similarly, denote the set of n-qubit quantum states generated by G gates (applied to any of the qubits) as S_2. Our claim is that the sample complexity of learning states in S_2 is at least the sample complexity of learning states in S_1.

By Proposition 6, we know that the sample complexity of learning states in S_1 is

$$N = \Omega\left(\min\left(\frac{2^n}{\epsilon^2}, \frac{G(1-\delta)}{\epsilon^2\log(G/\epsilon)}\right) + \frac{\log(1/\delta)}{\epsilon^2}\right) \tag{B.77}$$

By the definition of sample complexity, this means that there exists some state $\rho \in S_1$ requiring N copies to learn within ϵ trace distance. Then, because $S_1 \subseteq S_2$, then $\rho \in S_2$ as well. Thus, there exists a state $\rho \in S_2$ that requires N copies to learn, so the sample complexity of learning states within S_2 is at least N as well. □

3. Computational complexity

Theorem 12 states that the sample complexity for learning a description of an unknown n-qubit pure quantum state is linear (up to logarithmic factors) in the number of gates G used to generate the state. Nevertheless, the algorithm described in Appendix B 1 is not computationally efficient, as it constructs and searches over an exponentially large (in G) covering net for all pure states generated by G two-qubit gates. This raises the question: Does there exist a computationally efficient algorithm?

In this section, we first show that there is no polynomial-time algorithm for learning states generated by $G = \mathcal{O}(n\mathsf{polylog}(n))$ gates, assuming $\mathsf{RingLWE}$ cannot be solved efficiently on a quantum computer. This result also holds for states generated by a depth $d = \mathcal{O}(\mathsf{polylog}(n))$ circuit. Then we invoke a stronger assumption that $\mathsf{RingLWE}$ cannot be solved by any sub-exponential-time quantum algorithm, and show that any quantum algorithm for learning states generated by $\tilde{\mathcal{O}}(G)$ gates must use $\exp(\Omega(G))$ time. This means that the computational hardness already kicks in at $G = \tilde{\omega}(\log n)$. Finally, we explicitly construct an efficient learning algorithm for $G = \mathcal{O}(\log n)$, thus establishing $\log n$ gate complexity as a transition point of computational efficiency. Previous work [51, 52] arrives at similar hardness results for polynomial circuit complexity, but our detailed analysis allows us to sharpen the computational lower bound and obtain this transition point.

Theorem 14 (State learning computational complexity lower bound assuming polynomial hardness of $\mathsf{RingLWE}$)**.** *Let $\lambda = n$ be the security parameter and $\mathcal{K}$ be the key space parametrized by λ. Let U be a unitary consisting of $G = \mathcal{O}(n\mathsf{polylog}(n))$ gates (or a depth $d = \mathcal{O}(\mathsf{polylog}(n))$ circuit) that prepares a pseudorandom quantum state $|\phi_k\rangle$ for some randomly chosen key $k \in \mathcal{K}$. Such a unitary U exists by Proposition 3 assuming that $\mathsf{RingLWE}$ cannot be solved by polynomial-time quantum algorithms. Suppose we are given $N = \mathsf{poly}(\lambda)$ copies of $|\phi_k\rangle = U|0\rangle^{\otimes n}$. There does not exist a polynomial-time algorithm for learning a circuit description of $|\phi_k\rangle$ to within $\epsilon \leq 1/8$ trace distance with success probability at least $2/3$.*

Proof. Suppose for the sake of contradiction that there is an efficient algorithm $\mathcal{A}_0$ that can learn a description of $|\phi_k\rangle$ to within ϵ trace distance. Then by standard boosting of success probability (see e.g, [21, Proposition 2.4]), there is an efficient algorithm $\mathcal{A}$ that can learn $|\phi_k\rangle$ to the same accuracy with probability at least $p = 1 - 1/128$ with only a constant factor overhead in time complexity. Note that this boosting requires the distance metric to be efficiently computable, which is guaranteed by the SWAP

Algorithm 2: Distinguisher $\mathcal{D}$ for PRS

```
  Input: $\rho^{\otimes N} = |\psi\rangle\langle\psi|^{\otimes N}$
  Output: $b \in \{0,1\}$
1 Store one copy of $\rho$ in quantum memory.
2 Run $\mathcal{A}$ on inputs $\rho^{\otimes (N-1)}$, receiving $\hat{\rho}$.
3 Run the SWAP test on the remaining copy $\rho$ and $\hat{\rho}$, receiving a bit $b \in \{0,1\}$.
4 Output $b$.
```

test elaborated below. We will construct a polynomial-time quantum distinguisher $\mathcal{D}$ that invokes $\mathcal{A}$ to distinguish between $|\phi_k\rangle$ and a Haar-random state $|\phi\rangle$. This contradicts Definition 10.

The distinguisher $\mathcal{D}$ operates according to Algorithm 2.

Recall that the SWAP test [140, 141] takes two quantum states σ_1, σ_2 as input and outputs 1 with probability $(1+\mathrm{tr}(\sigma_1\sigma_2))/2$. We denote this algorithm as $\mathsf{SWAP}(\sigma_1, \sigma_2)$. Note that here we have switched the labels of 0 and 1 compared to the canonical SWAP test presented in [140, 141].

Notice that the hypothetical efficient learner $\mathcal{A}$ always produces the circuit description of the output state $\hat{\rho}$ in polynomial time. This means that the circuit description and thus the state $\hat{\rho}$ must also be efficiently implementable. As the SWAP test is also efficient, Step 3 of Algorithm 2 can thus indeed be performed efficiently on a quantum computer. Hence, the distinguisher is indeed an efficient quantum algorithm.

Throughout this section, we denote $\rho = |\psi\rangle\langle\psi|$. We analyze the probability that the distinguisher $\mathcal{D}$ outputs 1 when given the pseudorandom state $|\phi_k\rangle$ versus the Haar-random state $|\phi\rangle$.

Case 1: $|\psi\rangle = |\phi_k\rangle$, for a randomly chosen $k \in \mathcal{K}$. We have $\rho = |\psi\rangle\langle\psi| = |\phi_k\rangle\langle\phi_k|$. By the guarantees of $\mathcal{A}$, with probability at least p, we have $\mathrm{d}_{\mathrm{tr}}(\hat{\rho}, \rho) \leq \epsilon$, where $\hat{\rho}$ is the (potentially mixed) quantum state learned by algorithm $\mathcal{A}$. We can rewrite this as

$$\langle\psi|\hat{\rho}|\psi\rangle \geq 1 - \epsilon \tag{B.78}$$

where we used the relationship between fidelity and trace distance (when one state is pure)

$$\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \geq 1 - \langle\psi|\hat{\rho}|\psi\rangle\,. \tag{B.79}$$

Then it immediately follows from Equation (B.78) that

$$\begin{aligned}
\Pr_{\substack{k \leftarrow \mathcal{K} \\ \mathcal{A}, \mathsf{SWAP}}}\left[\mathcal{D}\left(|\phi_k\rangle^{\otimes N}\right) = 1\right] &= \Pr_{\substack{k \leftarrow \mathcal{K} \\ \mathcal{A}, \mathsf{SWAP}}}\left[\mathsf{SWAP}\left(|\phi_k\rangle\langle\phi_k|\,, \hat{\rho}\right) = 1\right] \\
&= \mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}}\left[\Pr_{\mathcal{A}, \mathsf{SWAP}}\left[\mathsf{SWAP}(|\phi_k\rangle\langle\phi_k|\,, \hat{\rho}) = 1 |\, |\phi_k\rangle\right]\right] \\
&\geq p \mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}}\left[\frac{1}{2} + \frac{1}{2}(1-\epsilon)\right] = p\left(1 - \frac{\epsilon}{2}\right),
\end{aligned} \tag{B.80}$$

where the probability is taken over the random choice of the key $k \in \mathcal{K}$, the randomness in the learning algorithm $\mathcal{A}$ when run on samples $|\phi_k\rangle^{\otimes N}$, and the randomness in the SWAP test. In the inequality, we split the probability into two terms conditioned on the success and failure of $\mathcal{A}$, and we lower bound the term conditioned on the failure of $\mathcal{A}$ by zero.

Case 2: $|\psi\rangle = |\phi\rangle \sim \mu$, where μ is the Haar measure over pure quantum states. We have $\rho = |\psi\rangle\langle\psi| = |\phi\rangle\langle\phi|$. We want to upper bound the probability that the distinguisher $\mathcal{D}$ outputs 1 when given copies of $|\phi\rangle$. The intuition is that a Haar-random state is likely to be far from any state generated by a circuits with a polynomial-sized description, the space in which output of $\mathcal{A}$ lie. Let $S_{\mathcal{A}}(|\phi\rangle)$ be the set of quantum states corresponding to all possible outputs of the algorithm $\mathcal{A}$ when run on N copies of $|\phi\rangle$. We follow a similar reasoning as in Equation (B.80) and obtain

$$\Pr_{\substack{|\phi\rangle \sim \mu \\ \mathcal{A}, \mathsf{SWAP}}}\left[\mathcal{D}\left(|\phi\rangle^{\otimes N}\right) = 1\right] \leq \mathop{\mathbb{E}}_{|\phi\rangle \sim \mu}\left[\max_{\hat{\rho} \in S_{\mathcal{A}}(|\phi\rangle)}\left(\frac{1}{2} + \frac{1}{2}\langle\phi|\hat{\rho}|\phi\rangle\right)\right] + (1-p) \tag{B.81}$$

$$= \frac{1}{2} + \frac{1}{2}\mathop{\mathbb{E}}_{|\phi\rangle \sim \mu}\left[\max_{\hat{\rho} \in S_{\mathcal{A}}(|\phi\rangle)}\langle\phi|\hat{\rho}|\phi\rangle\right] + (1-p) \tag{B.82}$$

$$\triangleq \frac{1}{2} + \frac{1}{2}\mathop{\mathbb{E}}_{|\phi\rangle \sim \mu}[O_\phi] + (1-p), \tag{B.83}$$

where in the first line we split the probability according to whether $\mathcal{A}$ succeeds or fails, and we upper bound the failing term by $(1-p)$, and in the last line we define the random variable

$$O_\phi \triangleq \max_{\hat{\rho} \in S_{\mathcal{A}}(|\phi\rangle)} \langle\phi|\hat{\rho}|\phi\rangle \,. \tag{B.84}$$

Furthermore, we can split $\mathbb{E}_{|\phi\rangle\sim\mu}[O_\phi]$ into two parts by introducing a cut-off θ:

$$\mathop{\mathbb{E}}_{|\phi\rangle\sim\mu}[O_\phi] \leq \Pr\left[O_\phi \leq 1-\frac{\theta}{2}\right] \cdot \left(1-\frac{\theta}{2}\right) + \Pr\left[O_\phi > 1-\frac{\theta}{2}\right] \cdot 1 \leq 1-\frac{\theta}{2} + \Pr\left[O_\phi > 1-\frac{\theta}{2}\right], \tag{B.85}$$

where in the first inequality, we used that $O_\phi \leq 1$. Plugging this into our previous expression, we have

$$\Pr_{\substack{|\phi\rangle\sim\mu \\ \mathcal{A},\mathsf{SWAP}}}\left[\mathcal{D}\left(|\phi\rangle^{\otimes N}\right)=1\right] \leq 1-\frac{\theta}{4}+\frac{1}{2}\Pr\left[O_\phi > 1-\frac{\theta}{2}\right] + (1-p) \tag{B.86}$$

We aim to upper bound the probability $\Pr[O_\phi > 1-\theta/2]$. Notice that we have

$$\Pr\left[O_\phi > 1-\frac{\theta}{2}\right] \leq \sum_{\hat{\rho}\in\mathcal{N}_{\sqrt{\theta/2}}} \Pr_{|\phi\rangle\sim\mu}\left[\langle\phi|\hat{\rho}|\phi\rangle > 1-\frac{\theta}{2}\right], \tag{B.87}$$

where $N_{\sqrt{\theta/2}}$ be a minimal $(\sqrt{\theta/2})$-covering net with respect to trace distance of the set $S_{\mathcal{A}}(|\phi\rangle)$ of quantum states corresponding to all possible outputs of the algorithm $\mathcal{A}$ when run on N copies of $|\phi\rangle$. We can bound this probability using concentration results. Let $d = 2^n$.

$$\begin{aligned}
\Pr_{|\phi\rangle\sim\mu}\left[\langle\phi|\hat{\rho}|\phi\rangle > 1-\frac{\theta}{2}\right] &\leq \Pr_{|\phi\rangle\sim\mu}\left[\exp\left(\frac{d}{2}\langle\phi|\hat{\rho}|\phi\rangle\right) \geq \exp\left(\frac{d}{2}\left(1-\frac{\theta}{2}\right)\right)\right] && \text{(B.88)}\\
&\leq \exp\left(-\frac{d}{2}\left(1-\frac{\theta}{2}\right)\right) \mathop{\mathbb{E}}_{|\phi\rangle\sim\mu}\left[\exp\left(\frac{d}{2}\langle\phi|\hat{\rho}|\phi\rangle\right)\right] && \text{(B.89)}\\
&= \exp\left(-\frac{d}{2}\left(1-\frac{\theta}{2}\right)\right) \sum_{k=0}^{\infty} \frac{1}{k!}\frac{d^k}{2^k} \mathop{\mathbb{E}}_{|\phi\rangle\sim\mu}[\langle\phi|\hat{\rho}|\phi\rangle^k] && \text{(B.90)}\\
&= \exp\left(-\frac{d}{2}\left(1-\frac{\theta}{2}\right)\right) \sum_{k=0}^{\infty} \frac{1}{k!}\frac{d^k}{2^k} \frac{1}{\binom{k+d-1}{k}} \operatorname{tr}\left(\hat{\rho}^{\otimes k} P_{\mathrm{sym}}^{(d,k)}\right) && \text{(B.91)}\\
&\leq \exp\left(-\frac{d}{2}\left(1-\frac{\theta}{2}\right)\right) \sum_{k=0}^{\infty} \frac{1}{2^k} \operatorname{tr}\left(\hat{\rho}^{\otimes k} P_{\mathrm{sym}}^{(d,k)}\right) && \text{(B.92)}\\
&\leq 2\exp\left(-\frac{d}{2}\left(1-\frac{\theta}{2}\right)\right). && \text{(B.93)}
\end{aligned}$$

Here, the first two lines follow from the following inequality, which holds for $\alpha > 0$ and a random variable X:

$$\Pr[X \geq \epsilon] \leq \Pr[\exp(\alpha X) \geq \exp(\alpha\epsilon)] \leq \exp(-\alpha X)\,\mathbb{E}[\exp(\alpha X)]. \tag{B.94}$$

The third line follows from the Taylor expansion of $\exp(x)$. The fourth line follow from the identity

$$\mathop{\mathbb{E}}_{|\phi\rangle\sim\mu} \langle\phi|O|\phi\rangle^k = \frac{1}{\binom{k+d-1}{k}} \operatorname{tr}\left(O^{\otimes k} P_{\mathrm{sym}}^{(d,k)}\right), \tag{B.95}$$

where we chose $O = \hat{\rho}$ and $P_{\mathrm{sym}}^{(d,k)}$ is the orthogonal projector onto the symmetric subspace of $(\mathbb{C}^d)^{\otimes k}$. See, e.g., Example 50 in [145] for a proof of this identity. The fifth line follows from the inequality $1/\binom{k+d-1}{k} \leq k!/d^k$. Finally, the last line is true by the following inequalities:

$$\begin{aligned}
\operatorname{tr}\left(\hat{\rho}^{\otimes k} P_{\mathrm{sym}}^{(d,k)}\right) &\leq \left|\operatorname{tr}\left(\hat{\rho}^{\otimes k} P_{\mathrm{sym}}^{(d,k)}\right)\right| && \text{(B.96)}\\
&\leq \left\|\hat{\rho}^{\otimes k} P_{\mathrm{sym}}^{(d,k)}\right\|_1 && \text{(B.97)}\\
&\leq \left\|P_{\mathrm{sym}}^{(d,k)}\right\|_\infty \|\hat{\rho}\|_1^k && \text{(B.98)}
\end{aligned}$$

$$\leq 1, \tag{B.99}$$

which follows via properties of the trace norm and because $P_{\text{sym}}^{(d,k)}$ is a projector. Plugging this back into Equation (B.87), we have

$$\Pr\left[O_\phi > 1 - \frac{\theta}{2}\right] \leq \sum_{\hat{\rho} \in \mathcal{N}_{\sqrt{\theta/2}}} \Pr_{|\phi\rangle \sim \mu}\left[\langle\phi|\hat{\rho}|\phi\rangle > 1 - \frac{\theta}{2}\right] \tag{B.100}$$

$$\leq 2\mathcal{N}(S_{\mathcal{A}}(|\phi\rangle), \mathrm{d}_{\mathrm{tr}}, \sqrt{\theta/2}) \exp\left(-\frac{2^n}{2}\left(1 - \frac{\theta}{2}\right)\right) \tag{B.101}$$

Moreover, since $S_{\mathcal{A}}(|\phi\rangle)$ is the set of quantum states corresponding to all possible outputs of the algorithm $\mathcal{A}$ when run on $|\phi\rangle^{\otimes N}$, then all states in $S_{\mathcal{A}}(|\phi\rangle)$ must have a $\mathsf{poly}(n)$-size circuit description (because $\mathcal{A}$ is assumed to be efficient). Thus our covering number upper bound (setting $G = \mathsf{poly}(n)$ in Appendix B 1) implies

$$\mathcal{N}(S_{\mathcal{A}}(|\phi\rangle), \mathrm{d}_{\mathrm{tr}}, \sqrt{\theta/2}) = \mathcal{O}\left((1/\theta)^{\mathsf{poly}(n)}\right). \tag{B.102}$$

Thus, the above bounds along with Equation (B.101) gives us,

$$\Pr\left[O_\phi > 1 - \frac{\theta}{2}\right] = \mathrm{negl}(n), \tag{B.103}$$

where $\mathrm{negl}(n)$ denotes a negligible function in n. Putting everything together with Equation (B.86), we have

$$\Pr_{\substack{|\phi\rangle \sim \mu \\ \mathcal{A}, \mathsf{SWAP}}}\left[\mathcal{D}\left(|\phi\rangle^{\otimes N}\right) = 1\right] \leq 1 - \frac{\theta}{4} + \mathrm{negl}(n) + (1 - p). \tag{B.104}$$

Combining with Equation (B.80), we conclude that

$$\left|\Pr_{\substack{k \leftarrow \mathcal{K} \\ \mathcal{A}, \mathsf{SWAP}}}\left[\mathcal{D}\left(|\phi_k\rangle^{\otimes N}\right) = 1\right] - \Pr_{\substack{|\phi\rangle \sim \mu \\ \mathcal{A}, \mathsf{SWAP}}}\left[\mathcal{D}\left(|\phi\rangle^{\otimes N}\right) = 1\right]\right| \geq p\left(1 - \frac{\epsilon}{2}\right) - 2 + \frac{\theta}{4} + p - \mathrm{negl}(n) \tag{B.105}$$

$$\geq \frac{1}{16} - \mathrm{negl}(n) \tag{B.106}$$

$$\geq \frac{1}{32}, \tag{B.107}$$

where we have taken $\theta = 1/2, \epsilon \leq 1/8, p = 1 - 1/128$, and the last inequality follows by taking n large enough. This contradicts the assumption that $\{|\phi_k\rangle\}_{k \leftarrow \mathcal{K}}$ are pseudorandom quantum states under the assumption that RingLWE cannot be solved by polynomial-time quantum algorithms. □

Next, we invoke the stronger assumption that RingLWE cannot be solved by any sub-exponential-time quantum algorithm and show that learning states generated by $\tilde{\mathcal{O}}(G)$ gates requires exponential-in-G time.

Theorem 15 (State learning computational complexity lower bound assuming sub-exponential hardness of RingLWE, restatement of lower bound in Theorem 2)**.** *Let $\lambda = l = \Theta(G)$ with $l \leq n$ be the security parameter and $\mathcal{K}$ be the key space parametrized by λ. Let U be an l-qubit unitary consisting of $\mathcal{O}(l\mathsf{polylog}(l)) = \mathcal{O}(G\mathsf{polylog}(G))$ gates (or a depth $d = \mathcal{O}(\mathsf{polylog}(G))$ circuit) that prepares an l-qubit pseudorandom quantum state $|\phi_k\rangle$ against sub-exponential adversaries for some randomly chosen key $k \in \mathcal{K}$. Such a unitary U exists by Proposition 3 assuming that RingLWE cannot be solved by sub-exponential quantum algorithms. Suppose we are given $N = \mathsf{poly}(\lambda)$ copies of $|\psi_k\rangle = |\phi_k\rangle \otimes |0\rangle^{\otimes(n-l)} = U|0\rangle^{\otimes n}$. Any quantum algorithm for learning a circuit description of $|\psi_k\rangle$ to within $\epsilon \leq 1/8$ trace distance with success probability at least $2/3$ must use $\exp(\Omega(\min\{G, n\}))$ time.*

Proof. With polynomial hardness of RingLWE replaced by sub-exponential hardness, Theorem 14 asserts that there are no sub-exponential (in l) quantum algorithms that can learn the l-qubit pseudorandom state $|\phi_k\rangle$ to within trace distance $\epsilon < 1/8$ with success probability at least $2/3$. That is, any such learning algorithms must use time at least $\exp(\Omega(l)) = \exp(\Omega(\min\{G, n\}))$ time, since $l \leq n$. Meanwhile, a learning algorithm for the n-qubit state $|\psi_k\rangle$ can be used to learn the l-qubit state $|\phi_k\rangle$ in the same runtime by post-selecting on the last $(n - l)$ qubits being $|0\rangle$, because trace distance does not increase under such an operation. This implies the $\exp(\Omega(\min\{G, n\}))$ time lower bound for the n-qubit learning algorithm. □

Finally, we briefly show that learning becomes efficient when $G = \mathcal{O}(\log n)$. The idea is that with $\mathcal{O}(\log n)$ gates, there can only be at most $\mathcal{O}(\log n)$ qubits affected. Thus we can focus on these qubits and learning the states amounts to manipulating vectors of size at most $2^{\mathcal{O}(\log n)} = \mathsf{poly}(n)$, which is efficient. Specifically, we have the following statement.

Proposition 7 (Learning states with logarithmic circuit complexity efficiently, restatement of upper bound in Theorem 2)**.** *Let $\epsilon > 0$. Suppose we are given N copies of a pure n-qubit state $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = U\,|0\rangle^{\otimes n}$ is generated by a unitary U consisting of $G = \mathcal{O}(\log n)$ two-qubit gates. There exists a learning algorithm that outputs a $\hat{\rho}$ such that $\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq \epsilon$ with probability at least $2/3$ using $\mathsf{poly}(n, 1/\epsilon)$ copies and time.*

Proof. We prove this by explicitly constructing a learning algorithm based on junta learning (Appendix B 1) and standard tomography methods as follows.

Firstly, we execute Algorithm 1 on copies of ρ and post-select on the trivial qubits being zero as in Appendix B 1. This step uses $\mathsf{poly}(n, 1/\epsilon)$ copies and time, and gives us post-selected states $\rho' = \rho'' \otimes (|0\rangle\langle 0|)^{\otimes(n-2G)}$ that satisfies $\mathrm{d}_{\mathrm{tr}}(\rho, \rho') \leq \epsilon/4$ by appropriate choice of accuracy. Here ρ'' is a state on $2G = \mathcal{O}(\log n)$ qubits.

Next, we carry out the most straightforward tomography method of measuring all the Pauli coefficients. Concretely, we can represent $\rho'' = \sum_P \alpha_P P$ as a linear combination of all Pauli strings over the $2G$ qubits. Using this representation, we estimate all the coefficients α_P by measuring $\mathrm{tr}(\rho' P)$ and obtain a $\hat{\rho} = \hat{\rho}'' \otimes (|0\rangle\langle 0|)^{\otimes(n-2G)}$. By measuring all Pauli string expectation values $\mathrm{tr}(\rho' P)$ to accuracy $\mathcal{O}(\epsilon/4^{2G})$, we have $\mathrm{d}_{\mathrm{tr}}(\rho', \hat{\rho}) \leq \epsilon/4$ and thus $\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq \epsilon/2$. From standard Chernoff-Hoeffding concentration inequalities, this can be achieved with $\mathcal{O}(4^{2G}/(\epsilon/4^{2G})^2) = \mathsf{poly}(n, 1/\epsilon)$ copies. Finally, we diagonalize $\hat{\rho}''$ and calculate its eigenvector $|\hat{\psi''}\rangle$ with the largest eigenvalue, such that $|\hat{\psi''}\rangle$ is the pure state closest to $\hat{\rho}''$ in trace distance. Let $|\hat{\psi}\rangle = |\hat{\psi''}\rangle \otimes |0\rangle^{\otimes(n-2G)}$. Recall that $\mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq \epsilon/2$ and ρ is a pure state. Therefore, $\mathrm{d}_{\mathrm{tr}}(|\hat{\psi}\rangle\langle\hat{\psi}|, \hat{\rho}) \leq \mathrm{d}_{\mathrm{tr}}(\rho, \hat{\rho}) \leq \epsilon/2$ and thus $\mathrm{d}_{\mathrm{tr}}(|\hat{\psi}\rangle\langle\hat{\psi}|, \rho) \leq \epsilon$. We output $|\hat{\psi}\rangle$ as the learning outcome whose circuit description can be found by finding a unitary with $|\hat{\psi''}\rangle$ as its first column using orthogonalization. Since we are manipulating matrices of size $\mathcal{O}(2^{2G}) = \mathsf{poly}(n)$, the computational complexity is also $\mathcal{O}(n, 1/\epsilon)$. □

Appendix C: Learning quantum unitaries

In this appendix, we give detailed proofs of Theorem 3 for worst-case unitary learning, Theorem 4 for average-case unitary learning, and Theorem 5 for learning with classically described data.

1. Worst-case learning

We begin with the worst-case unitary learning problem, which measures reconstruction error in terms of the diamond distance $\mathrm{d}_\diamondsuit(U, V) = \max_\rho \|(U \otimes I)\rho(U \otimes I)^\dagger - (V \otimes I)\rho(V \otimes I)^\dagger\|_1$. In particular, we consider the task of using queries to an unknown unitary U with bounded circuit complexity G to output a classical circuit description $\hat{U}$ such that $\mathrm{d}_\diamondsuit(\hat{U}, U) \leq \epsilon$ with probability at least $2/3$. The diamond distance has a similar operational meaning as the trace distance in state learning. It characterizes the ability to distinguish two processes with arbitrary input states and measurements. If we can learn the unitary with small error in the diamond distance, then we will only make small error even if we test $\hat{U}$ against U on the worst choice of input states. However, we find the following result stating that this task necessarily requires a number of queries exponential in G, indicating the hardness of worst-case unitary learning.

Theorem 16 (Worst-case unitary learning, restatement of Theorem 3)**.** *Given query access to an n-qubit unitary U composed of G two-qubit gates, any algorithm that can output a unitary $\hat{U}$ such that $\mathrm{d}_\diamondsuit(\hat{U}, U) \leq \epsilon \in (0, 1/4]$ with probability at least $2/3$ must query U at least $\Omega\left(2^{\min\{G/(2C), n/2\}}/\epsilon\right)$ times, where $C > 0$ is a universal constant. Meanwhile, there exists such an algorithm using $\mathcal{O}(2^n G \log\left(\sqrt{2^n} G/\epsilon\right)/\epsilon)$ queries.*

Proof. The upper bound follows from the average-case learning algorithm (Theorem 4, proved below) when working in the exponentially small error regime. Specifically, Theorem 4 gives us an algorithm that uses $\mathcal{O}(G\sqrt{d}\log(G/\epsilon')/\epsilon')$ queries to output a $\hat{U}$ that satisfies $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon'$. Meanwhile, from Lemma 1, Lemma 3 and Lemma 4, we know that $\mathrm{d}_\diamondsuit(\hat{U}, U) \leq 2d_2'(\hat{U}, U) \leq 2\sqrt{d}d_F'(\hat{U}, U) \leq 4\sqrt{d}\,\mathrm{d}_{\mathrm{avg}} \leq 4\sqrt{d}\epsilon'$. Setting $\epsilon = 4\sqrt{d}\epsilon'$, we arrive at the desired worst-case learning query complexity.

The proof of the lower bound is inspired by the adversary method [54, Chapter 6] and the optimality of Grover's algorithm [164]. The idea is to construct a set of unitaries that can be distinguished by the worst-case learning algorithm, but only make minor difference when acting on states so that a minimal number of queries have to be made in order to distinguish them.

Specifically, we consider all the length-2^k bit-strings x that have Hamming weight 1, i.e., $x_i = 1$ for some $i \in [2^k]$ and all the other bits are 0. We focus on the task of distinguishing this set of strings, denoted by X, from the all zero string $Y = \{0\dots 0\}$. We access any such bit-strings x through a phase oracle, which is defined as a k-qubit unitary U_x that obeys $U_x |j\rangle = e^{i\epsilon' x_j} |j\rangle$ for all $j \in [2^k]$. In other words, U_x is diagonal and each diagonal element is $e^{i\epsilon'}$ if the corresponding bit is 1 and is 1 if the bit is 0. The unitary for the all zero string is the identity.

To implement such unitaries with 2-qubit gates, we note that since the strings have Hamming weight at most one, each of the unitaries is equivalent to a $(k-1)$-controlled phase gate with proper control rule. The control rule can be realized by $\mathcal{O}(k)$ pairs of 1-qubit gates acting on each qubit, and the $(k-1)$-controlled phase gate can be decomposed into $\mathcal{O}(k)$ 2-qubit gates [165]. Therefore, with $\mathcal{O}(k)$ gates, one can implement U_x for any 2^k-bit string x with Hamming weight at most one.

Suppose Ck gates suffice to implement these U_x. Set $k = \min\{\lfloor G/C \rfloor, n\}$. Then for any $x \in X \cup Y$, $U_x \otimes I_{n-k}$ is an n-qubit gate composed of at most G gates. Meanwhile, the unitaries for X are far apart from that for Y, because for any $x \in X$, suppose $x_j = 1$, we can take another $x' \neq x$ from X with $x'_{j'} = 1$, and let $|\psi_{jj'}\rangle = (|j\rangle + |j'\rangle)/\sqrt{2}$. Then we have

$$\begin{aligned} \mathrm{d}_\Diamond(U_x, U_{0\dots0}) &\geq \|U_x |\psi_{jj'}\rangle\langle\psi_{jj'}| U_x^\dagger - U_{0\dots0} |\psi_{jj'}\rangle\langle\psi_{jj'}| U_{0\dots0}^\dagger\|_1 \\ &= \left\| \frac{e^{i\epsilon'}-1}{2} |j\rangle\langle j'| + \frac{e^{-i\epsilon'}-1}{2} |j'\rangle\langle j| \right\|_1 = 2\sin\frac{\epsilon'}{2} \geq \frac{\epsilon'}{2}, \end{aligned} \tag{C.1}$$

for $\epsilon' \in (0,1]$. Therefore, if we have a learning algorithm that can learn U_T^n using m queries with accuracy $\epsilon = \epsilon'/4 \in (0, 1/4]$ in diamond norm with probability 2/3, it can also distinguish X from Y with the same probability. Note that this also works if the learning algorithm is for (quotient) spectral distance, but not for $\mathrm{d}_{\mathrm{avg}}$ because $\mathrm{d}_{\mathrm{avg}}(U_x, U_{0\dots0})$ is exponentially small for every x with Hamming weight one.

In addition, we have the following query complexity lower bound from the adversary method.

Lemma 19. *(Phase adversary method, [54, Lemma 6.4]). Let D be a finite set of functions from a finite set Q to $\mathbb{R}$. To each function $x \in D$, assign an oracle U_x of the form $U_x|q\rangle = e^{ix(q)}|q\rangle$. Let X and Y be two disjoint subsets of D. Let $R \subseteq X \times Y$ be a binary relation on $X \times Y$. For $x \in X$, we write $R(x) = \{y \in Y : (x,y) \in R\}$, and similarly $R(y)$ for $y \in Y$. Define*

$$m = \min_{x\in X} |R(x)|, \quad m' = \min_{y \in Y} |R(y)|, \quad l_{q,x} = \sum_{y\in R(x)} |x(q) - y(q)|, \quad l_{q,y} = \sum_{x \in R(y)} |x(q)-y(q)|,$$

and let $l_{\max} = \max_{q\in Q, x\in X, y\in Y} l_{q,x} l_{q,y}$. Then to distinguish X and Y with success probability at least 2/3, any algorithm needs at least

$$\Omega\left(\sqrt{\frac{mm'}{l_{\max}}}\right) \tag{C.2}$$

queries to the oracle.

For our problem, let $R = X \times Y$. For all bit-strings x, define $x(q) = \epsilon x_q$. Then we have $m = |Y| = 1, m' = |X| = 2^k, l_{q,x} = \epsilon x_q, l_{q,y} = \epsilon$ because for a specific q, only one $x \in R(y) = X$ has $x_q = 1$. Thus $l_{\max} = \epsilon^2$. Plugging these into the above lemma, we obtain a query complexity lower bound of $\Omega(\sqrt{2^k}/\epsilon)$. Since $k = \min\{\lfloor G/C \rfloor, n\}$, we arrive at the final query complexity lower bound $\Omega\left(2^{\min\{G/(2C), n/2\}}/\epsilon\right)$. □

2. Average-case query complexity upper bounds

Having seen that worst-case unitary learning is hard, we move on to the setting of average-case learning. In particular, we consider the task of using queries to an unknown unitary U with bounded circuit complexity G to output the classical circuit description of a unitary $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) = \sqrt{\mathbb{E}_{|\psi\rangle}[\mathrm{d}_{\mathrm{tr}}(\hat{U}|\psi\rangle, U|\psi\rangle)^2]} \leq \epsilon$ with probability at least 2/3. In the following, we give explicit algorithms that solve this learning task with linear-in-G queries, using similar hypothesis selection techniques as in the state learning task (Appendix B 1).

Proposition 8 (Average case unitary learning upper bounds, upper bounds in Theorem 4)**.** *There exists an algorithm that, given query access to an n-qubit unitary U composed of G two-qubit gates, can output a unitary $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon$ with probability at least $2/3$ using*

$$\mathcal{O}\left(\min\left\{\frac{4^n}{\epsilon}, \frac{G\log(G/\epsilon)}{\epsilon^2}, \frac{\sqrt{2^n}G\log(G/\epsilon)}{\epsilon}\right\}\right) \tag{C.3}$$

queries to the unknown unitary U. Moreover, there is another such algorithm that uses $\mathcal{O}(G\log(G/\epsilon)/\epsilon^4)$ queries without employing auxiliary quantum systems.

The $\mathcal{O}(4^n/\epsilon)$ scaling comes from the diamond norm learning algorithm in [21, Theorem 1.1], which directly implies an average-case learning algorithm because $\mathrm{d}_{\mathrm{avg}}(U,V) \leq d'_F(U,V) \leq d'_2(U,V) \leq \frac{1}{\sqrt{2}}\,\mathrm{d}_{\diamond}(U,V)$ from Lemmas 1, 3 and 4. Note that this part of the bound does not make use of the promise that the unknown unitary can be implemented with G two-qubit gates. In the following, we prove the G-dependent parts of the upper bound.

a. Unitary learning without ancillary systems

We begin by describing the learning algorithm without ancillary systems. The algorithm works similarly to the state learning procedure. It constructs a covering net over G-gate unitaries with respect to $\mathrm{d}_{\mathrm{avg}}$, and regards them as candidates for the unknown unitary. In contrast to our state learning procedure, where the algorithm estimates the trace distance between states, here the algorithm estimates the overlap between unitaries by inputting random states and apply single-shot Clifford classical shadow, which translates into $\mathrm{d}_{\mathrm{avg}}$. Then, we select the candidate closest to the unknown unitary as the learning outcome.

Specifically, we consider a $\sqrt{\epsilon'}$-covering net $\mathcal{N}$ of the set of n-qubit unitaries implemented by G two-qubit gates with respect to $\mathrm{d}_{\mathrm{avg}}$ as in Corollary 1, and regard the elements $U_i \in \mathcal{N}$ as potential candidates for the unknown unitary U. Our strategy is to use classical shadow to estimate the distances $\mathrm{d}_{\mathrm{avg}}(U_i, U)$ for every U_i in the covering net. Then we can find the one with minimal distance as the output of our learning algorithm.

To achieve this, consider a randomly sampled tensor product of 1-qubit stabilizer states

$$|x\rangle = U_x\,|0\rangle^{\otimes n} \sim Q = \mathrm{Uniform}[\{|0\rangle, |1\rangle, |x+\rangle, |x-\rangle, |y+\rangle, |y-\rangle\}^{\otimes n}], \tag{C.4}$$

where $U_x = \otimes_{i=1}^n U_{x_i}$ is the state preparation unitary, and $x \in \mathbb{Z}_6^n$ labels the state. We apply the unknown unitary U to it and obtain $U|x\rangle$. Then we invoke a single use of the Clifford classical shadow protocol [100]: We randomly sample an n-qubit Clifford gate C and apply it to $U|x\rangle$, and then measure in the computational basis to get an outcome $|b\rangle, b \in \{0,1\}^n$, with probability $|\langle b|CU|x\rangle|^2$. Let $\hat{\rho} = (2^n+1)C^\dagger|b\rangle\langle b|C - I$. From [100], we know that $\mathbb{E}_{C,b}[\hat{\rho}] = U|x\rangle\langle x|U^\dagger$. Now we consider the observable $O_i = U_i|x\rangle\langle x|U_i^\dagger$ and the estimator $\hat{o}_i = \mathrm{tr}(O_i\hat{\rho})$. Then we have the expectation value

$$\mathop{\mathbb{E}}_{|x\rangle,C,b}[\hat{o}_i] = \mathop{\mathbb{E}}_{|x\rangle}\left[\mathrm{tr}\left(O_i \mathop{\mathbb{E}}_{C,b}[\hat{\rho}]\right)\right] = \mathop{\mathbb{E}}_{|x\rangle}\left[|\langle x|U_i^\dagger U|x\rangle|^2\right] = 1 - d_Q^2(U_i, U)\,, \tag{C.5}$$

where $d_Q(U_i,U) = \sqrt{\mathbb{E}_{|\psi\rangle\sim Q}[\mathrm{d}_{\mathrm{tr}}(U_i|\psi\rangle, U|\psi\rangle)^2]}$ is the root mean squared trace distance with respect to Q as defined in Lemma 5. Next, we show that $\hat{o}_i$ has bounded variance. Note that

$$\mathrm{Var}[\hat{o}_i] = \mathop{\mathbb{E}}_{|x\rangle,C,b}[\hat{o}_i^2] - \left(\mathop{\mathbb{E}}_{|x\rangle,C,b}[\hat{o}_i]\right)^2 \leq \mathop{\mathbb{E}}_{|x\rangle}\left[\mathop{\mathbb{E}}_{C,b}[\hat{o}_i^2]\right] \leq \mathop{\mathbb{E}}_{|x\rangle}[3\,\mathrm{tr}(O_i^2)] = 3, \tag{C.6}$$

where we have used the variance bound for Clifford shadows [100, Lemma S1 and Proposition S1] and the fact that $\mathrm{tr}(O_i^2) = \mathrm{tr}(O_i) = 1$.

To estimate the expectation values of $\hat{o}_i$, we can draw m i.i.d. samples of such input states $\{|x_j\rangle\}_{j=1}^m$ from Q, construct the observables $O_{ij} = U_i|x_j\rangle\langle x_j|U_i^\dagger$ and carry out the above protocol to get the estimators $\hat{o}_{ij}$ for $1 \leq i \leq |\mathcal{N}|, 1 \leq j \leq m$. Suppose we take $m = NK$ and construct a median-of-mean estimator

$$\hat{o}_i(N,K) = \mathrm{median}\{\hat{o}_i^{(1)}, \ldots, \hat{o}_i^{(K)}\}, \quad \text{where} \quad \hat{o}_i^{(k)} = \frac{1}{N}\sum_{j=N(k-1)+1}^{Nk} \hat{o}_{ij}, \quad 1 \leq k \leq K. \tag{C.7}$$

Then, with the same reasoning as in [100, Theorem S1], we have the following concentration guarantee: For any $0 < \epsilon', \delta < 1$, if $K = 2\log(2|\mathcal{N}|/\delta)$ and $N = 102/\epsilon'^2$, then

$$|\hat{o}_i(N,K) - (1 - d_Q^2(U_i, U))| \le \epsilon' \quad \text{for all} \quad 1 \le i \le |\mathcal{N}| \tag{C.8}$$

with probability at least $1 - \delta$.

With $\hat{o}_i$ in hand, we can select $i^\star \in \operatorname{argmax}_i \hat{o}_i$, and output $U_{i^\star}$. Then we have

$$\begin{aligned} \mathrm{d}_{\mathrm{avg}}(U_{i^\star}, U) &\le \sqrt{2} d_Q(U_{i^\star}, U) \le \sqrt{2(1 - \hat{o}_{i^\star} + \epsilon')} \\ &= \sqrt{2(\epsilon' + \min_i(1 - \hat{o}_i))} \le \sqrt{2(\epsilon' + \min_i(d_Q^2(U_i, U) + \epsilon'))} \le \sqrt{8\epsilon'} \end{aligned} \tag{C.9}$$

with probability at least $1 - \delta$, where we have used the concentration guarantee, Lemma 5, and $\min_i d_Q^2(U_i, U) \le \min_i 2\, \mathrm{d}_{\mathrm{avg}}(U_i, U)^2 \le 2\epsilon'$ because $\mathcal{N}$ is a $\sqrt{\epsilon'}$-covering net with respect to $\mathrm{d}_{\mathrm{avg}}$. Setting $\epsilon' = \epsilon^2/8$, we arrive at a learning algorithm that uses

$$m = NK = \mathcal{O}(\log(|\mathcal{N}|/\delta)/\epsilon^4) \tag{C.10}$$

samples to learn the unknown unitary with accuracy ϵ and success probability at least $1 - \delta$.

If we plug in the covering number upper bound $\log \mathcal{N} \le \mathcal{O}(G \log(G/\epsilon) + T \log n)$ from Corollary 1, we have sample complexity

$$\mathcal{O}\left(\frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^4}\right) \tag{C.11}$$

for large G, say $G \ge n/10$, as desired.

For $G < n/10$, a direct application of the above strategy will give us a suboptimal sample complexity of $\mathcal{O}(G \log(n/\epsilon)/\epsilon^4)$. To overcome this issue, we can carry out a junta learning step similar to Algorithm 1 and [50] to identify the subset of qubits $A \subset [n]$ that U acts non-trivially on. Since U only has G 2-qubit gates, we must have $|A| \le 2G$. The specific procedure is listed in Algorithm 3.

Algorithm 3: Identify qubits acted upon nontrivially (unitary version)

```
Input: Query access to the unknown unitary $U$ with $G$ two-qubit gates.
Output: List $\hat{A} \subseteq [n]$ of qubits.
Initialize $\hat{A} = \emptyset$.
Repeat the following $N = \mathcal{O}\left(\frac{G+\log(1/\delta)}{\epsilon^2}\right)$ times:
    (a) Sample a random tensor product of 1-qubit stabilizer states $|x\rangle = U_x |0\rangle^{\otimes n}$, apply $U$ and $U_x^\dagger$, and obtain $U_x^\dagger U U_x |0\rangle^{\otimes n}$
    (b) Measure in the computational basis and obtain a bit string $|b\rangle, b \in \{0,1\}^n$
    (b) Given the measurement outcome $|b\rangle$, set $\hat{A} \leftarrow \hat{A} \cup \mathrm{supp}(b)$, where $\mathrm{supp}(b) = \{i \in [n] : b_i \neq 0\}$.
```

Similar to Appendix B 1 a, we use Algorithm 3 to identify the non-trivial qubits with high probability. Importantly, from Lemma 11, we have the following guarantee that shows the expected state on the estimated trivial qubits is close to zero.

Lemma 20. *Let $\epsilon, \delta > 0$. Suppose we are given query access to an n-qubit unitary U composed of G two-qubit gates acting on a subset of the qubits $A \subseteq [n]$. Let $|x\rangle = U_x |0\rangle^{\otimes n}$ be a random tensor product of 1-qubit stabilizer states. Let $\rho^x = U_x^\dagger U U_x |0\rangle\langle 0| U_x^\dagger U^\dagger U_x$. Then, Algorithm 3 uses $N = \mathcal{O}\left(\frac{G+\log(1/\delta)}{\epsilon^2}\right)$ queries to U and outputs, with probability at least $1 - \delta$, a list $\hat{A} \subset [n]$ such that*

$$\left\langle 0_{\hat{B}} \middle| \mathbb{E}_x[\rho^x_{\hat{B}}] \middle| 0_{\hat{B}} \right\rangle \ge 1 - \epsilon^2, \tag{C.12}$$

where $\rho_{\hat{B}}$ denotes the reduced density matrix of ρ when tracing out all qubits other than those in the set $\hat{B} = [n] \setminus \hat{A}$ and $\left|0_{\hat{B}}\right\rangle$ denotes the zero state on all qubits in $\hat{B}$.

Proof. This follows directly from the proof of Lemma 11 because Algorithm 3 is the same as executing Algorithm 1 on the mixed state $\mathbb{E}_x[\rho^x]$, and for the trivial qubits, the $U_x^\dagger$ following U_x and U restores the state to $|0\rangle$. So the proof goes verbatim as in Lemma 11. □

With this, we can show that ignoring the rest of the qubits $\hat{B} = [n] \setminus \hat{A}$ does not make much of a difference. Let $B = [n] \setminus A$. We again consider a randomly sampled 1-qubit stabilizer state and apply U to get $|\psi_x\rangle = UU_x |0\rangle^{\otimes n}$. Let $\rho_x = |\psi_x\rangle \langle\psi_x|$ be the associated density matrix, and let $U_x^{\hat{B}} = \otimes_{j\in\hat{B}} U_{x_j}$ be the part of U_x that acts on $\hat{B}$. Now we measure the qubits in $\hat{B}$ in the basis $U_x^{\hat{B}} |b\rangle_{\hat{B}}$, where $b \in \{0,1\}^{|\hat{B}|}$. Note that for qubits in $\hat{B}$, the reduced density matrix in the basis $U_x^{\hat{B}} |b\rangle_{\hat{B}}$ is the same as the $\rho^x_{\hat{B}}$ from Lemma 20 in the junta learning step. So we have $\langle 0_{\hat{B}} | \mathbb{E}_x[\rho^x_{\hat{B}}] | 0_{\hat{B}} \rangle \geq 1 - \epsilon^2$. After the measurement of the qubits in $\hat{B}$, we do a post-selection on the observed measurement outcomes being $U_x^{\hat{B}} |0\rangle_{\hat{B}}$. This post-selection is represented by $\Lambda = I_A \otimes (U_x^{\hat{B}} |0\rangle_{\hat{B}} \langle 0| U_x^{\hat{B}\dagger})$, with $\Lambda^2 = \Lambda$. Let $\rho'_x = \frac{\sqrt{\Lambda}\rho_x\sqrt{\Lambda}}{\mathrm{tr}(\Lambda\rho_x)}$ be the post-selected state. Now we want to show ρ'_x is close to ρ_x on average. We invoke the following gentle measurement lemma for normalized ensembles.

Lemma 21 (Gentle measurement lemma for normalized ensembles, variant of [166, Lemma 9.4.3])**.** *Let $\{x, \rho_x\}$ be an ensemble of states. If Λ is a positive semi-definite operator with $\Lambda \leq I$ and $\mathrm{tr}(\Lambda\mathbb{E}_x[\rho_x]) \geq 1 - \epsilon$ where $\epsilon \in [0,1]$, then*

$$\mathbb{E}_x \left\| \rho_x - \frac{\sqrt{\Lambda}\rho_x\sqrt{\Lambda}}{\mathrm{tr}(\Lambda\rho_x)} \right\|_1 \leq 3\sqrt{\epsilon}. \tag{C.13}$$

Proof. Let $\rho'_x = \frac{\sqrt{\Lambda}\rho_x\sqrt{\Lambda}}{\mathrm{tr}(\Lambda\rho_x)}$. From [166, Lemma 9.4.3], we know that $\mathbb{E}_x \left\| \rho_x - \sqrt{\Lambda}\rho_x\sqrt{\Lambda} \right\|_1 \leq 2\sqrt{\epsilon}$. Note that the left hand side can be lower bounded by

$$\begin{aligned}
\mathbb{E}_x \left\| \rho_x - \sqrt{\Lambda}\rho_x\sqrt{\Lambda} \right\|_1 &= \mathbb{E}_x \left\| \rho_x - \rho'_x + \rho'_x - \sqrt{\Lambda}\rho_x\sqrt{\Lambda} \right\|_1 \\
&\geq \mathbb{E}_x\|\rho_x - \rho'_x\|_1 - \mathbb{E}_x\|\rho'_x - \sqrt{\Lambda}\rho_x\sqrt{\Lambda}\|_1 \\
&= \mathbb{E}_x\|\rho_x - \rho'_x\|_1 - \mathbb{E}_x(1 - \mathrm{tr}(\Lambda\rho_x))\|\rho'_x\|_1 \geq \mathbb{E}_x\|\rho_x - \rho'_x\|_1 - \epsilon,
\end{aligned} \tag{C.14}$$

where we have used triangle inequality, $\|\rho'_x\|_1 = 1$, and $\mathrm{tr}(\Lambda\mathbb{E}_x[\rho_x]) \geq 1 - \epsilon$. Therefore, we arrive at

$$\mathbb{E}_x\|\rho_x - \rho'_x\|_1 \leq 2\sqrt{\epsilon} + \epsilon \leq 3\sqrt{\epsilon}, \tag{C.15}$$

because $\epsilon \in [0,1]$, concluding the proof of Lemma 21. □

Using Lemma 21 for our scenario, we have $\mathbb{E}_x\|\rho_x - \rho'_x\|_1 \leq 3\epsilon$ with probability at least $1-\delta$. After the post-selection, we apply the same Clifford shadow strategy as in the $T \geq n/10$ case, with two differences. Firstly, note that after post-selection, the action on every qubit in $\hat{B}$ is identity. So we can without loss of generality pick an arbitrary subset A' of those qubits in $\hat{B}$ as $A \setminus \hat{A}$, and consider an $\sqrt{\epsilon}$-covering net $\mathcal{N}$ of G gate unitaries on qubits $\hat{A} \cup A'$ with respect to $\mathrm{d}_{\mathrm{avg}}$, with $|\hat{A} \cup A'| = |A| \leq 2G$. Then we have $\min_{U_i\in\mathcal{N}} \mathrm{d}_{\mathrm{avg}}(U_i, U) \leq \epsilon$, and $\log|\mathcal{N}| \leq \mathcal{O}(G\log(G/\epsilon) + G\log(|A \cup A'|)) \leq \mathcal{O}(G\log(G/\epsilon))$. Secondly, for each element U_i in the covering net, we can construct an observable $O_i = U_i |x\rangle \langle x| U_i^\dagger$ similar to before, but now the estimator will concentrate around a slightly different expectation value. Specifically, if we use a median-of-mean estimator $\hat{o}_i(N,K)$ with $K = 2\log(2|\mathcal{N}|/\delta)$ and $N = 102/\epsilon^2$, then we have

$$|\hat{o}_i(N,K) - \mathbb{E}_x[\mathrm{tr}(\rho'_x O_i)]| \leq \epsilon \quad \text{for all} \quad 1 \leq i \leq |\mathcal{N}|, \tag{C.16}$$

with probability at least $1 - \delta$. Nevertheless, since ρ'_x and ρ_x are close on average, we have

$$\begin{aligned}
|\hat{o}_i(N,K) - (1 - d_Q^2(U_i \otimes I, U))| &= |\hat{o}_i(N,K) - \mathbb{E}_x[\mathrm{tr}(\rho'_x O_i)] + \mathbb{E}_x[\mathrm{tr}(\rho'_x O_i)] - \mathbb{E}_x[\mathrm{tr}(\rho_x O_i)]| \\
&\leq |\hat{o}_i(N,K) - \mathbb{E}_x[\mathrm{tr}(\rho'_x O_i)]| + \mathbb{E}_x[|\,\mathrm{tr}(\rho'_x O_i) - \mathrm{tr}(\rho_x O_i)|] \\
&\leq \epsilon + \mathbb{E}_x[\|\rho'_x - \rho_x\|_1\|O_i\|] \leq \epsilon + 3\epsilon = 4\epsilon, \quad \text{for all} \quad 1 \leq i \leq |\mathcal{N}|,
\end{aligned} \tag{C.17}$$

with probability at least $1-2\delta$, where we have used triangle inequality, $\|O_i\| = 1$, and $\mathbb{E}_x\|\rho_x - \rho'_x\|_1 \leq 3\epsilon$. With this concentration guarantee, we can select the candidate with the largest $\hat{o}_i$: $i^\star \in \mathrm{argmax}_i \hat{o}_i$ and output $U_{i^\star} \otimes I$. As before, we have with probability at least $1 - 2\delta$,

$$\mathrm{d}_{\mathrm{avg}}(U_{i^\star} \otimes I, U) \leq \sqrt{2} d_Q(U_{i^\star} \otimes I, U) \leq \sqrt{2(4\epsilon + 2\epsilon + 4\epsilon)} = \sqrt{20\epsilon}. \tag{C.18}$$

Redefining 20ϵ to be ϵ^2 and 2δ to be δ, we arrive at a learning algorithm that uses

$$m = \mathcal{O}\left(\frac{G + \log(1/\delta)}{\epsilon^4}\right) + NK = \mathcal{O}\left(\frac{G\log(G/\epsilon) + \log(1/\delta)}{\epsilon^4}\right) \tag{C.19}$$

queries to the unitary to learn it with accuracy ϵ in $\mathrm{d}_{\mathrm{avg}}$ and success probability at least $1-\delta$ when $G < n/10$. Combined with the case of $G \geq n/10$, this concludes the learning algorithm without ancillary system in Proposition 8.

b. Unitary learning with ancillary systems

The above $\mathcal{O}(1/\epsilon^4)$ scaling is suboptimal. It arises from the fact that in the classical shadow estimation, the estimated quantity is the square of $\mathrm{d}_{\mathrm{avg}}$ rather than $\mathrm{d}_{\mathrm{avg}}$ itself. To improve the ϵ-dependence, we make use ancillary systems via the Choi–Jamiołkowski duality [58–60]. Specifically, we consider the maximally entangled state over a pair of n-qubit systems $|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{2^n}|i\rangle \otimes |i\rangle$ and define the Choi state $|U\rangle\!\rangle$ corresponding to a unitary U as $|U\rangle\!\rangle = (U \otimes I)\,|\Phi\rangle$. That is, the Choi state $|U\rangle\!\rangle$ of an n-qubit unitary U is a pure $(2n)$-qubit state constructed by applying U on half of the qubits in n EPR pairs. For any subset $A \subseteq [n]$ of the qubits that are acted upon by U, we refer to the corresponding $|A|$ qubits in the EPR pairs as the entangled qubits corresponding to A. We note the following fact, which relates the trace distance between Choi states to the average-case distance between the unitaries.

Lemma 22 (Equivalence of trace distance between Choi states and average-case distance)**.** *Let $U, V \in U(2^n)$ be two n-qubit unitaries, $|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{2^n}|i\rangle \otimes |i\rangle$ be a maximally entangled state, and $|U\rangle\!\rangle = (U \otimes I)\,|\Phi\rangle\,, |V\rangle\!\rangle = (V \otimes I)\,|\Phi\rangle$ be the corresponding Choi states. Then we have*

$$\frac{1}{\sqrt{2}}\,\mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |V\rangle\!\rangle) \leq \mathrm{d}_{\mathrm{avg}}(U,V) \leq \mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |V\rangle\!\rangle). \tag{C.20}$$

Proof. By the standard conversion between fidelity and the trace distance between pure states, we have

$$\mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |V\rangle\!\rangle) = \sqrt{1 - |\langle\!\langle U|V\rangle\!\rangle|^2} = \sqrt{1 - \frac{1}{d^2}|\operatorname{tr}(U^\dagger V)|^2.}, \tag{C.21}$$

where the last step used that $\langle\Phi|\,A \otimes B\,|\Phi\rangle = \frac{1}{d}\operatorname{tr}\bigl[A^T B\bigr]$, compare for instance [167, Example 1.2]. On the other hand, from Equation (A.14), we have

$$\mathrm{d}_{\mathrm{avg}}(U,V) = \sqrt{1 - \frac{d + |\operatorname{tr}(U^\dagger V)|^2}{d^2 + d}}. \tag{C.22}$$

Combining these two equations, we get

$$\mathrm{d}_{\mathrm{avg}}(U,V) = \sqrt{\frac{d}{d+1}}\,\mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |V\rangle\!\rangle) \in \left[\frac{1}{\sqrt{2}}\,\mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |V\rangle\!\rangle), \mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |V\rangle\!\rangle)\right]. \tag{C.23}$$

□

With Lemma 22, we construct a covering net over Choi states corresponding to G-gate unitaries as follows. From Corollary 1, we take an ϵ'-covering net $\mathcal{N}$ of G-gate unitaries with respect to $\mathrm{d}_{\mathrm{avg}}$ that has cardinality $|\mathcal{N}| \leq \mathcal{O}(G\log(G/\epsilon) + G\log n)$. Then for any G-gate unitary U, there exists a $U_i \in \mathcal{N}$ such that $\mathrm{d}_{\mathrm{avg}}(U, U_i) \leq \epsilon'$. Hence $\mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |U_i\rangle\!\rangle) \leq \sqrt{2}\,\mathrm{d}_{\mathrm{avg}}(U, U_i) \leq \sqrt{2}\epsilon'$ by Lemma 22. Therefore, the Choi states of the unitaries in $\mathcal{N}$ form a $(\sqrt{2}\epsilon)$-covering net of the Choi states of G-gate unitaries.

Now, we can use these pure Choi states as candidates for hypothesis selection. By Proposition 1, the hypothesis selection algorithm based on classical shadow uses $\mathcal{O}(\log(|\mathcal{N}|/\delta)/\epsilon'^2)$ samples of the Choi state $|U\rangle\!\rangle$ to output a candidate $|\hat{U}\rangle\!\rangle, \hat{U} \in \mathcal{N}$, such that $\mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |\hat{U}\rangle\!\rangle) \leq 3\sqrt{2}\epsilon' + \epsilon'$ with probability at least $1-\delta$. Setting $(3\sqrt{2}+1)\epsilon' = \epsilon$, we find a $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \mathrm{d}_{\mathrm{tr}}(|U\rangle\!\rangle, |\hat{U}\rangle\!\rangle) \leq \epsilon$ with probability at least $1-\delta$ using

$$\mathcal{O}\left(\frac{G\log(G/\epsilon) + G\log n + \log(1/\delta)}{\epsilon^2}\right) \tag{C.24}$$

queries to the unknown unitary U. When $G \geq n/10$, this gives the desired $\mathcal{O}((G\log(G/\epsilon) + \log(1/\delta))/\epsilon^2)$ query complexity.

Algorithm 4: Identify qubits acted upon nontrivially (Choi version)

```
Input: Query access to the unknown unitary $U$ with $G$ two-qubit gates.
Output: List $\hat{A} \subseteq [n]$ of qubits.
1 Initialize $\hat{A} = \emptyset$.
2 Repeat the following $N = \mathcal{O}\left(\frac{G+\log(1/\delta)}{\epsilon^2}\right)$ times:
    (a) Prepare the Choi state $|U\rangle\rangle$ by applying $U \otimes I$ to the maximally entangled state $|\Phi\rangle$
    (b) Measure in the basis of Pauli Choi states $|\sigma_x\rangle\rangle = \otimes_{i=1}^n (\sigma_{x_i} \otimes I)\,|\Phi\rangle, x \in \mathbb{Z}_4^n$, and obtain a string $|b\rangle, b \in \{0,1,2,3\}^n$
    (b) Given the measurement outcome $|b\rangle$, set $\hat{A} \leftarrow \hat{A} \cup \mathrm{supp}(b)$, where $\mathrm{supp}(b) = \{i \in [n] : b_i \neq 0\}$.
```

For $G < n/10$, we again need a junta learning step to identify the set of qubits $A \subseteq [n]$ that are acted on non-trivially. To do this, we follow the idea of Algorithm 1, Algorithm 3 and [50, Algorithm 8] and consider the following procedure that makes use of Choi states of Pauli matrices $\sigma_0 = I, \sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z$.

Similarly to Lemma 11 and Lemma 20, we have the following guarantee that the Choi state on the estimated trivial qubits is close to the Choi state of the identity.

Lemma 23. *Let $\epsilon, \delta > 0$. Suppose we are given query access to an n-qubit unitary U composed of G two-qubit gates acting on a subset of the qubits $A \subseteq [n]$. Let $\rho = |U\rangle\rangle\langle\langle U|$ be the Choi state of U. Then, Algorithm 4 uses $N = \mathcal{O}\left(\frac{G+\log(1/\delta)}{\epsilon^2}\right)$ queries to U and outputs, with probability at least $1-\delta$, a list $\hat{A} \subset [n]$ such that*

$$\langle\langle I_{\hat{B}}|\rho_{\hat{B}}|I_{\hat{B}}\rangle\rangle \geq 1 - \epsilon^2, \tag{C.25}$$

where $\rho_{\hat{B}}$ denotes the reduced density matrix for ρ by tracing out all qubits other than those in the set $\hat{B} = [n] \setminus \hat{A}$ and the corresponding entangled qubits, and $|I_{\hat{B}}\rangle\rangle$ denotes the Choi state of the identity on qubits in $\hat{B}$.

Proof. The proof goes similarly to that of Lemma 11 except that $|0\rangle$ is replaced by $|I\rangle\rangle$. The measurement over Pauli Choi states in Algorithm 4 can be understood as measuring each entangled pair of qubits in the basis $\{|I\rangle\rangle, |X\rangle\rangle, |Y\rangle\rangle, |Z\rangle\rangle\}$ and gives an element from $\{0,1,2,3\} = \mathbb{Z}_4$. Specifically, let A' be any set that could be output by Algorithm 4. We want to identify A' with the actual identified set $\hat{A}$. Let $B' \triangleq [n] \setminus A'$. Let $E_{i,A'}$ be the event that round i of measurement of the qubits in $B' = [n] \setminus A'$ in Algorithm 4 yields the all zero $\mathbb{Z}_4$ string. Let $X_{i,A'}$ be the indicator random variable corresponding to the event $E_{i,A'}$. Then, we have that $\bar{X}_{A'} \triangleq \frac{1}{N}\sum_{i=1}^N X_{i,A'}$ is the number of times the entangled pair in B' are all measured to be zero divided by the total number of measurements. In other words, $\bar{X}_{A'}$ is the estimated overlap that the state $\rho_{B'}$ on qubits in B' has with the identity Choi state on B'. Moreover, we have

$$\mathbb{E}[X_{A'}] \triangleq \mathbb{E}[X_{i,A'}] = \langle\langle I_{B'}|\rho_{B'}|I_{B'}\rangle\rangle \tag{C.26}$$

for all A'. This says that the true expectation of our random variables is the true overlap of the state $\rho_{B'}$ with the identity Choi state on B'. Then we have the same Claim 1 as in Lemma 11 and Lemma 23 follows. □

With this, we can again show that ignoring the rest of the qubits $\hat{B} = [n] \setminus \hat{A}$ does not make much difference. Let $B = [n] \setminus A$. We prepare the Choi state $\rho = |U\rangle\rangle\langle\langle U|, |U\rangle\rangle = (U \otimes I)\,|\Phi\rangle$, and measure in the basis of Pauli Choi states over the qubits in $\hat{B}$: $\{|\sigma_x\rangle\rangle_{\hat{B}} : x \in \mathbb{Z}_4^{|\hat{B}|}\}$. After the measurement, we do a post-selection on the observed measurement outcomes being $|I_{\hat{B}}\rangle\rangle$. This post-selection is represented by $\Lambda = I \otimes |I_{\hat{B}}\rangle\rangle\langle\langle I_{\hat{B}}|$, with $\Lambda^2 = \Lambda$, and the first identity over the entangled pairs outside $\hat{B}$. Let $\rho' = \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{tr}(\Lambda\rho)}$ be the post-selected state. Now we want to show ρ' is close to ρ. From Lemma 23, we know that $\mathrm{tr}(\Lambda\rho) \geq 1-\epsilon^2$ with probability at least $1-\delta$. Then by the gentle measurement lemma (Lemma 13), we have $\mathrm{d}_{\mathrm{tr}}(\rho', \rho) \leq \epsilon$ with the same probability.

Now we can apply the hypothesis selection protocol to ρ' as in the $G > n/10$ case, but with a different covering net. Specifically, note that after post-selection, the action on every entangled pair in $\hat{B}$ is identity. So we can with loss of generality pick an arbitrary subset A' of those qubits in $\hat{B}$ as $A \setminus \hat{A}$, and consider an ϵ-covering net $\mathcal{N}$ of G gate unitaries on qubits $\hat{A} \cup A'$ with respect to $\mathrm{d}_{\mathrm{avg}}$, with $|\hat{A} \cup A'| = |A| \leq 2G$, with each element tensor product with identity over the rest qubits. Then we have $\min_{U_i\in\mathcal{N}} \mathrm{d}_{\mathrm{tr}}(|U_i\rangle\!\rangle, |U\rangle\!\rangle) \leq \sqrt{2}\,\mathrm{d}_{\mathrm{avg}}(U_i, U) \leq \sqrt{2}\epsilon$, and $\log|\mathcal{N}| \leq \mathcal{O}(G\log(G/\epsilon) + G\log(|A\cup A'|)) \leq \mathcal{O}(G\log(G/\epsilon))$. Since $\mathrm{d}_{\mathrm{tr}}(\rho', \rho) \leq \epsilon$, we also have $\min_{U_i\in\mathcal{N}} \mathrm{d}_{\mathrm{tr}}(|U_i\rangle\!\rangle\langle\!\langle U_i|, \rho') \leq \epsilon + \sqrt{2}\epsilon = (\sqrt{2}+1)\epsilon$.

With this covering net, we apply the hypothesis selection based on classical shadow (Proposition 1) to ρ'. This procedure uses $\mathcal{O}(\log(|\mathcal{N}|/\delta)/\epsilon^2)$ copies of ρ' (each prepared using one query to U) and output a $|U_{i^\star}\rangle\!\rangle$ such that $\mathrm{d}_{\mathrm{tr}}(|U_{i^\star}\rangle\!\rangle\langle\!\langle U_{i^\star}|, \rho') \leq 3(\sqrt{2}+1)\epsilon + \epsilon = (3\sqrt{2}+4)\epsilon$ with probability at least $1-\delta$. This means that

$$\mathrm{d}_{\mathrm{avg}}(U_{i^\star}, U) \leq \mathrm{d}_{\mathrm{tr}}(|U_{i^\star}\rangle\!\rangle, |U\rangle\!\rangle) \leq \mathrm{d}_{\mathrm{tr}}(|U_{i^\star}\rangle\!\rangle\langle\!\langle U_{i^\star}|, \rho') + \mathrm{d}_{\mathrm{tr}}(\rho', \rho) \leq (3\sqrt{2}+4)\epsilon + \epsilon = 4(\sqrt{2}+1)\epsilon \quad \text{(C.27)}$$

with a total probability at least $1-2\delta$ (considering both the junta learning and hypothesis selection).

Therefore, by redefining $4(\sqrt{2}+1)\epsilon$ to be ϵ and 2δ to be δ, we arrive at a desired algorithm for $G \leq n/10$ that uses in total

$$\mathcal{O}\left(\frac{G+\log(1/\delta)}{\epsilon^2}\right) + \mathcal{O}\left(\frac{G\log(G/\epsilon)+\log(1/\delta)}{\epsilon^2}\right) = \mathcal{O}\left(\frac{G\log(G/\epsilon)+\log(1/\delta)}{\epsilon^2}\right) \quad \text{(C.28)}$$

queries to the unknown unitary U. Combined with the $G \geq n/10$ case, we conclude the learning algorithm with ancillary system that achieves the $\mathcal{O}((G\log(G/\epsilon)+\log(1/\delta)/\epsilon^2)$ query complexity in Proposition 8.

c. *Bootstrap to improve ϵ-dependence*

To further improve the ϵ-dependence, we modify the bootstrap method in [21] and achieve a Heisenberg scaling $\tilde{\mathcal{O}}(1/\epsilon)$. However, with our average case distance, which can only control the average behavior of the eigenvalues of the unitaries, we are not able to perform the bootstrap for general ϵ. Instead, the bootstrap works only when the error is exponentially small, $\epsilon = O(1/\sqrt{d})$, and achieves the Heisenberg scaling at the cost of a dimensional factor, leading to a query complexity of

$$\mathcal{O}\left(\frac{\sqrt{2^n}(G\log(G/\epsilon)+\log(1/\delta))}{\epsilon}\right). \quad \text{(C.29)}$$

Whether a general Heisenberg scaling without dimension-dependent scaling is achievable remains open.

Now we state the bootstrap method in Algorithm 5, which uses the unitary learning algorithm with ancillary systems (Appendix C 2 b) as a sub-routine. We need to prove two things about Algorithm 5: (1) it outputs a $\hat{U}$ that satisfies $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon$ with probability at least $1-\delta$; (2) the query complexity is $\mathcal{O}\left(\sqrt{d}(G\log(G/\epsilon)+\log(1/\delta))/\epsilon\right)$.

Algorithm 5: Bootstrapping to Heisenberg scaling

```
Input:  Query access to the unknown $n$-qubit $G$-gate unitary $U$.
        An error parameter $\epsilon \in (0, 1/\sqrt{d})$.
Output: A unitary $\hat{U}$.
Let $t \leftarrow \left\lceil \log_2(1/(\epsilon\sqrt{d})) \right\rceil$.
Let $V_0 \leftarrow I$.
Let $\mathcal{N} \leftarrow$ an $(\epsilon/10^5)$-covering net of $G$-gate unitaries with respect to $\mathrm{d}_{\mathrm{avg}}$.
for $j \leftarrow 0$ to $t$ do
    Let $p_j \leftarrow 2^j$.
    Let $\eta_j \leftarrow 8^{j-t-1}\delta$.
    Use the algorithm $\mathcal{A}$ in Appendix C 2 b with success probability $1-\eta_j$ and accuracy $1/(25000\sqrt{d})$ to
      find a candidate $R_j$ in $\{(U_iV_j^\dagger)^{p_j} \mid U_i \in \mathcal{N}\}$ that is closest to $(UV_j^\dagger)^{p_j}$ in $\mathrm{d}_{\mathrm{avg}}$.
    Let $V_{j+1} \leftarrow R_j^{1/p_j}V_j$.
return $\hat{U} \leftarrow V_{t+1}$
```

We first prove (1) by induction. Before doing so, we need to show that the learning algorithm $\mathcal{A}$ can indeed learn $(UV_j^\dagger)^{p_j}$ well for all j. Let $c = 10^{-5}$. Note that with the definition of $\mathcal{N}$, we know that for any G-gate unitary U, $\exists U_i \in \mathcal{N}$ such that $\mathrm{d}_{\mathrm{avg}}(U, U_i) \leq c\epsilon$, and therefore

$$\mathrm{d}_{\mathrm{avg}}((U_iV_j^\dagger)^{p_j}, (UV_j^\dagger)^{p_j}) \leq d'_F((U_iV_j^\dagger)^{p_j}, (UV_j^\dagger)^{p_j}) \leq p_j d'_F(U_i, U) \leq 2p_j\,\mathrm{d}_{\mathrm{avg}}(U_i, U) \leq 4c/\sqrt{d}, \quad \text{(C.30)}$$

where we have used Item 1 and 2 in Lemma 4, unitary invariance of d'_F, and $p_j = 2^j \leq 2^t \leq 2/(\epsilon\sqrt{d})$. Thus $\{(U_i V_j^\dagger)^{p_j}, U_i \in \mathcal{N}\}$ forms an $4c/\sqrt{d}$-covering net of $\{(UV_j^\dagger)^{p_j} \mid U \text{ is a } G\text{-gate unitary}\}$, which can be used by the hypothesis selection algorithm $\mathcal{A}$ as set of candidates. The output R_j of $\mathcal{A}$ satisfies $d'_F(R_j, (UV_j^\dagger)^{p_j}) \leq 2\,\mathrm{d}_{\mathrm{avg}}(R_j, (UV_j^\dagger)^{p_j}) \leq 4(\sqrt{2}+1)\cdot 4c/\sqrt{d} < 40c/\sqrt{d}$ (see Equation (C.27)). The number of queries to U that this procedure uses is $\mathcal{O}\left(p_j \frac{G\log(G/c\epsilon)+\log(1/\eta_j)}{(4c/\sqrt{d})^2}\right) = \mathcal{O}\left(p_j d(G\log(G/\epsilon)+\log(1/\eta_j))\right)$.

Now we proceed to prove (1) by induction. Let's assume that the learning algorithm succeeds for all $j = 1, \ldots, t$. Let $\delta_j = d'_F(U, V_j) = d'_F(UV_j^\dagger, I)$ be the error after iteration $j-1$. We will prove that $\delta_k \leq 2^{-k-5}/\sqrt{d}$. For iteration 0, we have $p_0 = 1$, and by the accuracy of $\mathcal{A}$, we know $\delta_1 = d'_F(U, V_1) < 40c/\sqrt{d} < 2^{-6}/\sqrt{d}$. Now we assume $\delta_k \leq 2^{-k-5}/\sqrt{d}$ and prove $\delta_{k+1} \leq 2^{-k-6}/\sqrt{d}$. Note that $(UV_k^\dagger)^{p_k}$ and R_k are sufficiently close to identity in the sense that

$$d'_F((UV_k^\dagger)^{p_k}, I) \leq p_k d'_F(UV_k^\dagger, I) = p_k\delta_k \leq \frac{2^{-5}}{\sqrt{d}} < \frac{4/(25\pi)}{\sqrt{d}}, \tag{C.31}$$

and

$$d'_F(R_k, I) \leq d'_F(R_k, (UV_k^\dagger)^{p_k}) + d'_F((UV_k^\dagger)^{p_k}, I) \leq \frac{40c}{\sqrt{d}} + \frac{2^{-5}}{\sqrt{d}} < \frac{4/(25\pi)}{\sqrt{d}}. \tag{C.32}$$

Thus, we can invoke Item 3 of Lemma 4 and obtain

$$\delta_{k+1} = d'_F(U, V_{k+1}) = d'_F(UV_k^\dagger, R_k^{1/p_k}) \leq \frac{2}{p_k} d'_F((UV_k^\dagger)^{p_k}, R_k) \leq \frac{80c}{p_k\sqrt{d}} < \frac{2^{-k-6}}{\sqrt{d}}. \tag{C.33}$$

Therefore, by induction, we have shown that $\delta_k \leq 2^{-k-5}/\sqrt{d}$. At the end of the iteration, when $k = t = \left\lceil \log_2(1/(\sqrt{d}\epsilon)) \right\rceil$, we have

$$\delta_{t+1} = d'_F(U, V_{t+1}) \leq \frac{2^{-t-6}}{\sqrt{d}} < \epsilon. \tag{C.34}$$

The above accuracy is conditioned on the success of all executions of the learning algorithm. By the union bound, the failure probability is upper bounded by

$$\sum_{j=0}^{t} \eta_j = \delta \sum_{j=0}^{t} 8^{-(t-j)-1} = \delta \sum_{j=0}^{t} 8^{-j-1} < \delta. \tag{C.35}$$

This concludes the proof of (1).

Next we move on to (2) and count the overall number of queries to the unknown unitary. Summing over all iterations, the number of queries is

$$\begin{aligned}
&\mathcal{O}\left(\sum_{j=0}^{t} p_j d(G\log(G/\epsilon) + \log(1/\eta_j))\right) \\
&= \mathcal{O}\left(dG\log(G/\epsilon)\sum_{j=0}^{t} 2^j + d\log(1/\delta)\sum_{j=0}^{t} 2^j(t-j+1)\right) \\
&= \mathcal{O}\left(d(G\log(G/\epsilon)+\log(1/\delta))2^t\right) = \mathcal{O}\left(\frac{\sqrt{d}(G\log(G/\epsilon)+\log(1/\delta))}{\epsilon}\right).
\end{aligned} \tag{C.36}$$

This concludes the proof of the $\mathcal{O}(1/\epsilon)$ scaling algorithm in Proposition 8.

Finally, we note that an analogous bootstrap method can also be applied to improve the ϵ-dependence for our unitary learning procedure without auxiliary systems, albeit again incurring a dimension factor. Namely, a variant of Algorithm 5 relying on the algorithm of Appendix C 2 a as a subroutine succeeds at outputting a $\hat{U}$ that satisfies $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon$ with probability at least $1-\delta$ using $\mathcal{O}\left(d^{3/2}(G\log(G/\epsilon)+\log(1/\delta))/\epsilon\right)$ queries to the unknown unitary U, assuming $\epsilon < {}^{1}/_{d^{3/2}}$.

3. Average-case query complexity lower bounds

For the lower bound, we construct a packing net consisting of G-gate unitaries that are pairwise sufficiently far apart, so that an average-case learning algorithm can discriminate them. Meanwhile, the success probability of distinguishing a set of unitaries is upper bounded by the number of queries made [63]. This gives us an $\Omega(G)$ query complexity lower bound. To incorporate ϵ-dependence, we follow [21] and map the problem to a fractional query problem [61, 62]. This way, we arrive at the following result.

Proposition 9 (Average case unitary learning lower bound, lower bound in Theorem 4)**.** *Let U be an n-qubit unitary composed of G two-qubit gates. Any algorithm that, given query access to U, $U^\dagger$, $cU = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$ and $cU^\dagger = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U^\dagger$, can output a unitary $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon \in (0, 1/32)$ with probability at least $2/3$, must use at least $\Omega(G/\epsilon)$ queries.*

Note that the lower bound holds even for learning algorithms that have a stronger form of access to U than considered for our upper bounds. There, we only assumed query access to U. In contrast, the lower bound holds even assuming query access to U and $U^\dagger$ as well as controlled versions thereof.

Proof of Proposition 9. The proof builds on the following lemma that maps the problem to a fractional query one [21].

Lemma 24 (Reduction to fractional query algorithms, [21, Lemma 4.5 and proof of Theorem 1.2])**.** *Let $R \in U(d)$ be a Hermitian unitary (i.e., $R^2 = I$). Define $R^\alpha = (I + R)/2 + e^{-i\pi\alpha}(I - R)/2$ for some $\alpha \in (0, 1]$. Suppose there exists an algorithm $\mathcal{A}$ that uses Q queries to R^α or $R^{\alpha\dagger}$ and produces some output with probability at least $2/3$. Then there exists another algorithm $\mathcal{A}'$ that uses $50 + 100\alpha Q$ queries to controlled-R and produces the same output with probability at least $\exp(-\alpha\pi Q)/2$.*

To use this lemma, we need to construct a packing net of Hermitian unitaries, and give an upper bound on the maximum probability of successfully distinguishing them. Thus we need the following two lemmas.

Lemma 25 (Packing net of Hermitian unitaries, variant of [21, Proposition 4.1])**.** *There exists a set of Hermitian unitaries $\mathcal{P} = \{R_i\}_i \subset U(d)$ with $\log |P| \geq \Omega(d^2)$ and $R_i^2 = I$ for $R_i \in \mathcal{P}$, such that for any $R_i \neq R_j \in \mathcal{P}$, $d'_F(R_i, R_j) \geq 1/8$.*

Proof. Let $d = 2r + 1$ if d is odd, or $d = 2r + 2$ if d is even. [135, Lemma 7] (or Lemma 8 in [19]) asserts that there exists a set of rank r density matrices in dimension $2r$ with cardinality at least $\exp(r^2/8)$, such that all the non-zero eigenvalues are equal to $1/r$, and any two different density matrices have trace distance at least $1/4$. We can write this set as $\{(I_{2r} + V_i)/(2r), i = 1, \ldots, N\}$, where $V_i \in U(2r)$ is a Hermitian unitary of trace zero. Then $N \geq \exp(r^2/8)$, and $\forall i \neq j$,

$$\frac{1}{4} \leq \frac{1}{2}\left\| \frac{I_{2r} + V_i}{2r} - \frac{I_{2r} + V_j}{2r} \right\|_1 = \frac{1}{4r}\|V_i - V_j\|_1 \leq \frac{1}{\sqrt{2r}}\|V_i - V_j\|_F. \tag{C.37}$$

where we have used $\|V_i\|_1 \leq \sqrt{2r}\|V_i\|_F$. Then we embed $V_i \to R_i = V_i \oplus I_b \in U(d)$, where $b = 1$ or 2, depending on whether d is odd or even. We have

$$d_F(R_i, R_j) = \frac{1}{\sqrt{d}}\|R_i - R_j\|_F \geq \frac{1}{4}\sqrt{\frac{2r}{2r + b}} \geq \frac{1}{8}. \tag{C.38}$$

Now we would like to translate d_F into d'_F. From Lemma 10, we know that changing to the quotient metric for any set of unitaries only decreases $\log N$ by an additive constant (since here we consider constant ϵ). Therefore, we still have $\log |P| \geq \Omega(d^2)$ for $d'_F(R_i, R_j) \geq \frac{1}{8}$. □

Lemma 26 (Upper bound on success probability of distinguishing unitaries, [63, Theorem 5])**.** *Let $\mathcal{P} \subseteq U(d)$ be a set of unitaries. Let $\mathcal{A}$ be any algorithm that uses Q queries to an input unitary U_x and output a guess $\hat{x}$. Suppose the input unitary is randomly picked from $\mathcal{P}$ with uniform probability. Then the maximal probability that the output satisfies $\hat{x} = x$ is upper bounded by $\frac{1}{|\mathcal{P}|}\binom{Q+d^2-1}{Q}$.*

Now we can proceed to prove the lower bound in Proposition 9. Suppose we have a learning algorithm $\mathcal{A}$ that uses Q queries and outputs a $\hat{U}$ that has accuracy ϵ in $\mathrm{d}_{\mathrm{avg}}$ with success probability at least $2/3$. From the theory of universal gates [136], we know that $G = \mathcal{O}(4^k)$ gates suffice to implement an arbitrary k-qubit unitary, i.e., there exists constant C such that G gates can implement arbitrary unitary on $k = \lfloor \log_4(G/C) \rfloor$ qubits. Let $d = \min\{2^n, 2^k\}$, and focus on the first $\min\{n, k\}$ qubits. The algorithm $\mathcal{A}$ thus is able to learn any unitary on these qubits.

Consider the packing net $\mathcal{P} = \{R_i\}$ from Lemma 25 for this choice of d. We want to identify $R \in \mathcal{P}$, but using only access to R^α for $1/\alpha = \lfloor 1/32\epsilon \rfloor > 1$. If we apply $\mathcal{A}$ to R^α, then with probability at least $2/3$, the output U satisfies $\mathrm{d}_{\mathrm{avg}}(U, R^\alpha) \le \epsilon$. From the equivalence of $\mathrm{d}_{\mathrm{avg}}$ and d'_F (Lemma 4), and the triangle inequality and unitary invariance of d'_F, we have

$$d'_F(U^{1/\alpha}, R) \le \sum_{p=1}^{1/\alpha} d'_F(U^p R^{1-\alpha p}, U^{p-1} R^{1-\alpha p+\alpha}) = \frac{2}{\alpha}\, \mathrm{d}_{\mathrm{avg}}(U, R^\alpha) \le \frac{2\epsilon}{\alpha} \le \frac{1}{16}. \tag{C.39}$$

Since $R \in \mathcal{P}$ have pairwise distance at least $1/8$, the algorithm can identify R with success probability at least $2/3$ by finding the closest element of $\mathcal{P}$ to $U^{1/\alpha}$.

Now, via Lemma 24, we know that there is a learning algorithm $\mathcal{A}'$ that can use $50 + 100\alpha Q$ queries to controlled-R to identify R with success probability at least $\exp(-\alpha\pi Q)/2$. On the other hand, we know the success probability cannot exceed the upper bound $\binom{Q+d^2-1}{Q}/|\mathcal{P}|$ set by Lemma 26 with $\log|P| \ge \Omega(d^2)$. Combined with a technical lemma [21, Lemma 4.3], this means that the number of queries must be at least $\Omega(d^2)$. That is,

$$50 + 100\alpha Q \ge \Omega(d^2) \implies Q \ge \Omega\left(\frac{d^2}{\alpha}\right) = \Omega\left(\frac{d^2}{\epsilon}\right) = \Omega\left(\frac{\min\{4^n, G\}}{\epsilon}\right). \tag{C.40}$$

This concludes the proof of Proposition 9. □

We comment on the connection of our results to the recent work [51] on the hardness of learning Haar-random unitaries, where the authors proved a sample complexity lower bound $\Omega\left(\frac{d^2}{\log^2 d}\right)$ for learning d-dimensional Haar-random unitaries to constant accuracy w.r.t. d'_F. The direct consequence of our lower bound when applied to learning the whole unitary group $U(d)$, without assumptions of limited complexity, is a lower bound of $\Omega\left(d^2\right)$, which is stronger than that of [51, Theorem 1] by a factor of $\log^2 d$. We note that this difference is a consequence of proof techniques that comes about in two ways. One $\log d$ factor comes from their analysis of the differential entropy, which only calculated the contribution of $\Theta\left(\frac{d}{\log d}\right)$ columns of the matrix elements, instead of all d columns. This issue does not arise for us because we focus on the discrete entropy with the use of a packing net. The other $\log d$ comes from the mutual information upper bound, where they use the straightforward Holevo bound: Each d-dimensional quantum state can carry at most $\mathcal{O}(\log d)$ bits of information. We manage to get rid of this factor by making use of a more refined bound on success probability as in Lemma 26.

Lastly, we remark on the proof technique used here compared to the Holevo information bound in the state learning case (Appendix B 2). The Holevo bound is particularly useful in proving these lower bounds because, combined with the data processing inequality, it gives an upper bound on the amount of information that can be extracted from quantum states. In particular, it asserts that, given an ensemble of d-dimensional states $\{\rho_X\}$ with random classical labels $X \in [M]$, the maximal mutual information with the underlying random label when using k copies of the state is upper bounded by $\chi(X; \rho_X^{\otimes k}) \triangleq S(\mathbb{E}_X[\rho_X^{\otimes k}]) - \mathbb{E}_X[S(\rho_X^{\otimes k})]$. Meanwhile, the information needed to distinguishing a packing net of d-dimensional states is lower bounded by $\Omega(d)$. Thus, upper bounding the Holevo χ via the number of samples k can give us sample complexity lower bounds. A naive upper bound is $\chi \le S(\mathbb{E}_X[\rho_X^{\otimes k}]) \le k \log d$ because $\mathbb{E}_X[\rho_X^{\otimes k}]$ is a d^k-dimensional mixed state and thus has entropy at most $k \log d$. This gives us a $\Omega(d/\log d)$ sample complexity lower bound with a sub-optimal logarithmic factor. To get rid of the $\log d$ factor, [168] noted that k copies of a d-dimensional pure state live in the symmetric subspace of the k-fold tensor power of d-dimensional Hilbert space. Therefore, the first term $S(\mathbb{E}_X[\rho_X])$, along with the Holevo χ, can be more tightly upper bounded by $\log\binom{k+d-1}{k}$, where the binomial coefficient is the dimension of the symmetric subspace. This can then be used to prove a $\Omega(d)$ lower bound, which is optimal in d.

However, an analogous result for unitaries (or more generally channels) queries is still lacking. Consider an ensemble of channels $\{C_X\}$ labeled by a classical random variable $X \in [M]$. In general, one can sequentially query the channel k times interleaved with processing operations to prepare a state carrying the information extracted from the queries. This then has the form $\rho_X^k = \mathcal{C}_k C_X \mathcal{C}_{k-1} C_X \cdots \mathcal{C}_1 C_X(\rho^0)$, where $\mathcal{C}_i$ are fixed channels independent of X, and ρ_0 is some fixed state. Then the amount of information that one can extract is given by the Holevo information $\chi(X; \rho_X^k) = S(\mathbb{E}_X[\rho_X^k]) - \mathbb{E}_X\, S([\rho_X^k])$. Upper bounding this quantity is in general difficult. [169] used induction and obtained $\chi \le k \log(d^2)$ which corresponds to the naive upper bound in the state case. Using this, however, can only give us a suboptimal $\Omega(d^2/\log d)$ query complexity lower bound. We suspect that an improved method, similar in spirit to [168], making use of the fact that all k queries are to the same channel C_X should be possible and give a

$$\chi(X;\rho_X^k) \leq \log \binom{k+d^2-1}{k} \tag{C.41}$$

upper bound. This would then also give an information-theoretic perspective on the binomial coefficient appearing in the unitary discrimination result Lemma 26 originally proved by positive-semi-definite programming. We leave the proof of this Holevo information bound as an open problem for future work.

4. Learning from classically described data

As we have seen in Theorems 1 and 4, the sample complexity of learning G-gate states and unitaries are both $\tilde{\Theta}(G)$. This suggests that they have similar source of complexity. However, differently from state learning, we can identify two sources of difficulty in unitary learning: (1) reading out the input and output quantum states, and (2) learning the mapping from inputs to outputs. The similar complexity $\tilde{\Theta}(G)$ of both state and unitary learning suggests that learning the mapping is actually easy and may only need a constant number of queries to the unknown unitary.

To formalize this idea, we consider a different access model for the unitary learning task: We focus on learning the mapping by assuming training data that contains classical descriptions of input and output states. Specifically, we consider a learning algorithm H that selects N input n-qubit states $\{|x_i\rangle\}_{i=1}^N$, and queries the unknown unitary to get $\{U|x_i\rangle\}_{i=1}^N$, where we have (repeated) access to the classical descriptions of all these input and output states. Based on these classically described data, we want to use the learning algorithm H to output a $\hat{U}$ that satisfies $\mathrm{d}_{\mathrm{avg}}(\hat{U},U) \leq \epsilon$.

A recent line of research on the quantum no-free-lunch theorem [45, 46] implies that the above task of learning the mapping from classically described data in the average-case distance requires at least $\Omega(2^n)$ samples. This seems to contradict our idea that learning the mapping should be easy. However, [46] also demonstrated how to circumvent the quantum no-free-lunch theorem. In particular, they showed that by entangling our input states with an ancillary system, applying the unitary on the original system, and collecting the output entangled states, we can reduce the sample requirement by a factor equal to the Schimidt rank r of the entangled states. In the limit of maximally entangled state where $r = 2^n$, the output state is in fact the Choi–Jamiołkowski state of the unitary, which already contains all the matrix elements of the unitary. Therefore, [46] concluded that using entangled data can reduce the data requirements and eventually make the unitary learning task easy, requiring only one sample with a maximally entangled input state.

Here, we aim to go beyond this result and provide a unified information-theoretic reformulation of the quantum no-free-lunch theorem (Theorem 17), which is not limited to entangled data. We find that the key ingredient to reduce the sample complexity of learning with classical description is to enlarge the representation space (i.e., the space that the output states live in). While entanglement is one way to achieve such an enlargement, it is not the only one. In fact, we find an alternative method that only uses classically mixed states and achieve the same reduction in sample complexity. Specifically, we establish the following theorem.

Proposition 10 (Upper bounds in learning with classical descriptions, restatement of upper bounds in Theorem 5)**.** *There exists a learning algorithm H_{entangle} that, for any n-qubit unitary $U \in U(2^n)$, uses $N = \lceil 2^n/r \rceil$ classically described data $\{(|x_i\rangle, (U\otimes I)|x_i\rangle)\}_{i=1}^N$, where $|x_i\rangle$ are bipartite entangled states over two n-qubit systems with Schmidt rank at most r, to output a $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U},U) \leq \epsilon$ for any $\epsilon > 0$.*

Similarly, there exists a learning algorithm H_{mixed} that, for any n-qubit unitary $U \in U(2^n)$, uses $N = \lceil 2^n/r \rceil$ classically described data $\{(\rho_i, (U\otimes I)\rho_i(U\otimes I)^\dagger)\}_{i=1}^N$, where ρ_i are classically mixed states over two n-qubit systems with rank at most r of the form

$$\rho_i = \sum_{j=1}^{r} p_{ij} |\phi_{ij}\rangle\!\langle\phi_{ij}| \otimes |\psi_{ij}\rangle\!\langle\psi_{ij}| \,, \tag{C.42}$$

to output a $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U},U) \leq \epsilon$ for any $\epsilon > 0$.

Note that, since the number N of training data points in Proposition 10 is independent of the desired accuracy $\epsilon > 0$, we can also learn w.r.t. $\mathrm{d}_\diamond$. In fact, we can even learn the unknown unitary exactly.

We prove Proposition 10 by explicitly constructing the learning algorithms. We remark that the $r = 2^n$ case for entangled data has previously appeared in [46], and a different strategy using mixed states was proposed in [68].

Proof. Let $d = 2^n$. We begin by describing the algorithm for entangled data. We consider the following set of input states

$$|x_j\rangle = \frac{1}{\sqrt{\mathcal{Z}_j}} \sum_{i=(j-1)r+1}^{\min\{jr,d\}} |i\rangle \otimes |i\rangle \,, \quad j = 1, \ldots, \lceil d/r \rceil \,. \tag{C.43}$$

where the normalization $\mathcal{Z}_j = r$ for $1 \leq j \leq \lceil d/r \rceil - 1$ and $\mathcal{Z}_j = d - (\lceil d/r \rceil - 1)r$ for $j = \lceil d/r \rceil$. They all have Schmidt rank at most r. If we apply $U \otimes I$ on $|x_j\rangle$, the output state reads

$$(U \otimes I)\,|x_j\rangle = \frac{1}{\sqrt{\mathcal{Z}_j}} \sum_{i=(j-1)r+1}^{\min\{jr,d\}} \sum_{k=1}^{d} \langle k|U|i\rangle \,|k\rangle \otimes |i\rangle \,. \tag{C.44}$$

Since we have the classical description, we can directly read off the matrix elements $\langle k|U|i\rangle$ with $1 \leq k \leq d$ and $(j-1)r + 1 \leq i \leq \min\{jr, d\}$. Combining different j, we can gather all the matrix elements we need to learn U.

Next, we describe the algorithm for mixed state data. We consider the input states to be

$$\rho_j = \sum_{i=(j-1)r+1}^{\min\{jr,d\}} p_j \,|ii\rangle \langle ii| \,, \quad j = 1, \ldots, \lceil d/r \rceil \,. \tag{C.45}$$

where the uniform mixing probability $p_j = 1/r$ for $1 \leq j \leq \lceil d/r \rceil - 1$ and $p_j = 1/(d - (\lceil d/r \rceil - 1)r)$ for $j = \lceil d/r \rceil$. Then all ρ_j have rank at most r. If we apply $U \otimes I$ on $|x_j\rangle$, the output state becomes

$$\rho_j = \sum_{i=(j-1)r+1}^{\min\{jr,d\}} p_j (U \otimes I)\,|ii\rangle \langle ii|\,(U \otimes I)^\dagger, \quad j = 1, \ldots, \lceil d/r \rceil \,. \tag{C.46}$$

We can interpret this output mixed state as randomly choosing a basis state in the ancillary system and applying the unitary to the same state in the original system. Since we have the classical description, we can use the ancillary system as a label for which state we inputted (e.g, $|i\rangle$), and read off all the amplitudes of $U|i\rangle$ on the original system, i.e., a column of the U matrix. Then by combing all the different basis elements $|i\rangle$, $1 \leq i \leq d$, we obtain all the matrix elements of U. □

Now we move on to the lower bound, which states that any noise-robust unitary learning algorithm needs at least $\Omega(2^n/r)$ samples to learn an arbitrary unknown unitary from classically described data. The noise-robust requirement here is in accordance with realistic learning scenarios where the tomography of input and output states necessarily involves reconstruction imperfection and noise. Specifically, we have the following proposition.

Proposition 11 (Lower bounds in learning with classical descriptions, restatement of lower bounds in Theorem 5)**.** *Let $\epsilon \in (0,1), \eta = \Theta(\epsilon)$. Let H_{entangle} be any learning algorithm that, for any n-qubit unitary $U \in U(2^n)$, uses classically described data $\{(|x_i\rangle, |y_i\rangle)\}_{i=1}^N$, where $|x_i\rangle$ are bipartite entangled states over two n-qubit systems with Schmidt rank at most r and $|y_i\rangle$ are η-noisy versions of $(U \otimes I)\,|x_i\rangle$ satisfying $\mathrm{d}_{\mathrm{tr}}(|y_i\rangle, (U \otimes I)\,|x_i\rangle) \leq \eta$, to output a $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon$. Then H_{entangle} needs at least $N \geq \Omega(2^n/r)$ samples.*

Similarly, let H_{mixed} be any learning algorithm that, for any n-qubit unitary $U \in U(2^n)$, uses classically described data $\{(\rho_i, \sigma_i)\}_{i=1}^N$, where ρ_i are classically mixed states over two n-qubit systems with rank at most r of the form

$$\rho_i = \sum_{j=1}^{r} p_{ij} \,|\phi_{ij}\rangle\!\langle\phi_{ij}| \otimes |\psi_{ij}\rangle\!\langle\psi_{ij}| \tag{C.47}$$

and σ_i are η-noisy versions of $(U \otimes I)\rho_i(U \otimes I)^\dagger$ satisfying $\mathrm{d}_{\mathrm{tr}}(\sigma_i, (U \otimes I)\rho_i(U \otimes I)^\dagger)) \leq \eta$, to output a $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(\hat{U}, U) \leq \epsilon$. Then H_{mixed} needs at least $N \geq \Omega(2^n/r)$ samples.

Proposition 11 is a consequence of the following information-theoretic reformulation of the quantum no-free-lunch theorem. The intuition behind this theorem is simple. On the one hand, to learn a unitary, we have to gather enough information to specify it. This required amount of information is quantified by the metric entropy of the unitary class. On the other hand, the information provided by each sample is limited and can be characterized by the metric entropy of the output state space. Therefore, the number of samples needed to learn the unitary is given by the former divided by the latter. In particular, we can see that the data requirement can be reduced if we increase the amount of information carried by each sample, represented by the metric entropy in the denominator.

Theorem 17 (Information-theoretic reformulation of quantum no-free-lunch theorem)**.** *Let $\eta, \epsilon \in (0,1)$. Let S be a set of input states (possibly with ancillas) and P be a distribution over S. Let $\{\rho_i\}_{i=1}^N \subset S^N$ be N classically described input states. Suppose that after applying the unknown n-qubit unitary U from a class $\mathcal{U} \subseteq U(2^n)$ of unitaries, they are transformed into the output states $\{\sigma_i\}_{i=1}^N$ through the map $f_U : \rho_i \mapsto \sigma_i = f_U(\rho_i)$. Let $\tilde{\sigma}_i$ be an η-noisy version of σ_i satisfying $\mathrm{d_{tr}}(\tilde{\sigma}_i, \sigma_i) \leq \eta$. Let $\mathcal{N}_\eta = \sup_{\rho \in S} \mathcal{N}(\{f_V(\rho) : V \in \mathcal{U}\}, \mathrm{d_{tr}}, \eta)$ be the maximal covering number of the set of all possible output states with different unitary acting on the input states. Let $\mathcal{F}_\mathcal{U} = \{f_V : V \in \mathcal{U}\}$ be the set of maps and $d_P(f_V, f_W) = \sqrt{\mathbb{E}_{\rho\sim P}[\mathrm{d_{tr}}(f_V(\rho), f_W(\rho))^2]}$ be the root mean squared trace distance. Then any learning algorithm H that uses the η-noisy classically described data $\{\rho_i, \tilde{\sigma}_i\}_{i=1}^N$ and outputs a $\hat{U}$ such that $d_P(f_{\hat{U}}, f_U) \leq \epsilon$ with probability at least $2/3$ needs at least*

$$N \geq \Omega\left(\frac{\log \mathcal{M}(\mathcal{F}_\mathcal{U}, d_P, 2\epsilon + 6\eta)}{\log \mathcal{N}_\eta}\right) \tag{C.48}$$

samples.

In particular, if $\eta = \Theta(\epsilon)$, $\mathcal{U} = U(2^n)$, P is a locally scrambled ensemble up to the second moment over n-qubit pure states (e.g., n-qubit Haar measure), S is the support of P, and $f_U(\rho) = U\rho U^\dagger$, then at least $\Omega(2^n)$ samples are needed.

We remark that $\eta = \Theta(\epsilon)$ is a convenient choice of noise level for stating the results, but in fact a weaker assumption $\log(1/\eta) = \Theta(\log(1/\epsilon))$ suffices.

In the following, we will first show that Theorem 17 implies Proposition 11 (the lower bounds in Theorem 5). Then we will turn to the proof of Theorem 17.

Proof of Proposition 11. In both cases (entangled or mixed), we prove the $\Omega(2^n/r)$ lower bound in two steps via Theorem 17: (1) show that the numerator $\log \mathcal{M}(\mathcal{F}_\mathcal{U}, d_P, 2\epsilon + 6\eta)$ in Theorem 17 is at least $\Omega(4^n \log(1/\epsilon))$; and (2) show that the denominator $\mathcal{N}_\epsilon$ is at most $\mathcal{O}(2^n r \log(1/\epsilon))$ when the input states are either entangled pure states of Schmidt rank at most r or mixed states of rank at most r. Then the desired results follow.

For step (1), we begin by defining the distribution P with respect to which the performance in Theorem 17 is measured. For both entangled and mixed cases, we define P to be the distribution of $|\psi\rangle \otimes |0\rangle^{\otimes n}$ where $|\psi\rangle$ is a Haar-random state on the original system, and $|0\rangle^{\otimes n}$ is a fixed state on the ancillary system. Note that this state is indeed both a bipartite entangled state with Schmidt rank at most r and of the form Equation (C.47) with rank at most r. Moreover, since in both cases, the map f_U is given by acting the unitary U on the original system and the identity on the ancillary system, the distance metric $d_P(f_V, f_W)$ is the same as $\mathrm{d_{avg}}$. Therefore, the packing number satisfies

$$\mathcal{M}(\mathcal{F}_{U(2^n)}, d_P, 2\epsilon + 6\eta) = \mathcal{M}(U(2^n), \mathrm{d_{avg}}, 2\epsilon + 6\eta). \tag{C.49}$$

To find the packing number $\mathcal{M}(U(2^n), \mathrm{d_{avg}}, 2\epsilon + 6\eta)$, we invoke the covering number bound for $U(2^n)$ with respect to the normalized Frobenius norm d_F (Lemma 9), the fact that quotient out global phase only change the metric entropy by a constant (Lemma 10), and the equivalence of d'_F and $\mathrm{d_{avg}}$ (Lemma 4, Item 1). We have

$$\log \mathcal{M}(\mathcal{F}_{U(2^n)}, d_P, 2\epsilon + 6\eta) = \log \mathcal{M}(U(2^n), \mathrm{d_{avg}}, 2\epsilon + 6\eta) \geq \Omega\left(4^n \log \frac{1}{\epsilon}\right), \tag{C.50}$$

where we used $\eta = \Theta(\epsilon)$.

Next, for step (2), we compute $\mathcal{N}_\eta$. For entangled data, note that applying unitaries on only the first n qubits does not change the bipartite Schmidt rank r, so the output states are pure states of the form $|\chi\rangle = \sum_{i,j=1}^{2^n} A_{ij} |i\rangle \otimes |j\rangle$, where $\|A\|_F = 1$ because of normalization, and the rank of A corresponds to the Schmidt rank which is at most r. Furthermore, the Euclidean distance between the output states is equal to the Frobenius distance between the corresponding A-matrices. With this correspondence, we can explicitly construct a covering net over the output states as follows. We take a minimal η-covering net $\mathcal{N}'$ over the set of complex matrices A with bounded rank r and $\|A\|_F = 1$ with respect to the Frobenius distance. Since they are contained in the unit ball ($\|A\|_F \leq 1$) in a real linear space of dimension $2 \cdot 2^n \cdot r$ [170, Theorem 1], by the monotinicity of covering number and the standard covering number bound for Euclidean balls via a volume argument [48, Corollary 4.2.13], we have $\log|\mathcal{N}'| \leq \mathcal{O}(2^n r \log(1/\eta))$. Meanwhile, similar to the proof in Lemma 1, the trace distance between any two pure states $|\psi\rangle, |\phi\rangle$ are bounded by the Euclidean distance, and thus the Frobenius distance between the corresponding A matrices:

$$\mathrm{d}_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle) = \sqrt{1 - |\langle\psi|\phi\rangle|^2} \leq \sqrt{2(1 - |\langle\psi|\phi\rangle|)} \leq \sqrt{2(1 - \mathrm{Re}[\langle\psi|\phi\rangle])} = \||\psi\rangle - |\phi\rangle\|_2. \tag{C.51}$$

Therefore $\mathcal{N}'$ gives an η-covering net over the output states with respect to the trace distance d_{tr}. Hence, $\log \mathcal{N}_\eta \leq \log|\mathcal{N}'| \leq \mathcal{O}(2^n r \log(1/\eta)) = \mathcal{O}(2^n r \log(1/\epsilon))$ since $\eta = \Theta(\epsilon)$, and from Theorem 17 we have the desired lower bound

$$N \geq \Omega\left(\frac{4^n \log(1/\epsilon)}{2^n r \log(1/\epsilon)}\right) = \Omega\left(\frac{2^n}{r}\right). \tag{C.52}$$

The case of mixed states is similar. For a given input state $\rho = \sum_{i=1}^r p_i |\phi_i\rangle\langle\phi_i| \otimes |\psi_i\rangle\langle\psi_i|$, the output state reads

$$\sigma = \sum_{i=1}^r p_i U |\phi_i\rangle\langle\phi_i| U^\dagger \otimes |\psi_i\rangle\langle\psi_i|. \tag{C.53}$$

Now we take a minimal η-covering net $\mathcal{N}''$ over all pure n-qubit states with respect to Euclidean distance, which is a unit ball in a $2 \cdot 2^n$ dimensional real linear space. By standard covering number bound for Euclidean balls, we know $\log|\mathcal{N}''| \leq \mathcal{O}(2^n \log(1/\eta)) = \mathcal{O}(2^n \log(1/\epsilon))$. Then for any $U|\phi_i\rangle$, there exists a $|\eta_i\rangle \in \mathcal{N}''$ such that $\|U|\phi_1\rangle - |\eta_1\rangle\|_2 \leq \eta$. Let $\sigma' = \sum_{i=1}^r p_i |\eta_i\rangle\langle\eta_i| \otimes |\psi_i\rangle\langle\psi_i|$. Then the trace distance is bounded by

$$\begin{aligned}
\frac{1}{2}\|\sigma - \sigma'\|_1 &\leq \frac{1}{2}\sum_{i=1}^r p_i \big\|U|\phi_i\rangle\langle\phi_i| U^\dagger \otimes |\psi_i\rangle\langle\psi_i| - |\eta_i\rangle\langle\eta_i| \otimes |\psi_i\rangle\langle\psi_i|\big\|_1 \\
&\leq \frac{1}{2}\sum_{i=1}^r p_i \|U|\phi_i\rangle \otimes |\psi_i\rangle - |\eta_i\rangle \otimes |\psi_i\rangle\|_2 \\
&= \frac{1}{2}\sum_{i=1}^r p_i \|U|\phi_i\rangle - |\eta_i\rangle\|_2 \leq \frac{\eta}{2}\sum_{i=1}^r p_i = \frac{\eta}{2},
\end{aligned} \tag{C.54}$$

where we have used the subadditivity of trace norm, the fact that trace distance is upper bounded by Euclidean norm for pure states, and $\sum_{i=1}^r p_i = 1$. Hence the set

$$\left\{\sum_{i=1}^r p_i |\eta_i\rangle\langle\eta_i| \otimes |\psi_i\rangle\langle\psi_i| : |\eta_i\rangle \in \mathcal{N}'', 1 \leq i \leq r\right\} \tag{C.55}$$

forms an $\eta/2$-covering net of set of the output states and has cardinality $|\mathcal{N}''|^r$. Therefore, we have $\log \mathcal{N}_\eta = r \log|\mathcal{N}''| = \mathcal{O}(2^n r \log(1/\epsilon))$. From Theorem 17, we again arrive at the desired result

$$N \geq \Omega\left(\frac{4^n \log(1/\epsilon)}{2^n r \log(1/\epsilon)}\right) = \Omega\left(\frac{2^n}{r}\right). \tag{C.56}$$

This concludes the proof of Proposition 11, and together with Proposition 10, we have proved Theorem 5. □

Now we move on to prove our quantum no-free-lunch theorem (Theorem 17). We first establish the following information-theoretic lower bound on the sample complexity of learning discrete functions. We remark that a version for binary-valued functions was proved in a different fashion in [171, Proposition 8] and [172, Lemma 4.8].

Proposition 12 (Information-theoretic lower bound for learning discrete functions)**.** *Let $\epsilon > 0$, $k \in \mathbb{N}$ and $\mathcal{F}$ be a class of functions mapping $\mathcal{X}$ to $\mathcal{Y} = \{1, \ldots, k\}$ with a distance metric d. Any learning* *algorithm H that uses N samples $\{x_i \in \mathcal{X}, y_i = f(x_i)\}_{i=1}^N$ and outputs an $\hat{f}$ such that $d(\hat{f}, f) \leq \epsilon$ with probability at least 2/3 for any $f \in \mathcal{F}$ must use at least*

$$N \geq \Omega\left(\frac{\log \mathcal{M}(\mathcal{F}, d, 2\epsilon)}{\log k}\right) \tag{C.57}$$

samples.

Proof of Proposition 12. We begin by taking a maximal 2ϵ-packing $\mathcal{P}$ of $\mathcal{F}$, i.e., $|\mathcal{P}| = \mathcal{M}(\mathcal{F}, d, 2\epsilon)$ and for any $f_i \neq f_j \in \mathcal{P}$, $d(f_i, f_j) > 2\epsilon$. Now we design a communication protocol between two parties, Alice and Bob, as follows. The packing $\mathcal{P}$ is shared by both parties. Alice takes a random variable W uniformly sampled from $\{1, \ldots, \mathcal{M}(\mathcal{F}, d, 2\epsilon)\}$ and picks the corresponding function f_W from the packing $\mathcal{P}$. She then feeds the inputs $x = (x_1, \ldots, x_N)$ into f_W, generating a dataset $Z = ((x_1, f_W(x_1)), \ldots, (x_N, f_W(x_N)))$, and sends the dataset to Bob. Bob's task is to use this dataset to determine which function Alice used. Suppose Bob is given a learning algorithm described as in the proposition. The algorithm will learn from the dataset and output a hypothesis function $\hat{f}$ that satisfies

$$\mathbb{P}[d(\hat{f}, f_W) \leq \epsilon] \geq 2/3\,, \tag{C.58}$$

no matter which W was chosen by Alice. With $\hat{f}$ in hand, Bob can make the guess

$$\hat{W} = \mathrm{argmin}_{f_w \in \mathcal{P}} d(\hat{f}, f_w). \tag{C.59}$$

Note that as long as $d(\hat{f}, f_W) \leq \epsilon$, then for any $f_i \neq f_W \in \mathcal{P}$,

$$d(\hat{f}, f_i) \geq d(f_W, f_i) - d(\hat{f}, f_W) > 2\epsilon - \epsilon = \epsilon \geq d(\hat{f}, f_W). \tag{C.60}$$

Therefore, the error probability of Bob's guess is bounded by

$$\mathbb{P}[\hat{W} \neq W] = \mathbb{P}[\exists i \neq W : d(\hat{f}, f_i) \leq d(\hat{f}, f_W)] \leq \mathbb{P}[d(\hat{f}, f_W) > \epsilon] \leq 1/3. \tag{C.61}$$

By Fano's inequality [173, Theorem 2.10.1], the conditional entropy $S(W|\hat{W}) \leq s_2(1/3) + \frac{1}{3}\log \mathcal{M}(\mathcal{F}, d, 2\epsilon)$, where $s_2(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$ is the binary entropy function. Then the mutual information is at least

$$I(W; \hat{W}) = S(W) - S(W|\hat{W}) \geq (2/3) \log \mathcal{M}(\mathcal{F}, d, 2\epsilon) - s_2(1/3). \tag{C.62}$$

On the other hand, the sample size N controls the amount of information that Bob has access to. Since Bob's guess is produced by the dataset Z, by the data processing inequality [173, Theorem 2.8.1], we have

$$I(W; \hat{W}) \leq I(W; Z) = S(Z) - S(Z|W) = S(f_W(x_1), \ldots, f_W(x_N)) \leq N \log k, \tag{C.63}$$

where we used $S(Z|W) = 0$, since Z is determined by W, and the fact that $(f_W(x_1), \ldots, f_W(x_N))$ can take no more than k^N different values. Combining the above two inequalities, we arrive at

$$N \geq \Omega\left(\frac{\mathcal{M}(\mathcal{F}, d, 2\epsilon)}{\log k}\right). \tag{C.64}$$

□

With Proposition 12, we can prove Theorem 17 by quantizing the output states to the nearest elements in covering nets, similar to an idea employed in [174].

Proof of Theorem 17. Let $k = \mathcal{N}_\eta$. Since $\mathcal{N}_\eta \geq \mathcal{N}(\{f_V(\rho), V \in \mathcal{U}\}, \mathrm{d_{tr}}, \eta)$ for every $\rho \in S$, we can find an η-covering net $\mathcal{N}_\rho$ of size k for each $\rho \in S$. We label the elements of $\mathcal{N}_\rho$ using $\{1, \ldots, k\}$ and define $L_\rho(\sigma) \in [k]$ as the label of a covering net element $\sigma \in \mathcal{N}_\rho$.

Now we define the quantized function Qf_U that maps an input state ρ to an element of the covering net $\mathcal{N}_\rho$. Specifically, for any $\rho \in S$ and any $\sigma \in \{f_V(\rho), V \in \mathcal{U}\}$, there exists a $\sigma' \in \mathcal{N}_\rho$, such that $\mathrm{d_{tr}}(\sigma, \sigma') \leq \eta$. For any unitary $U \in \mathcal{U}$, we define

$$Qf_U(\rho) = \mathrm{argmin}_{\sigma \in \mathcal{N}_\rho} \mathrm{d_{tr}}(f_U(\rho), \sigma) \tag{C.65}$$

and $LQf_U(\rho) = L_\rho[Qf_U(\rho)]$ be the corresponding label. (Ties are broken arbitrarily.) Then LQf_U is a discrete-output function mapping input states S to labels $[k]$ and it is in one-to-one correspondence with Qf_U. We use $\mathcal{F}^Q$ to denote all these labeled quantized functions, $\mathcal{F}^Q = \{LQf_U, U \in \mathcal{U}\}$, and define the distance metric on labeled functions as $d_L(LQf_V, LQf_W) = d_P(Qf_V, Qf_W)$. A useful property is that for any unitary $U \in \mathcal{U}$, we have

$$d_P(f_U, Qf_U) = \sqrt{\mathbb{E}_{\rho\sim P}[\mathrm{d}_{\mathrm{tr}}(f_U(\rho), Qf_U(\rho))^2]} \leq \sqrt{\mathbb{E}_{\rho\sim P}[\eta^2]} = \eta. \tag{C.66}$$

Now we claim that if there exists a noise-robust learning algorithm H for $\mathcal{U}$ to accuracy ϵ in d_P with probability at least $2/3$, then we can use it to construct a learning algorithm H^Q for $\mathcal{F}^Q$ to accuracy $\epsilon + 2\eta$ in d_L with success probability at least $2/3$. Hence, the sample complexity for $\mathcal{U}$ must satisfy

$$N \geq \Omega\left(\frac{\log \mathcal{M}(\mathcal{F}^Q, d_L, 2\epsilon + 4\eta)}{\log k}\right), \tag{C.67}$$

by Proposition 12.

To show this claim, we construct H^Q as follows. For any $LQf_U \in \mathcal{F}^Q$, let the dataset be

$$Z = (\rho_1, Qf_U(\rho_1)), \ldots, (\rho_N, Qf_U(\rho_N)). \tag{C.68}$$

From the definition of quantized functions, we know that the $Qf_U(\rho_i)$ are η-noisy version of $f_U(\rho_i)$ because $\mathrm{d}_{\mathrm{tr}}(Qf_U(\rho_i), f_U(\rho_i)) \leq \eta$. Now we define H^Q as

$$H^Q[Z] = LQf_{H[Z]}. \tag{C.69}$$

Since the learning algorithm H is η-noise-robust, we have $d_P(f_{H[Z]}, f_U) \leq \epsilon$ and thus $d_P(f_{H[Z]}, Qf_U) \leq d_P(f_{H[Z]}, f_U) + d_P(f_U, Qf_U) \leq \epsilon + \eta$ with probability at least $2/3$. Then by the triangle inequality (proved similarly as in Lemma 6), we have

$$d_L(H^Q[Z], LQf_U) = d_P(Qf_{H[Z]}, Qf_U) \leq d_P(Qf_{H[Z]}, f_{H[Z]}) + d_P(f_{H[Z]}, Qf_U) \leq \epsilon + 2\eta \tag{C.70}$$

with probability at least $2/3$. Thus the claim is proved.

At this point, it remains to prove that

$$\mathcal{M}(\mathcal{F}^Q, d_L, 2\epsilon + 4\eta) \geq \mathcal{M}(\mathcal{F}_{\mathcal{U}}, d_P, 2\epsilon + 6\eta). \tag{C.71}$$

To prove this, we can take a maximal $(2\epsilon + 6\eta)$-packing $\mathcal{P}$ of $\mathcal{F}_{\mathcal{U}}$ with respect to d_P, with $|\mathcal{P}| = \mathcal{M}(\mathcal{F}_{\mathcal{U}}, d_P, 2\epsilon + 6\eta)$. Then $\forall f_{U_1} \neq f_{U_2} \in \mathcal{P}$, we have

$$2\epsilon + 6\eta < d_P(f_{U_1}, f_{U_2}) \leq d_P(f_{U_1}, Qf_{U_1}) + d_P(Qf_{U_1}, Qf_{U_2}) + d_P(Qf_{U_2}, U_2) \leq 2\eta + d_P(Qf_{U_1}, Qf_{U_2}). \tag{C.72}$$

Therefore, $d_L(LQf_{U_1}, LQf_{U_2}) = d_P(Qf_{U_1}, Qf_{U_2}) > 2\epsilon + 4\eta$. Hence,

$$\mathcal{M}(\mathcal{F}^Q, d_L, 2\epsilon + 4\eta) \geq |\{LQf_U, U \in \mathcal{P}\}| = |\mathcal{P}| = \mathcal{M}(\mathcal{F}_{\mathcal{U}}, d_P, 2\epsilon + 6\eta). \tag{C.73}$$

This concludes the proof of the main part in Theorem 17.

Finally, we illustrate the special case where $\eta = \Theta(\epsilon)$, $\mathcal{U} = U(2^n)$ is the whole unitary group, P is a locally scrambled ensemble up to the second moment over n-qubit pure states (e.g., n-qubit Haar measure, see Definition 1), S is the support of P, and $f_U(\rho) = U\rho U^\dagger$. We show that at least $\Omega(2^n)$ samples are needed, thus reproducing the quantum no-free-lunch theorem in the usual sense and generalizing it to locally scrambled ensembles.

To see this, we first compute $\log \mathcal{M}(\mathcal{F}_{U(2^n)}, d_P, 2\epsilon + 6\eta)$. From the covering number bound for $U(2^n)$ with respect to the normalized Frobenius norm d_F (Lemma 9), the fact that quotienting out the global phase only changes the metric entropy by an additive $\mathcal{O}(\log(1/(2\epsilon + 6\eta)))$ term (Lemma 10), and by the equivalence of d_F', $\mathrm{d}_{\mathrm{avg}}$, and d_P (Lemma 4 Item 1 and Lemma 5), we know that $\log \mathcal{M}(\mathcal{F}_{U(2^n)}, d_P, 2\epsilon + 6\eta) \geq \Omega\left(4^n \log(1/\epsilon)\right)$, where we used $\eta = \Theta(\epsilon)$.

Next, we move on to $\mathcal{N}_\eta$. Since the output states are still n-qubit pure states, $\mathcal{N}_\eta$ is the covering number of the set of pure states with respect to d_{tr}. Considering that $\frac{1}{2}\left\|\left|\psi\middle\rangle\!\middle\langle\psi\right|\right\|_1$ is less than one for any pure state $|\psi\rangle$, the covering number is upper bounded by the covering number of a unit Euclidean ball in a $\Theta(2^n)$ dimensional linear space. Therefore, we have $\log \mathcal{N}_\eta \leq \mathcal{O}(2^n \log(1/\eta)) = \mathcal{O}(2^n \log(1/\epsilon))$ since $\eta = \Theta(\epsilon)$. Hence we arrive at

$$N \geq \Omega\left(\frac{4^n \log(1/\epsilon)}{2^n \log(1/\epsilon)}\right) = \Omega(2^n). \tag{C.74}$$

This concludes the proof of Theorem 17. □

The information theoretic version of quantum no-free-lunch theorem (Theorem 17) also gives us a way to generalize quantum no-free-lunch to a restricted unitary class. For example, for unitaries with bounded circuit complexity G, the packing number in the enumerator is lower bounded by $\Omega(G)$, while the covering number in the denominator is upper bounded by $\mathcal{O}(\min\{G\log G + G\log n, 2^n\})$. This gives us a quantum no-free-lunch theorem for G-gate unitaries, where the sample complexity is lower bounded by $\Omega(1)$ for $G \leq \mathcal{O}(2^n)$, by $\Omega(G/2^n)$ for $\Omega(2^n) < G \leq \mathcal{O}(4^n)$ and $\Omega(2^n)$ for $G \geq \Omega(4^n)$.

5. Computational complexity

Similar to the state learning case, our algorithm for average-case unitary learning described in Appendix C 2 is not computationally efficient. In this section, we follow Appendix B 3 and first show that there is no polynomial-time algorithm for learning unitaries composed of $G = \mathcal{O}(n\mathsf{polylog}(n))$ two-qubit gates, assuming $\mathsf{RingLWE}$ cannot be solved efficiently on a quantum computer. This result also holds for unitaries with circuit depth $\mathcal{O}(\mathsf{polylog}(n))$. Then we invoke a stronger assumption that $\mathsf{RingLWE}$ cannot be solved by any sub-exponential-time quantum algorithm, and show that any quantum algorithm for learning unitaries composed of $\tilde{\mathcal{O}}(G)$ gates must use $\exp(\Omega(G))$ time. Finally, we explicitly construct an efficient learning algorithm for $G = \mathcal{O}(\log n)$, thus establishing $\log n$ gate complexity as a transition point of computational efficiency.

Theorem 18 (Unitary learning computational complexity lower bound assuming polynomial hardness of $\mathsf{RingLWE}$)**.** *Let $\lambda = n$ be the security parameter. Let U be a unitary consisting of $G = \mathcal{O}(n\mathsf{polylog}(n))$ gates (or a depth $d = \mathcal{O}(\mathsf{polylog}(n))$ circuit) that implements a pseudorandom function in $\mathcal{RF}$. Such a unitary U exists by Corollary 3. There exists no polynomial-time quantum algorithm for learning a circuit description of U to within $\epsilon \leq 1/64$ average-case distance $\mathrm{d}_{\mathrm{avg}}$ with probability at least $2/3$ from $N = \mathsf{poly}(\lambda)$ queries, if quantum computers cannot solve* $\mathsf{RingLWE}$ *in polynomial time.*

Proof. Suppose for the sake of contradiction that there is an efficient algorithm $\mathcal{A}_0$ that can learn a description of U to within ϵ average-case distance with probability at least 2/3. Then by standard boosting of success probability (see e.g, [21, Proposition 2.4]), there is an efficient algorithm $\mathcal{A}$ that can learn U to the same accuracy with probability at least $p = 1-1/8192$ with only a constant factor overhead in time complexity. Note that this boosting requires the distance metric to be efficiently computable, which is guaranteed by the SWAP test elaborated below. We will construct a polynomial-time quantum distinguisher $\mathcal{D}$ that invokes $\mathcal{A}$ to distinguish between U and the unitary $V \in \mathcal{U}$ corresponding to a random classical function. This contradicts Theorem 11 Item 2.

The distinguisher $\mathcal{D}$ operates according to Algorithm 6.

```
Algorithm 6: Distinguisher $\mathcal{D}$ for PRF
Input: $N$ query access to $U$
Output: $b \in \{0,1\}$
1 Run $\mathcal{A}$ using $(N-1)$ queries to $U$, receiving $\hat{U}$.
2 Prepare a random tensor product of 1-qubit stabilizer states $|x\rangle, x \in \mathbb{Z}_6^n$.
3 Query $U$ one more time to prepare $U|x\rangle$.
4 Run the SWAP test on $U|x\rangle$ and $\hat{U}|x\rangle$, receiving a bit $b \in \{0,1\}$.
5 Output $b$.
```

Recall that the SWAP test [140, 141] takes two quantum states $|\alpha\rangle, |\beta\rangle$ as input and outputs 1 with probability $(1 + |\langle\alpha|\beta\rangle|^2)/2$. We denote this algorithm as $\mathsf{SWAP}(|\alpha\rangle, |\beta\rangle)$.

Note that Step 2 in Algorithm 6, the preparation of tensor product of 1-qubit stabilizer states $|x\rangle, x \in \mathbb{Z}_6^n$, is computationally efficient, because it can be achieved by random one-qubit gates acting on each of the n qubits. Moreover, Step 4 can be implemented efficiently on a quantum computer because $\hat{U}$ is given in terms of efficient circuit description and because the SWAP test is efficiently implementable. Thus, assuming the hypothetical learner $\mathcal{A}$ to be efficient, the distinguisher $\mathcal{D}$ is efficient as well.

We analyze the probability that the distinguisher $\mathcal{D}$ outputs 1 when given the pseudorandom function U versus the random classical Boolean function V. We denote the distribution of $|x\rangle$ by Q. From Lemma 5, we have

$$d_Q(U,\hat{U}) = \sqrt{\mathbb{E}_{|x\rangle\sim Q}[\mathrm{d}_{\mathrm{tr}}(U|x\rangle, \hat{U}|x\rangle)^2]} \leq \sqrt{2}\,\mathrm{d}_{\mathrm{avg}}(U,\hat{U}). \tag{C.75}$$

Case 1: $U \in \mathcal{RF}$**.** By the guarantees of $\mathcal{A}$, with probability at least p, we have $\mathrm{d}_{\mathrm{avg}}(\hat{U},U) \leq \epsilon \leq 1/64$, where $\hat{U}$ is the unitary learned by algorithm $\mathcal{A}$. This implies

$$\mathop{\mathbb{E}}_{|x\rangle\sim Q} |\langle x|\hat{U}^\dagger U|x\rangle|^2 = 1 - d_Q^2(U,\hat{U}) \geq 1 - 2\epsilon^2, \tag{C.76}$$

where we used the relationship between fidelity and trace distance. Then it immediately follows from

Equation (C.76) that

$$\begin{aligned}
\Pr_{U\in\mathcal{RF},\mathcal{D}}\left[\mathcal{D}^{|U\rangle}(\cdot)=1\right] &= \Pr_{\substack{U\in\mathcal{RF},|x\rangle\sim Q\\ \mathcal{A},\mathsf{SWAP}}}\left[\mathsf{SWAP}\left(U|x\rangle,\hat{U}|x\rangle\right)=1\right]\\
&= \mathop{\mathbb{E}}_{U\in\mathcal{RF},|x\rangle\sim Q}\left[\Pr_{\mathcal{A},\mathsf{SWAP}}\left[\mathsf{SWAP}\left(U|x\rangle,\hat{U}|x\rangle\right)=1\middle| U,|x\rangle\right]\right]\\
&\geq p\mathop{\mathbb{E}}_{U\in\mathcal{RF}}\left[\frac{1}{2}+\frac{1}{2}\mathop{\mathbb{E}}_{\hat{U},|x\rangle\sim Q}\left[|\langle x|\hat{U}^\dagger U|x\rangle|^2\right]\right]\\
&\geq p\mathop{\mathbb{E}}_{U\in\mathcal{RF}}\left[\frac{1}{2}+\frac{1}{2}(1-2\epsilon^2)\right]=p(1-\epsilon^2)>\frac{8189}{8192},
\end{aligned}\tag{C.77}$$

where in the first inequality we split the probability into two terms conditioned on the success and failure of $\mathcal{A}$, and we lower bound the failure term by zero, and in the last inequality we have used the fact that $p(1-\epsilon^2)\geq(1-1/8192)(1-1/4096)>8189/8192$.

Case 2: $U=V\in\mathcal{U}$, where V is the n-qubit unitary implementing a randomly chosen classical function. We want to upper bound the probability that the distinguisher $\mathcal{D}$ outputs 1 when given queries to V. Let $\mathcal{C}$ be the set of all possible output unitaries of $\mathcal{A}$. We follow the same reasoning as in Equation (C.77) and note that

$$\begin{aligned}
\Pr_{V\in\mathcal{U},\mathcal{D}}\left[\mathcal{D}^{|V\rangle}(\cdot)=1\right] &\leq \mathop{\mathbb{E}}_{V\in\mathcal{U}}\left[\max_{W\in\mathcal{C}}\mathop{\mathbb{E}}_{|x\rangle\sim Q}\left[\frac{1}{2}+\frac{1}{2}|\langle x|V^\dagger W|x\rangle|^2\right]\right]+(1-p)\\
&\leq \mathop{\mathbb{E}}_{V\in\mathcal{U}}\left[\max_{W\in\mathcal{C}}\left[1-\frac{1}{4}\mathrm{d_{avg}}(V,W)^2\right]\right]+(1-p)\\
&\triangleq \mathop{\mathbb{E}}_{V\in\mathcal{U}}[O_V]+(1-p),
\end{aligned}\tag{C.78}$$

where we define $O_V=\max_{W\in\mathcal{C}}\left[1-\frac{1}{4}\mathrm{d_{avg}}(V,W)^2\right]$. Furthermore, we can split the right hand side into two parts by introducing a constant θ:

$$\mathop{\mathbb{E}}_{V\in\mathcal{U}}[O_V]\leq\Pr\left[O_V\leq 1-\frac{\theta^2}{4}\right]\cdot\left(1-\frac{\theta^2}{4}\right)+\Pr\left[O_V>1-\frac{\theta^2}{4}\right]\cdot 1\leq 1-\frac{\theta^2}{4}+\Pr\left[O_V>1-\frac{\theta^2}{4}\right],\tag{C.79}$$

where we have used the fact that $O_V\leq 1$. Note that

$$\begin{aligned}
\Pr\left[O_V>1-\frac{\theta^2}{4}\right] &\leq \Pr_{V\in\mathcal{U}}\left[\exists W\in\mathcal{C}:\mathrm{d_{avg}}(V,W)<\theta\right]\\
&\leq \sum_{W\in\mathcal{N}}\Pr_{V\in\mathcal{U}}\left[\mathrm{d_{avg}}(V,W)<\theta\right]\\
&= \sum_{W\in\mathcal{N}}\frac{1}{|\mathcal{U}|}\sum_{V\in\mathcal{U}}1\left\{\mathrm{d_{avg}}(V,W)<\theta\right\}\\
&\leq \frac{|\mathcal{N}|\max_{W\in\mathcal{N}}N_{W,\theta}}{|\mathcal{U}|}.
\end{aligned}\tag{C.80}$$

In the second line, we define $\mathcal{N}$ be a minimal θ-covering net over $\mathcal{C}$ with respect to $\mathrm{d_{avg}}$. Also, in the last line, we define $N_{W,\theta}\triangleq\sum_{V\in\mathcal{U}}1\{\mathrm{d_{avg}}(V,W)<\theta\}$ to be the number of $V\in\mathcal{U}$ that are θ-close to W in $\mathrm{d_{avg}}$.

Now we aim to upper bound $N_{W,\theta}$ by counting. We first note that $N_{W,\theta}\leq\max_{V\in\mathcal{U}}N_{V,4\theta}+1$. This is because, by definition of $N_{W,\theta}$, there exist $V_1,\ldots,V_{N_{W,\theta}}\in\mathcal{U}$ such that $\mathrm{d_{avg}}(V_i,W)<\theta, 1\leq i\leq N_{W,\theta}$. Then for V_1 and any $V_i, 2\leq i\leq N_{W,\theta}$, we have

$$\mathrm{d_{avg}}(V_1,V_i)\leq d'_F(V_1,V_i)\leq d'_F(V_1,W)+d'_F(V_i,W)\leq 2\,\mathrm{d_{avg}}(V_1,W)+2\,\mathrm{d_{avg}}(V_i,W)<4\theta.\tag{C.81}$$

This means that there are at least $N_{W,\theta}-1$ elements of $\mathcal{U}$ that are (4θ)-close to V_1. Therefore, $N_{V_1,4\theta}\geq N_{W,\theta}-1$ and hence $N_{W,\theta}\leq\max_{V\in\mathcal{U}}N_{V,4\theta}+1$.

Next, we upper bound $N_{V,4\theta}$ for any $V\in\mathcal{U}$. Recall that each $V\in\mathcal{U}$ is an oracle unitary of a Boolean function on $\{0,1\}^n$. We can represent it by $f_V(i)\in\{0,1\}, 1\leq i\leq 2^n$. Consider a different $V'\in\mathcal{U}$ corresponding to the Boolean function $f_{V'}$. If f_V and $f_{V'}$ differ on at least $\lceil 64\theta^2\cdot 2^n\rceil$ of the 2^n possible inputs $i\in[2^n]$, then the corresponding columns of the unitaries V and V' must also differ. In particular, in each of these columns, there will be a matrix element that is 1 for V but 0 for V'. This means that V and V' are 4θ apart from each other w.r.t. d_{avg}:

$$\mathrm{d}_{\text{avg}}(V, V') \geq \frac{1}{2} \min_{e^{i\phi} \in U(1)} \left\| V - V' e^{i\phi} \right\|_F \geq \frac{1}{2\sqrt{d}} \min_{e^{i\phi} \in U(1)} \sqrt{64\theta^2 \cdot 2^n |1 - 0 \cdot e^{i\phi}|^2} = 4\theta. \tag{C.82}$$

Therefore, all functions $f_{V'}$ corresponding to the $V' \in \mathcal{U}$ counted in $N_{V,4\theta}$ must differ from f_V on strictly less than $\lceil 64\theta^2 \cdot 2^n \rceil$ of the 2^n inputs. This gives us

$$N_{V,4\theta} \leq \sum_{k=0}^{\lceil 64\theta^2 \cdot 2^n \rceil} \binom{2^n}{k}, \tag{C.83}$$

where each term represents choosing k inputs where the output is different from f_V. The right hand side can be further bounded as

$$\sum_{k=0}^{\lceil 64\theta^2 \cdot 2^n \rceil} \binom{2^n}{k} \leq \left(\frac{e 2^n}{\lceil 64\theta^2 \cdot 2^n \rceil} \right)^{\lceil 64\theta^2 \cdot 2^n \rceil} \leq 2^{(64\theta^2 \cdot 2^n + 1) \log_2(e/64\theta^2)}. \tag{C.84}$$

Note that when $\theta = 1/16$, we have $64\theta^2 = 1/4$ and $64\theta^2 \log_2(e/64\theta^2) = \log_2(4e)/4 < 0.87$. Therefore, recalling that the set of all n-bit classical Boolean functions has size $|\mathcal{U}| = 2^{2^n}$, we obtain

$$\Pr\left[O_V > 1 - \frac{\theta^2}{4} \right] \leq |\mathcal{N}| 2^{-0.13 \cdot 2^n + \log_2(4e) + 1}, \tag{C.85}$$

where the extra one in the exponent takes the one in $N_{W,\theta} \leq \max_{V \in \mathcal{U}} N_{V,4\theta} + 1$ into account.

Finally, we move on to bound $|\mathcal{N}|$. Similar to Equation (B.102) in the state learning case, since our learning algorithm is a polynomial time algorithm that can only output circuit descriptions with size $\mathsf{poly}(n)$, we must have

$$|\mathcal{N}| \leq \mathcal{O}\left((1/\theta)^{\mathsf{poly}(n)} \right) = \mathcal{O}\left(2^{\mathsf{poly}(n)} \right). \tag{C.86}$$

Thus we arrive at

$$\Pr\left[O_V > 1 - \frac{\theta^2}{4} \right] \leq \mathcal{O}\left(2^{\mathsf{poly}(n) - 0.13 \cdot 2^n} \right) = \mathrm{negl}(n) \tag{C.87}$$

and therefore

$$\Pr\left[\mathcal{D}^{|V\rangle}(\cdot) = 1 \right] \leq 1 - \frac{\theta^2}{4} + \mathrm{negl}(n) + (1 - p) = \frac{8185}{8192} + \mathrm{negl}(n), \tag{C.88}$$

where we have used $\theta = 1/16$ and $p = 1 - 1/8192$.

Combining Equation (C.77) and Equation (C.87), we have

$$\left| \Pr_{U \in \mathcal{RF}} [\mathcal{D}^{|U\rangle}(\cdot) = 1] - \Pr_{V \in \mathcal{U}} [\mathcal{D}^{|V\rangle}(\cdot) = 1] \right| \geq \frac{4}{8192} - \mathrm{negl}(n) \geq \frac{1}{4096} \tag{C.89}$$

for large n. This contradicts the defining property of pseudorandom functions $\mathcal{RF}$ (Theorem 11 Item 2) under the assumption that $\mathsf{RingLWE}$ is hard. □

Next, we invoke the stronger assumption that $\mathsf{RingLWE}$ cannot be solved by any sub-exponential-time quantum algorithms and show that learning unitaries composed of $G = \mathcal{O}(\log n \cdot \mathsf{polyloglog} n)$ gates is computationally hard.

Theorem 19 (Unitary learning computational complexity lower bound assuming sub-exponential hardness of $\mathsf{RingLWE}$, restatement of lower bound in Theorem 6)**.** *Let $\lambda = l = \Theta(G)$ with $l \leq n$ be the security parameter. Let V be an l-qubit unitary consisting of $\mathcal{O}(l\mathsf{polylog}(l)) = \mathcal{O}(G\mathsf{polylog}(G))$ gates (or a depth $d = \mathcal{O}(\mathsf{polylog}(G))$ circuit) that implements a pseudorandom function in $\mathcal{RF}$. Such a unitary V exists by Corollary 3. Let $U = V \otimes I$, where the identity I is over the last $(n - l)$ qubits. Any quantum algorithm for learning a circuit description of the n-qubit unitary U to within $\epsilon \leq 1/64$ average-case distance d_{avg} with probability at least $2/3$ from $N = \mathsf{poly}(\lambda)$ queries to U must use $\exp(\Omega(\min\{G, n\}))$ time, if quantum computers cannot solve $\mathsf{RingLWE}$ in sub-exponential time.*

Proof. With polynomial hardness of $\mathsf{RingLWE}$ replaced by sub-exponential hardness, Theorem 18 asserts that there are no sub-exponential (in l) quantum algorithms that can learn the l-qubit unitary V to within average case distance $\epsilon < 1/64$ with success probability at least $2/3$. That is, any such learning algorithms must use time at least $\exp(\Omega(l)) = \exp(\Omega(\min\{G, n\}))$, since $l \leq n$. Meanwhile, a polynomial learning algorithm for the n-qubit unitary $U = V \otimes I$ can be used to learn the l-qubit unitary V in the same runtime by discarding the last $(n - l)$ qubits, because trace distance does not increase under such operation and thus neither does $\mathrm{d}_{\mathrm{avg}}$. This implies the $\exp(\Omega(\min\{G, n\}))$ time lower bound for the n-qubit learning algorithm. □

Finally, we briefly show that learning becomes efficient when $G = \mathcal{O}(\log n)$. The idea is that with $\mathcal{O}(\log n)$ gates, there can only be at most $\mathcal{O}(\log n)$ qubits affected. Thus we can focus on these qubits and learning the unitary amounts to manipulating at most $2^{\mathcal{O}(\log n)} = \mathsf{poly}(n)$ size matrices, which is efficient. Specifically, we have the following statement.

Proposition 13 (Learning unitaries with logarithmic circuit complexity efficiently, restatement of upper bound in Theorem 6)**.** *Let $\epsilon > 0$. Suppose we are given N queries to an n-qubit unitary U consisting of $G = \mathcal{O}(\log n)$ two-qubit gates. There exists a learning algorithm that outputs a $\hat{U}$ such that $\mathrm{d}_{\mathrm{avg}}(U, \hat{U}) \leq \epsilon$ with probability at least $2/3$ using $\mathsf{poly}(n, 1/\epsilon)$ queries and time.*

Proof. We prove this by a learning algorithm similar to Proposition 7 via junta learning based on Choi states (Appendix C 2 b) as follows.

Firstly, we prepare the Choi state of U by applying it to a maximally entangled state over $2n$ qubits, execute Algorithm 4, and post-select on the trivial qubits being in the state $|I\rangle\!\rangle$ as in Appendix C 2 b. This step uses $\mathsf{poly}(n, 1/\epsilon)$ queries and time, and gives us the post-selected Choi state which is non-trivial on only $4G = \mathcal{O}(\log n)$ qubits. Then we use the Pauli tomography method as in Proposition 7 to learn a trace-distance approximation to the $4G$-qubit Choi state $|\hat{V}\rangle\!\rangle$ using $\mathsf{poly}(n, 1/\epsilon)$ queries and time. We can enforce this approximation to be a valid Choi state by projecting it to the subspace spanned by $(A \otimes I)\,|\Phi\rangle$ and normalize the projected state, where A is an arbitrary matrix and $|\Phi\rangle$ is the maximally entangled state. This can be done via a projector which is a $2^{4G} = \mathsf{poly}(n)$ dimensional matrix. Finally, we calculate the corresponding unitary $\hat{V}$ and set $\hat{U} = \hat{V} \otimes I$. Note that this step is efficient as it only involves manipulating matrices of size $2^{4G} = \mathsf{poly}(n)$. Since the trace distance between Choi states is equivalent to the average-case distance between the corresponding unitaries, this gives us a $\mathsf{poly}(n, 1/\epsilon)$ learning algorithm for average-case unitary learning. □

Appendix D: Learning physical functions

As stated in the main text, learning classical functions that map variables controlling the input states and evolution to some property of the outputs is an alternative way of learning about Nature. Learning such functions has long been a central task of statistics and, more recently, classical and quantum machine learning. However, the physical mechanism that gives rise to these functions has largely been overlooked for the convenience of mathematical abstraction.

In fact, we can formulate the physical mechanism underlying a classical function as an experiment procedure involving a unitary with bounded circuit complexity. Specifically, we consider the following general experimental setting.

1. Given a set of ν variables $x \in [0, 1]^\nu$, we prepare a pure state that can depend on x in a fixed way.

2. We evolve the state using a unitary $U(x; \{U_i\}_{i=1}^G, a)$ that contains at most G two-qubit gates $\{U_i\}_{i=1}^G$, which can be tuned arbitrarily, and any number of fixed unitaries, which can depend on x, according to a circuit architecture a in an architecture class A.

3. We measure the output state with a fixed observable O and read out the expectation value as the function output.

We can w.l.o.g. absorb the state preparation into the unitary. Then the experiment gives rise to the function

$$f(\cdot; \{U_i\}, a) : [0, 1]^\nu \ni x \mapsto f(x; \{U_i\}, a) = \left\langle 0^n \middle| U(x; \{U_i\}, a)^\dagger O U(x; \{U_i\}, a) \middle| 0^n \right\rangle. \tag{D.1}$$

We define

$$\mathcal{F}_{G,A}^\nu = \{f(\cdot, \{U_i\}, a) : a \in A, U_i \in U(2^2), i = 1, \ldots, G\} \subseteq \mathbb{R}^{[0,1]^\nu} \tag{D.2}$$

to be the function class given by a class of architectures A for G-gate unitaries. We call such functions *physical functions*, and $\mathcal{F}^{\nu}_{G,A}$ the class of ν-variable physical functions with G gates and architectures A.

This experiment can also be understood as a quantum machine learning problem, where we want to collect training data $\{x, f(x)\}$ to learn to approximate certain functions in a function class using the ansatz described above. Then, the tunable gates $\{U_i\}$ can be understood as variational/trainable parameters of our quantum neural network. We note that the data encoding unitaries may simply use x as the angles for rotation, or it can also be arbitrarily complex (e.g., complex enough to implement a quantum random access memory [175] that prepares the amplitude encoding of the data) as long as it is not trainable. This encompass the case where the input data are classical descriptions of the input pure state. Also the order of the data encoding unitaries and the trainable unitaries can be arbitrary, thus accommodating data re-uploading strategies [176, 177].

We will show that to approximate a certain class of functions well, we need a minimal number of samples to learn and a minimal number of gates G (Theorem 7). In particular, we consider the class of 1-bounded and 1-Lipschitz functions on $[0,1]^{\nu}$, which can (up to equivalence classes) be represented by the unit ball $B^{1,\infty}$ in the Sobolev space $W^{1,\infty}_{[0,1]^{\nu}}$. We establish the following theorem, where the learning criterion is the standard one for learning real functions [73, Definition 16.1].

Theorem 20 (Sample and gate complexity lower bounds on functions given by G-gate unitaries to approximate bounded Lipschitz functions, restatement of Theorem 7)**.** *Let $\mathcal{F}^{\nu}_{G,A} \subseteq \mathbb{R}^{[0,1]^{\nu}}$ be the function class given by an architecture class A of G two-qubit unitaries. Let $\epsilon \in (0,1)$ and let $l(|h(x) - y|)$ be a loss function where l is a strictly increasing function with derivative larger than some positive constant on $[1,\infty)$. Suppose for any 1-bounded and 1-Lipschitz function $f \in B^{1,\infty}$, there exists an $h \in \mathcal{F}^{\nu}_{G,A}$ such that $\|f - h\|_{\infty} < \epsilon$. Then the smallest training data size N such that there exists a learning algorithm $H : ([0,1]^{\nu}, [0,1])^N \to \mathcal{F}^{\nu}_{G,A}$ that satisfies*

$$\mathbb{P}_{S\sim P^N}\left\{\mathbb{E}_{(X,Y)\sim P} l(|H[S](X) - Y|) - \inf_{f\in\mathcal{F}^{\nu}_{G,A}} \mathbb{E}_{(X,Y)\sim P} l(|f(X) - Y|) \leq \epsilon\right\} \geq 0.99, \tag{D.3}$$

for any probability distribution P over $[0,1]^{\nu} \times [0,1]$ must be at least

$$N \geq \Omega\left(\frac{1}{\epsilon^{\nu}}\right). \tag{D.4}$$

Moreover, we need at least

$$G \geq \tilde{\Omega}\left(\frac{1}{\epsilon^{\nu/2}}\right) \tag{D.5}$$

two-qubit unitaries if A contains variable circuit structures, or $G \geq \tilde{\Omega}(1/\epsilon^{\nu})$ if the circuit structure is fixed. The $\tilde{\Omega}$ for variable circuit structures hides logarithmic factors in ϵ as well as in the number of qubits n, while the $\tilde{\Omega}$ for fixed structure only hides logarithmic factors in ϵ.

This means that to approximate 1-bounded and 1-Lipschitz functions in ν-variables well to $\mathcal{O}(1/n^D)$ accuracy, we need at least $\tilde{\Omega}(n^{\nu D/2})$ two-qubit unitaries and $\Omega(n^{\nu D})$ samples to train on. And $\sim 1/\exp(n)$ accuracy can only be achieved with exponential-size quantum circuits and exponentially many samples. This result establishes a limitation on the maximal efficiency of using parameterized quantum circuits to approximate functions, complementary to existing works on universal approximation theorems for parameterized quantum circuits [75–78].

The exponential dependence on the number of variables N suggests that if one has an extensively large input vector (whose length scales with n), then the number of samples and gates needed to approximate such functions is exponentially large. Moreover, if the variables are encoded using amplitude encoding (e.g., via QRAM), which accommodates exponentially many variables ($\sim 2^n$), then the gate and sample requirement would grow double exponentially in $1/\epsilon$. This phenomenon, named curse of dimensionality, was also established in the theory of classical neural networks [74, Chapter 3]. We show that it still exists in quantum machine learning.

This curse can be circumvented by introducing more structure or constraints on the function class. For example, if we constrain to Fourier-integrable functions, a ν-independent number of $\mathcal{O}(1/\epsilon^2)$ parameters suffice for both classical [74, Theorem 3.9] and quantum [75] machine learning. However, the curse of dimensionality shows that many-variable 1-bounded and 1-Lipschitz functions are not physical [45, 146] because Nature cannot efficiently implement them.

In order to prove Theorem 20, we proceed in three steps. Firstly, we show that the complexity of the function class $\mathcal{F}^{\nu}_{G,A}$ is limited by the number of gates G. Then we prove that to approximate certain functions (1-bounded and 1-Lipschitz functions) well enough, the complexity must not be too small. Finally, we show that to learn a function class from data, the number of samples we need is lower bounded by the complexity of the function class.

1. Circuit complexity and function complexity

The complexity of the function class $\mathcal{F}^{\nu}_{G,A}$, measured by the pseudo-dimension or fat-shattering dimension [178, 179], is limited by the number of trainable gates G and the size of the architecture class A. This is because from the linearity of quantum mechanics, the function $f(x; \{U_i\}, a)$ is a polynomial in the matrix elements of the trainable unitaries $\{U_i\}$, and the degree of this polynomial is limited by G. Following the idea of [72], we formalize this idea into the following lemma.

Lemma 27 (Functions given by G-gate unitaries are bounded degree polynomials)**.** *Let $\mathcal{F}^{\nu}_{G,A}$ be the function class given by an architecture class A of G two-qubit unitaries. Then there exists a set of functions $P^{\nu}_{G,A}$ in $32G + \nu$ real variables with size $|P^{\nu}_{G,A}| = |A|$ such that the following two properties hold.*

1. *$\forall f \in \mathcal{F}^{\nu}_{G,A}$, there exist a $p \in P^{\nu}_{G,A}$ and an assignment of the first $32G$ variables such that p under this assignment is the same as f in the last ν variables;*
2. *Each $p \in P^{\nu}_{G,A}$ depends polynomially on the first $32G$ variables with degree at most $2G$.*

Proof. We begin by noting that for any fixed architecture $a \in A$, the function $f(x, \{U_i\}, a)$ is a function of $32G + \nu$ real variables, where the first $32G = 2 \cdot 2^2 \cdot 2^2 \cdot G$ variables are the real and imaginary parts of the matrix elements of $\{U_i \in U(2^2)\}$, and the last ν variables are the input data $x \in [0, 1]^{\nu}$.

Next, we aim to prove that f is a bounded degree polynomial in the unitary matrix elements. We follow the idea of [72, Lemma 1] and analyze the function $f(x, \{U_i\}, a)$ gate by gate. We note the following fact from linear algebra: for any state $|\psi\rangle$ and matrix U, the product $U|\psi\rangle$ is a state whose amplitudes are linear combinations of the amplitudes of $|\psi\rangle$ and of matrix elements of U. Therefore, by applying $\{U_i\}_{i=1}^{G}$ and other unitaries that do not depend on $\{U_i\}$ sequentially according to the architecture a, we get a state whose amplitude is a polynomial of the matrix elements of $\{U_i\}$ with degree at most G. Hence, the output scalar $\langle 0^n | U(x; \{U_i\}, a)^{\dagger} O U(x; \{U_i\}, a) | 0^n \rangle$ is a polynomial of the matrix elements of $\{U_i\}$ with degree at most $2G$. Fixing those $32G$ variables corresponds to fixing $\{U_i\}$ and thus specifying any particular function in $\mathcal{F}^{\nu}_{G,A}$ with this architecture a. Taking into account the dependence on x and gathering the function for each architecture $a \in A$, we arrive at the desired set of functions $P^{\nu}_{G,A}$ with $|P^{\nu}_{G,A}| = |A|$. □

The fact that these functions are of bounded degree in the variables specifying the trainable unitaries implies an upper bound on pseudo-dimension. We prove this with a reasoning analogous to [180] and [72, Theorem 2].

Proposition 14 (Pseudo-dimension upper bound for functions given by G-gate unitaries)**.** *Let $\mathcal{F}^{\nu}_{G,A}$ be the function class given by an architecture class A of G two-qubit unitaries. Then the pseudo-dimension of $\mathcal{F}^{\nu}_{G,A}$ is at most $128G \log_2(16eG|A|)$.*

Proof. Let $\{(x_i, y_i)\}_{i=1}^{m} \subseteq [0, 1]^{\nu} \times \mathbb{R}$ be a set of data points satisfying that for any $C \subseteq \{1, \dots, m\}$, there exists $f_C \in \mathcal{F}^{\nu}_{G,A}$ such that $f(x_i) - y_i \geq 0$ if and only if $i \in C$. That is, $\{(x_i, y_i)\}_{i=1}^{m}$ is pseudo-shattered by $\mathcal{F}^{\nu}_{G,A}$. From Lemma 27 we know that there exists a set of functions P in $32G + \nu$ real variables with size $|P| = |A|$ such that for every C, there is a $p_C \in P$ and an assignment Ξ_C to the first $32G$ variable that satisfies $p_C(\Xi_C, x_i) - y_i \geq 0$ if and only if $i \in C$. This means that the set of functions $\{p(\cdot, x_i) - y_i : i = 1, \dots, m, p \in P\}$ is a set of $m|A|$ polynomials of degree at most $2G$ in $32G$ real variables that has at least 2^m different consistent sign assignments[3]. Now we invoke the following technical lemma.

Lemma 28 (Bounded degree polynomials have a bounded number of consistent sign assignments, [72, 180, 181])**.** *Let P be a set of real polynomials in v variables with $|P| \geq v$, each of degree at most $D \geq 1$. Then the number of consistent sign assignments to P is at most $(8De|P|/v)^v$.*

[3] A consistent sign assignment to a set of polynomials $p_1, \dots, p_k$ is a vector $b \in \{-1, 0, 1\}^k$ such that there exists a set of input variables $z_1, \dots, z_N \in \mathbb{R}$ such that $\text{sgn}[p_i(z_1, \dots, z_N)] = b_i$ for all $1 \leq i \leq k$.

Thus we have

$$2^m \leq \left(\frac{8 \cdot 2G \cdot em|A|}{32G}\right)^{32G}. \tag{D.6}$$

Taking the logarithm yields

$$m \leq 32G(\log_2(16eG|A|) + \log_2(m/(32G))). \tag{D.7}$$

Let's first assume $m \geq 32G$. If $\log_2(16eG|A|) \geq \log_2(m/(32G))$, then we have $m \leq 64G\log_2(16eG|A|)$. Otherwise, $\log_2(16eG|A|) < \log_2(m/(32G))$ and we have $m \leq 64G\log_2(m/(32G))$, which translates into $\frac{\log_2(m/(32G))}{m/(32G)} \geq \frac{1}{2}$. Thus $m/(32G) \leq 4$ and $m \leq 128G$. In both cases, we have $m \leq 128G\log_2(16eG|A|)$. If $m < 32G$, this is also true. Therefore, we have pseudo-dimension (by definition in Definition 6) at most $128G\log_2(16eG|A|)$. □

A special case is for fixed circuit architecture $|A| = 1$, where we have pseudo-dimension at most $128G\log_2(16eG)$. On the other hand, if we allow variable structure of the trainable unitaries, then $|A| \leq \binom{n}{2}^G \leq n^{2G}$, and we have pseudo-dimension at most $128G\log_2(16eG) + 256G^2\log_2(16eGn)$.

2. Function complexity and approximation power

Now that we know the pseudo-dimension of such function class is upper bounded via the number of gates G, we can derive the minimal number of gates needed to obtain certain function approximation power. Consider the class of 1-bounded and 1-Lipschitz functions on $[0,1]^\nu$, which can be represented by the unit ball $B^{1,\infty}$ in the Sobolev space $W^{1,\infty}_{[0,1]^\nu}$. In order to approximate these functions well, the pseudo-dimension (and also the fat-shattering dimension) of our function class cannot be too small.

Lemma 29 (Pseudo/fat-shattering dimension and approximation power, variant of [179, Theorem 2.10] and [182, Theorem 4])**.** *Let $\epsilon > 0$ and $\mathcal{F} \subseteq \mathbb{R}^{[0,1]^\nu}$ be a class of functions such that for any $f \in B^{1,\infty}$, there is an $h \in \mathcal{F}$ such that $\|f - h\|_\infty < \epsilon$. Then the pseudo-dimension of $\mathcal{F}$ must be at least $1/(4\epsilon)^\nu$. The ϵ-fat-shattering dimension of $\mathcal{F}$ must be at least $1/(8\epsilon)^\nu$.*

Proof. Let $m \in \mathbb{N}$ to be chosen later. Let $x_1, \ldots, x_M \in [0,1]^d$ be $M = (m+1)^\nu$ points on a cubic lattice such that $\|x_i - x_j\| \geq 1/m$ for all $i \neq j$. Let $y \in \mathbb{R}^M$, and we will now construct a smooth function that takes the y values at these lattice points. Specifically, we define

$$f(x) = \sum_{i=1}^{M} y_i \phi(m(x - x_i)), \tag{D.8}$$

where $\phi(z) = \prod_{j=1}^{\nu} \varphi(z_j)$ and φ is a smoothed version of the triangular function that takes value 0 at $|z| \geq 1/2$ and value 1 at $z = 0$ and $|\partial_j \phi(z)| \leq C$ for any $C > 2$. In this way, we have $f(x_i) = y_i$ for all $1 \leq i \leq M$.

Next, for any $\alpha \in \{0,1\}^M$, set $y_i = \alpha_i/(Cm)$. This means that $|y_i| \leq 1/(Cm)$ and thus $f \in B^{1,\infty}$. Then by assumption there must be an $h \in \mathcal{F}$ such that $\|f - h\|_\infty < \epsilon$. In particular, we have $|f(x_i) - h(x_i)| = |y_i - h(x_i)| < \epsilon$ for all i.

Now, for the pseudo-dimension, we can choose m large enough (say, $m = \lfloor 1/(C^2\epsilon) \rfloor$) such that $\epsilon < 1/(2Cm)$. Then

$$h(x_i) \geq \frac{1}{2Cm} \iff \alpha_i = 1, y_i = \frac{1}{Cm}. \tag{D.9}$$

Therefore, by definion in Definition 6, $\{x_1, \ldots, x_M\}$ is pseudo-shattered by $\mathcal{F}$, and thus the pseudo-dimension of $\mathcal{F}$ is at least $M = (m+1)^\nu \geq 1/(C^2\epsilon)^\nu$. Taking the limit $C \to 2$ yields the desired result.

For fat-shattering dimension, we can choose m large enough (say, $m = \lfloor 1/(C^3\epsilon) \rfloor$) such that $\epsilon < 1/(4Cm)$. Then

$$\alpha_i = 1 \implies h(x_i) \geq \frac{1}{Cm} - \epsilon \geq \frac{1}{2Cm} + \epsilon, \tag{D.10}$$

and

$$\alpha_i = 0 \implies h(x_i) \leq \epsilon \leq \frac{1}{2Cm} - \epsilon. \tag{D.11}$$

Therefore, by definion in Definition 7, $\{x_1, \dots, x_M\}$ is ϵ-fat-shattered by $\mathcal{F}$, and thus the ϵ-fat-shattering dimension of $\mathcal{F}$ is at least $M = (m+1)^\nu \geq 1/(C^3\epsilon)^\nu$. Taking the limit $C \to 2$ yields the desired result. □

3. Function complexity and sample complexity

Now we aim to show that in order to learn a function class, the number of samples we need is lower bounded by its complexity. In particular, we achieve this through the fat-shattering dimension.

Proposition 15 (Sample complexity lower bound for real-valued functions by fat-shattering dimension, variant of [73, Theorem 19.5])**.** *Let $\mathcal{F} \subseteq [0,1]^{\mathcal{X}}$ with loss function $l_h(x,y) = l(|h(x)-y|)$. Suppose l is an increasing (almost everywhere) differentiable function, i.e., $C = \inf_{t\geq 1} l'(t) > 0$. For $0 < \epsilon < 1, 0 < \delta \leq 0.01$, the smallest training data size N such that there exists a learning algorithm $H : (\mathcal{X}, [0,1])^N \to \mathcal{F}$ that satisfies*

$$\mathbb{P}_{S\sim P^N}\left\{\mathbb{E}_{(X,Y)\sim P} l(|H[S](X) - Y|) - \inf_{f\in\mathcal{F}} \mathbb{E}_{(X,Y)\sim P} l(|f(X) - Y|) \leq \epsilon\right\} \geq 1-\delta, \tag{D.12}$$

for any probability distribution P over $\mathcal{X} \times [0,1]$ must be at least

$$N \geq C\frac{\mathrm{fat}(\mathcal{F}, \epsilon/\alpha) - 1}{32\alpha}, \quad \forall \alpha \in (0, 1/4). \tag{D.13}$$

Note that this contains L_p loss functions as a special case, where $l_h(x,y) = |h(x)-y|^p$, and $l'(t) = pt^{p-1} \geq p = C$.

Proof. Similarly to the proof of Theorem 19.5 in [73], the idea is to reduce the problem to a discrete classification problem. Consider the class H_d of all functions mapping from a finite set $\{x_1, \dots, x_d\} \subset \mathcal{X}$ to $\{0,1\}$. It's known that any learning algorithm for H_d has sample complexity at least $(d-1)/(32\epsilon)$ for small ϵ, δ ([73, Theorem 5.3]). Here we show that, for any fixed α between 0 and 1/4, any learning algorithm for $\mathcal{F}$ to accuracy ϵ can be used to construct a learning algorithm for H_d to accuracy α/C, where $d = \mathrm{fat}(\mathcal{F}, \epsilon/\alpha)$. Then the proposition follows.

To see this, suppose $\{x_1, \dots, x_d\}$ is ϵ/α-shattered by $\mathcal{F}$, witnessed by $r_1, \dots, r_d$. Suppose L is a learning algorithm for $\mathcal{F}$, then we can construct a learning algorithm for H_d as follows. For each labeled example (x_i, y_i), assuming y_i is deterministic given x_i, the algorithm passes to L the labeled example $(x_i, \tilde{y}_i)$, where $\tilde{y}_i = 2$ if $y_i = 1$ and $\tilde{y}_i = -1$ if $y_i = 0$. Let P be the original distribution on $\mathcal{X} \times \{0,1\}$, and $\tilde{P}$ the induced distribution on $\mathcal{X} \times \{-1, 2\}$. Then suppose L produces a function $f : \mathcal{X} \to [0,1]$, the learning algorithm for H_d then outputs $h : \mathcal{X} \to \{0,1\}$, where $h(x_i) = 1$ if and only if $f(x_i) > r_i$. Thus we only need to prove if $\mathbb{E}_{\tilde{P}} l_f - \inf_{g\in\mathcal{F}} \mathbb{E}_{\tilde{P}} l_g < \epsilon$, then $\mathbb{E}_P 1(h(x) \neq y) \leq \alpha/C$.

To show this, we claim that

$$\inf_{g\in\mathcal{F}} \mathbb{E}_{\tilde{P}} l_g = \inf_{g\in\mathcal{F}} \mathbb{E}_{\tilde{P}} l(|g(x) - \tilde{y}|) \leq \mathbb{E}_{\tilde{P}} \min\{l(|\hat{y} - \tilde{y}|), \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\}, \tag{D.14}$$

where $r(x_i) = r_i$. This is because that $\tilde{P}$ is concentrated on the shattered set. Then for any assignment $\{\hat{y}_i \in \{r_i \pm \epsilon/\alpha\}, i = 1, \dots, d\}$, there exists a $g \in \mathcal{F}$ s.t. $g(x_i) \geq \hat{y}_i$ if $\hat{y}_i = r_i + \epsilon/\alpha$ and $g(x_i) \leq \hat{y}_i$ if $\hat{y}_i = r_i - \epsilon/\alpha$. In particular, we consider the assignment of $\hat{y}_i$ s.t. $l(|\hat{y}_i - \tilde{y}_i|)$ is minimized. Then there exists a function g^* staistifying the following property. If $\tilde{y}_i = -1$, then the minimizer is $\hat{y}_i = r_i - \epsilon/\alpha$, and we have $l(|g^*(x_i) - \tilde{y}_i|) \leq l(|\hat{y} - \tilde{y}_i|)$ since $\tilde{y}_i < g^*(x_i) \leq \hat{y}_i$. Similarly, if $\tilde{y}_i = 2$, then the minimizer is $\hat{y}_i = r_i + \epsilon/\alpha$, and we still have $l(|g^*(x_i) - \tilde{y}_i|) \leq l(|\hat{y} - \tilde{y}_i|)$ since $\hat{y}_i \leq g^*(x_i) \leq \tilde{y}_i$. Therefore, since $\tilde{y}_i$ and y_i is deterministic given x_i, we have found a single g^* s.t. $\mathbb{E}_{\tilde{P}} l(|g^*(x) - \tilde{y}|) \leq \mathbb{E}_{\tilde{P}} \min\{l(|\hat{y} - \tilde{y}|), \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\}$. Hence, the infimum over $g \in \mathcal{F}$ $\inf_{g\in\mathcal{F}} \mathbb{E}_{\tilde{P}} l(|g(x) - \tilde{y}|) \leq \mathbb{E}_{\tilde{P}} l(|g^*(x) - \tilde{y}|) \leq \mathbb{E}_{\tilde{P}} \min\{l(|\hat{y} - \tilde{y}|), \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\}$. Therefore,

$$\mathbb{E}_{\tilde{P}} l_f - \inf_{g\in\mathcal{F}} \mathbb{E}_{\tilde{P}} l_g \geq \mathbb{E}[l(|f(x) - \tilde{y}|) - \min\{l(|\hat{y} - \tilde{y}|), \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\}]. \tag{D.15}$$

Consider the quantity inside the expectation, for $x = x_i$ with $y = 0$, $\tilde{y} = -1$, let $a = f(x_i) + 1, b = r_i - \epsilon/\alpha + 1$. Then by Lagrange's mean value theorem, there exists a c between a and b, such that this quantity can be written as

$$l(a) - l(b) = l'(c)(a-b) = l'(c)(f(x_i) - r_i + \epsilon/\alpha). \tag{D.16}$$

If $l(|f(x)-\tilde{y}|) - \min\{l(|\hat{y}-\tilde{y}|), \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\} < C\epsilon/\alpha$, then

$$f(x_i) - r_i < \frac{\epsilon}{\alpha}\frac{C-l'(c)}{l'(c)} < 0, \tag{D.17}$$

and we have $f(x_i) < r_i$ and $h(x_i) = 0 = y_i$. Similar arguments apply for $y = 1$. Thus,

$$\begin{aligned}
\mathbb{E}_P 1(h(x) \neq y) &\leq \tilde{P}[|f(x)-\tilde{y}|^p - \min\{|\hat{y}-\tilde{y}|^p, \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\} \geq C\epsilon/\alpha] && \text{(D.18)}\\
&\leq \frac{\alpha}{C\epsilon}\mathbb{E}_{\tilde{P}}[|f(x)-\tilde{y}|^p - \min\{|\hat{y}-\tilde{y}|^p, \hat{y} \in \{r(x) \pm \epsilon/\alpha\}\}] && \text{(D.19)}\\
&\leq \frac{\alpha}{C\epsilon}(\mathbb{E}_{\tilde{P}} l_f - \inf_{g\in\mathcal{F}} \mathbb{E}_{\tilde{P}} l_g) \leq \frac{\alpha}{C}. && \text{(D.20)}
\end{aligned}$$

This completes the proof of Proposition 15. □

With Proposition 14, Lemma 29 and Proposition 15, we can finally proceed to prove Theorem 20.

Proof of Theorem 20. To show the gate number lower bound, note that from Proposition 14, $\mathrm{Pdim}(\mathcal{F}^{\nu}_{G,A})$ is upper bounded by $128G\log_2(16eG) + 256G^2\log_2(16eGn)$ for variable circuit structures and by $128G\log_2(16eG)$ for fixed circuit structure. Meanwhile, from Lemma 29, we know that to approximate any ν-variable 1-bounded and 1-Lipschitz functions to ϵ error in $\|\cdot\|_\infty$, we must have $\mathrm{Pdim}(\mathcal{F}^{\nu}_{G,A}) \geq 1/(4\epsilon)^\nu$ and $\mathrm{fat}(\mathcal{F}^{\nu}_{G,A},\epsilon) \geq 1/(8\epsilon)^\nu$. Therefore, for variable circuit structures, we have

$$1/(4\epsilon)^\nu \leq \mathrm{Pdim}(\mathcal{F}^{\nu}_{G,A}) \leq 128G\log_2(16eG) + 256G^2\log_2(16eGn), \tag{D.21}$$

and thus $G \geq \tilde{\Omega}(1/(\epsilon)^{\nu/2})$. Similarly, for fixed circuit structure, we have $G \geq \tilde{\Omega}(1/\epsilon^\nu)$.

To show the sample complexity lower bound, note that from Proposition 15, we have the sample complexity $N \geq C\frac{\mathrm{fat}(\mathcal{F}^{\nu}_{G,A},\epsilon/\alpha)-1}{32\alpha}$. Setting $\alpha = 1/8$ and using the fat-shattering bound from Lemma 29, we arrive at $N \geq \Omega(1/\epsilon^\nu)$. □

Appendix E: Preliminary results on learning brickwork circuits

As stated in the outlook section, an interesting circuit structure is the brickwork circuit, which is generated by repeatedly applying the following two layers of gates (suppose n is even): (1) $U_{1,2}\otimes U_{3,4}\otimes\cdots\otimes U_{n-1,n}$ and (2) $U_{2,3}\otimes U_{4,5}\otimes\cdots\otimes U_{n-2,n-1}$, where $U_{i,j}$ denotes a 2-qubit unitary acting on the ith and jth qubit. Here we utilize the tools from unitary t-designs [120] to prove that the metric entropy of G-gate brickwork circuits is lower bounded by $\Omega(tn)$, if they can implement (approximate) unitary t-designs. Specifically, we have the following result.

Proposition 16 (Metric entropy lower bound of brickwork circuits)**.** *Let $U^{n,\mathrm{brick}}_G \subseteq U(2^n)$ be the set of n-qubit unitaries that can be implemented with G-gate brickwork circuits. Suppose that the uniform distribution over $U^{n,\mathrm{brick}}_G$ forms an ϵ-approximate t-design of $U(2^n)$ for some $\epsilon \in (0,1/2)$. Then we have*

$$\log\mathcal{M}(U^{n,\mathrm{brick}}_G, \mathrm{d}_{\mathrm{avg}}, \epsilon) \geq \Omega(tn). \tag{E.1}$$

Proof. Suppose $U^{n,\mathrm{brick}}_G$ with the uniform distribution forms an ϵ-approximate t-design $\mathcal{E}$ of $U(2^n)$. We begin by recalling a moment bound for approximate unitary designs.

Lemma 30 (Moment bound of approximate unitary designs, [28, proof of Lemma 1])**.** *Suppose $\mathcal{E}$ is an ϵ-approximate unitary t-design of $U(d)$. Then for any unitary $V \in U(d)$, we have*

$$\mathbb{E}_{U\sim\mathcal{E}}\left[|\operatorname{tr}\big(U^\dagger V\big)|^{2t}\right] \leq (1+\epsilon)t!\,. \tag{E.2}$$

Consequently, by Markov's inequality, we have the following lemma saying that a random element of a design is far apart from a fixed unitary with high probability.

Lemma 31. *(Design elements are far away from any fixed unitary). Suppose $\mathcal{E}$ is an ϵ-approximate unitary t-design of $U(d)$. Then for any unitary $V \in U(d)$, we have*

$$\mathbb{P}_{U\sim\mathcal{E}}\left[\|U-V\|_F^2 \leq 2d(1-\Delta)\right] \leq \mathbb{P}_{U\sim\mathcal{E}}\left[|\operatorname{tr}\big(U^\dagger V\big)| \geq d\Delta\right] \leq \frac{1+\epsilon}{\Delta^{2t}}\frac{t!}{d^{2t}}. \tag{E.3}$$

Proof. To prove this, we use the above moment bound and Markov's inequality:

$$\mathbb{P}_{U\sim\mathcal{E}}\left[|\operatorname{tr}(U^\dagger V)| \geq d\Delta\right] = \mathbb{P}_{U\sim\mathcal{E}}\left[|\operatorname{tr}(U^\dagger V)|^{2t} \geq d^{2t}\Delta^{2t}\right] \leq \frac{\mathbb{E}_{U\sim\mathcal{E}}\left[|\operatorname{tr}(U^\dagger V)|^{2t}\right]}{d^{2t}\Delta^{2t}} \leq \frac{1+\epsilon}{\Delta^{2t}}\frac{t!}{d^{2t}}. \tag{E.4}$$

Furthermore, since $\|U-V\|_F^2 = 2d - 2\mathrm{Re}[\operatorname{tr}(U^\dagger V)] \leq 2d(1-\Delta)$ implies $|\operatorname{tr}(U^\dagger V)| \geq \mathrm{Re}[\operatorname{tr}(U^\dagger V)] \geq d\Delta$, Lemma 31 follows. □

Now, we apply a probabilistic argument by randomly choosing M i.i.d. unitaries $U_1, \ldots, U_M$ from $\mathcal{E}$. The probability that any two of them are far away from each other is given by

$$\begin{aligned}
&\mathbb{P}_{U_1,\ldots,U_M\sim\mathcal{E}}[\forall 1 \leq i \neq j \leq M, \|U_i - U_j\|_F^2 \geq 2d(1-\Delta)] && \text{(E.5)}\\
&= 1 - \mathbb{P}_{U_1,\ldots,U_M\sim\mathcal{E}}[\exists 1 \leq i \neq j \leq M, \|U_i - U_j\|_F^2 \leq 2d(1-\Delta)] && \text{(E.6)}\\
&\geq 1 - \sum_{1\leq i\neq j\leq M} \mathbb{P}_{U_1,\ldots,U_M\sim\mathcal{E}}[\|U_i - U_j\|_F^2 \leq 2d(1-\Delta)] && \text{(E.7)}\\
&\geq 1 - \frac{M(M-1)}{2}\frac{1+\epsilon}{\Delta^{2t}}\frac{t!}{d^{2t}} && \text{(E.8)}\\
&\geq 1 - M^2\frac{1+\epsilon}{\Delta^{2t}}\frac{t!}{d^{2t}}, && \text{(E.9)}
\end{aligned}$$

where we have used the union bound in the first inequality and Lemma 31 in the last. Therefore, as long as we take $M < \sqrt{\left\lfloor \frac{\Delta^{2t}}{1+\epsilon}\frac{d^{2t}}{t!}\right\rfloor}$, we have

$$\mathbb{P}_{U_1,\ldots,U_M\sim\mathcal{E}}[\forall 1 \leq i \neq j \leq M, \|U_i - U_j\|_F^2 \geq 2d(1-\Delta)] > 0. \tag{E.10}$$

Hence there must be at least one instance $V_1, \ldots, V_M \in \mathcal{E}$ such that $\|V_i - V_j\|_F^2 \geq 2d(1-\Delta)$ for any pair V_i, V_j. These unitaries form a $\sqrt{2d(1-\Delta)}$-packing net of $U_G^{n,\mathrm{brick}}$ with respect to $\|\cdot\|_F$. Thus we have

$$\log\mathcal{M}(U_G^{n,\mathrm{brick}}, \|\cdot\|_F, \sqrt{2d(1-\Delta)}) \geq \Omega\left(\frac{1}{2}\log\left\lfloor\frac{\Delta^{2t}}{1+\epsilon}\frac{d^{2t}}{t!}\right\rfloor\right). \tag{E.11}$$

If we set $\sqrt{2d(1-\Delta)} = \sqrt{d}\epsilon$ (i.e., $\Delta = 1 - \epsilon^2/2$), we arrive at

$$\log\mathcal{M}(U_G^{n,\mathrm{brick}}, d_F, \epsilon) \geq \Omega(tn). \tag{E.12}$$

From the fact that quotienting out a global phase only changes the metric entropy by an additive $\Omega(\log(1/\epsilon))$ terms (Lemma 10) and the equivalence of d_F' and $\mathrm{d}_{\mathrm{avg}}$ (Lemma 4 Item 1), we arrive at the desired result. □

Learning pure quantum states (almost) without regret

Josep Lumbreras[1],[*] Mikhail Terekhov[2],[†] and Marco Tomamichel[1,3‡]

[1] *Centre for Quantum Technologies, National University of Singapore, Singapore*

[2] *School of Computer and Communication Sciences, EPFL, Switzerland and*

[3] *Department of Electrical and Computer Engineering,*
Faculty of Engineering, National University of Singapore, Singapore

(Dated: July 23, 2024)

We initiate the study of quantum state tomography with minimal regret. A learner has sequential oracle access to an unknown pure quantum state, and in each round selects a pure probe state. Regret is incurred if the unknown state is measured orthogonal to this probe, and the learner's goal is to minimise the expected cumulative regret over T rounds. The challenge is to find a balance between the most informative measurements and measurements incurring minimal regret. We show that the cumulative regret scales as $\Theta(\operatorname{polylog} T)$ using a new tomography algorithm based on a median of means least squares estimator. This algorithm employs measurements biased towards the unknown state and produces online estimates that are optimal (up to logarithmic terms) in the number of observed samples.

1. INTRODUCTION

Quantum state tomography is one of the most fundamental tasks in quantum learning, playing a critical role in the characterization and validation of quantum states. Given t copies of some unknown d-dimensional quantum state ρ, the goal of a quantum state tomography algorithm is to decide which measurements to perform on ρ and use classical post-processing with the outcomes of these measurements to produce an estimate $\hat{\rho}$ that is close to ρ in some distance metric. Two of the most relevant distances for this task are the trace distance and infidelity. The sample complexity of this problem (i.e., how many copies are sufficient to estimate ρ up to some precision on these distances) is well understood for both coherent measurements (allowing for joint measurements on multiple copies of the state) and incoherent measurements (only allowing measurements on single copies of the state) [9, 13, 23, 27].

For incoherent measurements, the most general algorithms are adaptive. Such algorithms can sequentially measure copies of ρ, deciding which measurement to perform based on the outcomes of the previous measurements. While adaptive algorithms are strictly more general than non-adaptive ones, it was early understood [4, 5, 11] that there is no separation in sample complexity when learning pure quantum states. Recently, it was shown in [9] that there is no separation in sample complexity between adaptive and non-adaptive algorithms for trace distance when learning both mixed and pure quantum states. The only regime where adaptive algorithms outperform non-adaptive ones is when learning "almost" pure quantum states [5, 15, 21]. For non-adaptive algorithms it was known that the rate $\Omega(1/\sqrt{t})$ is unavoidable [13]; however, in [9] they constructed an adaptive algorithm that achieves the rate $O(1/t)$ both for mixed and pure states.

[*] josep.lumbreras@u.nus.edu

[†] mikhail.terekhov@epfl.ch

[‡] marco.tomamichel@nus.edu.sg

In this work we take a different perspective on the adaptive incoherent setting of quantum state tomography, where we not only try to learn the state efficiently but also use measurements that only minimally disturb the state. Specifically, we have sequential access to an unknown pure quantum state $|\psi\rangle$ and at each round t we select a probe state $|\psi_t\rangle$ and perform a measurement in the direction of the probe state. The goal is to efficiently learn the unknown state while performing measurements that align well with the unknown state. Mathematically, this problem can be modelled as a bandit problem [17] since fundamentally we are interested in optimising an exploration–exploitation trade-off. The "exploration–exploitation" is one of the most fundamental concepts in reinforcement learning and decision-making captured by the bandit framework and the rigorous study was initiated almost one century ago in the early work by Thompson [26]. In our setting the exploration is related to the learning of the unknown state $|\psi\rangle$ through the selection of probes that are sufficiently informative, and the exploitation to performing measurements on the direction of $|\psi\rangle$.

Formally the measurements on the direction of the probe $|\psi_t\rangle$ are described by a two outcome rank-1 POVM $\{\Pi_t, \mathbb{I} - \Pi_t\}$ with corresponding outcomes $r_t \in \{1, 0\}$ and $\Pi_t = |\psi_t\rangle\langle\psi_t|$. In order to quantify the penalty that the learner suffers for selecting probes that are orthogonal to the unknown state we use as a figure of merit the regret, which is defined as

$$\mathrm{Regret}(T) = \sum_{t=1}^{T} 1 - \langle\psi|\Pi_t|\psi\rangle, \tag{1}$$

where $F(\Pi, \Pi_t) = \langle\psi|\Pi_t|\psi\rangle$ is the fidelity between the environment $\Pi = |\psi\rangle\langle\psi|$ and the selected probe $\Pi_t = |\psi_t\rangle\langle\psi_t|$ at time step $t \in [T]$. It is important to note that the regret is defined as the cumulative sum of infidelities $\gamma_t = 1 - \langle\psi|\Pi_t|\psi\rangle$, which means that there is a high penalty for measuring on directions orthogonal to the environment. The goal of the learners is to minimise the regret and we can frame this task as pure quantum state tomography with minimal regret since minimizing the individual contributions to the regret $1 - \langle\psi|\Pi_t|\psi\rangle$ implies finding Π_t close to Π in infidelity distance.

We note that the task of minimizing the regret (1) is captured by the multi-armed quantum bandit (MAQB) framework initiated in [6, 19], where some of the present authors consider the exploration–exploitation trade-off when learning properties of quantum states using classical algorithms. The work [19] considers a more general problem where the environment can be mixed or pure and the measurements are not only restricted to rank-1 projectors. They showed that for almost all cases the regret suffers a square root lower bound $\mathrm{Regret}(T) = \Omega(\sqrt{T})$ in a worst-case scenario. However, this bound does not apply to our case and the reason is due to the noise model of the outcomes given by Born's rule. For our particular model Born's rule gives that the outcomes become more deterministic as $|\psi_t\rangle$ gets close to $|\psi\rangle$ and the lower bounds considered in [20] rely on the fact that the variance of the outcomes r_t can not get arbitrary close to deterministic. Since our problem is closely related to the MAQB problem we name it pure state multi-armed quantum bandit (PSMAQB) and we use it to study the following questions at the intersection of the fields of quantum state tomography and linear stochastic bandits.

- **Question 1.** Can we perform single copy sample-optimal state tomography in infidelity and achieve at the same time sublinear regret? How much adaptiveness is needed for this task?

It is important to note that adaptiveness plays a huge role for algorithms that try to minimise the regret of the PSMAQB problem and peform sample-optimal state tomography. We could try to adapt one of the existing sample-optimal algorithms in the incoherent setting such as [12, 13, 16] for the PSMAQB problem but since all these algorithms use fixed basis or randomized measurements this will lead inevitably to the linear scaling $\mathrm{Regret}(T) = O(T)$ (we omit dimensional dependences). In [19] a simple algorithm with one round of adaptiveness was proposed for the PSMASQ problem that achieves $\mathrm{Regret}(T) = O(\sqrt{T})$ but gives the infidelity scaling $\gamma_t = O(1/\sqrt{T})$. Thus, it is interesting to see how adaptiveness can help in order to keep $\gamma_t = O(1/T)$ and at the same time achieve a sublinear regret.

For the qubit case we can relate the PSMAQB problem to a linear bandit with the action set being the unit sphere $\mathbb{S}^2 = \{x \in \mathbb{R}^3 : \|x\|_2 = 1\}$ and this motivates the following question that is related to fundamental bounds for linear stochastic bandits with continuous action sets.

- **Question 2.** Can we break the square root barrier of the regret for the PSMAQB problem?

In [19] it was shown that the MAQB problem can be reduced to a classical linear stochastic bandit problem [17, Chapter 19] and that we can adapt algorithms such as LinUCB [1, 10, 24] or linear Thompson sampling [2, 3] to achieve $\mathrm{Regret}(T) = \widetilde{O}(\sqrt{T})$, where we omit the dependency on the Hilbert space dimension. Classically, it is well known that linear bandits with smooth action sets such as the unit sphere have a lower bound of $\mathrm{Regret}(T) = \Omega(\sqrt{T})$ [24] [17, Chapter 24] and in particular if the unknown state is mixed the same bound applies to the quantum setting [19]. However, from [19] a lower bound for the PSMAQB problem is missing and this opens the possibility to achieve a better scaling than the $\sqrt{T}$ given by the standard classical bandit algorithms. Achieving a better scaling on the time horizon T for the PSMAQB would imply the first non-trivial linear stochastic bandit with continuous action sets that breaks the square root barrier. Breaking the square root barrier will require new algorithms and techniques that take advantage of the extra structure of the PSMAQB problem.

2. RESULTS AND TECHNICAL CONTRIBUTION

In this work, we provide affirmative answers at the same time to Questions 1 and 2 through the following Theorem.

Theorem 1 (informal)**.** *Given a PSMAQB with an unknown qubit environment $\Pi = |\psi\rangle\langle\psi|$, we can find an algorithm that achieves*

$$\mathbb{E}\left[\mathrm{Regret}(T)\right] = O\big(\log^2(T)\big). \tag{2}$$

Also, at each time step $t \in [T]$, this strategy outputs an estimator Π_t of Π with infidelity scaling

$$\mathbb{E}\left[1 - F\left(\Pi, \Pi_t\right)\right] = \widetilde{O}\left(\frac{1}{t}\right). \tag{3}$$

The above results also hold with high probability.

The proof of Theorem 1 is constructive which means that we design a qubit quantum state tomography algorithm and perform the theoretical analysis for it. The exact algorithm and Theorem can be found in Sections 4 and 5. We note that our algorithm is almost fully adaptive since it uses $O(T/\log(T))$ rounds of adaptiveness. Intuitively, our algorithm needs to be almost fully adaptive because keeping the scaling $1 - F(\Pi, \Pi_t) = O(1/t)$ and breaking the square root regret barrier implies that we want to update our measurements Π_t at each round to get as close as possible to Π. We say that our algorithm is "online" because it is able to output at each time step $t \in [T]$ an estimator with the almost optimal infidelity scaling (3). We provide numerical experiments in Section 5. Now we sketch the main idea of how our algorithm updates the measurements.

1. **Estimation.** At each time step $t \in [T]$ we use the past information of measurements $\Pi_{a_1}, ..., \Pi_{a_{t-1}}$ and associated outcomes $r_1, ..., r_{t-1} \in \{0,1\}^{\otimes t-1}$ to build a high probability confidence region $\mathcal{C}_t$ for the unknown environment $|\psi\rangle$.

2. **Exploration-exploitation.** A batch of measurements is performed, given by the directions of maximum uncertainty of $\mathcal{C}_t$ such that they give enough information to construct $\mathcal{C}_{t+1}$ (exploration) and also minimise the regret (1) (exploitation).

For the estimation part, we work with the Bloch sphere representation of the unknown state $\Pi = |\psi\rangle\langle\psi| = \frac{I+\theta\cdot\sigma}{2}$ where $\theta \in \mathbb{S}^2$ and for σ we can take the standard Pauli Basis i.e $\sigma = (\sigma_x, \sigma_y, \sigma_z)$. For each action Π_{a_t}, our algorithm performs k independent measurements using the same action, and it builds the following k online weighted least squares estimators of θ,

$$\widetilde{\theta}_{t,i} = V_t^{-1} \sum_{s=1}^{t} \frac{1}{\hat{\sigma}_s^2(a_s)} r_{s,i} a_s \quad \text{for } i \in [k], \tag{4}$$

where $r_{s,i} \in \{0,1\}$ is the outcome of the measurement (up to some renormalization) using the projector Π_{a_s} with Bloch vector $a_s \in \mathbb{S}^2$, $V_t = \mathbb{I} + \sum_{s=1}^{t} \frac{1}{\hat{\sigma}_s^2(a_s)} a_s a_s^{\mathsf{T}}$ is the design matrix and $\hat{\sigma}_s^2(a_s)$ is a variance estimator of the real variance associated to the outcome r_s. The key point where we take advantage from the structure of the PSMAQB problem is that the variance of the outcome r_a associated to the action Π_a can be bounded as $\mathbb{V}[r_a] \leq 1 - \mathrm{Tr}(\Pi\Pi_a)$. The idea is that through a careful choice of actions we can make the terms $1/\hat{\sigma}_s^2(a_s)$ arbitrarily large and "boost" the confidence on the directions a_s in the estimators (4) that are close to θ. However, this comes at a price, and is that in order to get good concentration bounds for our estimator we need to deal with unbounded random variables and finite variance. We address this issue using the new ideas of median of means (MoM) for online least squares estimators introduced in [7, 22, 25]. The construction takes inspiration from the old method of median of means [18, Chapter 3] for real random variables with unbounded support and bounded variance but requires non-trivial adaptation for online linear least squares estimators. Similarly to the real case we use the k independent estimators (4) in order to construct the MoM estimator $\widetilde{\theta}_t^{\text{wMoM}}$ such that we can build a confidence region with concentration bounds scaling as $1 - \exp(-k)$. We give the exact construction in Section 4.1.

For the exploration-exploitation part, we take the ideas that we develop in [20]. We give the precise action choice in Section 4.2, and here we sketch the main points. We take inspiration from the optimistic principle for bandit algorithms which in short tells us to choose the most rewarding actions with the available information. In order to use this idea, we use the confidence region that we build in the estimation part and we select measurements that align with the (unknown) direction of Π. See Figure 1. Our algorithm also achieves the relation $1 - F(\Pi, \Pi_{a_t}) = O\left(1/\lambda_{\min}(V_t)\right)$, where $\lambda_{\min}(V_t)$ quantifies the direction of maximum uncertainty (exploration) of our estimator. The maximum eigenvalue $\lambda_{\max}(V_t)$ quantifies the amount of exploitation. We can relate these two concepts through the Theorem we formally state and prove in [20, Theorem 3], which states that for our particular action selection choice we have $\lambda_{\min}(V_t) = \Omega(\sqrt{\lambda_{\max}(V_t)})$. Using this relation and a careful analysis, we can show that $\lambda_{\max}(V_t) = \Omega(t^2)$ which gives $\lambda_{\min}(V_t) = \Omega(t)$ and the scaling $1 - F(\Pi, \Pi_{a_t}) = O(1/t)$. We emphasize that the key point that allows to achieve the rate $\lambda_{\min}(V_t) = \Omega(t)$ is the fact that the variance estimators $\hat{\sigma}_s^2$ can get as close as possible to zero since the variance of the rewards of the PSMAQB problems goes to zero if we select measurements close to Π. To check the optimality of the regret, we derive a minimax expected regret lower bound based on the optimal quantum state tomography for pure state results in [14]. The proof does not follow directly from [14], and we have to adapt it to the bandit setting.

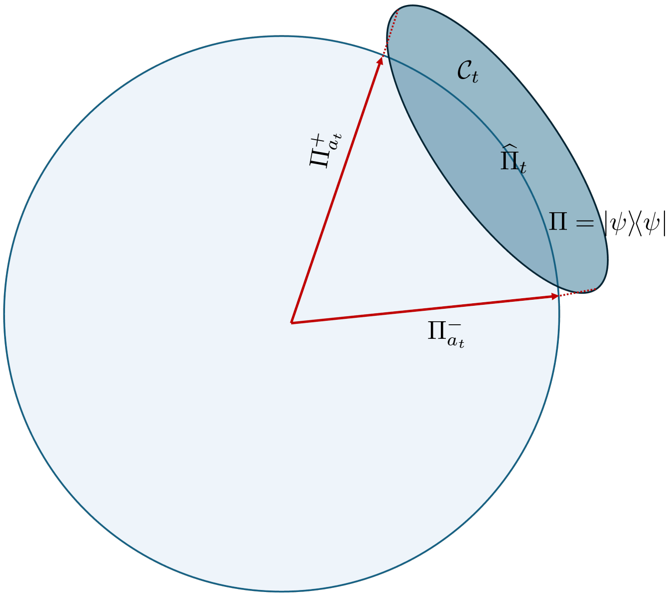


FIG. 1. The algorithm at each time step outputs an estimator $\widehat{\Pi}_t$ and builds a high-probability confidence region $\mathcal{C}_t$ (shaded region) around the unknown state $\Pi = |\psi\rangle\langle\psi|$ on the Bloch sphere representation. Then uses the optimistic principle to select projectors $\Pi_{a_t}^{\pm}$ that are close the unknown state Π projecting into the Bloch sphere the extreme points of the largest principal axis of $\mathcal{C}_t$. This particular choice allows optimal learning of Π (exploration) and simultaneously minimizes the regret (exploitation).

Theorem 2 (informal)**.** *Given a PSMAQB with a qubit environment, the cumulative expected regret for any strategy is bounded by*

$$\mathbb{E}\left[\mathrm{Regret}(T)\right] = \Omega(\log T), \tag{5}$$

where the expectation is taken over the probability distribution of rewards and actions induced by the learner strategy and also uniformly over the set of pure state environments.

This result is formally derived in Section 6. There it is also generalized to the d-dimensional PSMAQB, in which case the bound is given by $\mathbb{E}\left[\mathrm{Regret}(T)\right] = \Omega(d\log(T/d))$. The proof relies on the fact that individual actions of a strategy at time $t \in [T]$ can be viewed as quantum state tomographies using t copies of the state. A relation between the fidelity of these tomographies and the regret of the strategy allows us to convert the fidelity upper bound from [14] to a regret lower bound. We use measure-theoretic tools to adapt the proof from [14] to a more general case where the tomography can output an arbitrary distribution of states. We remark that this is a noteworthy result since in [20] they argue how regret lower bound techniques for classical linear bandits fail for noise models with vanishing variance.

3. THE MODEL

In this section first we formally state the PSMAQB problem and make a connection with a linear stochastic bandit problem. Then we define a slightly more general model where the key feature is that the variance of the rewards vanishes with the same behaviour as the PSMAQB problem.

3.1. Notation

First, we introduce some basic notation and conventions. Let $[t] = \{1, 2, ..., t\}$ for $t \in \mathbb{N}$. For real vectors $x, y \in \mathbb{R}^d$ we denote their inner product as $\langle x, y \rangle = x_1 y_1 + ... + x_d y_d$. Given a real vector $x \in \mathbb{R}^d$ we denote the 2-norm as $\|x\|_2$ and for a real semi-positive definite matrix $A \in \mathbb{R}^{d\times d}$, $A \geq 0$ the weighted norm with A as $\|x\|_A^2 = \langle x, Ax \rangle$. The set corresponding to the surface of the unit sphere is $\mathbb{S}^{d-1} = \{x \in \mathbb{R}^d : \|x\|_2 = 1\}$. For a real symmetric matrix $A \in \mathbb{R}^{d\times d}$ we denote $\lambda_{\max}(A)$, $\lambda_{\min}(A)$ its maximum and minimum eigenvalues respectively. We use the ordering $\lambda_{\min}(A) \leq \lambda_2(A), ..., \lambda_{d-1}(A) \leq \lambda_{\max}(A)$ for the i-th $\lambda_i(A)$ eigenvalue in increasing order. For a random variable X (discrete or continuous) we denote $\mathbb{E}[X]$ and $\mathbb{V}[X]$ its expectation value and variance respectively. A random variable X is *σ-subgaussian* if $\forall \lambda \in \mathbb{R}, \mathbb{E}\left[\exp(\lambda X)\right] \leq \exp\left(\lambda^2\sigma^2/2\right)$.

Let $\mathcal{S}_d = \{\rho \in \mathbb{C}^{d\times d} : \mathrm{Tr}(\rho) = 1, \rho \geq 0\}$ be the set of *quantum states* in a d-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$ and $\mathcal{S}_d^* = \{\rho \in \mathcal{S}_d : \rho^2 = \rho\}$ the set of *pure states* or rank-1 projectors. We will use the parametrization given in [8] of a d-dimensional quantum state $\rho_\theta \in \mathcal{S}_d$,

$$\rho_\theta = \frac{\mathbb{I}}{d} + \left(\sqrt{\frac{d(d-1)}{2d^2}}\right)\theta \cdot \sigma \tag{6}$$

where $\theta \in \mathbb{R}^{d^2-1}$, and $\sigma = (\sigma_1, ..., \sigma_{d^2-1})$ is a vector of orthogonal, traceless, Hermitian matrices with the normalization condition $\mathrm{Tr}(\sigma_i\sigma_j) = 2\delta_{i,j}$. We will use the subscript θ in the quantum state ρ_θ in order to denote the vector of the parametrization (6). In particular the normalization is taken such that $\|\theta\|_2^2 \leq 1$ with equality if ρ_θ is pure. Note that the parametrization enforces $\rho_\theta^\dagger = \rho_\theta$ and $\mathrm{Tr}(\rho_\theta) = 1$. Also there are some extra conditions on the vector θ regarding the positivity of the density matrix ρ_θ but we will not use them. For two quantum states $\rho, \sigma \in \mathcal{S}_d$ the fidelity is $F(\rho, \sigma) = \left(\mathrm{Tr}(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}})\right)^2$ and the infidelity $1 - F(\rho, \sigma)$. For a Hilbert space $\mathcal{H}$, the set of linear operators on it will be denoted by $\mathrm{End}(\mathcal{H})$. The joint state of a system consisting of n copies of a pure state $\Pi_\theta \in \mathcal{S}_d^*$ is given by the n-th tensor power $\Pi_\theta^{\otimes n} \in \mathrm{End}(\mathcal{H}^{\otimes n})$. Using Dirac notation, we can express $\Pi_\theta = |\psi_\theta\rangle\langle\psi_\theta|$ for some normalized $|\psi_\theta\rangle \in \mathcal{H}$. Then, the span of all n-copy states of the form $|\psi_\theta\rangle^{\otimes n}$ is called the symmetric subspace of $\mathcal{H}^{\otimes n}$, denoted by $\mathcal{H}_+^{\otimes n}$. Its dimension is $D_n = \binom{n+d-1}{d}$. The symmetrization operator $\Pi_n^+ \in \mathrm{End}(\mathcal{H}^{\otimes n})$ is the projector onto $\mathcal{H}_+^{\otimes n}$.

3.2. Multi-armed quantum bandit for pure states

The model that we are interested in is the general multi-armed quantum bandit model described in [19][Section 2.3] with the action set being all rank-1 projectors and with pure state environments. For completeness, we state the basic definitions for this particular case.

Definition 3. *Let $d \in \mathbb{N}$. A d-dimensional pure state multi-armed quantum bandit (PSMAQB) is given by a measurable space $(\mathcal{A}, \Sigma)$, where $\mathcal{A} = \mathcal{S}_d^*$ is the action set and Σ is a σ-algebra of subsets of $\mathcal{A}$. The bandit is in an environment, a quantum state $\Pi_\theta \in \mathcal{S}_d^*$, that is unknown.*

The interaction with the PSMAQB is done by a learner that interacts sequentially over $t \in [T]$ rounds with the unknown environment $\Pi_\theta \in \mathcal{S}_d^*$. At each time step $t \in [T]$:

1. The learner selects an action $\Pi_{a_t} \in \mathcal{A}$.

2. Performs a measurement on the unknown environment Π_θ using the two-outcome POVM

$\{\Pi_{a_t}, I_{d\times d} - \Pi_{a_t}\}$ and receives a reward $r_t \in \{0,1\}$ sampled according to the Born's rule, i.e

$$\Pr_{\Pi_\theta}(r_t|\Pi_{a_t}) = \begin{cases} \mathrm{Tr}(\Pi_\theta \Pi_{a_t}) & r_t = 1, \\ 1 - \mathrm{Tr}(\Pi_\theta \Pi_{a_t}) \quad \text{if} & r_t = 0, \\ 0 \quad \text{else.} \end{cases} \tag{7}$$

We note that the reward at time step t after selecting $\Pi_{a_t} \in \mathcal{A}$ can be written as

$$r_t = \mathrm{Tr}(\Pi_\theta \Pi_{a_t}) + \epsilon_t, \tag{8}$$

where ϵ_t is a Bernoulli random variable with values $\epsilon_t \in \{1 - \mathrm{Tr}(\Pi_\theta \Pi_{a_t}), -\mathrm{Tr}(\Pi_\theta \Pi_{a_t})\}$ such that

$$\mathbb{E}\left[\epsilon_t|\mathcal{F}_{t-1}\right] = 0, \quad \mathbb{V}\left[\epsilon_t|\mathcal{F}_{t-1}\right] = \mathrm{Tr}(\Pi_\theta \Pi_{a_t})\left(1 - \mathrm{Tr}(\Pi_\theta \Pi_{a_t})\right), \tag{9}$$

where $\mathcal{F}_{t-1} := \{r_1, \Pi_{a_1}, ..., r_{t-1}, \Pi_{a_{t-1}}, \Pi_t\}$ is a σ-filtration.

Formally the learner is described by a policy.

Definition 4. *A policy π is a set of conditional probability measures $\{\pi_t\}_{t\in\mathbb{N}}$ on the action set $\mathcal{A}$ of the form*

$$\pi_t(\cdot|r_1, \Pi_{a_1}, ..., r_{t-1}, \Pi_{a_{t-1}}) : \Sigma \to [0,1]. \tag{10}$$

Then the policy interacting with the environment Π_θ defines the probability measure over the set of actions and rewards $P_{\Pi_\theta,\Pi} : (\Sigma \times \{0,1\})^{\times T} \to [0,1]$ as

$$\int \cdots \int \Pr_{\Pi_\theta}(r_T|\Pi_{a_T})\, \pi_T(d\Pi_T|r_1, \Pi_{a_1}, ..., r_{T-1}, \Pi_{a_{T-1}}) \cdots \Pr_{\Pi_\theta}(r_1|\Pi_{a_1})\, \pi_1(d\Pi_{a_1}), \tag{11}$$

where the integrals are taken with respect to the corresponding subsets of actions.

The goal of the learner is to maximize the cumulative expected reward. This is quantified by the notion of regret that serves to compare with the best possible choice of action.

Definition 5. *Given a d-dimensional pure state multi-armed quantum bandit, a policy π and $T \in \mathbb{N}$, the cumulative regret is defined as*

$$\mathrm{Regret}(T, \pi, \Pi_\theta) := \sum_{t=1}^{T} 1 - \mathrm{Tr}(\Pi_\theta \Pi_{a_t}). \tag{12}$$

We note that since the quantity $\max_{\Pi\in\mathcal{A}} \mathrm{Tr}(\Pi_\theta \Pi)$ is maximized by $\Pi = \Pi_\theta$, then $1 = \max_{\Pi\in\mathcal{A}} \mathrm{Tr}(\Pi_\theta \Pi)$ is the maximal expected reward and the above definition quantifies how close is the chosen action to the unknown Π_θ. Moreover, expressing $\Pi_\theta = |\psi_\theta\rangle\langle\psi_\theta|$, $\Pi_{a_t} = |\psi_{a_t}\rangle\langle\psi_{a_t}|$ for normalized complex vectors $|\psi_\theta\rangle, |\psi_{a_t}\rangle \in \mathbb{C}^d$ we have

$$\mathrm{Regret}(T, \pi, \Pi_\theta) = \sum_{t=1}^{T} 1 - F(\Pi_\theta, \Pi_{a_t}) = \sum_{t=1}^{T} 1 - |\langle\psi_\theta|\psi_{a_t}\rangle|^2, \tag{13}$$

and the term $1 - |\langle\psi_\theta|\psi_{a_t}\rangle|^2$ is the infidelity between the pure quantum states $|\psi_\theta\rangle$ and $|\psi_{a_t}\rangle$.

The goal of the learner is to minimize the *expected cumulative regret* that is simply defined as $\mathbb{E}_{\Pi_\theta}[\mathrm{Regret}(T, \pi, \Pi_\theta)]$ where the expectation $\mathbb{E}_{\Pi_\theta}$ is taken over the probability measure (11). When the context is clear, we will use the notation $\mathrm{Regret}(T)$. We refer to the PSMAQB problem as the task of finding a policy that minimizes the expected regret $\mathbb{E}_{\Pi_\theta}[\mathrm{Regret}(T, \pi, \Pi_\theta)]$. Minimizing the regret means achieving sublinear regret on T since $\mathrm{Regret}(T) \le T$ holds for any policy.

3.3. Classical model

In order to study the PSMAQB it is helpful to study it using the linear stochastic bandit framework. The idea will be to express the actions and unknown quantum states as real vectors using the parametrization (6).

In the linear stochastic bandit model, the action set is a subset of real vectors i.e $\mathcal{A} \subseteq \mathbb{R}^d$, and the reward at time step $t \in [T]$ after selecting action $a_t \in \mathcal{A}$ is given by

$$r_t = \langle a_t, \theta \rangle + \epsilon_t \tag{14}$$

where $\theta \in \mathbb{R}^d$ is the unknown parameter and ϵ_t is some bounded $\sigma-$subgaussian noise that in general can depend on θ and a_t. The regret for this model is given by

$$\text{Regret}_{cl}(T, \pi, \theta) := \sum_{t=1}^{T} \max_{a \in \mathcal{A}} \langle \theta, a \rangle - \langle \theta, a_t \rangle, \tag{15}$$

where the policy π is defined analogously to Definition 4. We used the subscript *cl* to differentiate between quantum and classical model.

In order to express the PSMAQB model as a linear stochastic bandit we can use the parametrization (6) and express the expected reward for action $\Pi_{a_t} \in \mathcal{S}_d^*$ as

$$\text{Tr}(\Pi_{a_t}\Pi_\theta) = \frac{1}{d}\left(1 + (d-1)\langle a_t, \theta \rangle\right). \tag{16}$$

Inverting the above expression we have

$$\langle a_t, \theta \rangle = \frac{d\,\text{Tr}(\Pi_\theta \Pi_{a_t}) - 1}{d-1}. \tag{17}$$

Let's quickly revisit the regret expression and use the above identities in order to connect the quantum and classical versions of the regret. We denote $\Pi_{a^*} = \text{argmax}_{\Pi \in \mathcal{A}} \text{Tr}(\Pi\Pi_\theta)$ the optimal action and recall that $1 = \text{Tr}(\Pi_{a^*}\Pi_\theta)$. Then we have

$$\text{Regret}(T, \pi, \Pi_\theta) = \sum_{t=1}^{T} \text{Tr}(\Pi_{a^*}\Pi_\theta) - \text{Tr}(\Pi_{a_t}\Pi_\theta) = \frac{d-1}{d}\sum_{t=1}^{T}\langle \theta, a^* - a_t \rangle. \tag{18}$$

Note that by the normalization (6) we have that for ρ_θ and Π_{a_t} the corresponding real vecotrs are normalized $\|\theta\|_2 = \|a_t\| = 1$. Thus, since $a^* = \theta$ the regret can be written as

$$\text{Regret}(T, \pi, \Pi_\theta) = \frac{d-1}{d}\sum_{t=1}^{T}\left(1 - \langle \theta, a_t \rangle\right) = \frac{d-1}{2d}\sum_{t=1}^{T}\|\theta - a_t\|_2^2. \tag{19}$$

Now we want to formulate a classical bandit such that the environment and actions are given by the real vectors that parameterize the quantum states (6). In order to have an expected linear reward that is linear with respect to θ and a_t it is sufficient to define a renormalized reward as

$$\tilde{r}_t = \frac{dr_t - 1}{d-1} \in \left\{1, \frac{-1}{d-1}\right\}, \tag{20}$$

where we used the reward of the quantum model $r_t \in \{0, 1\}$ given by 7. Using $\mathbb{E}[r_t|\mathcal{F}_{t-1}] = \text{Tr}(\Pi_{a_t}\rho_\theta)$ and (16) it is easy to see that

$$\mathbb{E}[\tilde{r}_t|\mathcal{F}_{t-1}] = \langle \theta, a_t \rangle, \tag{21}$$

where naturally we use $\mathcal{F}_{t-1} = \{\tilde{r}_1, a_1, ..., \tilde{r}_{t-1}, a_{t-1}, a_t\}$. Thus, we can write the reward in the form (14)

$$\tilde{r_t} = \langle\theta, a_t\rangle + \epsilon_t, \quad \mathbb{E}[\epsilon_t|\mathcal{F}_{t-1}] = 0, \quad \mathbb{V}[\epsilon_t|\mathcal{F}_{t-1}] = (1 - \langle\theta, a_t\rangle)\left(1 + (d-1)\langle\theta, a_t\rangle\right), \tag{22}$$

where the expectation and variance follow from a direct calculation. Then we can study a d-dimensional PSMAQB as a linear stochastic bandit choosing the action set

$$\mathcal{A}_d^{\text{quantum}} := \{a \in \mathbb{R}^{d^2-1} : \Pi_a \in \mathcal{S}_d^*\} \tag{23}$$

with unknown parameter $\theta \in \mathbb{R}^{d^2-1}$ such that $\Pi_\theta \in \mathcal{S}_d^*$. The regret of this linear model is given by $\text{Regret}_{cl} = \frac{1}{2}\sum_{t=1}^{T} \|\theta - a_t\|_2^2$ and we have the following relation with the quantum model:

$$\text{Regret}(T, \pi, \Pi_\theta) = \frac{d-1}{d}\text{Regret}_{cl}(T, \pi, \theta), \tag{24}$$

where we take the same strategy π in both sides since we can identify the actions of both bandits through the parametrization (6) and the relation between rewards given by (20). When the context is clear we will simply use Regret(T) for both quantum and classical model.

3.4. Linear bandit with linearly vanishing variance noise

In [20] some of the present authors introduced the framework of stochastic linear bandits with linear vanishing noise where the setting is a linear bandit with action set $\mathcal{A} = \mathbb{S}^d$, unknown parameter $\theta \in \mathbb{S}^d$ and reward $r_t = \langle\theta, a_t\rangle + \epsilon_t$ such that ϵ_t is σ_t-subgaussian with $\mathbb{E}[\epsilon_t|\mathcal{F}_{t-1}] = 0$ and the property of vanishing noise $\sigma_t^2 \leq 1 - \langle\theta, a_t\rangle^2$. In order to study a PSMAQB we will relax the condition on the subgaussian noise and we will replace it by the following condition on the noise

$$\mathbb{E}\left[\epsilon_t|\mathcal{F}_{t-1}\right] = 0, \quad \mathbb{V}\left[\epsilon_t|\mathcal{F}_{t-1}\right] \leq 1 - \langle\theta, a_t\rangle^2. \tag{25}$$

As in the classical model of the previous section using that $\max_{a\in\mathcal{A}}\langle\theta, a\rangle = 1$ we have that the regret is given by

$$\text{Regret}(T) = \sum_{t=1}^{T} 1 - \langle\theta, a_t\rangle = \frac{1}{2}\sum_{t=1}^{T} \|\theta - a_t\|_2^2. \tag{26}$$

We note that finding an strategy that minimizes regret for the above model will also work for a $d = 2$ PSMAQB with unknown $\Pi_\theta \in \mathcal{S}_2^*$ using the relations of last sections since

$$\mathcal{A}_2^{\text{quantum}} = \{a \in \mathbb{R}^3 : \|a\|_2 = 1\} = \mathbb{S}^2, \tag{27}$$

and the variance of the PSMAQB (22) fullfills the relation (25).

4. ALGORITHM FOR BANDITS WITH LINEARLY VANISHING VARIANCE NOISE

In this Section we are going to present an algorithm for the linear bandit model explained in Section 3.4 that is based on the algorithm LINUCB-VN studied in [20] for linear bandits with linearly vanishing noise. Later we will show how to use this algorithm for the qubit PSMAQB problem.

4.1. Median of means for an online least squares estimator

First we discuss the medians of means method for the online linear least squares estimator introduced in [25]. We are going to use this estimator later in order to design a strategy that minimizes the regret for the model introduced in Section 3.4. The reason we need this estimator is that in the analysis of our algorithm we need concentration bounds for linear least squares estimators where the random variables have bounded variance and a possibly unbounded subgaussian parameter. The condition of bounded variance is weaker than the usual assumption of bounded subgaussian noise, however we can recover similar concentration bounds of the estimator if we implement a median of means.

In order to build the median of means online least squares estimator for linear bandits we need to sample k independent rewards for each action. Specifically given an action set $\mathcal{A} \subset \mathbb{R}^d$, an unknown parameter $\theta \in \mathbb{R}^d$, at each time step t we select an action $a_t \in \mathcal{A}$ and sample k independent rewards using a_t where the outcome rewards are distributed as

$$r_{t,i} = \langle \theta, a_t \rangle + \epsilon_{t,i} \quad \text{for } i \in [k], \tag{28}$$

for some noise such that $\mathbb{E}[\epsilon_{t,i}|\mathcal{F}_{t-1}] = 0$. We refer to k as the number of subsamples per time step. Then at time step t we define k least squares estimators as

$$\widetilde{\theta}_{t,i} = V_t^{-1} \sum_{s=1}^{t} r_{s,i} a_s \quad \text{for } i \in [k], \tag{29}$$

where V_t is the design matrix defined as

$$V_t = \lambda \mathbb{I} + \sum_{s=1}^{t} a_s a_s^{\mathsf{T}}, \tag{30}$$

with $\lambda > 0$ being a parameter that ensures invertibility of V_t. We note that the design matrix is independent of i. Then the median of means for least squares estimator (MOMLSE) is defined as

$$\widetilde{\theta}_t^{\text{MoM}} := \tilde{\theta}_{t,k^*} \quad \text{where } k^* = \operatorname*{argmin}_{j \in [k]} y_j, \tag{31}$$

where

$$y_j = \text{median}\{\|\tilde{\theta}_{t,j} - \tilde{\theta}_{t,i}\|_{V_t} : i \in [k]/j\} \quad \text{for } j \in [k]. \tag{32}$$

Using the results in [25] we have that the above estimator has the following concentration property around the true estimator.

Lemma 6 (Lemma 2 and 3 in [25])**.** *Let* $\widetilde{\theta}_t^{\text{MoM}}$ *be the MOMLSE defined* (31) *in with k subsamples with* $\{r_{s,i}\}_{(s,i)\in[t]\times[k]}$ *rewards and corresponding actions* $\{a_s\}_{s\in[t]}$*. Assume that the noise of all rewards has bounded variance, i.e* $\mathbb{E}\left[\epsilon_{s,i}^2|\mathcal{F}_{t-1}\right] \leq 1$ *for all* $s \in [t]$ *and* $i \in [k]$*. Then we have*

$$\Pr\left(\|\theta - \widetilde{\theta}_t^{MoM}\|_{V_t}^2 \leq 9\left(\sqrt{9d} + \lambda\|\theta\|_2\right)^2\right) \geq 1 - \exp\left(\frac{-k}{24}\right). \tag{33}$$

We will use a slight modification of the above result with a weighted least squares estimator like the one used in [20]. The weights will be related to a variance estimator of the noise for action $a \in \mathcal{A}$ that at each time step t can be generally defined as

$$\hat{\sigma}_t^2 : \mathcal{H}_{t-1} \times A \to \mathbb{R}_{>0}, \tag{34}$$

where $\mathcal{H}_{t-1} = \{r_{s,i}\}_{(s,i)\in[t-1]\times[k]} \cup \{a_s\}_{s\in[t-1]}$ contains the past information of rewards and actions played. For our purposes we will use only the information of the past actions and in order to simplify notation we will use $\hat{\sigma}_t^2(a)$ to denote an estimator of the variance for the reward associated action $a \in \mathcal{A}$ with the information collected up to time step $t-1$. Then the corresponding weighted versions with k subsamples are defined as

$$\widetilde{\theta}_{t,i} = V_t^{-1} \sum_{s=1}^{t} \frac{1}{\hat{\sigma}_s^2(a_s)} r_{s,i} a_s \quad \text{for } i \in [k], \tag{35}$$

with the weighted design matrix

$$V_t = \lambda \mathbb{I} + \sum_{s=1}^{t} \frac{1}{\hat{\sigma}_s^2(a_s)} a_s a_s^{\mathsf{T}}. \tag{36}$$

Then the weighted version of the median of means linear estimator is defined analogously to (31) with the corresponding weighted versions (35)(36) and we will denote it as $\widetilde{\theta}_t^{\mathrm{wMOM}}$. In our algorithm analysis we will use the following analogous concentration bound under the condition that the estimators $\hat{\sigma}_t^2$ overestimate the true variance.

Corollary 7. *Let $\widetilde{\theta}_t^{\mathrm{wMOM}}$ be the weighted version of the MOMLSE with k subsamples, $\{r_{s,i}\}_{(s,i)\in[t]\times[k]}$ rewards with corresponding actions $\{a_s\}_{s\in[t]}$ and variance estimator $\hat{\sigma}_t^2$. Define the following event*

$$G_t := \{(\mathcal{H}_{t-1}, a_t) : \mathbb{V}[\epsilon_{s,i}] \leq \hat{\sigma}^2(a_s) \forall s, i \in [t] \times [k]\}. \tag{37}$$

Then we have

$$\Pr\left(\|\theta - \widetilde{\theta}_t^{\mathrm{wMOM}}\|_{V_t}^2 \leq \beta \mid G_t\right) \geq 1 - \exp\left(\frac{-k}{24}\right), \tag{38}$$

where

$$\beta := 9\left(\sqrt{9d} + \lambda\|\theta\|_2\right)^2. \tag{39}$$

Proof. The result follows from applying Lemma 6 to the sequences of re-normalized rewards $\{\frac{r_{s,i}}{\hat{\sigma}_s(a_s)}\}_{(s,i)\in[t]\times[k]}$ and actions $\{\frac{a_{s,i}}{\hat{\sigma}_s(a_s)}\}_{s\in[t]}$. We only need to check that the sequence $\{\frac{\epsilon_{s,i}}{\hat{\sigma}_s(a_s)}\}_{(s,i)\in[t]\times[k]}$ has finite variance. Conditioning with the event G_t and the fact that by definition $\hat{\sigma}_s^2(a_s)$ only depend on the past $s-1$ action and rewards we have that the re-normalized noise has bounded variance since

$$\mathbb{E}\left[\left(\frac{\epsilon_{s,i}}{\hat{\sigma}_s(a_s)}\right)^2 \middle| \mathcal{F}_{t-1}\right] = \frac{1}{\hat{\sigma}_s^2(a_s)} \mathbb{E}[\epsilon_{s,i}^2 | \mathcal{F}_{t-1}] = \frac{\mathbb{V}[\epsilon_{s,i}]}{\hat{\sigma}_s^2(a_s)} \leq 1. \tag{40}$$

□

4.2. Algorithm

The algorithm that we design for linear bandits with linearly variance vanishing noise is LinUCB-VVN (LinUCB vanishing variance noise) stated in Algorithm 1. The algorithm runs in batches of $2(d-1)$ actions selected as

$$a_{t,i}^{\pm} := \frac{\widetilde{a}_{t,i}^{\pm}}{\|\widetilde{a}_{t,i}^{\pm}\|_2}, \quad \widetilde{a}_{t,i}^{\pm} = \theta_t^{\mathrm{wMoM}} \pm \frac{1}{\sqrt{\lambda_{\min}(V_{t-1})}}, \quad \theta_t^{\mathrm{wMoM}} := \frac{\widetilde{\theta}_t^{\mathrm{wMoM}}}{\|\widetilde{\theta}_t^{\mathrm{wMoM}}\|_2}, \tag{41}$$

for $i \in [d-1]$ and where for each action $a^{\pm}_{t,i}$ we sample $k \geq 1$ independent rewards in order to build the weighted MOMLSE defined as in Section 4.1. The design matrix V_t is updated as

$$V_t = V_{t-1} + \omega(V_{t-1}) \sum_{i=1}^{d-1} \left(a^{+}_{t,i}(a^{+}_{t,i})^{\mathsf{T}} + a^{-}_{t,i}(a^{-}_{t,i})^{\mathsf{T}} \right) \tag{42}$$

where the weights ω and variance estimator are chosen as

$$\omega(V_{t-1}) := \frac{\sqrt{\lambda_{\max}(V_{t-1})}}{12\sqrt{d-1}\beta}, \quad \hat{\sigma}^2_t(a^{\pm}_{t,i}) := \frac{1}{\omega(V_{t-1})}. \tag{43}$$

We note that the definition for $\hat{\sigma}^2_t(a^{\pm}_{t,i})$ fulfills the definition of variance estimator (34) stated in the previous section since it only depends on the past history $\mathcal{H}_{t-1}$.

Algorithm 1: LinUCB-VVN

```
Require: $\lambda_0 \in \mathbb{R}_{>0}$, $k \in \mathbb{N}$, $\omega : \mathrm{P}^d_+ \to \mathbb{R}_{\geq 0}$
Set initial design matrix $V_0 \leftarrow \lambda_0 \mathbb{I}_{d\times d}$
Choose initial estimator $\theta_0 \in \mathbb{S}^d$ for $\theta$ at random
for $t = 1, 2, \cdots$ do
    Optimistic action selection
    for $i = 1, 2, \cdots d-1$ do
        Select actions $a^{+}_{t,i}$ and $a^{-}_{t,i}$ according to Eq. (41)
        Sample k independent rewards for each $a^{\pm}_{t,i}$
        for $j = 1, ..., k$ do
            Receive associated rewards $r^{+}_{t,i,j}$ and $r^{-}_{t,i,j}$
        end
    end
    Update estimator of sub-gaussian noise for $a^{+}_{t,i}$
    $\hat{\sigma}^2_t \leftarrow \frac{1}{\omega(V_{t-1}(\lambda_0))}$ for $t \geq 2$ or $\hat{\sigma}^2_t \leftarrow 1$ for $t = 1$.
    Update design matrix
    $V_t \leftarrow V_{t-1} + \frac{1}{\hat{\sigma}^2_t} \sum_{i=1}^{d-1} \left(a^{+}_{t,i}(a^{+}_{t,i})^{\mathsf{T}} + a^{-}_{t,i}(a^{-}_{t,i})^{\mathsf{T}}\right)$
    Update LSE for each subsample
    for $j = 1, 2, ..., k$: do
        $\widetilde{\theta}^{\mathrm{w}}_{t,j} \leftarrow V_t^{-1} \sum_{s=1}^{t} \frac{1}{\hat{\sigma}^2_t} \sum_{i=1}^{d-1} (a^{+}_{s,i} r^{+}_{t,i,j} + a^{-}_{s,i} r^{-}_{t,i,j})$
    end
    Compute $\widetilde{\theta}^{\mathrm{wMOM}}_t$ using $\{\widetilde{\theta}^{\mathrm{w}}_{t,j}\}_{j=1}^k$
end
```

4.3. Regret analysis

In this Section we present the analysis of the regret for Algorithm 1. The analysis is similar to the LinUCB-VN presented in [20][Appendix C.1]. Thus, we focus on the changes respect to LinUCB-VN and although we present a complete proof we refer to [20] for more detailed computations. The main result we use from [20] is a theorem that quantifies the growth of the maximum and minimum eigenvalues of the design matrix V_t (42).

Theorem 8 (Theorem 3 in [20]). *Let $\{c_t\}_{t=0}^{\infty} \subset \mathbb{S}^{d-1}$ be a sequence of normalized vectors and $\omega : \mathrm{P}_{+}^{d} \to \mathbb{R}_{\geq 0}$ a function such that*

$$\omega(X) \leq C\sqrt{\|X\|_{\infty}}, \tag{44}$$

for a constant $C > 0$ and any $X \in \mathrm{P}_{+}^{d}$. Let $\lambda_0 \geq \max\{2, \sqrt{\frac{2}{3(d-1)}}2dC + \frac{2}{3(d-1)}\}$, and define a sequence of matrices $\{V_t\}_{t=0}^{\infty} \subset \mathbb{R}^{d\times d}$ as

$$V_0 := \lambda_0 \mathbb{I}_{d\times d}, \quad V_{t+1} := V_t + \omega(V_t)\sum_{i=1}^{d-1} P_{t,i}, \tag{45}$$

where

$$P_{t,i} := a_{t+1,i}^{+}(a_{t+1,i}^{+})^{\mathsf{T}} + a_{t+1,i}^{-}(a_{t+1,i}^{-})^{\mathsf{T}}, \quad a_{t+1,i}^{\pm} := \frac{\tilde{a}_{t+1,i}^{\pm}}{\|\tilde{a}_{t+1,i}^{\pm}\|_2}, \quad \tilde{a}_{t+1,i}^{\pm} := c_t \pm \frac{1}{\sqrt{\lambda_{t,1}}} v_{t,i}, \tag{46}$$

with $\lambda_{t,i} = \lambda_i(V_t)$ the eigenvalues of V_t with corresponding normalized eigenvectors $v_{t,1}, ..., v_{t,d} \in \mathbb{S}^{d-1}$. Then we have

$$\lambda_{\min}(V_t) \geq \sqrt{\frac{2}{3(d-1)}\lambda_{\max}(V_t)} \quad \textit{for all} \quad t \geq 0. \tag{47}$$

For the proof of the above Theorem we refer to the original reference. Then using this Theorem and the concentration bound for MOMLSE given in Corollary 7 we can provide the following regret analysis for a stochastic linear bandit with vanishing variance noise.

Theorem 9. *Let $d \geq 2$, $k \in \mathbb{N}$ and $T = 2(d-1)k\widetilde{T}$ for some $\widetilde{T} \in \mathbb{N}$, $\widetilde{T} \geq 2$. Let $\omega(X)$ defined as in (43) using λ_0 satisfying the constraints in Theorem 8. Then if we apply LinUCB-VVN 1(λ_0, k, ω) to a d dimensional stochastic linear bandit with variance as in (25) with probability at least $(1 - \exp(-k/24))^{\widetilde{T}}$ the regret satisfies*

$$\mathrm{Regret}(T) \leq 4k(d-1) + 144d(d-1)k\beta^2 \log\left(\frac{T}{2(d-1)k}\right) + 24(d-1)^{\frac{3}{2}}k\beta\log\left(\frac{T}{2(d-1)k}\right), \tag{48}$$

and at each time step $t \in [T]$ with the same probability it can output an estimator $\hat{\theta}_t \in \mathbb{S}^{d-1}$ such that

$$\|\theta - \hat{\theta}_t\|_2^2 \leq \frac{576d^2\beta^2 k + 96d\sqrt{d-1}\beta k}{t}, \tag{49}$$

with β defined as in (39).

From the above Theorem we have that if we set $k = \lceil 24\log\left(\frac{\widetilde{T}}{\delta}\right)\rceil$ for some $\delta \in (0,1)$ then with probability at least $1-\delta$ LinUCB-VNN achieves

$$\mathrm{Regret}(T) = O\left(d^4\log^2(T)\right), \quad \|\theta - \hat{\theta}_t\|_2^2 = O\left(\frac{\log(T)}{t}\right). \tag{50}$$

Proof. From the expression of the regret (26) we have that to give an upper bound it suffices to gives an upper bound between the distance of the unknown parameter θ and the actions $a_{t,i}^{\pm}$

selected by the algorithm (41). We denote the step $\tilde{t} \in [\widetilde{T}]$ to run over the batches the algorithm updates the MoM estimator $\widetilde{\theta}_{\tilde{t}}^{\mathrm{wMOM}}$. First we will do the computation assuming that the event

$$E_{\tilde{t}} := \{\mathcal{H}_{\tilde{t}} : \forall s \in [\tilde{t}], \theta \in \mathcal{C}_s\}, \tag{51}$$

holds where $\mathcal{C}_s = \{\theta' \in \mathbb{R}^d : \|\theta' - \widetilde{\theta}_{\tilde{t}}^{wMOM}\|_{V_s}^2 \leq \beta\}$. Here the history $\mathcal{H}_{\tilde{t}}$ is defined with the previous outcomes and actions of our algorithm i.e

$$\mathcal{H}_{\tilde{t}} := \left(r_{s,i,j}^{+}, a_{s,i}^{+}, r_{s,i,j}^{-}, a_{s,i}^{-}\right)_{(s,i,j)\in[\tilde{t}]\times[d-1]\times[k]} \tag{52}$$

Later we will quantify the probability that this event always hold. Using the definition of the actions (41), $\theta, \widetilde{\theta}_{\tilde{t}}^{\mathrm{wMOM}} \in \mathbb{S}^{d-1}$ and the arguments from [20][Appendix C.1, Eq. (165)] we have that

$$\|\theta - a_{\tilde{t},i}^{\pm}\|_2^2 \leq \frac{9\beta}{\lambda_{\min}(V_{\tilde{t}-1})}. \tag{53}$$

Then using that the design matrix $V_{\tilde{t}}$ (42) is updated as in Theorem 8 and the choice of weights (43) we fix

$$\lambda_0 \geq \max\left\{2, 2\sqrt{\frac{2}{3(d-1)}}\frac{d}{12\sqrt{d-1}\beta} + \frac{2}{3(d-1)}\right\} \tag{54}$$

and we have that $\lambda_{\min}(V_{\tilde{t}}) \geq \sqrt{\frac{2}{3(d-1)}\lambda_{\max}(V_{\tilde{t}})}$ applying Theorem 8. Inserting this into the above we have

$$\|\theta - a_{\tilde{t},i}^{\pm}\|_2^2 \leq \frac{12\sqrt{d-1}\beta}{\sqrt{\lambda_{\max}(V_{\tilde{t}})}}. \tag{55}$$

Thus, it remains to provide a lower bound on $\lambda_{\max}(V_{\tilde{t}})$. We note that in [20][Appendix C.1] they also had to provide an upper bound but this was because the constant β beta they use depends on t. From the definition of V_t (42) we can bound the trace as

$$\mathrm{Tr}(V_{\tilde{t}}) \geq \sum_{s=2}^{\tilde{t}} 2(d-1)\omega(V_{s-1}) \tag{56}$$

$$= \frac{\sqrt{d-1}}{6\beta}\sum_{s=1}^{\tilde{t}-1}\sqrt{\lambda_{\max}(V_s)}. \tag{57}$$

Then using the bound $\mathrm{Tr}(V_{\tilde{t}}) \geq \lambda_{\max}(V_{\tilde{t}})/d$ and some algebra we arrive at

$$\lambda_{\max}(V_{\tilde{t}}) \geq \frac{1}{1 + 6\frac{d}{\sqrt{d-1}}\beta}\sum_{s=1}^{\tilde{t}}\sqrt{\lambda_{\max}(V_s)}. \tag{58}$$

Now we have an inequality with the function $\lambda_{\max}(V_s)$ at both sides. In order to solve it we use the technique from [20][Appendix C.1, Equation (197-208)] which consist on extending $\lambda_{\max}(V_{\tilde{t}})$ to the continuous with a linear interpolation and then transforming the sum to an integral which leads to a differential inequality. Solving this leads to

$$\lambda_{\max}(V_{\tilde{t}}) \geq \frac{\tilde{t}^2}{4(1 + 6\frac{d}{\sqrt{d-1}}\beta)^2}. \tag{59}$$

Now we can insert the above into (55) and we have

$$\|\theta - a^{\pm}_{\tilde{t},i}\|_2^2 \leq \frac{24\sqrt{d-1}\beta(1 + 6\frac{d}{\sqrt{d-1}}\beta)}{\tilde{t}-1} \tag{60}$$

$$= \frac{144d\beta^2 + 24\sqrt{d-1}\beta}{\tilde{t}-1}. \tag{61}$$

Thus, we can inserted the above bound into the regret expression (26) and we have

$$\begin{aligned}
\text{Regret}(T) &= \frac{1}{2}\sum_{t=1}^{T} \|\theta - a_t\|_2^2 && (62)\\
&= \frac{1}{2}\sum_{\tilde{t}=1}^{\tilde{T}}\sum_{i=1}^{d-1}\sum_{j=1}^{k}\left(\|\theta - a^{+}_{\tilde{t},i}\|_2^2 + \|\theta - a^{-}_{\tilde{t},i}\|_2^2\right) && (63)\\
&\leq 4k(d-1) + \frac{1}{2}\sum_{\tilde{t}=2}^{\tilde{T}}\sum_{i=1}^{d-1}\sum_{j=1}^{k}\left(\|\theta - a^{+}_{\tilde{t},i}\|_2^2 + \|\theta - a^{-}_{\tilde{t},i}\|_2^2\right) && (64)\\
&\leq 4k(d-1) + (144d(d-1)k\beta^2 + 24(d-1)^{\frac{3}{2}}k\beta)\sum_{\tilde{t}=2}^{\tilde{T}}\frac{1}{t-1} && (65)\\
&\leq 4k(d-1) + 144d(d-1)k\beta^2\log\widetilde{T} + 24(d-1)^{\frac{3}{2}}k\beta\log\widetilde{T} && (66)\\
&= 4k(d-1) + 144d(d-1)k\beta^2\log\left(\frac{T}{2(d-1)k}\right) + 24(d-1)^{\frac{3}{2}}k\beta\log\left(\frac{T}{2(d-1)k}\right). && (67)
\end{aligned}$$

It remains to quantify the probability that the event $E_{\tilde{t}}$ holds. For that we will use the concentration bounds of the median of means for least squares estimator stated in Corollary 7. From the variance condition of our model (25) we have

$$\mathbb{V}[\epsilon^{\pm}_{\tilde{t},i,j}|\mathcal{F}_{\tilde{t}-1}] \leq 1 - \langle\theta, a^{\pm}_{\tilde{t},i}\rangle^2 \leq 2(1 - \langle\theta, a^{\pm}_{\tilde{t},i}\rangle) = \|\theta - a^{\pm}_{\tilde{t},i}\|_2^2, \tag{68}$$

where we used $1 + \langle\theta, a^{\pm}_{\tilde{t},i}\rangle \leq 2$. Thus from our choice of weights (43) and (60) we have that

$$\text{if } \theta \in \mathcal{C}_{s-1} \Rightarrow \mathbb{V}[\epsilon^{\pm}_{\tilde{t},i,j}|\mathcal{F}_{\tilde{t}-1}] \leq \hat{\sigma}^2_s(a^{\pm}_{s,i}). \tag{69}$$

Then in order to apply Corollary 7 we note that from the choice $\hat{\sigma}^2_s(a^{\pm}_{1,i}) = 1$ the event $G_{\tilde{t}}$ at $\tilde{t} = 1$ is always satisfied i.e $\Pr(G_1) = 1$. Then applying Bayes theorem, union bound over the events $G_1, E_1, ..., G_{t-1}, E_t$ and Corollary 7 we have

$$\Pr(E_{\widetilde{T}} \cap G_{\widetilde{T}}) \geq (1 - \exp(-k/24))^{\widetilde{T}}. \tag{70}$$

This probability also quantifies the probability that (60) holds since the only assumption we used is $\theta \in \mathcal{C}_{\tilde{t}-1}$. Then we can take simply one of the actions $a^{\pm}_{\tilde{t},i}$ as the estimator $\hat{\theta}_t$ and the result follows using the relabeling $t = 2(d-1)k\tilde{t}$ and the inequality $1/(\tilde{t}-1) \leq 2/\tilde{t}$ for $\tilde{t} \geq 2$. A more detailed analogous computation of the above probability can be found in [20][Appendix C.1]. □

In the previous Theorem we did not set a specific value for the parameter k or the number of subsamples per action. We note that the regret scales linearly with k but since the success probability scales exponentially with k it will suffice to set $k \sim \log(T)$ such that in expectation we get the $\log^2(T)$ behaviour. We formalize this in the following Corollary.

Corollary 10. *Under the same assumptions of Theorem 9 we can fix* $k = \lceil 24\log(\widetilde{T}^2)\rceil$ *and we have*

$$\mathbb{E}\left[\mathrm{Regret}(T)\right] \leq 344(d-1)\log(T) + \left(3546d(d-1)\beta^2 + 1152(d-1)^{\frac{3}{2}}\beta\right)\log^2(T) \tag{71}$$

and for $t \in [T]$,

$$\mathbb{E}\left[\|\theta - \hat{\theta}_t\|_2^2\right] \leq \frac{27648d^2\beta^2\log(T) + 4608d\sqrt{d-1}\beta\log(T)}{t} + \frac{4(d-1)\log(T)}{T}. \tag{72}$$

Using that $\beta = O(d)$ *gives*

$$\mathbb{E}\left[\mathrm{Regret}(T)\right] = O(d^4\log^2(T)), \quad \mathbb{E}\left[\|\theta - \hat{\theta}_t\|_2^2\right] = \tilde{O}\left(\frac{d^4}{t}\right). \tag{73}$$

Proof. The result of Theorem 9 holds with probability at least $(1-\exp(-k/24))^{\widetilde{T}}$. Setting $k = \lceil 24\log(\widetilde{T}^2)\rceil$ gives

$$(1-\exp(-k/24))^{\widetilde{T}} \geq \left(1 - \frac{1}{\widetilde{T}^2}\right)^{\widetilde{T}} \geq 1 - \frac{1}{\widetilde{T}}. \tag{74}$$

Then given the event R_T such that Algorithm 1 achieves the bounds given by Theorem 9 we have that the probability of failure is bounded by

$$\Pr(R_T^C) \leq \frac{1}{\widetilde{T}}, \tag{75}$$

where we used $1 = \Pr(R_T) + \Pr(R_T^C)$. Then the expectation of the bad events can be bounded as

$$\mathbb{E}\left[\mathrm{Regret}(T)\mathbb{I}\{R_T^C\}\right] \leq 4(d-1)k\widetilde{T}\Pr(R_T^C) \leq 4(d-1)k \tag{76}$$

$$\mathbb{E}\left[\|\theta - \hat{\theta}_t\|_2^2\mathbb{I}\{R_T^C\}\right] \leq 4\Pr(R_T^C) \leq \frac{4}{\widetilde{T}} \tag{77}$$

where we used $\mathrm{Regret}(T) \leq 2T = 4(d-1)k\widetilde{T}$, $\|\theta - \hat{\theta}_t\|_2^2 \leq 4$. Finally the result follows inserting the value of $k = 24\log(\widetilde{T}^2)$ into the bounds of Theorem 9 and using $\widetilde{T} \leq T$. □

5. ALGORITHM FOR QUBIT PSMAQB AND NUMERICAL EXPERIMENTS

In this Section we prove our main result that is a regret bound for LinUCB-VVN when applied to the qubit PSMAQB problem.

Theorem 11. *Let* $\widetilde{T} \in \mathbb{N}$ *and fix* $T = \lceil 96\widetilde{T}\log(\widetilde{T}^2)\rceil$. *Then given a* PSMAQB *with action set* $\mathcal{A} = \mathcal{S}_2^*$ *and environment* $\Pi_\theta \in \mathcal{S}_2^*$ *(qubits) we can apply Algorithm 1 for* $d = 3$ *and it achieves*

$$\mathbb{E}\left[\mathrm{Regret}(T)\right] \leq C_1\log(T) + C_2\log^2(T). \tag{78}$$

for some universal constants $C_1, C_2 \geq 0$. *Also at each time step* $t \in [T]$ *it outputs an estimator* $\hat{\Pi}_t \in \mathcal{S}_2^*$ *of* Π_θ *with infidelity scaling*

$$\mathbb{E}\left[1 - F\left(\Pi_\theta, \hat{\Pi}_t\right)\right] \leq \frac{C_3\log(T)}{t}, \tag{79}$$

for some universal constant $C_3 \geq 0$.

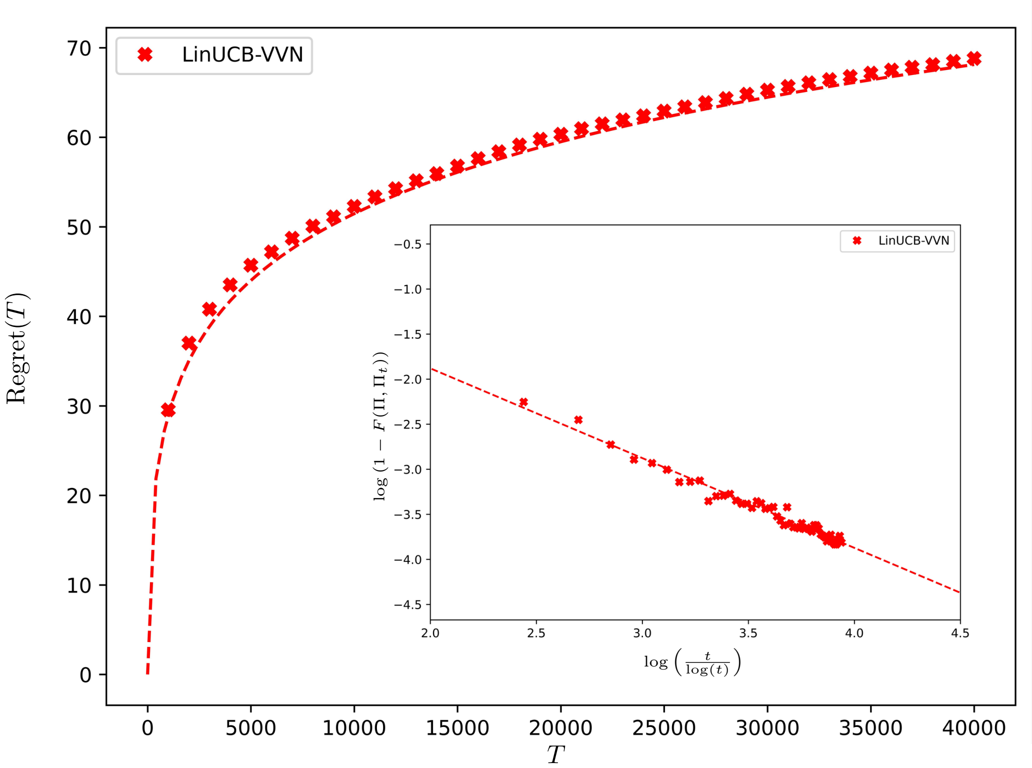


FIG. 2. Expected regret vs the number or rounds T for the LinUCB-VNN algorithm. We run $T = 4 \cdot 10^4$ rounds with $k = 10$ subsamples for the median of means construction. We use 100 independents experiments and average over them. We obtain results for each round but only plot (red crosses) few for clarity of the figure. We fit the regression $\text{Regret}(T) = m_1 \log^2 T + b_1$ with $m_1 = 3.2164 \pm 0.0009$ and $b_1 = 0.84 \pm 0.016$. In the inset plot we plot the expected infidelity of the output estimator at each rounds $t \in [T]$ versus the number of rounds t. We take $\Pi_t = \Pi_{\theta_t^{\text{wMoM}}}$ as the estimator given by the median of means linear least squares estimator. We fit the regression $1 - F(\Pi, \Pi_t) = b_2 \left(\frac{\log t}{t}\right)^{m_2}$ and we obtain $m_2 = -0.996 \pm 0.002$ $b_2 = 0.112 \pm 0.007$. We note that the number of subsamples of the theoretical results is very conservative in comparison with the value we take for the simulations.

Proof. In order to apply Algorithm 1 to a PSMAQB we set $d = 3$ (dimension for a classical linear stochastic bandit) and the actions that we select will be given by $\Pi_{a^{\pm}_{t,i}}$ where $a^{\pm}_{t,i}$ are updated as in (41). Note that they are valid action since $a^{\pm}_{t,i} \in \mathbb{S}^2$ imply $\Pi_{a^{\pm}_{t,i}} \in \mathcal{S}^*_2$. The rewards received by the algorithm follow (22) with the normalization given in (20). This model fits into the linear bandit with linearly vanishing variance noise model explained in Section 3.4 and thus we can apply the guarantees established in Theorem 9 and Corollary 10.

The algorithm is set with $k = \lceil 24 \log(\widetilde{T}^2) \rceil$ batches for the MoM construction. We set $\lambda_0 = 2$, and using $\|\theta\|_2 = 1$ we have that the constant β given in (39) has the value

$$\beta = 9\left(3\sqrt{3} + 2\right)^2 = 279 + 108\sqrt{3}. \tag{80}$$

Then we can check that for $d = 3$ the condition (54) for the input parameter λ_0 for Theorem 9 to hold is satisfied since

$$\lambda_0 = 2 \geq \max\left\{2, \frac{1}{3} + \frac{1}{2\sqrt{6}(279 + 108\sqrt{3})}\right\} = 2. \tag{81}$$

In the above we just substituted all numerical values. Then we are under the assumptions of Theorem 9 and Corollary 10 and the result follows applying both results with the relation of regrets between the classical and quantum model given in (24), the relation

$$\|\theta - \hat{\theta}_t\|_2^2 = 4\left(1 - F\left(\Pi_\theta, \Pi_{\hat{\theta}_t}\right)\right), \tag{82}$$

and substituting all numerical values. We take the estimator $\hat{\theta}_t$ given in Theorem 9 for $d = 3$. We use also the bound $\widetilde{T} \leq T$ and reabsorb all the constants into C_1, C_2, C_3. □

Remark 1. The constant dependence can be slightly improved taking the estimator for Π_θ as $\Pi_{\theta_t^{\mathrm{wMoM}}}$ with θ_t^{wMoM} defined in (41).

Remark 2. The result of Theorem 11 also holds with high probability. In particular for the choice of batches $k = 24\log(\widetilde{T}^2)$ with probability at least $1 - \frac{1}{\widetilde{T}}$.

6. REGRET LOWER BOUND FOR PSMAQB

While the algorithm for PSMAQB presented above is inspired by classical bandit theory, the lower bound on the regret that we derive is essentially based on quantum information theory. The key insight here is that a policy for PSMAQB can be viewed as a sequence of state tomographies. The expected fidelity of these tomographies is linked to the regret. Hence, existing upper bounds on tomography fidelity also provide a lower bound for the expected regret of the policy.

6.1. Average fidelity bound for pure state tomography

In its most general form, a tomography procedure takes n copies of an unknown state $\Pi \in \mathcal{S}_d^*$ and performs a joint measurement on the state $\Pi^{\otimes n}$. This is captured in the following definition. Let $(\mathcal{S}_d^*, \Sigma)$ be a σ-algebra. A *tomography scheme* is a positive operator-valued measure (POVM) $\mathcal{T} : \Sigma \to \mathrm{End}(\mathcal{H}^{\otimes n})$ such that $\mathcal{T}(\mathcal{S}_d^*) = \Pi_n^+$, where Π_n^+ is the symmetrization operator on $\mathcal{H}^{\otimes n}$. For any $\rho \in \mathrm{End}(\mathcal{H}^{\otimes n})$, this POVM gives rise to a complex-valued measure

$$P_{\mathcal{T},\rho}(A) = \mathrm{Tr}(\mathcal{T}(A)\rho) \tag{83}$$

for $A \in \Sigma$. $P_{\mathcal{T},\rho}$ becomes a probability measure if ρ satisfies $\rho \geq 0$, $\Pi_n^+\rho = \rho\Pi_n^+ = \rho$, and $\mathrm{Tr}\,\rho = 1$. Given n copies of Π, the tomography scheme produces the distribution $P_{\mathcal{T},\Pi^{\otimes n}}$ of the predicted states. Note that $\Pi^{\otimes n}$ satisfies the properties above, so $P_{\mathcal{T},\Pi^{\otimes n}}$ is indeed a probability distribution. The fidelity of this distribution is given by

$$F(\mathcal{T}, \Pi) = \int \mathrm{Tr}(\Pi\sigma) dP_{\mathcal{T},\Pi^{\otimes n}}(\sigma). \tag{84}$$

Finally, the average fidelity of the tomography scheme is defined as

$$F(\mathcal{T}) = \int F(\mathcal{T}, |\psi\rangle\langle\psi|) d\psi, \tag{85}$$

where the integration is taken with respect to the normalized uniform measure over all pure states. In the following, $\int d\psi$ will always imply this measure. We will provide a lower bound on $F(\mathcal{T})$ in terms of d and n, following the proof technique from [14]. In [14], the proof is only presented for tomography schemes producing a finite number of predictions. For our definition, we will require more general measure-theoretic tools. Before we introduce the upper bound on the fidelity, we will prove some auxiliary lemmas about the nature of the measure $P_{\mathcal{T},\rho}$.

Lemma 12. *Let (Ω, Σ) be a σ-algebra, and let $O : \Sigma \to \mathrm{End}(\widetilde{\mathcal{H}})$ be a POVM with values acting on a finite-dimensional Hilbert space $\widetilde{\mathcal{H}}$ with $\dim \widetilde{\mathcal{H}} = \tilde{d}$ s.t. $O(\Omega) \leq \mathbb{1}$, where $\mathbb{1}$ is the identity operator. Further, let $P_{O,\sigma} : \Sigma \to \mathbb{C}$ be a complex-valued measure, defined for any $\sigma \in \mathrm{End}(\widetilde{\mathcal{H}})$ as*

$$P_{O,\sigma}(A) = \mathrm{Tr}[O(A)\sigma]. \tag{86}$$

Then, there exists a set of functions $\{f_\sigma\}$ indexed by $\sigma \in \mathrm{End}\,\widetilde{\mathcal{H}}$ that are linear w.r.t. σ for all ω and that satisfy

$$f_\sigma : \Omega \to \mathbb{C} \quad s.t. \quad \forall A \in \Sigma \;\; P_{O,\sigma}(A) = \int_A f_\sigma(\omega) dP_{O,\mathbb{1}}(\omega). \tag{87}$$

We purposefully formulated this lemma with slightly more general objects than the ones used in the definition of tomography. That is, Ω does not need to be $\mathcal{S}_d^*$, and $\widetilde{\mathcal{H}}$ does not need to be the n-th power $\mathcal{H}^{\otimes n}$, although we will focus on this case.

Proof. Let $\{|i\rangle\}_{i=1}^{\tilde{d}}$ be a basis of $\widetilde{\mathcal{H}}$ We will first show that $P_{O,\sigma}$ is dominated by $P_{O,\mathbb{1}}$ for all σ. Indeed, let $A \in \Sigma$. Assume that $P_{O,\mathbb{1}}(A) = 0$. This gives us

$$\mathrm{Tr}[O(A)\mathbb{1}] = \mathrm{Tr}[O(A)] = 0, \tag{88}$$

and, because $O(A) \geq 0$, we also have $O(A) = 0$. Therefore,

$$P_{O,\sigma}(A) = \mathrm{Tr}[O(A)\sigma] = 0. \tag{89}$$

Hence, for any $|i\rangle, |j\rangle$ from the basis we can introduce the Radon-Nikodym derivatives $f_{|i\rangle\langle j|}$, which will satisfy (87). Then, for any $\sigma \in \mathrm{End}\,\widetilde{\mathcal{H}}$ we can define

$$f_\sigma(\omega) = \sum_{i,j=1}^{\tilde{d}} \langle i| \sigma |j\rangle f_{|i\rangle\langle j|}(\omega). \tag{90}$$

These f_σ are linear in σ by definition. A direct calculation shows that they also satisfy (87). □

Note that for $\sigma \geq 0$, the measure $P_{O,\sigma}$ is finite and nonnegative, but nonnegativity (and even real-valuedness) do not hold for a general $\sigma \in \mathrm{End}(\widetilde{\mathcal{H}})$. By our definition of $f_\sigma(\omega)$, it can be written as

$$f_\sigma(\omega) = \mathrm{Tr}\left[K(\omega)\sigma\right], \quad \text{where } K(\omega) = \sum_{i,j=1}^{\tilde{d}} f_{|i\rangle\langle j|}(\omega)|j\rangle\langle i|. \tag{91}$$

As the following lemma demonstrates, $K(\omega) \geq 0$ for $P_{O,\mathbb{1}}$-almost every ω:

Lemma 13. *Let (Ω, Σ, μ) be a measurable space and $V : \Omega \to \mathrm{End}(\widetilde{\mathcal{H}})$ be a measurable operator-valued function with values acting on a finite-dimensional Hilbert space $\widetilde{\mathcal{H}}$ such that*

$$\forall A \in \Sigma \quad \int_A V(\omega) d\mu(\omega) \geq 0. \tag{92}$$

Then, $V(\omega) \geq 0$ μ-almost everywhere.

Proof. Let $|\psi\rangle \in \widetilde{\mathcal{H}}$ and define

$$g_\psi(\omega) = \langle\psi| V(\omega) |\psi\rangle . \tag{93}$$

By the given condition, for any $A \in \Sigma$

$$\int_A g_\psi(\omega) d\mu(\omega) = \langle\psi| \int_A V(\omega) d\mu(\omega) |\psi\rangle \geq 0. \tag{94}$$

It follows that $g_\psi(\omega) \geq 0$ μ-almost everywhere. Let

$$Z_\psi = \{\omega \in \Omega \text{ s.t. } g_\psi(\omega) < 0\} \tag{95}$$

We have shown that $\mu(Z_\psi) = 0$. Next, since $\widetilde{\mathcal{H}}$ is finite-dimensional, it is separable. Therefore, there exists a countable set $\{|\psi_k\rangle\}_k$ dense in $\widetilde{\mathcal{H}}$. Let

$$Z = \bigcup_k Z_{\psi_k}. \tag{96}$$

We have that $\mu(Z) = 0$. Finally, let $\omega \in \Omega \setminus Z$ and $|\psi\rangle \in \widetilde{\mathcal{H}}$. Because $\{|\psi_k\rangle\}$ is dense in $\widetilde{\mathcal{H}}$, there exists a sequence $\{|\psi_{k_i}\rangle\}$ converging to $|\psi\rangle$. Then,

$$0 \leq \langle\psi_{k_i}| V(\omega) |\psi_{k_i}\rangle \xrightarrow{i\to\infty} \langle\psi| V(\omega) |\psi\rangle . \tag{97}$$

Overall, we get that

$$\forall \omega \in \Omega \setminus Z,\ |\psi\rangle \in \widetilde{\mathcal{H}} \quad \langle\psi| V(\omega) |\psi\rangle \geq 0. \tag{98}$$

Together with $\mu(Z) = 0$, this gives the desired result. □

Now we can apply this analysis to the POVM corresponding to our tomography scheme, and get the desired upper bound on the fidelity.

Theorem 14. *For any tomography scheme $\mathcal{T}$ utilizing n copies of the input state, the average fidelity is bounded by*

$$F(\mathcal{T}) \leq \frac{n+1}{n+d}. \tag{99}$$

Proof. We will introduce the density $K(\omega)$ from (91) for our tomography scheme $\mathcal{T}$ and the corresponding measure $P_{\mathcal{T},\sigma}$. Lemma 12 allows us to introduce for any $\sigma \in \mathrm{End}(\mathcal{H}^{\otimes n})$ the density $f_\sigma : \Omega \to \mathbb{C}$ s.t.

$$\forall A \in \Sigma \ \ P_{\mathcal{T},\sigma}(A) = \int_A f_\sigma(\omega) dP_{\mathcal{T},\mathbb{1}}(\omega). \tag{100}$$

This density can be written as $f_\sigma(\omega) = \mathrm{Tr}\left(K(\omega)\sigma\right)$ for some $K(\omega) \in \mathrm{End}(\mathcal{H}^{\otimes n})$. $K(\omega)$ can be considered as the operator-valued density of $\mathcal{T}$ w.r.t. $P_{\mathcal{T},\mathbb{1}}$:

$$\forall A \in \Sigma \quad \mathcal{T}(A) = \int_A K(\omega) dP_{\mathcal{T},\mathbb{1}}(\omega). \tag{101}$$

Since $\mathcal{T}(A) \geq 0$, it follows by Lemma 13 that $K(\omega) \geq 0$ for $P_{\mathcal{T},\mathbb{1}}$-almost all ω. Furthermore, as $\mathcal{T}(\mathcal{S}_d^*) = \Pi_n^+$, we have that for all $A \in \Sigma$, $\mathcal{T}(A) \leq \Pi_n^+$. Therefore, $\mathcal{T}(A)\Pi_n^+ = \Pi_n^+\mathcal{T}(A) = \mathcal{T}(A)$.

This means that $\tilde{K}(\omega) = \Pi_n^+ K(\omega) \Pi_n^+$ would also satisfy (101). In the following, we will without loss of generality assume that

$$K(\omega) = \Pi_n^+ K(\omega) = K(\omega)\Pi_n^+. \tag{102}$$

With these tools at hand, we are ready to adapt the proof from [14] to the general case of POVM tomography schemes. We begin by rewriting the expression (84) for average fidelity:

$$\begin{aligned} F(\mathcal{T}) &= \int d\psi \int dP_{\mathcal{T},(|\psi\rangle\langle\psi|)^{\otimes n}}(\sigma)\, \mathrm{Tr}(\sigma\, |\psi\rangle\langle\psi|) && (103)\\ &= \int d\psi \int dP_{\mathcal{T},\mathbb{1}}(\sigma)\, \mathrm{Tr}(|\psi\rangle\langle\psi|\, \sigma)\, \mathrm{Tr}\left(K(\sigma)(|\psi\rangle\langle\psi|)^{\otimes n}\right). && (104) \end{aligned}$$

Since fidelity is nonnegative and its average is bounded by 1, we can change the order of integration. Following [14], we introduce notation

$$\sigma_n(k) = \mathbb{1}^{\otimes(k-1)} \otimes \sigma \otimes \mathbb{1}^{\otimes(n-k)} \in \mathcal{H}^{\otimes n}. \tag{105}$$

The product of traces in (104) can be rewritten in the following manner:

$$F(\mathcal{T}) = \int dP_{\mathcal{T},\mathbb{1}}(\sigma) \int d\psi\, \mathrm{Tr}\Big((K(\sigma)\otimes \mathbb{1})(|\psi\rangle\langle\psi|)^{\otimes(n+1)}\sigma_{n+1}(n+1)\Big). \tag{106}$$

We can now take the inner integral in closed form. As shown in [14, Eq. (4)],

$$\int d\psi (|\psi\rangle\langle\psi|)^{\otimes n} = \frac{\Pi_n^+}{D_n}, \tag{107}$$

where $D_n = \binom{n+d-1}{d}$. Another useful result in this paper is [14, Eq. (8)]:

$$\mathrm{Tr}_{n+1}\left(\Pi_{n+1}^+ \sigma_{n+1}(n+1)\right) = \frac{1}{n+1}\Pi_n^+ \left(\mathbb{1} + \sum_{k=1}^{n} \sigma_n(k)\right), \tag{108}$$

where $\mathrm{Tr}_{n+1} : \mathrm{End}(\mathcal{H}^{\otimes(n+1)}) \to \mathrm{End}(\mathcal{H}^{\otimes n})$ is the partial trace on the $(n+1)$-st copy of the system. These expressions allow us to rewrite (106) as follows:

$$\begin{aligned} F(\mathcal{T}) &= \frac{1}{D_{n+1}} \int dP_{\mathcal{T},\mathbb{1}}(\sigma)\, \mathrm{Tr}\left((K(\sigma)\otimes\mathbb{1})\Pi_{n+1}^+\sigma_{n+1}(n+1)\right) && (109)\\ &= \frac{1}{D_{n+1}} \int dP_{\mathcal{T},\mathbb{1}}(\sigma)\, \mathrm{Tr}\left(K(\sigma)\, \mathrm{Tr}_{n+1}\left(\Pi_{n+1}^+\sigma_{n+1}(n+1)\right)\right) && (110)\\ &= \frac{1}{(n+1)D_{n+1}} \int dP_{\mathcal{T},\mathbb{1}}(\sigma)\, \mathrm{Tr}\left(K(\sigma)\left(\mathbb{1} + \sum_{k=1}^{n}\sigma_n(k)\right)\right). && (111) \end{aligned}$$

Finally, $\sigma_n(k) \leq \mathbb{1}$, so $\mathrm{Tr}(K(\sigma)\sigma_n(k)) \leq \mathrm{Tr}(K(\sigma))$, and we can bound the above as

$$F(\mathcal{T}) \leq \frac{1}{D_{n+1}} \int dP_{\mathcal{T},\mathbb{1}}(\sigma)\, \mathrm{Tr}\left(K(\sigma)\right) = \frac{\mathrm{Tr}\,\Pi_n^+}{D_{n+1}} = \frac{D_n}{D_{n+1}} = \frac{n+1}{n+d}. \tag{112}$$

□

6.2. Bandit policy as a sequence of tomographies

Theorem 15. *Given a d-dimensional pure state general multi-armed quantum bandit we have that for any policy π the average expected regret is bounded by*

$$\int d\psi\, \mathbb{E}_{|\psi\rangle\langle\psi|,\pi}\left[\mathrm{Regret}(T,\pi,|\psi\rangle\langle\psi|)\right] \geq (d-1)\log\left(\frac{T}{d+1}\right), \tag{113}$$

where the expectation is taken w.r.t. the measure (11) *over actions taken by the bandit, and the regret is defined in* (12).

The above Theorem gives $\mathbb{E}\left[\mathrm{Regret}(T)\right] = \Omega(d\log\frac{T}{d})$. In the case of qubit environments, we have $d=2$ and $\mathbb{E}\left[\mathrm{Regret}(T)\right] = \Omega(\log T)$.

Proof. Given a policy π, we can introduce a POVM $E_t : (\Sigma\times\{0,1\})^{\times t} \to \mathrm{End}(\mathcal{H}^{\otimes t})$ such that

$$P^t_{|\psi\rangle\langle\psi|,\pi}(A_1,r_1,\ldots,A_t,r_t) = \mathrm{Tr}\left((|\psi\rangle\langle\psi|)^{\otimes t}E_t(A_1,r_1,\ldots,A_t,r_t)\right), \tag{114}$$

where $P^t_{|\psi\rangle\langle\psi|,\pi}$ is the probability measure defined by (11), but only for actions and rewards until step t. The construction of this POVM is presented in the proof of Lemma 9 in [19]. We will also define the coordinate mapping

$$\Psi_t(\Pi_1,r_1,\ldots,\Pi_t,r_t) = \Pi_t, \tag{115}$$

where $\Pi_i \in \mathcal{A}$ are actions and $r_i\in\{0,1\}$ are rewards of the PSMAQB. Now we can for each step t define a tomography scheme $\mathcal{T}_t = E_t\circ\Psi_t^{-1}$ as the pushforward POVM from E_t to the space $(\mathcal{A},\Sigma)$. Informally, this tomography scheme takes t copies of the state, runs the policy π on them, and outputs the t-th action of the policy as the predicted state. For $A\in\Sigma$, we can rewrite the tomography's distribution on predictions as

$$P_{\mathcal{T},(|\psi\rangle\langle\psi|)^{\otimes t}}(A) = \mathrm{Tr}\left(\mathcal{T}_t(A)(|\psi\rangle\langle\psi|)^{\otimes t}\right) = \mathrm{Tr}\left(E_t(\Psi_t^{-1}(A))(|\psi\rangle\langle\psi|)^{\otimes t}\right) = \left(P^t_{|\psi\rangle\langle\psi|,\pi}\circ\Psi^{-1}\right)(A). \tag{116}$$

Then, the fidelity of $\mathcal{T}_t$ on the input $|\psi\rangle\langle\psi|$ can be rewritten as

$$F(\mathcal{T}_t,|\psi\rangle\langle\psi|) = \int\langle\psi|\rho|\psi\rangle dP_{\mathcal{T}_t,(|\psi\rangle\langle\psi|)^{\otimes t}}(\rho) \tag{117}$$

$$= \int\langle\psi|\Psi_t(\Pi_1,r_1,\ldots,\Pi_t,r_t)|\psi\rangle dP^t_{|\psi\rangle\langle\psi|,\pi}(\Pi_1,r_1,\ldots,\Pi_t,r_t) \tag{118}$$

$$= \mathbb{E}_{|\psi\rangle\langle\psi|,\pi}\left[\langle\psi|\Pi_t|\psi\rangle\right]. \tag{119}$$

Using the bound for average tomography fidelity on $\mathcal{T}_t$ from Theorem 14, we can now bound the average regret of π:

$$\int\mathbb{E}_{|\psi\rangle\langle\psi|}\left[\mathrm{Regret}(T,\pi,|\psi\rangle\langle\psi|)\right]d\psi = T - \sum_{t=1}^{T}\int\mathbb{E}_{|\psi\rangle\langle\psi|}\left[\langle\psi|\Pi_t|\psi\rangle\right]d\psi \tag{120}$$

$$= T - \sum_{t=1}^{T}F(\mathcal{T}_t) \geq \sum_{t=1}^{T}1-\frac{t+1}{t+d} \tag{121}$$

$$= \sum_{t=1}^{T}\frac{d-1}{t+d} \geq (d-1)\log\left(\frac{T}{d+1}\right), \tag{122}$$

where the last inequality follows from bounding the sum by below with the integral of the function $f(t) = 1/(t+d)$. □

7. OUTLOOK

From a quantum state tomography perspective, our work introduces completely new techniques for the adaptive setting such as the median of means online least squares estimator or the optimistic principle. We expect these techniques to find applications in other quantum learning settings where adaptiveness is needed. At a fundamental level our algorithm goes beyond traditional tomography ideas like adaptive/non-adaptive basis measurements, randomized measurements or SIC POVM's and show that is enough to project near the state in order to optimally learn it. From a bandit perspective, it is surprising that the simple setting of learning pure quantum states gives the first non-trivial example of a linear bandit with continuous action sets that achieves polylogarithmic regret. This model motivated our classical work [20] and jointly with the current work we establish the first bridge between the fields of quantum state tomography and linear stochastic bandits.

Acknowledgements: JL thanks Jan Seyfried and Yanglin Hu for comments and suggestions and Roberto Rubboli for many technical discussions.

Mikhail Terekhov is grateful to be supported by the EDIC Fellowship from the School of Computer Science at EPFL. Josep Lumbreras and Marco Tomammichel are supported by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant and the Quantum Engineering Programme grant NRF2021-QEP2-02-P05.

[1] Y. Abbasi-Yadkori, D. Pál, and C. Szepesvári. *“Improved Algorithms for Linear Stochastic Bandits”*. In *Advances in Neural Information Processing Systems*, volume 24, (2011).

[2] M. Abeille and A. Lazaric. *“Linear Thompson Sampling Revisited”*. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, volume 54, pages 176–184, (2017).

[3] S. Agrawal and N. Goyal. *“Thompson sampling for contextual bandits with linear payoffs”*. In *International conference on machine learning*, pages 127–135, (2013).

[4] E. Bagan, M. Baig, and R. Muñoz Tapia. *“Optimal Scheme for Estimating a Pure Qubit State via Local Measurements”*. Phys. Rev. Lett. **89**: 277904 (2002).

[5] E. Bagan, M. A. Ballester, R. D. Gill, A. Monras, and R. Muñoz Tapia. *“Optimal full estimation of qubit mixed states”*. Phys. Rev. A **73**: 032301 (2006).

[6] S. Brahmachari, J. Lumbreras, and M. Tomamichel. *“Quantum contextual bandits and recommender systems for quantum data”*. arXiv preprint arXiv:2301.13524 (2023).

[7] S. Bubeck, N. Cesa-Bianchi, and G. Lugosi. *“Bandits With Heavy Tail”*. IEEE Transactions on Information Theory **59**(11): 7711–7717 (2013).

[8] M. S. Byrd and N. Khaneja. *“Characterization of the positivity of the density matrix in terms of the coherence vector representation”*. Physical Review A **68**(6): 062322, (2003).

[9] S. Chen, B. Huang, J. Li, A. Liu, and M. Sellke. *“When Does Adaptivity Help for Quantum State Learning?”*. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 391–404, Los Alamitos, CA, USA(2023).

[10] V. Dani, T. P. Hayes, and S. M. Kakade. *“Stochastic Linear Optimization under Bandit Feedback.”*. In *Proceedings of the 21st Conference on Learning Theory*, volume 2, page 3, (2008).

[11] R. D. Gill and S. Massar. *“State estimation for large ensembles”*. Phys. Rev. A **61**: 042312 (2000).

[12] M. Guţă, J. Kahn, R. Kueng, and J. A. Tropp. *“Fast state tomography with optimal error bounds”*. Journal of Physics A: Mathematical and Theoretical **53**(20): 204001 (2020).

[13] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu. *“Sample-optimal tomography of quantum states”*. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 913–925, (2016).

[14] A. Hayashi, T. Hashimoto, and M. Horibe. *“Reexamination of optimal quantum state estimation of pure states”*. Physical review A **72**(3): 032325, (2005).

[15] M. Hayashi and K. Matsumoto. *“Asymptotic performance of optimal state estimation in qubit system”*.

Journal of Mathematical Physics **49**(10): 102101 (2008).

[16] R. Kueng, H. Rauhut, and U. Terstiege. *"Low rank matrix recovery from rank one measurements"*. Applied and Computational Harmonic Analysis **42**(1): 88–116 (2017).

[17] T. Lattimore and C. Szepesvári. *Bandit Algorithms.* Cambridge University Press (2020).

[18] M. Lerasle. *"Lecture notes: Selected topics on robust statistical learning theory"*. arXiv:1908.10761 , (2019).

[19] J. Lumbreras, E. Haapasalo, and M. Tomamichel. *"Multi-armed quantum bandits: Exploration versus exploitation when learning properties of quantum states"*. Quantum **6**: 749, (2022).

[20] J. Lumbreras and M. Tomamichel. *"Linear bandits with polylogarithmic minimax regret"*. arXiv preprint arXiv:2402.12042 (2024).

[21] D. H. Mahler, L. A. Rozema, A. Darabi, C. Ferrie, R. Blume-Kohout, and A. M. Steinberg. *"Adaptive Quantum State Tomography Improves Accuracy Quadratically"*. Phys. Rev. Lett. **111**: 183601 (2013).

[22] A. M. Medina and S. Yang. *"No-regret algorithms for heavy-tailed linear bandits"*. In *Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48*, ICML'16, page 1642–1650, (2016).

[23] R. O'Donnell and J. Wright. *"Efficient quantum tomography"*. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page 899–912, (2016).

[24] P. Rusmevichientong and J. N. Tsitsiklis. *"Linearly Parameterized Bandits"*. Mathematics of Operations Research **35**(2): 395–411 (2010).

[25] H. Shao, X. Yu, I. King, and M. R. Lyu. *"Almost optimal algorithms for linear stochastic bandits with heavy-tailed payoffs"*. In *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, NIPS'18, page 8430–8439, Red Hook, NY, USA(2018).

[26] W. R. Thompson. *"On the likelihood that one unknown probability exceeds another in view of the evidence of two samples"*. Biometrika **25**(3-4): 285–294, (1933).

[27] H. Yuen. *"An Improved Sample Complexity Lower Bound for (Fidelity) Quantum State Tomography"*. Quantum **7**: 890 (2023).

Extended abstract — Learning quantum states of continuous variable systems

Francesco A. Mele,[1, *] Antonio A. Mele,[2, †] Lennart Bittel,[2, †] Jens Eisert,[2, 3, ‡] Vittorio Giovannetti,[4, *] Ludovico Lami,[5, 6, 7, ‡] Lorenzo Leone,[2, †] and Salvatore F. E. Oliviero[4, *]

[1] *NEST, Scuola Normale Superiore and Istituto Nanoscienze, Piazza dei Cavalieri 7, IT-56126 Pisa, Italy*
[2] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[3] *Helmholtz-Zentrum Berlin für Materialien und Energie, Berlin, Germany*
[4] *NEST, Scuola Normale Superiore and Istituto Nanoscienze,*
Consiglio Nazionale delle Ricerche, Piazza dei Cavalieri 7, IT-56126 Pisa, Italy
[5] *QuSoft, Science Park 123, 1098 XG Amsterdam, the Netherlands*
[6] *Korteweg–de Vries Institute for Mathematics, University of Amsterdam,*
Science Park 105-107, 1098 XG Amsterdam, the Netherlands
[7] *Institute for Theoretical Physics, University of Amsterdam,*
Science Park 904, 1098 XH Amsterdam, the Netherlands

Keywords: Quantum state tomography, continuous variable systems, Bosonic systems, quantum learning theory, optimal performance guarantees, Gaussian states, t-doped Gaussian states, energy-constrained states

For the full version of this work, see Ref. [1], (arxiv.org/abs/2405.01431).

I. Overview

Quantum state tomography is a fundamental task in quantum information, aiming to construct a classical description of an unknown quantum state based on experimental data. A crucial question regarding quantum state tomography is the following: what is the minimum number of samples — copies of the unknown state — required to construct a classical description of an estimator which is ε-close in trace distance to the true state with high probability? While this question has been extensively addressed for qudit systems, this is an open question for *continuous variable* (CV) systems [2–4], characterised by an infinite-dimensional Hilbert space. The literature regarding quantum state tomography of CV systems mainly relies on phase-space approximations [5–8] which — crucially — do not provide any rigorous performance guarantees with respect to the trace distance (which is the most meaningful notion of distance between quantum states [9, 10]). This gap in the literature is particularly surprising given the pivotal role of quantum optical platforms — described by CV systems — in quantum technologies such as quantum computation, communication, and metrology. Our work fills this gap, by presenting an exhaustive analysis of quantum state tomography of CV systems in terms of the trace distance. We analyse tomography of three classes of states:

- *Energy-constrained states.* We consider energy-constrained states since, without any constraints, a tomography algorithm would inevitably require an unbounded number of resources. By assuming that the mean photon number per mode of the unknown state is upper bounded by N_s, and by denoting ε as the precision in trace distance and n as the number of modes, we establish that the sample complexity of any tomography algorithm must scale at least as $\tilde{\Omega}\left(\left(\frac{N_s}{\varepsilon^2}\right)^n\right)$ (see the preliminaries in the technical manuscript for a quick review of the asymptotic notation), which is an unfavourable scaling not only in n but also in ε. Contrary to what happens for finite-dimensional states, the sample complexity of CV tomography does not scale with $O(\varepsilon^{-2})$, but with $O(\varepsilon^{-2n})$. This establishes that, even if CV systems have to satisfy stringent energy constraints, CV tomography is extremely inefficient, much more than tomography of qudit systems. In addition, we devise a tomography algorithm for possibly mixed states with sample complexity scaling as $O\left(\left(\frac{N_s}{\varepsilon^2}\right)^{2n}\right)$. Remarkably, restricting to the pure state case, we prove that $\tilde{\Theta}\left(\left(\frac{N_s}{\varepsilon^2}\right)^n\right)$ samples are necessary and sufficient for pure state tomography.

- *Gaussian states.* We prove that tomography of (energy-constrained) Gaussian states is efficient, as there exists a tomography algorithm whose sample and time complexity scales polynomially in the number of modes. Notably, our result demonstrates that Gaussian states can be efficiently learned by estimating the first moment and the covariance matrix, a result that has been previously assumed but never rigorously proved in the literature. To conduct the complexity analysis, we investigate the following fundamental question, which is of independent interest for the field of Gaussian quantum information: if we approximate the first moment and covariance matrix of an unknown Gaussian state with precision ε, what is the resulting trace distance error on the state? In our work, we answer this question by finding an upper bound on the trace distance between two Gaussian states in terms of the distance between their first moments and their covariance matrices.

* {francesco.mele, vittorio.giovannetti, salvatore.oliviero}@sns.it
† {a.mele, l.bittel, lorenzo.leone}@fu-berlin.de
‡ {jenseisert, ludovico.lami}@gmail.com

- *t-doped Gaussian states.* t-doped Gaussian states are n-mode pure states prepared by applying Gaussian unitaries and at most t non-Gaussian κ-mode unitaries on the vacuum state. We prove that, if $2\kappa t \le n$, one can turn any t-doped state into a tensor product between a $2\kappa t$-mode non-Gaussian state and the $(n-2\kappa t)$-mode vacuum state, via a suitable Gaussian unitary. By leveraging such a decomposition, we devise a tomography algorithm which has a sample and time complexity that scales polynomially in n as long as $\kappa t = O(1)$, thereby establishing that tomography of (energy-constrained) t-doped states is efficient in this regime. This establishes the robustness of tomography of Gaussian states, in the sense that, even if few non-Gaussian unitaries are applied to a Gaussian state, the resulting state remains efficiently learnable. Our results on t-doped bosonic states are derived by extending to the bosonic setting some results on t-doped fermionic states of an ongoing parallel work [?]. However, extending these results is far from trivial, since in the bosonic setting one must deal with the subtleties arising from the energy constraints and from the infinite-dimensional Hilbert space.

With these results, our work significantly advances also the field of Quantum Learning Theory [11].

II. Tomography of energy-constrained states

For a system of n qudits with local dimension d, the minimum number of samples required to achieve quantum state tomography with precision ε in trace distance scales as $\tilde\Theta\left(\frac{d^{2n}}{\varepsilon^2}\right)$ [12–14], which is exponential in the number of qudits. We generalize this result to energy-constrained CV systems.

Theorem 1 ((Informal version))**.** *Let us consider an unknown n-mode state ρ satisfying the k-th moment constraint $(\mathrm{Tr}\left[\hat N_n^k\rho\right])^{1/k} \le nN_s$, where $\hat N_n$ is the total photon number operator. The number of samples required to achieve quantum state tomography with precision ε in trace distance has to scale at least as $\tilde\Omega\left(\left(\frac{N_s}{\varepsilon^{2/k}}\right)^n\right)$. Moreover, there exists a tomography algorithm for possibly mixed states with sample complexity that scales as $O\left(\left(\frac{N_s}{\varepsilon^{2/k}}\right)^{2n}\right)$. Notably, if we assume the unknown state to be pure, then $\tilde\Theta\left(\left(\frac{N_s}{\varepsilon^{2/k}}\right)^n\right)$ samples are necessary and sufficient for tomography.*

Proof ideas. The proof of the lower bound on the sample complexity involves ε-net techniques [15–18]. For the upper bound, we devise an explicit algorithm consisting of two main steps: first, performing a two-outcome measurement to project onto a suitable finite dimensional space with a fixed maximum photon number, and, second, applying known tomography algorithms for qudits.

We note that the CV classical shadow algorithm proposed in [19], primarily designed for estimating expectation values, effectively offers an alternative tomography algorithm. However, its sample complexity scales as $O\left(\left(\frac{n^2N_s^2}{\varepsilon^{2/k}}\right)^{2n}\right)$, which, being super-exponential in n, is much worse than the scaling $O\left(\left(\frac{N_s}{\varepsilon^{2/k}}\right)^{2n}\right)$ of our algorithm. Regarding the CV classical shadow algorithm proposed in [20], it provides guarantees in terms of the operator norm rather than the trace distance, making it unsuitable for quantum state tomography.

III. Tomography of Gaussian states

It is well established that: "In order to *know* a Gaussian state it is sufficient to *know* its first moment and its covariance matrix". However, in practice, we never know the first moment and the covariance matrix *exactly*, but we can only have estimates of them, meaning that we can only approximately know the Gaussian state. It is thus a fundamental problem – yet never tackled before – of Gaussian quantum information to determine what is the error incurred in trace distance when estimating the first moment and covariance matrix of an unknown Gaussian state up to a precision ε. The forthcoming Theorem 2 addresses this problem. One might be inclined to believe that there is a simple approach to solving this problem, involving first bounding the trace distance in terms of fidelity and then employing the known formula for fidelity between Gaussian states [21]. While this approach may seem promising at first glance, it ultimately fails because the expressions involved in the fidelity formula are too complicated to allow for the derivation of a simple bound in terms of the distance between the first moments and the covariance matrices.

Theorem 2. *Let ρ_1 and ρ_2 be Gaussian states with mean total photon number upper bounded by N_s, i.e. it holds that $\mathrm{Tr}\left[\rho_1\,\hat N_n\right] \le N_s$ and $\mathrm{Tr}\left[\rho_2\,\hat N_n\right] \le N_s$. The trace distance between ρ_1 and ρ_2 can be upper bounded as*

$$\frac{1}{2}\|\rho_1-\rho_2\|_1 \le \sqrt{2(N_s+1)}\left(\|m_1-m_2\|_2+\sqrt{2}\sqrt{\|V_1-V_2\|_1}\right),$$

where m_1 and m_2 are the first moments and V_1 and V_2 are the covariance matrices of ρ_1 and ρ_2, respectively. Here, $\|\cdot\|_1$ and $\|\cdot\|_2$ denote the trace norm and the 2-norm.

Proof tools. We use non-standard properties of the Gaussian channel $\mathcal{N}_K$ that acts on the covariance matrices as $V \mapsto V+K$ and leaves the first moments unchanged, where K is a fixed positive semi-definite matrix. Specifically, leveraging results from [22], we prove that the *energy-constrained* diamond distance [23?] between N_K and the identity satisfies $\frac{1}{2}\|\mathcal{N}_K-\mathrm{Id}\|_{\diamond N_s} \le \sqrt{2(N_s+1)}\sqrt{\mathrm{Tr}\,K}$, which constitutes a new technical tool.

Theorem 2, which we regard as a significant technical contributions, establishes that an ε-estimate of the first moment and of the covariance matrix of a Gaussian state leads an $\sqrt{\varepsilon}$-estimate of the state in trace distance. Moreover, Theorem 2 allows us to analyse the sample complexity of tomography of Gaussian states.

Theorem 3 ((Informal version))**.** *Let ρ be an unknown n-mode Gaussian state with mean energy per mode upper bounded by E, i.e.* $\mathrm{Tr}\left[\rho\hat{E}_n\right] \leq nE$ *where* $\hat{E}_n := \sum_{i=1}^{n}\left(\frac{\hat{x}_i^2}{2}+\frac{\hat{p}_i^2}{2}\right) = \hat{N}_n + \frac{n}{2}\mathbb{1}$ *is the energy operator. For any* $\varepsilon, \delta \in (0,1)$, *a number* $O\left(\frac{n^7E^4}{\varepsilon^4}\log\left(\frac{n^2}{\delta}\right)\right)$ *of copies of* ρ *suffices to construct a classical description of a Gaussian state estimator* $\tilde{\rho}$ *such that* $\frac{1}{2}\|\tilde{\rho}-\rho\|_1 \leq \varepsilon$ *with probability at least* $1-\delta$.

Proof ideas. The key step of the proof involves applying Theorem 2. Moreover, note that to obtain rigorous performance guarantees on the estimate of the covariance matrix, we need to establish an upper bound on the second moment of the energy. We do this by proving that any Gaussian state ρ satisfies $\mathrm{Tr}\left[\rho\hat{E}_n^2\right] \leq 3(\mathrm{Tr}\left[\rho\hat{E}_n\right])^2$, which constitutes a new technical tool.

We can improve the trace distance bound in Theorem 2 if we assume one of the states, say ρ_1, to be a pure Gaussian state (interestingly, such an improved bound holds even if ρ_2 is not Gaussian). By exploiting this improved bound, we can show that $O\left(\frac{n^5E^3}{\varepsilon^4}\log\left(\frac{n^2}{\delta}\right)\right)$ samples suffices to achieve tomography of pure Gaussian states.

Tomography of t-doped Gaussian states.— An n-mode unitary U_t is said to be a t-doped Gaussian unitary *if it is a composition of Gaussian unitaries and at most t non-Gaussian κ-mode unitaries. In other words, U_t is of the form $U_t = G_tW_t\cdots G_1W_1G_0$, where each G_i is an n-mode Gaussian unitary and W_i is a κ-mode non-Gaussian unitary. Strictly speaking, we assume each W_i to be a unitary generated by an Hamiltonian which is a (non-quadratic) polynomial in the quadratures of at most κ modes. An n-mode state $|\psi\rangle$ is said to be a* t-doped Gaussian state *if it can be prepared by applying a t-doped Gaussian unitary to the vacuum: $|\psi\rangle = U_t\,|0\rangle^{\otimes n}$. Remarkably, the following decomposition of t-doped unitaries and states hold.*

Theorem 4 ((Non-Gaussianity compression in t-doped Gaussian unitaries and states))**.** *If $n \geq 2\kappa t$, any t-doped Gaussian unitary U_t can be decomposed as $U_t = G(u_{2\kappa t}\otimes\mathbb{1}_{n-2\kappa t})G_{passive}$, for some suitable Gaussian unitary G, passive Gaussian unitary $G_{passive}$, and $2\kappa t$-mode (non-Gaussian) unitary $u_{2\kappa t}$. In particular, any t-doped Gaussian state can be decomposed as*

$$|\psi\rangle = G\left(|\phi_{2\kappa t}\rangle \otimes |0\rangle^{\otimes(n-2\kappa t)}\right) \tag{1}$$

for some suitable Gaussian unitary G and $2\kappa t$-mode (non-Gaussian) state $|\phi_{2\kappa t}\rangle$.

Theorem 4 establishes that it is possible to compress all the non-Gaussianity of a t-doped Gaussian state via a suitable Gaussian unitary. By leveraging the decomposition in (1)*, we can design a tomography algorithm for t-doped Gaussian states, whose performance are analysed in the Theorem 5 below. The idea behind our algorithm involves first estimating the Gaussian unitary G, then applying its inverse to the state in order to compress the non-Gaussianity, and finally performing the tomography algorithm mentioned in Theorem 1 over the first $2\kappa t$ modes.*

Theorem 5 ((Informal version))**.** *Let $|\psi\rangle$ be an unknown n-mode t-doped Gaussian state with second moment of the energy per mode upper bounded by E_2, i.e.* $\sqrt{\mathrm{Tr}\left[\rho\hat{E}_n^2\right]} \leq nE_2$. *For any $\varepsilon, \delta \in (0,1)$, a number* $O\left(\left(\frac{n^2(E_2)^2}{\varepsilon^2}\right)^{\kappa t}\right)$ *of copies of $|\psi\rangle$ suffices to construct a classical description of an estimator* $\left|\tilde{\psi}\right\rangle$ *such that* $\frac{1}{2}\left\|\left|\tilde{\psi}\middle\rangle\!\middle\langle\tilde{\psi}\right| - |\psi\rangle\!\langle\psi|\right\|_1 \leq \varepsilon$ *with probability at least* $1-\delta$.

Proof tools. *We exploit concentration inequalities typically used in statistical learning theory. Moreover, we employ a variety of established tools in Gaussian quantum information while also introducing novel tools. For instance, we utilise the known perturbation bound on symplectic eigenvalues of covariance matrices established by [24]. As an example of novel tool, we introduce the inequality* $E\left(U_S\rho U_S^\dagger\right) \leq \|S\|_\infty^2 E(\rho)$, *where* $E(\rho) := \mathrm{Tr}\left[\rho\hat{E}_n\right]$ *is the mean energy of ρ, U_S is the Gaussian unitary associated with a symplectic matrix S, and $\|\cdot\|_\infty$ is the operator norm.*

Theorem 5 implies that tomography of t-doped Gaussian states is efficient in the regime $\kappa t = O(1)$, as its sample, time, and memory complexity scales polynomially in n.

Conclusions.— Our work serves as bridge between the two fields of quantum learning theory and CV quantum information. We provide the first investigation of tomography of continuous variable systems with rigorous performance guarantees in terms of the trace distance. We first investigate moment-constrained states, by showing both lower and upper bounds on the sample complexity of tomography. Remarkably, we identify the optimal sample complexity for tomography of moment-constrained pure states. Second, we rigorously prove that tomography of Gaussian states is efficient. To achieve this, in Theorem 2 we introduce an upper bound on the trace distance between Gaussian states in terms of the distance between their first moments and their covariance matrices, which constitutes a technical tool of independent interest for the community of continuous variable quantum information. Finally, we analyse t-doped Gaussian states, demonstrating a valuable decomposition in Theorem 4, which guides the development of an apt tomography algorithm.

[1] Francesco Anna Mele, Antonio Anna Mele, Lennart Bittel, Jens Eisert, Vittorio Giovannetti, Ludovico Lami, Lorenzo Leone, and Salvatore F. E. Oliviero. Learning quantum states of continuous variable systems, 2024.

[2] Alessio Serafini. *Quantum continuous variables: A primer of theoretical methods.* CRC Press, Taylor & Francis Group, Boca Raton, USA, 2017.

[3] Chris Weedbrook, Stefano Pirandola, Raul García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, 2012.

[4] Jens Eisert and Martin B. Plenio. Introduction to the basics of entanglement theory in continuous-variable systems. *Int. J. Quant. Inf.*, 1:479, 2003.

[5] Daniel T. Smithey, Mark Beck, Michael G. Raymer, and Adel Faridani. Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum. *Phys. Rev. Lett.*, 70(9):1244–1247, 1993.

[6] Ulf Leonhardt and Harry Paul. Measuring the quantum state of light. *Progr. Quant. Electr.*, 19(2):89–130, 1995.

[7] Matteo Paris and Jaroslav Řeháček, editors. *Quantum state estimation*, volume 649 of *Lecture Notes in Physics*. Springer, Berlin, Heidelberg, 2004.

[8] Alex I. Lvovsky and Michael G. Raymer. Continuous-variable optical quantum-state tomography. *Rev. Mod. Phys.*, 81(1):299–332, 2009.

[9] C. W. Helstrom. *Quantum detection and estimation theory.* Academic press, New York, USA, 1976.

[10] A. S. Holevo. Investigations in the general theory of statistical decisions. *Trudy Mat. Inst. Steklov*, 124:3–140, 1976. (English translation: Proc. Steklov Inst. Math. 124:1–140, 1978).

[11] Anurag Anshu and Srinivasan Arunachalam. A survey on the complexity of learning quantum states. *Nature Rev. Phys.*, 6(1):59–69, 2024.

[12] Ryan O'Donnell and John Wright. Efficient quantum tomography, 2015.

[13] Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. *IEEE Trans. Inf. Th.*, 2017.

[14] Richard Kueng, Holger Rauhut, and Ulrich Terstiege. Low rank matrix recovery from rank one measurements, 2014.

[15] Roman Vershynin. High-dimensional probability. 2019.

[16] Jeongwan Haah, Robin Kothari, and Ewin Tang. Optimal learning of quantum Hamiltonians from high-temperature Gibbs states, 2021.

[17] Haimeng Zhao, Laura Lewis, Ishaan Kannan, Yihui Quek, Hsin-Yuan Huang, and Matthias C. Caro. Learning quantum states and unitaries of bounded gate complexity, 2023.

[18] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Information-theoretic bounds on quantum advantage in machine learning. *Phys. Rev. Lett.*, 126(19), 2021.

[19] S. Becker, N. Datta, L. Lami, and C. Rouzé. Classical shadow tomography for continuous variables quantum systems. *IEEE Trans. Inf. Theory*, 70(5):3427–3452, 2024.

[20] Srilekha Gandhari, Victor V. Albert, Thomas Gerrits, Jacob M. Taylor, and Michael J. Gullans. Precision bounds on continuous-variable state tomography using classical shadows, 2023.

[21] Leonardo Banchi, Samuel L. Braunstein, and Stefano Pirandola. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.*, 115(26):260501, 2015.

[22] Simon Becker, Nilanjana Datta, Ludovico Lami, and Cambyse Rouzé. Energy-constrained discrimination of unitaries, quantum speed limits and a Gaussian Solovay–Kitaev theorem. *Phys. Rev. Lett.*, 126:190504, 2021.

[23] Maxim E. Shirokov. On the energy-constrained diamond norm and its application in quantum information theory. *Probl. Inf. Transm.*, 54(1):20–33, 2018.

[24] Martin Idel, Sebastián Soto Gaona, and Michael M. Wolf. Perturbation bounds for Williamson's symplectic normal form. *Lin. Alg. Appl.*, 525:45–58, 2017.

Virtual Channel Purification

Zhenhuan Liu, Xingjian Zhang, Yue-Yang Fei, and Zhenyu Cai

The full version of this paper can be found at arXiv:2402.07866.

Introduction–Despite the rapid advances in quantum hardware in recent years, there is still an extended stretch of time ahead before we can successfully implement quantum error correction (QEC) to achieve fully fault-tolerant computation. In order to reach practical quantum advantages during this time, it is essential to develop noise suppression techniques compatible with existing quantum technologies. One key method is quantum error mitigation (QEM) [1], which can extract target information from noisy quantum circuits without physically recovering the noiseless quantum state. Due to the low hardware requirement, QEM has become a prevailing tool in many quantum computation experiments [2–4] and is expected to play a key role also in the early fault-tolerant era.

Over the years, various QEM protocols have been proposed, but each comes with its own sets of assumptions. Probabilistic error cancellation [5, 6] relies on detailed knowledge about the noise models and the assumption that the noise remains the same across different times and different qubits. Zero-noise extrapolation [5, 7] requires the ability to tune hardware noise without significantly modifying the noise model and it can only offer rigorous performance guarantee at small noise. Virtual state purification [8, 9] requires the ideal input and output state to be pure states and also the noiseless component to be the dominant component of the noisy output state. Symmetry verification [10, 11] require problem-specific knowledge about the symmetry or energy constraints on the output state.

In this article, we introduce a QEM technique called *virtual channel purification* that *removes all of the assumptions above*, i.e. it is the first QEM protocol that imposes no requirements on specific knowledge about the gate error models, the incoming and output state, and the problem we try to solve; does not require additional hardware capability beyond gate-model computation; while still offers rigorous performance guarantee for the most practical noise regime. The only assumption it makes is that the noise in the ideal unitary operation is incoherent, which is the case for most practical scenarios [12, 13], especially with the help of Pauli twirling [14–17].

Protocol–Virtual channel purification (VCP) is obtained by combining ideas from virtual state purification (VSP), Choi–Jamiołkowski isomorphism, and the circuit for flag fault-tolerance [18]. Just like how VSP uses M copies of a noisy state to virtually prepare a purified output state whose infidelity falls exponentially with M, VCP is able to use M copies of a noisy *channel* $\mathcal{U}_{\mathcal{E}} = \mathcal{E}\mathcal{U}$ with $\mathcal{E} = p_0\mathcal{I} + \sum_{i=1}^{4^N-1} p_i\mathcal{E}_i$ to virtually implement a purified channel $\mathcal{U}_{\mathcal{E}^{(M)}} = \mathcal{E}^{(M)}\mathcal{U}$ with

$$\mathcal{E}^{(M)} = \frac{1}{\sum_{i=0}^{4^N-1} p_i^M}\left(p_0^M\mathcal{I} + \sum_{i=1}^{4^N-1} p_i^M\mathcal{E}_i\right) \tag{1}$$

whose infidelity falls exponentially with M. As shown in Fig. 1(a) and (c), the circuit implementation costs of VSP and VCP are similar, but VCP removes many assumptions of VSP as mentioned and provides much stronger error suppression power, extending the applicability of such methods into deeper and noisier circuits.

Performance– Compared to its state counterpart, virtual state purification (VSP), VCP can suppress global noise exponentially stronger in the number of qubits due to the larger dimensionality of channels compared to states, as shown in Fig. 2(c). While VSP requires the ideal output state to be a pure state, VCP places no such restrictions as it directly purifies the noisy channel and thus can be applied to any input state. Furthermore, while VSP can only be applied to the entire quantum circuit as a whole, VCP can be applied in a layer-by-layer manner or even target specific gates in the circuits, as demonstrated in Fig. 1(f)-(h). This provides flexibility and, more importantly, removes the restriction in VSP that the noiseless component must be the dominant component for the noisy circuit output. In this way, VCP is applicable to much deeper and noisier circuits than VSP.

When considering the practical implementation of VCP, the single-layer variant only requires one additional layer of CSWAPs compared to VSP. Furthermore, the noise of this additional layer of CSWAP is naturally mitigated by VCP itself. We have seen in Fig. 2(d) that the errors due to CSWAPs are essentially the same for both VCP and VSP. Hence, single-layer VCP is almost always preferred over VSP due to its stronger noise suppression power at a similar implementation error cost. We can further optimise the number of VCP layers to outperform the single-layer variant. In numerical simulation across a range of circuit depths and gate error rates, optimal-layer VCP always outperform VSP and can offer up to 4 times more error suppression, shown in Fig. 2(e)-(g). The advantage is expected to be even stronger using more copies of noise channels and more qubits.

Applications in Quantum Networks– Using the same circuit as VCP, but performing post-selection on the

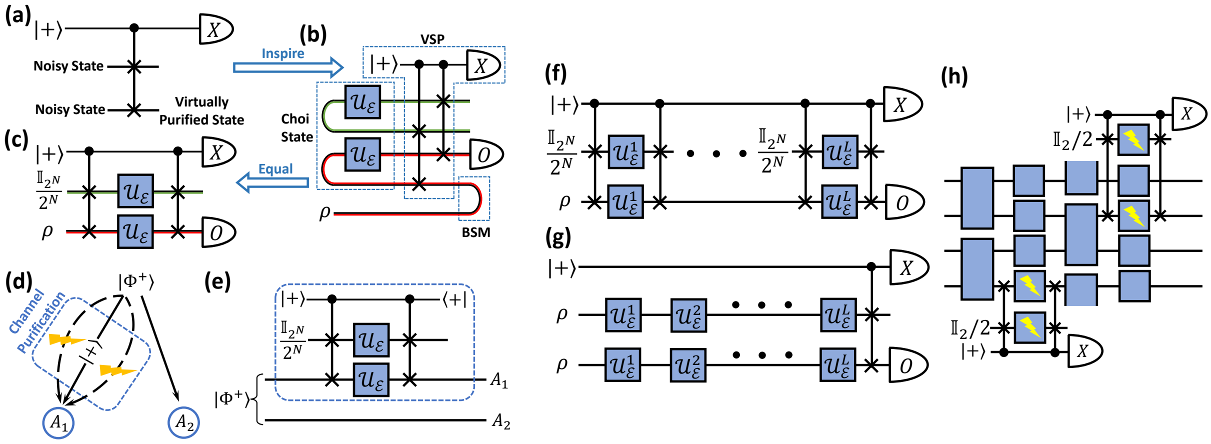

(a)
$|+\rangle$
X
Noisy State
Noisy State
Virtually Purified State
(b)
VSP
Inspire
$|+\rangle$
X
Choi State
$\mathcal{U}_\mathcal{E}$
$\mathcal{U}_\mathcal{E}$
O
Equal
ρ
BSM
(c)
$|+\rangle$
X
$\frac{\mathbb{I}_{2^N}}{2^N}$
$\mathcal{U}_\mathcal{E}$
ρ
$\mathcal{U}_\mathcal{E}$
O
(d)
Channel Purification
$|\Phi^+\rangle$
A_1
A_2
(e)
$|+\rangle$
$\langle+|$
$\frac{\mathbb{I}_{2^N}}{2^N}$
$\mathcal{U}_\mathcal{E}$
$\mathcal{U}_\mathcal{E}$
$|\Phi^+\rangle$
A_1
A_2
(f)
$|+\rangle$
X
$\frac{\mathbb{I}_{2^N}}{2^N}$
$\mathcal{U}_\mathcal{E}^1$
$\mathcal{U}_\mathcal{E}^L$
ρ
$\mathcal{U}_\mathcal{E}^1$
$\mathcal{U}_\mathcal{E}^L$
O
(g)
$|+\rangle$
X
ρ
$\mathcal{U}_\mathcal{E}^1$
$\mathcal{U}_\mathcal{E}^2$
$\mathcal{U}_\mathcal{E}^L$
ρ
$\mathcal{U}_\mathcal{E}^1$
$\mathcal{U}_\mathcal{E}^2$
$\mathcal{U}_\mathcal{E}^L$
O
(h)
$|+\rangle$
X
$\mathbb{I}_2/2$
$\mathbb{I}_2/2$
$|+\rangle$
X

FIG. 1. (a)-(c)The logic for constructing VCP circuit, taking $M = 2$ without loss of generality. (a) The circuit for VSP, consists of two copies of the noisy input state, a single control qubit initialised as $|+\rangle$, and a CSWAP gate. By measuring the control qubit in Pauli-X basis, one can virtually prepare the purified state on the second register. (b) One possible circuit implementation of VCP, obtained from performing the VSP circuit in (a) on two copies of Choi states of the noisy channel. Each curved line at the input end stands for a $2N$-qubit maximally entangled state $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2^N}}\sum_{i=0}^{2^N-1}|ii\rangle$, which is used to prepare the Choi state of the noisy channel $\mathcal{U}_\mathcal{E}$. Then, the VSP circuit acts on two noisy Choi states to virtually obtain a purified Choi state. The curved line at the output end stands for Bell state measurement (BSM) post-selected on the all-zero result, which is for implementing the purified channel using the purified Choi state. (c) A circuit implementation of VCP, obtained from straightening the curved lines in green and red in (b). By measuring the control qubit in Pauli-X basis, one can virtually implement the purified channel on the second register. This circuit is easily generalised to a larger value of M by employing $M-1$ copies of maximally mixed state and changing SWAP to the Mth order permutation. (d) Application of channel purification in entanglement distribution. Blue circles represent two users and $\left|\Phi^+\right\rangle$ is the entangled state that is distributed. (e) The circuit for channel purification. Compared to the VCP circuit, we post-select on the measurement results of the control qubit and keep only the $|+\rangle$ outcome. The dashed blue box corresponds to the purification process in (d). (f)-(h) Comparison between VSP and VCP with $M = 2$. (f) For a quantum circuit with depth D, VCP protocol can be applied layer-by-layer. (g) VSP protocol can only be performed once at the end of the quantum circuit with one control qubit and two identical copies. (h) VCP can target specific noisy gates in the quantum circuit.

controlled qubit measurement results instead of post-processing, as shown in Fig. 1(e), we can physically (instead of virtually) obtain a purified channel, which can then be applied to many tasks in quantum networks. As shown in Fig. 1(d), in entanglement distribution, compared to previous works based on entanglement purification, our channel purification protocol does not require multipartite joint operations and multiple identical copies of the distributed states for local quantum noises. Furthermore, with a single clean channel to transmit a single clean qubit, our protocol can purify noisy channels with arbitrarily large dimensions and enable the activation of valuable quantum resources. The fact that our protocol is applicable to arbitrary incoming states and arbitrary incoherent noise also opens up the door for many other possible applications in communication.

Connection with QEC– Due to the key roles we expect QEC and QEM to both play in practical quantum computation, there is always a strong desire to develop a framework that combines the two. So far the attempts are mostly about concatenating QEM on top of QEC [19–21]. Through further generalisation of VCP and the use of the Knill-Laflamme condition [22], we are able to obtain one of the first integrated protocols that combine QEM and QEC beyond concatenation. In this protocol, by paying the same sampling cost as channel purification using two copies, we are able to *remove all noise* in the noisy channel, reaching beyond the standard bias-variance trade-off limit in pure QEM [1].

In the standard configuration of VCP, the additional copies of the noisy channels are acting on a maximally mixed input state at the ancillary registers. Using the Knill-Laflamme condition, we show that we can also perform purification using a quantum error correction (QEC) code state as the ancillary input state. Furthermore, if we are able to perform stabiliser checks on the ancillary register at the end of the circuit and post-select, we can remove *all noise* from the main register using just two copies of the noise channel. This comes with a higher sampling cost following the usual bias-variance trade-off in QEM. Now instead of post-selecting on the stabiliser check results of the ancillary register, if we perform correction on the *main register* based on these check results, we can actually remove *all noise* from the main register while paying only the sampling cost of the second-order VCP. This provides one of

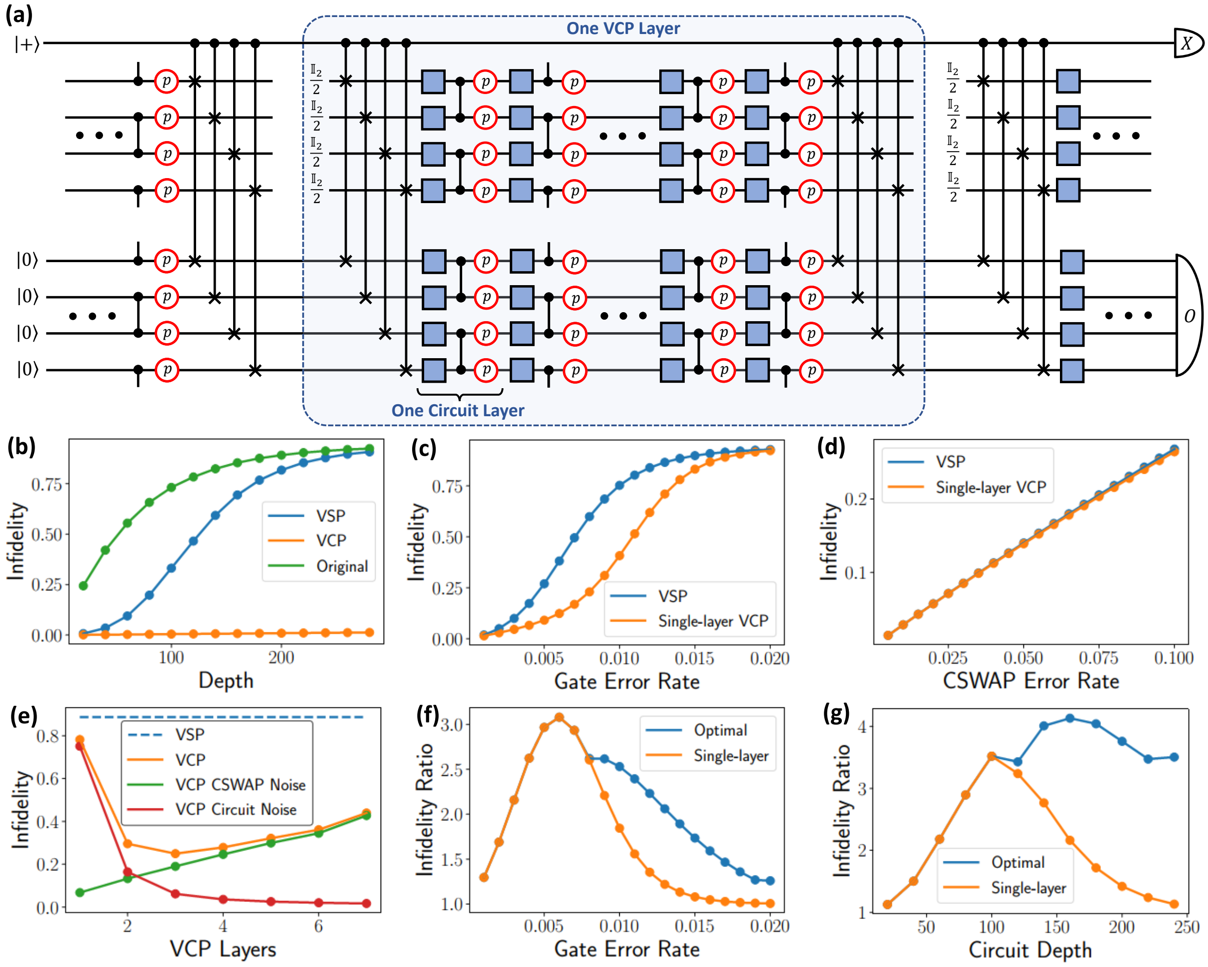


FIG. 2. (a) The circuit for our numerical simulation with VCP applied. The main circuit is a four-qubit system initialised in the all-0 state evolving through a random circuit consisting of alternating layers of random single-qubit gates (blue boxes) and CNOT gates (two dots connected by a vertical line). The CNOT gates are affected by two single-qubit depolarising channels each with an error rate p (red circles). The whole circuit is divided into L VCP layers to perform the circuit shown in 1(f). In all numerical tests besides (b), every CSWAP gate is followed by three single-qubit depolarising channels each with an error rate $5p$. (b) The infidelities after VSP and VCP for different circuit depths *without any CSWAP noise*. The gate error rate is $p = 0.005$ and the depth of each VCP layer is 20. (c) The infidelities after VSP and single-layer VCP at different values of p. The circuit depth is set to be 80. (d) The error rates caused by the CSWAP noise in VSP and single-layer VCP using the same circuit as (c), where we have removed the CNOT noise while keeping only the CSWAP noise. (e) The infidelity behaviour after VCP with different numbers of VCP layers for a circuit with a depth 240 and a gate error rate $p = 0.005$. The green and red lines represent cases without CNOT and CSWAP errors, respectively. (f) The infidelity ratios between VSP and single-layer VCP, and between VSP and VCP with the optimal number of VCP layers, at different gate noise rates with a circuit depth of 80. (g) The infidelity ratios at different circuit depths with a fixed gate error rate of $p = 0.005$.

the first frameworks that seamlessly combines QEM and QEC beyond the concatenation of QEC and QEM [19–21].

Outlook– Due to the presence of the controlled permutation operator at the beginning of the circuit which is coherently connected to the controlled permutation operator at the end, VCP actually lies outside the QEM frameworks presented for the discussion of the fundamental limits of QEM [23–25]. Hence, hopefully VCP can inspire a new range of QEM protocols outside these frameworks, like the combination with symmetry verification. One can also develop more general frameworks of QEM that incorporate VCP, which may have more desirable properties compared to the previous QEM framework. One promising way to do this is by finding deeper connections to QEC. It will also be interesting to search for other QEM methods that can be naturally merged with QEC beyond concatenation, similar to what we have done. This can be the start of a more general error suppression framework that naturally incorporates both QEM and QEC.

[1] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, Quantum error mitigation, Rev. Mod. Phys. **95**, 045005 (2023).

[2] Google Quantum AI and Collaborators, Hartree-Fock on a superconducting qubit quantum computer, Science **369**, 1084 (2020).

[3] Google Quantum AI and Collaborators, Formation of robust bound states of interacting microwave photons, Nature **612**, 240 (2022).

[4] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. van den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme, and A. Kandala, Evidence for the utility of quantum computing before fault tolerance, Nature **618**, 500 (2023).

[5] K. Temme, S. Bravyi, and J. M. Gambetta, Error Mitigation for Short-Depth Quantum Circuits, Phys. Rev. Lett. **119**, 180509 (2017).

[6] S. Endo, S. C. Benjamin, and Y. Li, Practical Quantum Error Mitigation for Near-Future Applications, Phys. Rev. X **8**, 031027 (2018).

[7] Y. Li and S. C. Benjamin, Efficient Variational Quantum Simulator Incorporating Active Error Minimization, Phys. Rev. X **7**, 021050 (2017).

[8] W. J. Huggins, S. McArdle, T. E. O'Brien, J. Lee, N. C. Rubin, S. Boixo, K. B. Whaley, R. Babbush, and J. R. McClean, Virtual Distillation for Quantum Error Mitigation, Phys. Rev. X **11**, 041036 (2021).

[9] B. Koczor, Exponential Error Suppression for Near-Term Quantum Devices, Phys. Rev. X **11**, 031057 (2021).

[10] S. McArdle, X. Yuan, and S. Benjamin, Error-Mitigated Digital Quantum Simulation, Phys. Rev. Lett. **122**, 180501 (2019).

[11] X. Bonet-Monroig, R. Sagastizabal, M. Singh, and T. E. O'Brien, Low-cost error mitigation by symmetry verification, Phys. Rev. A **98**, 062339 (2018).

[12] B. Koczor, The dominant eigenvector of a noisy quantum state, New J. Phys. **23**, 123047 (2021).

[13] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits transform local noise into global white noise, arXiv:2111.14907 [quant-ph] (2021).

[14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).

[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[16] Z. Cai and S. C. Benjamin, Constructing Smaller Pauli Twirling Sets for Arbitrary Error Channels, Sci Rep **9**, 1 (2019).

[17] J. J. Wallman and J. Emerson, Noise tailoring for scalable quantum computation via randomized compiling, Phys. Rev. A **94**, 052325 (2016).

[18] R. Chao and B. W. Reichardt, Quantum Error Correction with Only Two Extra Qubits, Phys. Rev. Lett. **121**, 050502 (2018).

[19] Y. Suzuki, S. Endo, K. Fujii, and Y. Tokunaga, Quantum Error Mitigation as a Universal Error Reduction Technique: Applications from the NISQ to the Fault-Tolerant Quantum Computing Eras, PRX Quantum **3**, 010345 (2022).

[20] M. Lostaglio and A. Ciani, Error Mitigation and Quantum-Assisted Simulation in the Error Corrected Regime, Phys. Rev. Lett. **127**, 200506 (2021).

[21] C. Piveteau, D. Sutter, S. Bravyi, J. M. Gambetta, and K. Temme, Error Mitigation for Universal Gates on Encoded Qubits, Phys. Rev. Lett. **127**, 200505 (2021).

[22] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A **55**, 900 (1997).

[23] R. Takagi, H. Tajima, and M. Gu, Universal Sampling Lower Bounds for Quantum Error Mitigation, Phys. Rev. Lett. **131**, 210602 (2023).

[24] K. Tsubouchi, T. Sagawa, and N. Yoshioka, Universal Cost Bound of Quantum Error Mitigation Based on Quantum Estimation Theory, Phys. Rev. Lett. **131**, 210601 (2023).

[25] Y. Quek, D. S. França, S. Khatri, J. J. Meyer, and J. Eisert, Exponentially tighter bounds on limitations of quantum error mitigation, arXiv:2210.11505 [math-ph, physics:quant-ph] (2022).

Quantum bounds for compiled XOR games and d-outcome CHSH games*

Matilde Baroni[1] † Quoc-Huy Vu[2] ‡ Boris Bourdoncle[3] § Eleni Diamanti[1] ¶
Damian Markham[3] ‖ Ivan Šupić[3] **

[1] *Sorbonne Université, CNRS, LIP6, 4 place Jussieu, 75005 Paris, France*
[2] *Léonard de Vinci Pôle Universitaire, Research Center, Paris-La Défense, France*
[3] *Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France*

Abstract. Nonlocal games play a crucial role in quantum information theory and have numerous applications in certification and cryptographic protocols. Kalai et al. (STOC 2023) introduced a procedure to compile a nonlocal game into a single-prover interactive proof, using a quantum homomorphic encryption scheme, and showed that their compilation method preserves the classical bound of the game. Natarajan and Zhang (FOCS 2023) then showed that the quantum bound is preserved for the specific case of the CHSH game. Extending the proof techniques of Natarajan and Zhang, we show that the compilation procedure of Kalai et al. preserves the quantum bound for two classes of games: XOR games and d-outcome CHSH games. We also establish that, for any pair of qubit measurements, there exists a compiled XOR game such that its near-optimal winning probability serves as a robust self-test for that particular pair of measurements. Finally, we derive computational self-testing of three anticommuting qubit observables, based on the compilation of the nonlocal game corresponding to the so-called elegant Bell inequality.

Keywords: Bell non-locality, quantum cryptography

1 Introduction

Nonlocal games play a crucial role in quantum information theory and have numerous applications in certifications protocols. The first proofs of separation between classical and quantum resources are based on nonlocal games, with the most emblematic example being the Clauser-Horne-Shimony-Holt (CHSH) game [6, 10]. In such games, an honest classical referee has a 1-round classical interaction with 2 or more non-communicating players. They will then evaluate a function of the outputs and the inputs, called predicate, to establish whether to accept or not; the acceptance probability is the score of the game. The difficulty to win does not arise from the complexity of the predicate, but rather from the players' partial information. For some games the maximal score that quantum provers can achieve is strictly higher than any classical strategy, hence they can be used as proofs of quantumness. In addition to its far-reaching foundational interest, Bell nonlocality [9] enjoys a rich array of applications concerned with the certification of quantum resources and cryptographic tasks, such as device-independent quantum key distribution [1, 23, 4], certified randomness [11, 19, 2] and self-testing [17, 22].

The framework of Bell nonlocality however requires at least two non-communicating parties, and the strongest guarantees of information-theoretic security can thus only be achieved if these parties are space-like separated, which turns out to be experimentally very challenging. Moreover, from a pragmatical point of view, if one wants to certify resources on a quantum computer as it is an integral device, spatial separation and the absence of communication cannot be imposed. These are strong motivations to try to relax the constraint of spatial separation, while preserving classical verification of quantum computation.

Cryptography seems to offer a very promising tool: (quantum) homomorphic encryption, which allows to perform computations on encrypted (quantum) data without decrypting them. This could be used to mimic spatial separation by hiding to the single prover the complete knowledge of the inputs, which would otherwise make the game trivial. Kalai *et al.* formalised in [13] the idea of using quantum homomorphic encryption [16, 7] to emulate spatial separation between the nonlocal parties. They propose a procedure to compile every k-players nonlocal game into a single-prover interactive proof of $2k$-rounds, by fixing a sequential structure of the input-output requests and encrypting the first $k-1$ rounds. They then prove: (i) the *completeness* of the procedure, that is, there is an explicit and efficient quantum strategy that achieves the quantum bound of the original nonlocal game; and (ii) its *classical soundness*, that is, no classical prover can outperform the optimal classical bound up to a negligible function in the security parameter, which is the advantage of the classical adversary in the indistinguishability (IND-CPA) security game of the encryption scheme.

However Kalai *et al* do not provide an upper bound to the optimal score of a quantum prover. Indeed [13] uses classical rewinding techniques to show the soundness against classical adversaries, but this is no longer possible against quantum provers. Follow-up works by Natarajan and Zhang [18] and Brakerski *et al.* [8] prove that the quantum bound is preserved in the specific case of the compiled CHSH game. Their proofs heavily relies

*For the full version of this work, see the pdf attached.

†matilde.baroni@lip6.fr

‡quoc.huy.vu@ens.fr

§boris.bourdoncle@gmail.com

¶eleni.diamanti@lip6.fr

‖damian.markham@lip6.fr

**ivan.supic@lip6.fr

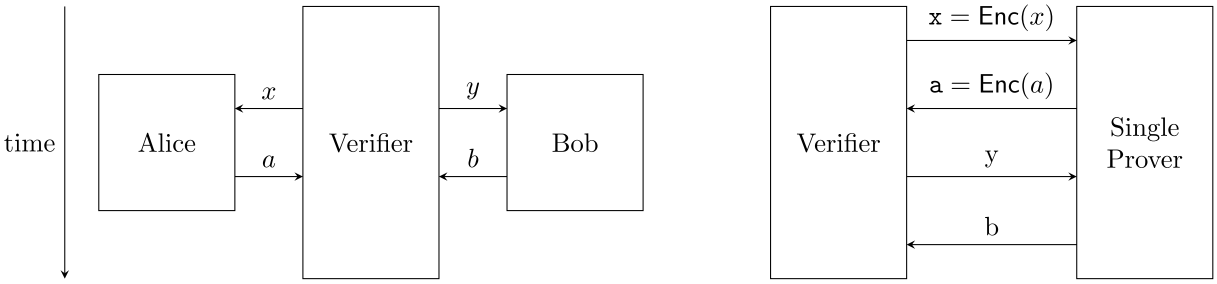

time
Alice
Verifier
Bob
x
a
y
b
Verifier
Single Prover
$\mathsf{x} = \mathsf{Enc}(x)$
$\mathsf{a} = \mathsf{Enc}(a)$
y
b

Figure 1: Pictorial representation of the Kalai *et. al.* compilation protocol for 2-player nonlocal games. On the left, a general 2-player nonlocal game; the two parties are spatially separated, and only communicate to a classical verifier which is sampling questions (x, y) and collecting their answers (a, b). On the right, the single prover game resulting from the compilation procedure. In this representation, time flows downwards.

on specific properties of CHSH, providing little insight on whether Kalai *et al.* compiler preserves the quantum bound for any other nonlocal games.

2 Our Contributions

In this work, we continue this research direction and provide a partial answer for the above open question. In particular, we prove that the quantum bound is preserved for two classes of compiled games: XOR games, where the predicate depends on the logical XOR of the outputs, and d-outcome CHSH games, that generalise the CHSH game to a scenario involving many-output measurements. We also extend our results to self-testing, which relies on the fact that for specific non-local games there is a unique strategy that can achieve the optimal quantum score; then, reaching this bound is a device-independent certification of quantum resources.

The techniques we use are based on the cryptographic SOS decomposition delineated in [18]. The score of a nonlocal game is usually formulated as the expectation value of some function of the observables of the players. This is closely related to the Bell operator $\mathcal{B}$, and its shifted version $\beta\mathbb{1} - \mathcal{B}$, where β is what we call the shift. SOS decomposition - standing for sum of squares - is a method widely used in Bell nonlocality to prove quantum bounds. It consists on mathematically rearranging the terms of the shifted Bell operator as a sum of polynomials squared, whose expectation value is positive semi-definite by definition.

$$\langle\psi|\,\beta\mathbb{1} - \mathcal{B}\,|\psi\rangle = \sum_i \langle\psi|\,P_i^2\,|\psi\rangle \geq 0 \implies \langle\psi|\,\mathcal{B}\,|\psi\rangle \leq \beta$$

Hence the shifted Bell operator is also positive semi-definite, meaning that the shift β is an upper bound for the optimal quantum score. The bound becomes tight if an explicit quantum strategy achieving β is found. If the polynomials appearing in the decomposition are of degree n, then we say we have a nth-order SOS decomposition.

Elaborating on the results of [18], we define a function that maps polynomials of nonlocal observables to correlations observed in the compiled nonlocal game. This function, that we refer to as the pseudo-expectation value map $\tilde{\mathbb{E}}$, allows us to translate the SOS decomposition proof from the nonlocal to the compiled game. For polynomials of observables with a physical interpretation, we intuitively translate the probabilities using some change of variables compatible with the structure of the compiled game; therefore it acts trivially on the identity, and when applied to the Bell functional it gives the score of the compiled game. We call it pseudo-expectation because it is not a positive semi-definite function by definition. In particular, the pseudo-expectation of the polynomials squared from the SOS decomposition is not positive by definition anymore. Nevertheless, we prove that - for specific polynomials - these quantities are positive up to a negligible function in the security parameter κ of the QHE scheme.

Lemma 1 (Informal) *Consider a Bell inequality $\mathcal{B}$ with a SOS decomposition, whose polynomials can be written as $P_i = A_i - \hat{B}_i$, where $\{A_i\}_i$ are Alice's observables and $\{\hat{B}_i\}_i$ are linear sums of Bob's observables. Then there exists a negligible function $\eta_{\mathrm{QHE}}(\cdot)$ such that we have $\tilde{\mathbb{E}}\left[P_i^2\right] \geq -\eta_{\mathrm{QHE}}(\kappa)$.*

Technically, this is done by extending cryptographic arguments based on the security of the encryption scheme. Then, applying the pseudo-expectation map to the nonlocal SOS decomposition, we prove that the quantum bound of the compiled game is preserved up to a negligible function in the security parameter.

$$\begin{aligned}\tilde{\mathbb{E}}[\beta\mathbb{1} - \mathcal{B}] = \sum_i \tilde{\mathbb{E}}[P_i^2] &\geq -\eta_{\mathrm{QHE}}(\kappa) \\ \implies \tilde{\mathbb{E}}[\mathcal{B}] &\leq \beta + \eta_{\mathrm{QHE}}(\kappa)\end{aligned}$$

The pseudo-expectation map is well defined for polynomials of degree 2 in the number of observables, restricting us to work with first-order SOS decompositions. We lack of a meaningful interpretation for polynomials containing two different Alice's observables in the compiled scenario, but we can fix the shape of the SOS polynomials P_i to contain only one observable for Alice for several non-local games of interest.

In particular, in the paper we revise some known results for XOR games, and derive a new result on the decomposition of the shifted game operator. Notably, we prove that it is always possible to have a decomposition with polynomials P_i containing only one Alice's observable. This helps us to prove that the quantum score of all XOR games is preserved by Kalai *et al.* compilation.

Theorem 2 *Given an XOR game with optimal quantum bound β_q, the optimal quantum bound of the compiled XOR game is $\beta_q + \delta_{\mathrm{QHE}}(\kappa)$, where $\delta_{\mathrm{QHE}}(\cdot)$ is a negligible function.*

We also extend the pseudo-expectation map to treat higher dimensional inputs and outputs, hence generalised observables. As an example we apply it to the SATWAP inequality proposed in [20], a generalisation of CHSH for which we know it exists a SOS decomposition in our desired form [21]. We prove that the quantum score of the compiled game is preserved in this case as well. Apart from its mathematical relevance, this could lead to much more efficient certifications.

Theorem 3 *Consider the d-dimensional SATWAP Bell inequality with quantum bound $(\beta_d^{SATWAP})_q$, and its compiled version. If d is polynomial w.r.t. the security parameter κ, then the quantum bound of the compiled SATWAP inequality is $(\beta_d^{SATWAP})_q + \theta(\kappa)$, where $\theta(\cdot)$ is a negligible function.*

The SOS decomposition imposes constraints on the strategies achieving the optimal quantum score; sometimes these constraints are enough to uniquely identify these strategies, leading to self-testing protocols. From the cryptographic SOS decomposition we develop computational self-testing techniques for interactive single prover games, built on top of the nonlocal self-testing proofs. In particular, we focus on two relevant XOR games. In these cases Jordan's lemma applies, and fixing the anti-commutators of the observables is usually enough to have robust self-testing statements [14]. By achieving the optimal quantum score of some compiled XOR games, using classical interaction with a single device we can robustly self test the following resources:

- any pair of binary measurements, from the compilation of the family of Bell inequalities presented in [15, 5, 24];
- triplets of mutually unbiased base (MUB) qubit measurements, from the compilation of the elegant Bell inequality [12, 3].

To conclude, our work aims to bridge topics at the interface between quantum nonlocality, quantum cryptography and quantum complexity theory, proving fruitful combinations between these fields. Our findings reveal that the compilation procedure introduced in [13] effectively preserves the quantum bound of many interesting games, leaving the question of extending this preservation to even more nonlocal games.

References

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[2] A. Acín and L. Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, 2016.

[3] A. Acín, S. Pironio, T. Vértesi, and P. Wittek. Optimal randomness certification from one entangled bit. *Physical Review A*, 93(4), Apr. 2016.

[4] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, 9(1):459, 2018.

[5] V. Barizien, P. Sekatski, and J.-D. Bancal. Custom bell inequalities from formal sums of squares, 2023.

[6] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[7] Z. Brakerski. Quantum FHE (almost) as secure as classical. In *Annual International Cryptology Conference*, pages 67–95. Springer, 2018.

[8] Z. Brakerski, A. Gheorghiu, G. D. Kahanamoku-Meyer, E. Porat, and T. Vidick. Simple tests of quantumness also certify qubits. In H. Handschuh and A. Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 162–191. Springer, 2023.

[9] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014.

[10] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880, 1969.

[11] R. Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation.* PhD thesis, University of Cambridge, 2007.

[12] N. Gisin. *Bell Inequalities: Many Questions, a Few Answers*, pages 125–138. Springer Netherlands, Dordrecht, 2009.

[13] Y. Kalai, A. Lombardi, V. Vaikuntanathan, and L. Yang. Quantum Advantage from Any Non-local Game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1617–1628, 2023.

[14] J. Kaniewski. Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95:062323, Jun 2017.

[15] T. P. Le, C. Meroni, B. Sturmfels, R. F. Werner, and T. Ziegler. Quantum correlations in the minimal scenario. *Quantum*, 7:947, Mar. 2023.

[16] U. Mahadev. Classical Homomorphic Encryption for Quantum Circuits. *SIAM Journal on Computing*, 52(6):FOCS18–189–FOCS18–215, 2023.

[17] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, 2004.

[18] A. Natarajan and T. Zhang. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification, 2023.

[19] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[20] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119:040402, Jul 2017.

[21] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. *npj Quantum Information*, 7(1), Oct. 2021.

[22] I. Šupić and J. Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, Sept. 2020.

[23] U. Vazirani and T. Vidick. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[24] L. Wooltorton, P. Brown, and R. Colbeck. Device-independent quantum key distribution with arbitrarily small nonlocality, 2023.

Quantum bounds for compiled XOR games and d-outcome CHSH games

Matilde Baroni *[1], Quoc-Huy Vu[2], Boris Bourdoncle[3], Eleni Diamanti[1], Damian Markham[1], and Ivan Šupić[1]

[1]Sorbonne Université, CNRS, LIP6, 4 place Jussieu, 75005 Paris, France
{matilde.baroni,eleni.diamanti,damian.markham,ivan.supic}@lip6.fr
[2]Léonard de Vinci Pôle Universitaire, Research Center, Paris-La Défense, France
quoc.huy.vu@ens.fr
[3]Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France
boris.bourdoncle@gmail.com

Abstract

Nonlocal games play a crucial role in quantum information theory and have numerous applications in certification and cryptographic protocols. Kalai et al. (STOC 2023) introduced a procedure to compile a nonlocal game into a single-prover interactive proof, using a quantum homomorphic encryption scheme, and showed that their compilation method preserves the classical bound of the game. Natarajan and Zhang (FOCS 2023) then showed that the quantum bound is preserved for the specific case of the CHSH game. Extending the proof techniques of Natarajan and Zhang, we show that the compilation procedure of Kalai et al. preserves the quantum bound for two classes of games: XOR games and d-outcome CHSH games. We also establish that, for any pair of qubit measurements, there exists an XOR game such that its optimal winning probability serves as a self-test for that particular pair of measurements.

1 Introduction

In quantum information theory, nonlocal games are a class of games that exemplifies the separation between classical and quantum resources. In such games, a referee sends classical inputs to two or more distant parties, and the parties reply with classical outputs. A predicate on the tuples of inputs and outputs defines the winning conditions for the game. In some cases, if the distant parties have access to quantum resources, namely entangled states, they can achieve a score higher than if they only have classical resources. Building on the work of Bell [Bel64], Clauser, Horne, Shimony and Holt introduced the setting for the most famous example of such a game, the CHSH game [CHSH69]. While players with classical resources can only reach a maximal value of 0.75, players sharing entanglement can obtain a value of $\cos^2(\pi/8)$.

In addition to its far-reaching foundational interest, Bell nonlocality [BCP+14] enjoys a rich array of applications concerned with the certification of quantum resources and cryptographic tasks, such as device-independent quantum key distribution [ABG+07, VV14, AFDF+18], certified randomness [Col07, PAM+10, AM16] and self-testing [MY04, ŠB20]. The framework of Bell nonlocality however requires several non-communicating parties, and the strongest guarantees of information-theoretic security can thus only be achieved if these parties are spatially separated. Bell nonlocality is also connected to the powerful notion of multiprover interactive proof systems in quantum complexity theory, MIP*, in which two or more non-communicating provers are allowed to share quantum entanglement. In the classical setting, techniques and results from studying MIP (the classical version of MIP*) usually also find applications in the cryptographic setting, where all parties are computationally bounded, such as the celebrated PCP theorems and succinct arguments. Crucially, a series of works [ABOR00, KRR14] showed that, using a homomorphic encryption scheme, any MIP sound against non-signalling provers can be compiled into a single-prover protocol in which the single prover is computationally bounded and restrained by cryptographic tools.

In the quantum setting, recently, Kalai *et al.* [KLVY23] proposed a general method to compile nonlocal games into single-prover systems based on quantum homomorphic encryption [Mah23, Bra18], and showed that

[*] matilde.baroni@lip6.fr

the classical bound of the compiled game is preserved by their procedure. Follow-up works by Natarajan and Zhang [NZ23] and Brakerski *et al.* [BGK+23] proved that the quantum bound is also preserved in the specific case of the compiled CHSH game. Their works left open the question of whether Kalai *et al.* compiler also preserves the quantum bound for any nonlocal games. In this work, we continue this research direction and provide a partial answer for the above open question. In particular, we prove that the quantum bound is preserved for two classes of compiled games: XOR games, where the predicate depends on the XOR of the outputs, and d-outcome CHSH games, which generalize the CHSH game to the scenario involving many-output measurements.

Nonlocality serves as a tool for exploring certifiable quantum advantage, leading to the development of various quantum certification methods through self-testing, distinguished by their information-theoretic security. Notably, these certification protocols are formulated within the framework of the Bell scenario, designed for scenarios with two or more spatially separated parties. While effective for foundational proofs of quantumness, applying such setups to computing platforms faces challenges due to their incompatibility with Bell-type scenarios. In this context, gaining a deeper understanding of the additional properties of compiled nonlocal games becomes significant, as it holds the promise of translating diverse certification techniques into a single-device setting. However, this translation would come at the cost of exchanging information-theoretic security for computational security.

1.1 Outline of the paper

The paper is structured in the following way. Section 2 is dedicated to preliminary notions. We introduce nonlocal games and Bell inequalities, with a focus on a sub-class: XOR games. For these, in Section 2.3 we revise some known results and derive a new result on the decomposition of the shifted game operator. Then, we introduce quantum homomorphic encryption and Kalai's compilation protocol [KLVY23]. We elaborate on the results of [NZ23], in particular on their idea of defining a pseudo-expectation value that maps polynomials of measurement observables to correlations observed in the compiled nonlocal game.

The second part focuses on those cases for which we can prove that such a pseudo-expectation map can be used to upper bound the optimal quantum winning probabilities in compiled nonlocal games. In Section 3 we use the decomposition introduced in the preliminaries to prove the soundness of the quantum bound for any compiled XOR game. Section 4 generalizes our approach to encompass an inequality with a higher number of outputs. Finally, in section 5 we develop computational self-testing techniques for interactive single prover games, built on top of the nonlocal self-testing proofs. In particular, we show that a certain class of compiled XOR games can be used to self-test any pair of qubit measurements.

1.2 Concurrent and independent work

While finishing this manuscript we became aware of a recent work by Cui *et al.* [CMM+24] who also show that the compilation procedure of Kalai et al. [KLVY23] preserves the quantum bias of all XOR games. Even though both papers use a similar techniques based on [NZ23], [CMM+24] and our work also achieve different results. Their work shows a type of self-testing result for all compiled XOR games, while we explore the self-testing properties of carefully designed compiled XOR games, such that any pair of qubit measurements and tomographically complete sets of qubit measurements can be self-tested from the optimal winning probability. The work of Cui *et al.* explores the compilation of parallelly repeated XOR games and the Magic Square game, while we work with the compiled d-CHSH game which cannot be seen as a parallel repetition of XOR games.

2 Preliminaries

2.1 Nonlocal games and Bell inequalities

In a two-party nonlocal game, a referee randomly selects questions, also called inputs, according to a predetermined distribution and sends them to the non-communicating parties, usually called Alice and Bob. Upon receiving the answers, also called outputs, from Alice and Bob, the referee determines whether they won or lost based on the game rule, which is public. Winning is nontrivial because the players can't communicate during the game: they must generate their output solely based on their respective inputs and potentially a shared resource. $x \in \mathsf{X}$ and $y \in \mathsf{Y}$ denote the questions sent to Alice and Bob, respectively, $a \in \mathsf{A}$ and $b \in \mathsf{B}$ denote their respective answers. $|\cdot|$ denotes the cardinality of a set. The referee samples the questions from a distribution $q(x, y)$, and the game rule is a predicate $V : (a, b, x, y) \mapsto \{0, 1\}$. Alice and Bob define a strategy to answer the questions, based on the resources that they have, and the conditional probabilities of obtaining outputs a and b when inputting x and y, is denoted by $p(a, b|x, y)$. The winning probability of the game is then given by:

$$\omega = \sum_{x,y} q(x,y) V(a,b,x,y) p(a,b|x,y). \tag{1}$$

If Alice and Bob use classical resources, in the most general case they can share a random variable t sampled from a distribution $p(t)$, and they can determine their respective output based on the value of t and the received input. In the context of Bell nonlocality, such strategy corresponds to a local hidden variable model (LHV). In that case, the maximal winning probability is called the classical score of the game. Alice and Bob can always reach the maximal winning probability with deterministic response functions $f(x,t)$, $g(y,t)$ to choose their outputs [Fin82], and the maximal classical score is then equal to:

$$\omega_c = \max_{f,g} \sum_{x,y,t} p(t) q(x,y) V(f(x,t), g(y,t), x, y). \tag{2}$$

If Alice and Bob have access to quantum resources, they can share a quantum state $|\psi\rangle$ and perform quantum measurements on it. For each output, they can perform a different measurement, meaning that Alice has $|\mathsf{X}|$ different measurements, one for each for each x, characterized by $|\mathsf{A}|$ operators $\{M_{a|x}\}_a$, such that:

$$\forall x \in |\mathsf{X}|\,, \forall a \in |\mathsf{A}|\,, M_{a|x} \succeq 0, \tag{3}$$

$$\forall x \in |\mathsf{X}|\,, \sum_a M_{a|x} = \mathbb{1}. \tag{4}$$

Bob's measurements are defined similarly and denoted by $\{N_{b|y}\}_b$. The probability that Alice and Bob get outputs a and b, given inputs x and y is determined by the Born rule $p(a,b|x,y) = \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle$. In that case, the winning probability is equal to:

$$\omega = \sum_{x,y} q(x,y) V(a,b|x,y) \langle\psi|M_{a|x} \otimes N_{b|y}|\psi\rangle. \tag{5}$$

and the maximal quantum score is given by:

$$\omega_q = \max_{\{M_{a|x}\}_x, \{N_{b|y}\}_y, |\psi\rangle} \omega. \tag{6}$$

Note that, more generally, Alice and Bob could have access to a mixed state ρ, but since we don't impose any restriction on the dimension of the underlying Hilbert space, any score reachable with a mixed state can also be reached with a pure state by increasing the dimension of the Hilbert space.

If the players output bits, i.e. $|A| = |B| = \{0,1\}$, the game is said to be binary, and the quantum strategies can be characterised in a simpler way: their measurements are defined by the Hermitian measurement observables

$$A_x = \sum_a (-1)^a M_{a|x}, \qquad B_y = \sum_b (-1)^b N_{b|y}. \tag{7}$$

In the rest of the paper, we use the following notations:

$$|A_x\rangle = A_x|\psi\rangle, \qquad |A\rangle = \sum_x |A_x\rangle \otimes |x\rangle, \tag{8}$$

$$|B_y\rangle = B_y|\psi\rangle, \qquad |B\rangle = \sum_y |B_y\rangle \otimes |y\rangle, \tag{9}$$

which allows us to express the players' correlations through a correlation matrix as:

$$C = \sum_{x,y} c_{xy} |x\rangle\langle y| \qquad \text{with } c_{xy} = \langle A_x|B_y\rangle. \tag{10}$$

Nonlocal games are closely related to Bell inequalities [SMA08, AH12]. A Bell inequality can be defined via a linear form on the space of the conditional distributions $p(a,b|x,y) \in \mathbb{R}^{|A||B||X||Y|}$:

$$\sum_{a,b,x,y} \gamma_{a,b,x,y} p(a,b|x,y) \leq \beta_c, \tag{11}$$

which means that any nonlocal game can be seen as a Bell inequality by taking $\gamma_{a,b,x,y} = q(x,y)V(a,b,x,y)$. Importantly quantum Bell score can be written as $\beta = \langle\psi|\mathcal{B}|\psi\rangle$ where $\mathcal{B}$ is the Bell operator

$$\mathcal{B} = \sum_{a,b,x,y} \gamma_{a,b,x,y} M_{a|x} \otimes N_{b|y} \tag{12}$$

When there is a gap between the maximal classical and quantum scores, the quantum strategies that achieve a score higher than the classical value also violate a Bell inequality. For instance, the quantum state and measurements yielding the maximal value for the CHSH game also yield the maximal quantum value, known as Tsirelson's bound, for the CHSH inequality. In the remainder of this paper, we sometimes switch between the nonlocal game and the Bell inequality formulations. The local bound of a Bell inequality will be denoted with β_c, while the maximal value considering quantum strategy will be denoted as β_q. For a Bell inequality with quantum bound β_q we will often use the shifted Bell operator

$$\beta_q \mathbb{1} - \mathcal{B}, \tag{13}$$

which is by construction positive semi-definite.

2.2 Self-testing

Self-testing is a powerful technique that allows one to certify quantum resources by just looking at the correlations. To be more precise, the correlations $p(a,b|x,y)$ are said to self-test the state and measurements $|\psi'\rangle, \{M'_{a|x}\}, \{N'_{b|y}\}$ if for all states and measurements $\varrho_{\mathrm{AB}}, \{M_{a|x}\}, \{N_{b|y}\}$ compatible with $p(a,b|x,y)$ there exists

(i) local Hilbert spaces $\mathcal{H}_{\mathrm{A}}, \mathcal{H}_{\mathrm{B}}$ such that $\varrho_{\mathrm{AB}} \in \mathcal{L}[\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}]$, $M_{a|x} \in \mathcal{L}[\mathcal{H}_{\mathrm{A}}]$, $N_{b|y} \in \mathcal{L}[\mathcal{H}_{\mathrm{B}}]$

(ii) a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$

such that for any purification $|\psi\rangle^{\mathrm{ABP}}$ of $\varrho^{\mathrm{AB}}_{\mathrm{AB}}$ it holds

$$\begin{aligned}\Phi \otimes \mathbb{I}_{\mathrm{P}} &\left[\mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y} \otimes \mathbb{I}_{\mathrm{P}} |\psi\rangle^{\mathrm{ABP}}\right] \\ &= \left(\mathsf{M}'_{a|x} \otimes \mathsf{N}'_{b|y} |\psi'\rangle^{\mathrm{A'B'}}\right) \otimes |\xi\rangle^{\mathrm{ABP}}\end{aligned}$$

for all a, x, b, y and for some state $|\xi\rangle^{\mathrm{ABP}}$. In this paper, we are especially interested in self-testing of measurements. A compact way of writing the self-testing statement for Bob's measurements from the description given above is that there exists an isometry Φ_B that maps each $M_{b|y}$ to $M'_{b|y} \otimes \mathbb{1}$.

2.2.1 Self-testing binary observables based on anti-commutation

We will be very interested in the self-testing of binary observables, for which some standard techniques have been developed.

A very relevant result is Jordan's lemma [PAB+09]. It states that two hermitian matrices with eigenvalues ±1 can always be simultaneously block-diagonalised, with blocks of size at most 2×2. Effectively this means that the correlations of n binary observables can always be simulated with n projective measurements in the Bloch sphere. Fixing the dimension, and in particular $d = 2$, is a massive simplification to the construction of self-testing protocols.

The characterisation of a set of projective measurements in the Bloch sphere has a simple geometrical intuition. Let's start considering two measurements, but it can be easily generalised to more. We need three coordinates to fix the first measurement, and two angles to define the second one with respect to the first one. Without loss of generalisation for the self-test, we can apply a local unitary to constrain the two observables to be on the XZ-plane of Bloch sphere, and the first one to be exactly σ_X. Hence, one angle is sufficient to characterise two projective measurements up to a global rotation; this unique degree of freedom is encoded in the commutator of the two observables. This is the core idea presented in [Kan17], where the author presents a self-testing protocol of binary observables based on commutation. Using this, they also find better bounds for the robustness of self-testing of some games.

In the following sections we will be often interested in robust self-testing protocols for binary measurements. We will prove that a score which is ϵ close to the quantum bound implies that the anti-commutator is ϵ close to the ideal (noisyless) value

$$\omega = \omega_q - \epsilon \implies D\big|_{|\psi\rangle}(\{B_0, B_1\}, a^{\text{ideal}}\mathbb{1}) \le \eta(\epsilon)$$

for some meaningful distance, restricted to the support of the states used in the game $|\psi\rangle$.

2.3 XOR games

XOR games are a subclass of binary games, in which the winning conditions for each outputs depend only on the parity of the two answer bits, i.e. $V(a,b,x,y)=1$ if and only if $f(x,y)=a\oplus b$. Hence, the winning probability takes the form

$$\omega=\sum_{a,b,x,y} q(x,y)p(a\oplus b=f(x,y)|x,y). \tag{14}$$

The winning probability of an XOR game is connected to its bias

$$\xi=\sum_{x,y} q(x,y)(-1)^{f(x,y)}c_{x,y}, \tag{15}$$

through the relation $\omega=(1+\xi)/2$. The term "bias" comes from the fact that in XOR games, the score $1/2$ can be achieved by players that do not use any resources, but randomly output their bits, independently of the inputs. An XOR game can be characterized by its so-called game matrix Φ:

$$\Phi=\sum_{x,y} q(x,y)(-1)^{f(x,y)}|x\rangle\langle y|. \tag{16}$$

The bias can then be compactly written as $\xi=\operatorname{Tr}\left[C^T\Phi\right]$. We can also define the operator associated to an XOR game as

$$\mathcal{B}=\sum_{x,y} q(x,y)(-1)^{f(x,y)}A_x\otimes B_y, \tag{17}$$

and the bias can then be computed as the value of the Bell operator $\xi=\langle\psi|\mathcal{B}|\psi\rangle$.

Lemma 1 ([Tsi87])**.** *Alice's optimal quantum strategy in an XOR game, encoded in the vector $|A_q\rangle$, is fully determined by Bob's optimal strategy $|B_q\rangle$ through a linear transformation:*

$$|A_q\rangle=\mathbb{1}\otimes F|B_q\rangle. \tag{18}$$

Proof. This lemma was proven by Tsirelson in [Tsi87], but we reproduce here the proof of [ECW20]. The optimal quantum bias of an XOR game can be obtained as the solution to a semidefinite program (SDP) [Weh06]. For that purpose let us define the Gram matrix $\tilde{Q}$

$$\tilde{Q}=\left[\begin{array}{c|c} R & C \\ \hline C^T & S\end{array}\right],\ \text{with } R=\sum_{x,x'}\langle A_x|A_{x'}\rangle|x\rangle\langle x'|,\ \text{and } S=\sum_{y,y'}\langle B_y|B_{y'}\rangle|y\rangle\langle y'|. \tag{19}$$

A Gram matrix is positive semidefinite and the diagonal of the Gram matrix of unit vectors contains only 1. Thus, the SDP yielding the optimal quantum bias for an XOR game takes the form

$$\begin{aligned} \xi_q &= \max_{\tilde{Q}} \operatorname{Tr}\left[\tilde{Q}\tilde{\Phi}\right], \\ \text{s.t.} \quad & \tilde{Q}_{ii}=1, \quad \text{for} \quad i=1,\cdots,|\mathsf{X}|+|\mathsf{Y}|, \\ & \tilde{Q}\succeq 0, \end{aligned} \tag{20}$$

where $\tilde{\Phi}=\frac{1}{2}\begin{pmatrix}0 & \Phi\\ \Phi^T & 0\end{pmatrix}$. From this primal form of the SDP, we can obtain the dual formulation by introducing the Lagrangian $\mathcal{L}=\operatorname{Tr}[\tilde{Q}\tilde{\Phi}]-\frac{1}{2}\sum_i\lambda_i(\operatorname{Tr}\left[|i\rangle\langle i|\tilde{Q}\right]-1)$, where λ_i are nonnegative Lagrangian multipliers. Let us define the diagonal matrix $\Lambda=\operatorname{diag}(\lambda_1,\cdots,\lambda_{|\mathsf{X}|+|\mathsf{Y}|})$. The minimal value of the Lagrangian upper bounds the solution to the primal SDP if $\frac{1}{2}\Lambda-\tilde{\Phi}\succeq 0$, so the dual SDP takes the form

$$\min \operatorname{Tr}\left[\frac{\Lambda}{2}\right], \qquad \text{s.t.} \quad \frac{\Lambda}{2}-\tilde{\Phi}\succeq 0. \tag{21}$$

As a consequence of the aforementioned construction, it can be deduced that any given pair of primal and dual feasible solutions satisfy $\operatorname{Tr}[\tilde{Q}\tilde{\Phi}]\leq\xi_q\leq\operatorname{Tr}[\Lambda]/2$. The optimal values of the primal and of the dual coincide if strong duality holds. A sufficient condition for strong duality to hold, when the primal and dual are finite, is the existence of a strictly feasible solution to the dual problem, which is satisfied here. Hence, the optimal value can be obtained if the complementary slackness condition is satisfied

$$\mathrm{Tr}\left[\tilde{Q}\left(\frac{1}{2}\Lambda - \tilde{\Phi}\right)\right] = 0. \tag{22}$$

Let us now introduce the notations $\Lambda = \Lambda_A \oplus \Lambda_B$, where Λ_A (Λ_B) is a diagonal $|\mathsf{X}| \times |\mathsf{X}|$ ($|\mathsf{Y}| \times |\mathsf{Y}|$) matrix, and $|Q\rangle = |A\rangle \oplus |B\rangle$. We can write the quantum bias as $\xi = \langle Q|\mathbb{1} \otimes \tilde{\Phi}|Q\rangle$. The slackness condition (22) gives $\mathrm{Tr}\left[\mathbb{1} \otimes \left(\frac{1}{2}\Lambda - \tilde{\Phi}\right)|Q\rangle\langle Q|\right] = 0$, or equivalently $\mathbb{1} \otimes (\frac{1}{2}\Lambda - \tilde{\Phi})|Q\rangle = 0$, since $\frac{1}{2}\Lambda - \tilde{\Phi}$ is positive semidefinite. The form of Λ and $\tilde{\Phi}$ implies the following conditions for the optimal strategies of Alice and Bob:

$$\mathbb{1} \otimes \Lambda_A|A_q\rangle = \mathbb{1} \otimes \Phi|B_q\rangle, \quad \text{and} \quad \mathbb{1} \otimes \Lambda_B|B_q\rangle = \mathbb{1} \otimes \Phi^T|A_q\rangle. \tag{23}$$

Taking $F = \Lambda_A^{-1}\Phi$ gives the desired result. □

Another convenient way to write the relations obtained above is

$$|A_x\rangle = \lambda_x^{-1}\sum_{y=1}^{m_B}\Phi_{xy}|B_y\rangle, \qquad \text{for } x = 1, \cdots, |\mathsf{X}|\,. \tag{24}$$

The matrix $\tilde{Q}$ can be seen as a moment matrix corresponding to the first level of Navascues-Pironio-Acín hierarchy (NPA) [NPA07]. The n-th level NPA moment matrix is obtained by defining all degree-n monomials S_i of the operators of the set $\{A_1, \cdots, A_{|\mathsf{X}|}, B_1, \cdots, B_{|\mathsf{Y}|}\}$ and taking $\tilde{Q}^{(n)} = \langle\psi|S_i^\dagger S_j|\psi\rangle|i\rangle\langle j|$. Upper bounds on the maximal quantum score of an arbitrary nonlocal game can be obtained as solutions to an SDP analogous to (20), but taking $\tilde{Q}^n$ instead of $\tilde{Q}$ and the appropriate game matrix $\tilde{\Phi}$. The larger n is, the tighter the upper bound is. In the case of XOR games, the moment matrix of the first level of the NPA hierarchy actually suffices to find the exact optimal value, as it was proven in [NW10]. The dual formulation can be seen as an optimization over sum-of-squares (SOS) polynomials, given the duality theory between positive semidefinite moment matrices and SOS polynomials [Lau09]. In the case of the NPA hierarchy the difference between the solutions of the dual and primal problems can be seen as the expectation value of an SOS polynomial $\sum_i S_i^\dagger S_i$, where S_i belongs to the monomials used to create the corresponding moment matrix [TPKBA24]. For XOR games, this implies that for every Gram matrix $\tilde{Q}$ obtained by measuring the state $|\psi\rangle$, the following holds:

$$\xi_q - \mathrm{Tr}[\tilde{Q}\tilde{\Phi}] = \langle\psi|\sum_i P_i^\dagger P_i|\psi\rangle, \tag{25}$$

where the P_i-s are first degree polynomials over $\{A_1, \cdots, A_{|\mathsf{X}|}, B_1, \cdots, B_{|\mathsf{Y}|}\}$, i.e. $P_i = \sum_{x,y}(\alpha_x^i A_x + \beta_y^i B_y)$. As Eq. (25) holds for all quantum realizations, it can be written as

$$\xi_q\mathbb{1} - \mathcal{B} = \sum_i P_i^\dagger P_i, \tag{26}$$

where $\xi_q\mathbb{1} - \mathcal{B}$ is usually called the shifted game operator. The following theorem stipulates that for XOR games, the shifted game operator can be written as a sum of squares, with each term containing a single Alice operator, plus a positive polynomial depending only of Bob's operators.

Theorem 1. *Let $\mathcal{B}$ be the game operator of an XOR game with optimal quantum bias ξ_q. Then the following holds:*

$$\xi_q\mathbb{1} - \mathcal{B} = \sum_x \frac{\lambda_x}{2}\left(A_x - \sum_y F_{xy}B_y\right)^2 + P\left(\{B_y\}_y\right), \tag{27}$$

where F is the matrix of Lemma 1 and $P(\{B_y\}_y)$ is a positive polynomial over Bob's measurement operators.

To prove this theorem, we first use the following lemma proven by Ostrev.

Lemma 2. *[Ost16]*

1. *Let $\lambda_1, \cdots, \lambda_{|\mathsf{X}|+|\mathsf{Y}|}$ be an optimal solution to the dual semidefinite program (21). Then there exist vectors $\{|u_i\rangle = \sum_{j=1}^{|\mathsf{X}|}u_{ij}|j\rangle\}_{i=1}^r$ and $\{|v_i\rangle = \sum_{j=1}^{|\mathsf{Y}|}v_{ij}|j\rangle\}_{i=1}^r$ such that*

$$\sum_{i=1}^r |u_i\rangle\langle u_i| = \frac{1}{2}\Lambda_A, \qquad \sum_{i=1}^r |v_i\rangle\langle v_i| = \frac{1}{2}\Lambda_B, \qquad \sum_{i=1}^r |u_i\rangle\langle v_i| = \frac{1}{2}\Phi. \tag{28}$$

2. *Let $|A\rangle$ and $|B\rangle$ be a quantum strategy for an XOR game. Let $\{|u_i\rangle = \sum_{j=1}^{|\mathsf{X}|} u_{ij}|j\rangle\}_{i=1}^{r}$ and $\{|v_i\rangle = \sum_{j=1}^{|\mathsf{X}|} v_{ij}|j\rangle\}_{i=1}^{r}$ satisfy (28). Then the following identity holds:*

$$\sum_{i=1}^{r}\left\|\sum_{j=1}^{|\mathsf{X}|} u_{ij}|A_j\rangle - \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|B_j\rangle\right\|^2 = \frac{1}{2}\mathrm{Tr}[\Lambda] - \sum_{ij}\langle A_j|\Phi_{ij}|B_j\rangle. \tag{29}$$

Proof. The interested reader can find the proof of the first part in [Ost16] (Lemma 4 therein), we reproduce here the proof of the second part (Lemma 5 in [Ost16]). The l.h.s. of (29) reads

$$\begin{aligned}
&\sum_{i=1}^{r}\left\|\sum_{j=1}^{|\mathsf{X}|} u_{ij}|A_j\rangle - \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|B_j\rangle\right\|^2 = \\
&= \langle A|\mathbb{1}\otimes\left(\sum_{i=1}^{r}|u_i\rangle\langle u_i|\right)|A\rangle + \langle B|\mathbb{1}\otimes\left(\sum_{i=1}^{r}|v_i\rangle\langle v_i|\right)|B\rangle - 2\langle A|\mathbb{1}\otimes\left(\sum_{i=1}^{r}|u_i\rangle\langle v_i|\right)|B\rangle = \\
&= \frac{1}{2}\langle A|\mathbb{1}\otimes\Lambda_A|A\rangle + \frac{1}{2}\langle B|\mathbb{1}\otimes\Lambda_B|B\rangle - \langle A|\left(\mathbb{1}\otimes\Phi\right)|B\rangle = \\
&= \frac{1}{2}\mathrm{Tr}[\Lambda_A] + \frac{1}{2}\mathrm{Tr}[\Lambda_B] - \langle A|\mathbb{1}\otimes\Phi|B\rangle,
\end{aligned}$$

which is exactly the second statement of the lemma, given that $\Lambda = \Lambda_A + \Lambda_B$. □

We now define a robust version of Ostrev's lemma.

Lemma 3. 1. *Let $\lambda_1, \cdots, \lambda_{|\mathsf{X}|+|\mathsf{Y}|}$ be an optimal solution to the dual semidefinite program (21). Then there exist vectors $\{|u_i\rangle = \sum_{j=1}^{|\mathsf{X}|} u_{ij}|j\rangle\}_{i=1}^{r}$ and $\{|v_i\rangle = \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|j\rangle\}_{i=1}^{r}$ such that*

$$\sum_{i=1}^{r}|u_i\rangle\langle u_i| = \frac{1}{2}\Lambda_A, \qquad \sum_{i=1}^{r}|v_i\rangle\langle v_i| \preceq \frac{1}{2}\Lambda_B, \qquad \sum_{i=1}^{r}|u_i\rangle\langle v_i| = \frac{1}{2}\Phi \tag{30}$$

2. *Let $|A\rangle$ and $|B\rangle$ be a quantum strategy for an XOR game. Let $\{|u_i\rangle = \sum_{j=1}^{|\mathsf{X}|} u_{ij}|j\rangle\}_{i=1}^{r}$ and $\{|v_i\rangle = \sum_{j=1}^{|\mathsf{X}|} v_{ij}|j\rangle\}_{i=1}^{r}$ satisfy (28). Then the following identity holds:*

$$\sum_{i=1}^{r}\left\|\sum_{j=1}^{|\mathsf{X}|} u_{ij}|A_j\rangle - \sum_{j=1}^{|\mathsf{Y}|} v_{ij}|B_j\rangle\right\|^2 \leq \frac{1}{2}\mathrm{Tr}[\Lambda] - \sum_{ij}\langle A_j|\Phi_{ij}|B_j\rangle. \tag{31}$$

Proof. For the proof of the first part, we give an explicit construction of the vectors $|u_i\rangle$ and $|v_i\rangle$. We choose $u_{ij} = \sqrt{\frac{\lambda_i}{2}}\delta_{ij}$, where δ_{ij} is the Kronecker delta, and we take $|v_i\rangle = \frac{1}{\lambda_i}\sum_j \Phi_{ij}|u_j\rangle$. The first and third relations in (30) are satisfied, as $\sum_i |u_i\rangle\langle u_i| = \frac{1}{2}\mathrm{diag}(\lambda_1, \cdots, \lambda_{|\mathsf{X}|})$, and $\sum_i |u_i\rangle\langle v_i| = \frac{1}{2}\Phi$. Concerning the second relation, we get $\sum_i |v_i\rangle\langle v_i| = \frac{1}{2}\Phi^T\Lambda_A^{-1}\Phi$. To analyze it, we use the complementary slackness condition, which implies that $\Lambda - \tilde{\Phi} \succeq 0$. By Schur's complement lemma , this matrix is positive if and only if $\Lambda_B - \Phi^T\Lambda_A^{-1}\Phi \succeq 0$. This completes the proof of the first part of the lemma. The second part follows analogously to the second part of Lemma 2. □

We can now prove Theorem 1.

Proof. Taking the $|u_i\rangle$-s and $|v_i\rangle$-s used to prove the first part of Lemma 3 in (31), we get

$$\xi_q - \langle\psi|\mathcal{B}|\psi\rangle - \sum_{x=1}^{m_A}\frac{\lambda_x}{2}\left\|A_x|\psi\rangle - \lambda_x^{-1}\sum_y \Phi_{x,y}B_y|\psi\rangle\right\|^2 \geq 0. \tag{32}$$

When opening the sum of squares, we get

$$\xi_q - \sum_{x=1}^{m_A}\frac{1}{\lambda_x}\langle\psi|\sum_{y,y'}B_y\Phi_{y,x}\Phi_{x,y'}B_{y'}|\psi\rangle \geq 0, \tag{33}$$

which holds for every valid quantum state $|\psi\rangle$, implying

$$2P\left(\{B_y\}_y\right) \equiv \xi_q \mathbb{1} - \sum_{x=1}^{m_A} \frac{1}{\lambda_x} \sum_{y,y'} B_y \Phi_{y,x} \Phi_{x,y'} B_{y'} \geq 0. \tag{34}$$

The simple expansion of all the squares shows that

$$\xi_q \mathbb{1} - \mathcal{B} = \frac{\lambda_x}{2} \left(A_x - \lambda_x^{-1} \sum_y \Phi_{x,y} B_y \right)^2 + P\left(\{B_y\}_y\right), \tag{35}$$

which together with (34) proves the theorem. □

2.4 Quantum homomorphic encryption

Homomorphic encryption is a cryptographic technique that enables to execute computations directly on encrypted data, without prior decryption. The results of these computations remain in an encrypted form and, upon decryption, yield outputs identical to those obtained through operations on the unencrypted data. The term "homomorphic" draws from algebraic homomorphism, wherein encryption and decryption functions are likened to homomorphisms between plaintext and ciphertext spaces. A cryptosystem supporting arbitrary computation on ciphertexts is termed fully homomorphic encryption (FHE), representing the most robust form of homomorphic encryption. Originally conceptualized as a privacy homomorphism by Rivest, Adleman, and Dertouzous [RAD⁺78] shortly after the invention of the RSA cryptosystem [RSA78], the first plausible construction for FHE using lattice-based cryptography was presented by Gentry [Gen09]. Leveraging the hardness of the (Ring) Learning With Errors (RLWE) problem, more efficient schemes for fully homomorphic encryption have been devised [BGV14, BV14]. The possibility of quantum homomorphic encryption (QHE), allowing for quantum computations on encrypted data, was introduced by Mahadev [Mah18], with Brakerski [Bra18] subsequently enhancing it to achieve improved noise tolerance.

Before reminding the formalism of QHE, we first recall the definition of quantum polynomial time algorithms. Throughout the paper, κ denotes the security parameter.

Definition 1 (Quantum polynomial time algorithm)**.** *A quantum algorithm is quantum polynomial time (QPT) it can be implemented by a family of quantum circuits with size polynomial in the security parameter κ.*

We now reproduce the definition of QHE as it appears in [KLVY23].

Definition 2 (Quantum Homomorphic Encryption (QHE))**.** *A quantum homomorphic encryption scheme* $\mathsf{QHE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ *for a class of quantum circuits C consists of the following four quantum algorithms which run in quantum polynomial time in terms of the security parameter:*

- Gen *takes as input the security parameter 1^κ and outputs a (classical) secret key* sk *of size* $\mathrm{poly}(\kappa)$ *bits;*
- Enc *takes as input a secret key* sk *and a classical input x, and outputs a ciphertext* ct*;*
- Eval *takes as input a tuple $(C, |\Psi\rangle, \mathsf{ct}_{\mathrm{in}})$, where $C : \mathcal{H} \times (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes m}$ is a quantum circuit, $|\Psi\rangle \in \mathcal{H}$ is a quantum state, and $\mathsf{ct}_{\mathrm{in}}$ is a ciphertext corresponding to an n-bit plaintext.* Eval *computes a quantum circuit* $\mathsf{Eval}_C(|\Psi\rangle \otimes |0\rangle^{\otimes \mathrm{poly}(\lambda,n)}, \mathsf{ct}_{\mathrm{in}})$ *which outputs a ciphertext $\mathsf{ct}_{\mathrm{out}}$. If C has classical output, we require that Eval_C also has classical output.*
- Dec *takes as input a secret key* sk *and ciphertext* ct*, and outputs a state $|\phi\rangle$. Additionally, if* ct *is a classical ciphertext, the decryption algorithm outputs a classical string y.*

As in [KLVY23] the following property is required from QHE, in order for it to behave “nicely" with entanglement:

Definition 3 (Correctness with auxiliary input)**.** *For every security parameter $\kappa \in \mathbb{N}$, any quantum circuit $C : \mathcal{H}_A \times (\mathbb{C}^2)^{\otimes n} \to \{0,1\}^*$ (with classical output), any quantum state $|\Psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, any message $x \in \{0,1\}^n$, any secret key* $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\kappa)$ *and any ciphertext* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$*, the following states have negligible trace distance:*

Game 1 *Start with $(x, |\Psi\rangle_{AB})$. Evaluate C on x and register A, obtaining classical string y. Output y and the contents of register B.*

Game 2 *Start with* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)$ *and* $|\Psi\rangle_{AB}$. *Compute* $\mathsf{ct}' \leftarrow \mathsf{Eval}_C(\cdot \otimes |0\rangle^{\mathrm{poly}(\lambda,n)}, \mathsf{ct})$ *on register* A. *Compute* $y' = \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')$. *Output* y' *and the contents of register* B.

In simple terms, “correctness with auxiliary input" stipulates that when QHE evaluation is employed on a register A within a joint (entangled) state in $\mathcal{H}_A \otimes \mathcal{H}_B$, the entanglement between the QHE-evaluated output and B must be maintained.

Finally, the following definition characterizes another property expected from QHE, and it is in cryptography well-known indistinguishability under chosen plaintext attack (IND-CPA).

Definition 4 (IND-CPA security against quantum distinguishers)**.** *For any two messages* x_0, x_1 *and any QPT adversary* $\mathcal{A}$*:*

$$\left|\Pr\left[\mathcal{A}^{\mathsf{Enc}(\mathsf{sk},\cdot)}(\mathsf{ct}_0) = 1 \,\middle|\, \begin{array}{l}\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)\\ \mathsf{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{sk}, x_0)\end{array}\right] - \Pr\left[\mathcal{A}^{\mathsf{Enc}(\mathsf{sk},\cdot)}(\mathsf{ct}_1) = 1 \,\middle|\, \begin{array}{l}\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)\\ \mathsf{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{sk}, x_1)\end{array}\right]\right| \leq \mathsf{negl}(\kappa) \ ,$$

for some negligible funcion $\mathsf{negl}(\cdot)$.

2.5 Compiled nonlocal games

In [KLVY23], Kalai *et al.* introduced a compilation technique that can be used to construct single-prover proofs of quantumness. Their procedure transforms any k-player nonlocal game into a single-prover interactive game, employing post-quantum cryptography to emulate spatial separation among the parties. The proposed protocol maintains classical soundness, ensuring that no classical polynomially-bounded prover can surpass the maximal classical score of the original game. Additionally, leveraging quantum homomorphic encryption (QHE), the authors devise an explicit and efficient quantum strategy that achieves the quantum bound of the original nonlocal game. This enables the translation of proofs of quantumness into the single-prover interactive proof framework.

In this context, we refer to a single-prover interactive game that is generated through the KLVY compilation of a nonlocal game as a compiled nonlocal game. We recall the definition of compiled nonlocal games introduced in [KLVY23]. Using the interactive proof terminology, the entity called “referee” in the nonlocal game will be referred to as the “verifier”.

Definition 5 (Compiled nonlocal game)**.** *In a compiled nonlocal game, a verifier, equipped with access to a Quantum Homomorphic Encryption (QHE) scheme as defined in Def. 2, engages with a prover. According to a probability distribution* $q(x, y)$*, the verifier samples* x *and* y*. In the first round, the verifier transmits* $\mathtt{x} = \mathsf{Enc}(x)$ *to the prover, who responds with an encrypted output* $\mathtt{a} = \mathsf{Enc}(a)$*. In the second round, the verifier sends the input* y *to the prover in the clear, and the prover replies with the answer* b*. The verifier assesses the outcome using the game predicate* $V(\mathsf{Dec}(\mathtt{a}), b|\mathsf{Dec}(\mathtt{x}), y) \in \{0, 1\}$ *to determine whether the prover has passed or failed in the game.*

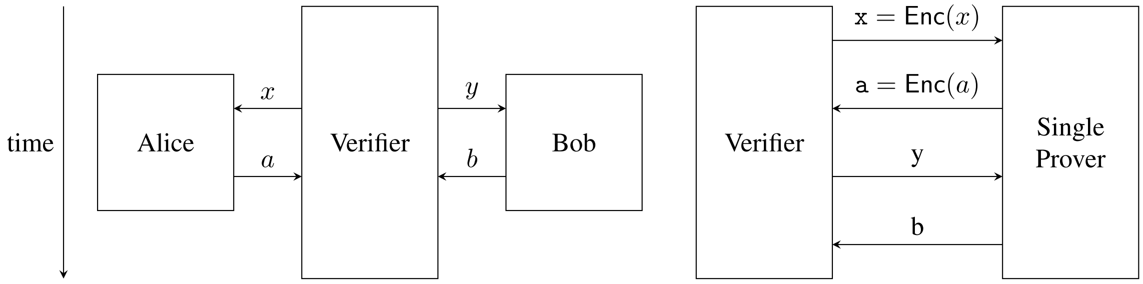


Figure 1: Pictorial representation of the Kalai *et. al.* compilation protocol for 2-player nonlocal games. On the left, a general 2-player nonlocal game; the two parties are spatially separated, and only communicate to a verifier which is sampling questions (x, y) and collecting their answers (a, b). On the right, the single prover game resulting from the compilation procedure. In this representation time flows downwards.

The following theorem (Theorem 1.1 in [KLVY23]) relates the classical and quantum score of a nonlocal game to the scores of the corresponding compiled game.

Theorem 2 ([KLVY23])**.** *Given any* 2*-player nonlocal game with quantum bound* ξ_q *and classical bound* ξ_c *and any QHE scheme (with security parameter* κ*) that satisfies correctness with auxiliary inputs and IND-CPA* *security against quantum distinguishers then, there is a 4-round single prover interactive game with completeness ξ_q realized by a quantum polynomial-time algorithm and soundness $\xi_c + negl(\kappa)$ against any classical polynomial-time algorithm.*

The classical soundness statement in this theorem guarantees that the maximal winning probability that a classical polynomial-time prover can achieve in a compiled nonlocal game is nearly identical to the optimal classical winning probability in the corresponding nonlocal game, with a negligible deviation dependent on the security parameter. The main insight in [KLVY23] is that the success of the classical prover is primarily hindered by the sequential nature of the game. This sequential structure forces the prover to commit to an answer a before receiving the input y. The combination of this sequential setup with secure QHE effectively replicates the locality requirement of a nonlocal game that is ensured by the spatial separation of the players. The quantum soundness statement ensures that a QPT prover can win the compiled nonlocal game with a probability that is at least as large as the optimal quantum winning probability in the corresponding nonlocal game.

2.5.1 Modelling the quantum prover

Let us now model the behavior of the single quantum prover, in the same way as it was done in [NZ23]. In a compiled game, denoted as per Def. 5, the prover, initially in state $|\psi\rangle$, undergoes a process involving encrypted questions and answers. Specifically, in the first round, the prover receives an encrypted question x, performs a POVM measurement, and computes an encrypted answer a. Using Naimark dilation theorem, the prover's POVM measurement is simulated by a projective measurement, denoted here with $M_{\mathsf{a}|\mathsf{x}}$. The prover's action could potentially involve a unitary operation $U_{\mathsf{x},\mathsf{a}}$ following the measurement, crucial in the sequential setting. The projectors and unitaries can be unified into a set of potentially non-Hermitian operators $\mathsf{M}_{\mathsf{a}|\mathsf{x}}$, satisfying $\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}}\mathsf{M}_{\mathsf{a}|\mathsf{x}} = M_{\mathsf{a}|\mathsf{x}}$ and hence $\sum_{\mathsf{a}} \mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}}\mathsf{M}_{\mathsf{a}|\mathsf{x}} = \mathbb{1}$. The prover's state after the first round of the game corresponds to the post-measurement state

$$|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle, \tag{36}$$

and the probability to get output a for input x is

$$p(\mathsf{a}|\mathsf{x}) = \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle = \left\| |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 . \tag{37}$$

In the second round, the prover's behavior is characterized by a set of projective operators $\{\{N_{b|y}\}_b\}_y$. If the second-round answers are bits, the measurements can be characterized by specifying a Hermitian observable $B_y = \sum_b (-1)^b N_{b|y}$. Similarly, if Alice's outputs in the corresponding nonlocal game are bits, we can define a "decrypted" observable

$$\begin{aligned} \mathrm{A}_x &= \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}}\mathsf{M}_{\mathsf{a}|\mathsf{x}} && (38)\\ &= \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} A_{\mathsf{x}}, && (39) \end{aligned}$$

where A_{x} are binary observables, while A_x in general is not. If both a and b are bits, we can define the correlators allowing to characterize the winning probability of a quantum prover in a computational single-prover game:

$$\langle \mathrm{A}_x, B_y \rangle = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y | \psi_{\mathsf{a}|\mathsf{x}} \rangle \tag{40}$$

The correlators have the same operational meaning as in nonlocal games: when the verifier samples a question pair (x, y) in the compiled game and receives (decrypted) answers (a, b), $\langle \mathrm{A}_x, B_y \rangle$ is precisely the expected value of $(-1)^{a+b}$.

The marginals of the second-round observables in principle depends on the encrypted x of the first round and have form:

$$\langle B_y \rangle_x = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y | \psi_{\mathsf{a}|\mathsf{x}} \rangle . \tag{41}$$

2.6 Technical tools for estimating quantum bounds of compiled nonlocal games

2.6.1 Block encodings

We now examine certain outcomes related to the block encoding of quantum processes. Block encoding is a method for the efficient implementation of a quantum operation. Our motivation for exploring this process stems from the contextual constraint imposed in the subsequent sections of this paper, where we address computational limitations among participants. Consequently, we aim to identify operations that can be efficiently executed by leveraging available quantum resources.

Definition 6 (Block encoding)**.** *Given a matrix $A \in \mathbb{C}^{c\times c}$, we say that $U \in \mathbb{C}^{d\times d}$ is a Q-block encoding of A if*

- *U is a unitary matrix whose quantum circuit can be implementable with $O(Q)$ gates,*
- *U has the following form $U = \begin{pmatrix} \tau A & \cdot \\ \cdot & \cdot \end{pmatrix}$, where we call τ the scale factor of the block encoding.*

We say U is QPT-implementable if Q is polynomially bounded in the size of the input.

If U is a block encoding of A, then A can be implemented by performing the following operation

$$\tau\left(\langle 0| \otimes \mathbb{1}\right) U (|0\rangle \otimes \mathbb{1})$$

where $\mathbb{1}$ is the identity matrix of the size of A.

Through the linear combination and multiplication of matrices possessing a block encoding, our anticipation is the persistence of this property in the resulting matrix. Although the explicit construction in complete generality is not immediately apparent, [GSLW19, Lemmas 52 and 53] provides a technical framework for the block encoding of linear combinations and products of matrices with block encoding. Here, we present a streamlined version of their results, tailored to our specific requirements.

First, we present a lemma about the block encoding of a linear combination of matrices that have block encoding, whose proof can be found in [GSLW19, Lemma 52].

Lemma 4 (Linear combination of block encoded matrices)**.** *Let $A = \sum_{j=1}^{m} y_j A_j$, where $y \in \mathbb{C}^m$ is a complex bounded vector $\|y\|_1 \leq \beta$ and A_j are matrices for which we know a Q_j-block encoding U_j. Then we can implement a $\left(m + \sum_{j=1}^{m} Q_j\right)$-block encoding of A.*

Corollary 1. *Let $A = \sum_{j=1}^{m} y_j A_j$, where $y \in \mathbb{C}^m$ is a complex bounded vector $\|y\|_1 \leq \beta$. If $m = \mathrm{poly}(\kappa)$ and each A_j is an operator with QPT-implementable block encodings with scale factor $O(1)$ for all j, A also has a QPT-implementable block encoding with scale factor $O(1)$.*

The subsequent lemma guarantees the presence of a block encoding for the product of matrices, each possessing its own block encoding, whose proof can be found in [GSLW19, Lemma 53].

Lemma 5 (Product of block encoded matrices)**.** *Let U and V be the Q_U and Q_V-block encodings of A and B respectively. Then we can implement a $(Q_U + Q_V)$-block encoding of AB.*

Corollary 2. *Let U and V be the Q_U and Q_V-block encodings of A and B respectively. If U and V are QPT-implementable, each with scale factor $O(1)$, AB also has a QPT-implementable block encoding with scale factor $O(1)$.*

For operators with a QPT-implementable block-encoding, the following technical lemma from [NZ23] applies.

Lemma 6 ([NZ23, Lemma 14])**.** *Let $\mathscr{B}$ be an operator with a QPT-implementable block encoding with $O(1)$ scale factor and $\|\mathscr{B}\| \leq O(1)$. Then there exists a QPT-measurable POVM $\{M_\beta\}_\beta$ such that for any state ρ, the following holds:*

$$\left| \sum_\beta \beta \cdot \mathrm{Tr}\left[M_\beta \rho\right] - \mathrm{Tr}\left[\mathscr{B}\rho\right] \right| \leq \varepsilon, \tag{42}$$

for any $\varepsilon = 1/\mathrm{poly}(\kappa)$.

These results, together with the definition of the IND-CPA security, allow us to state the following:

Lemma 7 (adapted from [NZ23, Lemmas 15-17])**.** *Let $\mathscr{B}$ be an operator with a QPT-implementable block encoding with $O(1)$ scale factor and $\|\mathscr{B}\| \leq O(1)$. Let $\mathrm{QHE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ be a secure quantum homomorphic encryption scheme (see Definition 2), let D_0, D_1 be any two QPT sampleable distributions over plaintext questions x, and let $|\psi\rangle$ be any efficiently preparable state of the prover. Then, for any security parameter $\kappa \in \mathbb{N}$, there exists a negligible function $\delta_{qhe}(\kappa)$ such that*

$$\left| \mathop{\mathbb{E}}_{x\leftarrow D_0} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \mathscr{B} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle - \mathop{\mathbb{E}}_{x\leftarrow D_1} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \mathscr{B} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \right| \leq \delta_{qhe}(\kappa). \tag{43}$$

The proof of this Lemma encompasses Lemmas 15, 16 and 17 in [NZ23]. Importantly, $\mathscr{B}$ does not have to be a binary observable, it just has to be efficiently implementable by quantum circuits. This lemma establishes a link between QPT-implementable block encodings and IND-CPA security. Looking ahead, using the fact that XOR games and SATWAP Bell inequalities have a nice form of SOS decomposition into linear combination and product of block encodings as presented in previous sections, this lemma will allow us to relate the quantum bound of the compiled nonlocal games to those of the original nonlocal games, at the expense of a negligible security loss.

2.6.2 Crypto-correlation matrix and pseudo-expectation map

In this section, we revisit and further expound upon the concepts delineated in Section 4.4 of [NZ23]. In that section, the authors introduced a compelling argument to establish the optimal quantum winning probability for the compiled CHSH game through the introduction of a cryptographic SOS decomposition. Our objective is to broaden their findings to encompass a more extensive array of games, namely XOR games and d-outcome CHSH games.

Consider a game with an optimal quantum bias ξ_q. Its game operator (17) is

$$\mathcal{B} = \sum_{x,y} \gamma^{AB}_{x,y} A_x B_y, \tag{44}$$

and the corresponding shifted game operator has an SOS decomposition

$$\xi_q \mathbb{1} - \mathcal{B} = \sum_j b_i P_i^\dagger P_i + \sum_i d_i [A_{x_i}, B_{y_i}] + \sum_i e_i (\mathbb{1} - A^2_{x_i}) + \sum_i f_i (\mathbb{1} - B^2_{y_i}), \tag{45}$$

where $b_j \in \mathbb{R}^+$ are real positive coefficients for the terms of the SOS decomposition, d_i-s could be complex numbers referring to the constraint that Alice's and Bob's operators commute, e_i-s and f_i-s multiply terms that vanish if the measurements of Alice and Bob are projective. All terms on the r.h.s. of (45) except the first one are general constraints that are usually implicitly assumed. Here, the aim is to develop an analogous procedure for bounding the optimal quantum bias of compiled games, so one has to be careful as some of the constraints satisfied in the case of nonlocal games might not be satisfied in the case of compiled games. For example, operations in two rounds of the compiled game do not necessarily commute.

Analogously to matrix $\tilde{Q}$ from Section 2.3, expounding on the ideas from [NZ23], we define a $(|\mathsf{X}| + |\mathsf{Y}|) \times (|\mathsf{X}| + |\mathsf{Y}|)$ matrix $\tilde{\mathcal{Q}}$ as follows

$$\tilde{\mathcal{Q}} = \left[\begin{array}{c|c} \mathbb{1}_{|\mathsf{X}|} & C \\ \hline C^T & S \end{array}\right], \tag{46}$$

where $\mathbb{1}_{|\mathsf{X}|}$ is the $|\mathsf{X}| \times |\mathsf{X}|$ identity matrix, where

$$C = \sum_{x,y} \langle \mathrm{A}_x, B_y \rangle |x\rangle\langle y|, \tag{47}$$

$$S = \sum_{y,y'} \mathop{\mathbb{E}}_{x \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y B_{y'} | \psi_{\mathsf{a}|\mathsf{x}} \rangle |y\rangle\langle y'|, \tag{48}$$

and where $\langle \mathrm{A}_x, B_y \rangle$ correspond to Eq. (40). The matrix $\tilde{\mathcal{Q}}$, unlike $\tilde{Q}$, is not necessarily positive semidefinite, as there is no real consistency in assigning values to its entries. Similarly to $\tilde{Q}$, $\tilde{\mathcal{Q}}$ has ones on the diagonal, in the first block by construction and in the second because

$$\begin{aligned} S_{y,y} &= \mathop{\mathbb{E}}_{x \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | \mathbb{1} | \psi_{\mathsf{a}|\mathsf{x}} \rangle \\ &= \mathop{\mathbb{E}}_{x \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi | \mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \mathsf{M}_{\mathsf{a}|\mathsf{x}} | \psi \rangle \\ &= \mathop{\mathbb{E}}_{x \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \langle \psi | \psi \rangle \\ &= 1. \end{aligned}$$

Then, as in [NZ23], we define a linear operator $\tilde{\mathbb{E}}$ that maps every homogeneous degree-2 polynomial in the variables A_x, B_y to linear combinations of elements of the matrix $\tilde{\mathcal{Q}}$ in the following way:

$$\tilde{\mathbb{E}}[A_x B_y] = C_{x,y}, \qquad \tilde{\mathbb{E}}[B_y \mathrm{A}_x] = C^T_{y,x}, \tag{49}$$

$$\tilde{\mathbb{E}}[A_x A_{x'}] = \delta_{x,x'}, \qquad \tilde{\mathbb{E}}[B_y B_{y'}] = S_{y,y'}. \tag{50}$$

For $y = y'$ or $x = x'$ in Eq. (50), we get a consistent mapping of identity

$$\tilde{\mathbb{E}}[A_x A_x] = \tilde{\mathbb{E}}[\mathbb{1}] = 1, \qquad \tilde{\mathbb{E}}[B_y B_y] = \tilde{\mathbb{E}}[\mathbb{1}] = S_{y,y} = 1. \tag{51}$$

As in [NZ23], we call the map $\tilde{\mathbb{E}}$ a pseudo-expectation. Such defined pseudo-expectation maps the game operator $\mathcal{B}$ introduced in Eq. (44)) to a bias in the compiled nonlocal game:

$$\tilde{\mathbb{E}}[\mathcal{B}] = \sum_{x,y} \gamma_{x,y} \tilde{\mathbb{E}}[A_x B_y] = \sum_{x,y} \gamma_{x,y} \langle \mathrm{A}_x, B_y \rangle = \bar{\xi}. \tag{52}$$

The optimal quantum bias can be upper bounded using the SOS decomposition of the shifted game operator(eq. (45)):

$$\tilde{\mathbb{E}}\left[\xi_q \mathbb{1} - \mathcal{B}\right] = \tilde{\mathbb{E}}\left[\sum_i b_i P_i^\dagger P_i + \sum_i d_i [A_{x_i}, B_{y_i}] + \sum_i e_i (\mathbb{1} - A_{x_i}^2) + \sum_i f_i (\mathbb{1} - B_{y_i}^2)\right] \tag{53}$$

Given (49), the terms multiplied by d_i vanish because, under pseudo-expectation map, operators A_x and B_y commute. The terms multiplied by e_i and f_i also vanish because of Eq. (51). Hence

$$\tilde{\mathbb{E}}\left[\xi_q \mathbb{1} - \mathcal{B}\right] = \sum_i b_i \tilde{\mathbb{E}}\left[P_i^\dagger P_i\right] \tag{54}$$

Thus, if $\tilde{\mathbb{E}}\left[P_i^\dagger P_i\right]$ is non-negative, the bias in a compiled game cannot be larger than the optimal quantum bias of the corresponding nonlocal game.

3 Quantum bound of compiled XOR games

In Section 2.3, we established key insights into XOR games. Here, building upon the methodology outlined in [NZ23] and revisited in 2.6.2, we present our first important result: compiled XOR games exhibit a quantum bias that closely aligns with the quantum bias of the corresponding nonlocal game, fluctuating only slightly with the security parameter. The power of the quantum prover to win a compiled XOR game with a probability larger than the optimal quantum winning probability for the corresponding XOR game crucially depends on their ability to transmit from the first round information about the received plaintext input. However, inputs are encrypted in such a way that the encryption satisfies IND-CPA security, meaning that even the quantum prover cannot do better than randomly guessing its question x knowing the encryption x of x. This inability of a QPT prover to break the encryption is articulated in Lemma 7. In essence, this lemma conveys that regardless of the measurement employed by a QPT prover in the second round of the game, they are unable to differentiate between states resulting from distinct samples of plaintext questions taken in the first round.

Before stating our main result let us state two lemmas about the behavior of the XOR game operator under the pseudo-expectation map defined in Sec. 2.6.2. The first lemma is a generalization of Claims 31 and 33 from [NZ23].

Lemma 8. *Let $P_x = A_x - \sum_y F_{xy} B_y$ with$\{A_x\}_x$ and $\{B_y\}_y$ binary observables. Then there exists a negligible function $\delta_{\mathrm{QHE}}(\cdot)$ such that we have $\tilde{\mathbb{E}}\left[P_j^\dagger P_j\right] \geq -\delta_{\mathrm{QHE}}(\kappa)$, where $\tilde{\mathbb{E}}[\cdot]$ is the pseudo-expectation map defined in Sec. 2.6.2.*

Proof. Let us introduce the shortened notation $\hat{B}_x = \sum_y F_{xy} B_y$. We get

$$\begin{aligned}
\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right] &= \tilde{\mathbb{E}}\left[A_x A_x\right] - 2\tilde{\mathbb{E}}\left[A_x \hat{B}_y\right] + \tilde{\mathbb{E}}\left[\hat{B}_y \hat{B}_{y'}\right] \\
&= 1 - 2\sum_y F_{xy} C_{xy} + \sum_{y,y'} F_{yx} F_{xy'} S_{yy'} \\
&= 1 - 2\sum_y F_{xy} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} B_y \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle + \\
&\qquad \sum_{y,y'} F_{yx} F_{xy'} \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} B_y B_{y'} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&= 1 - 2 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle + \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \hat{B}_x^\dagger \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} 1 - 2 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} (-1)^{\mathsf{Dec}(\mathsf{a})} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle + \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \hat{B}_x^\dagger \hat{B}_x \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \left(\mathbb{1} - 2(-1)^{\mathsf{Dec}(\mathsf{a})} \hat{B}_x + \hat{B}_x^2\right) \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} \left((-1)^{\mathsf{Dec}(\mathsf{a})}\mathbb{1} - \hat{B}_x\right)^2 \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle
\end{aligned}$$

In the first two lines, we used the linearity and the definition of the pseudo-expectation map. In the third line, we used the definition of matrices C (eq. (49)) and S (eq. (50)). In the fourth line, we just used the definition of $\hat{B}_x$. To get the fifth line we used the fact that $\hat{B}_x^\dagger \hat{B}_x$ has a QPT-implementable block encoding (Corrolaries 1 and 2) and thus we can apply Lemma 7 given above. To get the sixth line we used linearity and we grouped all terms inside of one average over $\mathsf{x} = \mathsf{Enc}(x)$; in particular we noticed that we could write the first term 1 as $\mathbb{1}$ inside this average. Finally, in the seventh line we recognised that the expression within round brackets can be expressed as the square of an operator. This is necessarely positive, implying that up to a negligible factor $\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right]$ must also be positive. □

Lemma 9. *Let P be a positive semi-definite homogeneous degree-2 polynomial over binary observables $\{B_y\}_y$. Then $\tilde{\mathbb{E}}[P] \geq 0$, where $\tilde{\mathbb{E}}[\cdot]$ is the pseudo-expectation map defined in Sec. 2.6.2.*

Proof. The pseudo-expectation of P reads

$$\tilde{\mathbb{E}}[P] = \mathop{\mathbb{E}}_{x\in\mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}^\dagger_{\mathsf{a}|\mathsf{x}} P \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \geq 0 \tag{55}$$

Since all elements in the sum are positive because P is positive semi-definite the relation trivially holds. □

We can now state the main theorem, providing the quantum optimal bias of compiled XOR games.

Theorem 3. *Given an XOR game with optimal quantum bias ξ_q, the optimal quantum bias of the compiled XOR game is $\xi_q + \delta_{\mathrm{QHE}}(\kappa)$, where $\delta_{\mathrm{QHE}}(\cdot)$ is a negligible function.*

Proof. Let us recall Theorem 1 which states that for every XOR game we have

$$\xi_q \mathbb{1} - \mathcal{B} = \sum_x \frac{\lambda_x}{2}\left(A_x - \sum_y F_{xy} B_y\right)^2 + P\left(\{B_y\}_y\right),$$

By applying the pseudo-expectation map we get

$$\begin{aligned}
\tilde{\mathbb{E}}\left[\xi_q \mathbb{1} - \mathcal{B}\right] &= \tilde{\mathbb{E}}\left[\sum_x \frac{\lambda_x}{2}\left(A_x - \sum_y F_{xy} B_y\right)^2 + P\left(\{B_y\}_y\right)\right] && (56)\\
&= \sum_x \frac{\lambda_x}{2} \tilde{\mathbb{E}}\left[\left(A_x - \sum_y F_{xy} B_y\right)^2\right] + \tilde{\mathbb{E}}\left[P\left(\{B_y\}_y\right)\right] && (57)
\end{aligned}$$

To get the second line we used the linearity of the pseudo-expectation map. Based on Lemmas 8 implies that the first term on the r.h.s is up to a negligible function nonnegative, while Lemma 9 implies that the second term on the r.h.s. must be nonnegative. The pseudo-expectation map on the l.h.s. gives $\xi_q - \bar{\xi}_q$, implying that in the worst case the compiled game optimal bias can be only negligibly larger than the optimal quantum bias of the corresponding XOR game:

$$\bar{\xi}_q \leq \xi_q + \delta_{\mathrm{QHE}}(\kappa), \tag{58}$$

which completes the proof. □

4 Quantum bound of compiled nonlocal games with many outputs and conditions for self-testing of qudit measurements from a single prover

We now introduce a family of nonlocal games in which the players respond with more than two outputs. In this case, the quantum strategy involves d-outcome measurements, $\{M_{a|x}\}_{a=0}^{d-1}$ for Alice and $\{N_{b|y}\}_{b=0}^{d-1}$ for Bob. These measurements can be represented through generalized observables

$$A_x^{(k)} = \sum_{a=0}^{d-1} \omega^{ak} M_{a|x}, \qquad B_y^{(l)} = \sum_{b=0}^{d-1} \omega^{bl} N_{b|y}, \quad \forall k, l = 0, \cdots, d-1, \tag{59}$$

where $\omega = \exp\left(\frac{2\pi i}{d}\right)$. Clearly , the eigenvalues of the generalized unitary observables $A_x^{(k)}$ and $B_y^{(l)}$ are roots of unity. We will refer to the indices k and l as the orders of the generalised measurement; notice that the orders $k = 0 \mod d$ are the identity. For $d > 2$, generalized observables are not Hermitian, but still satisfy the following regular property:

$$(A^{(k)})^\dagger = A^{(-k)} \qquad (B^{(l)})^\dagger = B^{(-l)}$$

and hence $\left[A^{(k)}\right]^\dagger A^{(k)} = \mathbb{1}$ for every k. Considering only projective measurements, it is easy to check that $A^{(k)} = \left[A^{(1)}\right]^k$ and $B^{(l)} = \left[B^{(1)}\right]$; we will use these two notations interchangeably.

In this section, we adopt the perspective of Bell inequalities. The CHSH inequality is the simplest Bell inequality whose maximal violation self-tests the maximally entangled pair of qubits. Several propositions have been formulated to capture different features of the CHSH inequality, some focusing on self-testing maximally entangled shared states [SAT+17], some on self-testing mutually unbiased bases measurements for both parties [KŠT+19]. We concentrate on the Salavrakos-Augusiak-Tura-Wittek-Acin-Pironio (SATWAP) Bell inequality introduced in [SAT+17], for which a self-test of arbitrary local dimension with minimal number of measurements (2 per part) has been proposed in [SSKA21].

The SATWAP inequality is defined for two spatially separated players, each receiving a bit as input, $\mathsf{X} = \mathsf{Y} = \{1, 2\}$, and subsequently producing an output that can take one of d different values, $\mathsf{A} = \mathsf{B} = \{0, \ldots, d-1\}$. Many Bell inequalities can be expressed by conveniently defining some regular combination of probabilities given fixed inputs, called correlators. The definition of generalised correlator is:

$$\langle A_x^{(k)} B_y^{(l)} \rangle = \sum_{a=0}^{d-1} \sum_{b=0}^{d-1} \omega^{ak+bl} p(ab|xy) \tag{60}$$

The SATWAP inequality is given in terms of these

$$\beta_d^{\text{SATWAP}} = \sum_{k=1}^{d-1} \left(a_k \langle A_1^k B_1^{d-k} \rangle + a_k^* \omega^k \langle A_1^k B_2^{d-k} \rangle + a_k^* \langle A_2^k B_1^{d-k} \rangle + a_k \langle A_2^k B_2^{d-k} \rangle \right), \tag{61}$$

with the following definition of the phases $a_k = \frac{\omega^{\frac{2k-d}{8}}}{\sqrt{2}} = \frac{1-i}{2} \omega^{k/4}$ such that $a_k^* = a_{d-k}$ and $a_{\pm d} = \pm \frac{1+i}{2}$. To simplify the notation it is convenient to group Bob's observables in the following sums:

$$C_1^{(k)} = a_k B_1^{-k} + a_k^* \omega^k B_2^{-k}, \qquad C_2^{(k)} = a_k^* B_1^{-k} + a_k B_2^{-k}. \tag{62}$$

Using these definitions, the corresponding Bell operator is thus

$$\mathcal{B}_d^{\text{SATWAP}} = \sum_{k=1}^{d-1} \left(A_1^k \otimes C_1^{(k)} + A_2^k \otimes C_2^{(k)} \right). \tag{63}$$

Bell value is thus given as $\beta_d^{\text{SATWAP}} = \langle\psi|\mathcal{B}_d^{\text{SATWAP}}|\psi\rangle$. The classical and the quantum bounds of this inequality are

$$\left(\beta_d^{\text{SATWAP}}\right)_l = \frac{1}{2}\left(3\cot\left(\frac{\pi}{4}d\right) - \cot\left(\frac{3\pi}{4}d\right)\right) - 2, \qquad \left(\beta_d^{\text{SATWAP}}\right)_q = 2(d-1).$$

The quantum bound can be found by explicitly building the SOS decomposition of the shifted Bell operator, as shown in [SAT+17]. The terms of the SOS decomposition are labeled by $x \in \{1,2\}$ and $k \in \{0,\dots,d-1\}$:

$$P_{x,k} = (A_x^k)^\dagger - C_x^{(k)}.$$

A quick calculation allows us to check the correctness of the SOS decomposition :

$$\begin{aligned}
\beta_q \mathbb{1} - \mathcal{B}_d^{\text{SATWAP}} &= \frac{1}{2}\sum_{k=1}^{d-1}\left(P_{1,k}^\dagger P_{1,k} + P_{2,k}^\dagger P_{2,k}\right) && (64)\\
&= -\mathbb{B}_d^{\text{SATWAP}} + (d-1)\mathbb{1} + \frac{1}{2}\sum_{k=1}^{d-1}\left(C_1^{(d-k)}C_1^{(k)} + C_2^{(d-k)}C_2^{(k)}\right)\\
&= -\mathcal{B}_d^{\text{SATWAP}} + 2(d-1).
\end{aligned}$$

The maximal quantum violation of this inequality is a self-test of a maximally entangled pair of qudits, together with measurements that are unitarily equivalent to the measurements used to maximally violate well-known Collins-Gisin-Linden-Massar-Popescu (CGLMP) Bell inequalities [CGL+02]. We summarise this technical result in the following lemma, proven in [SSKA21].

Lemma 10 ([SSKA21])**.** *The maximal violation of the SATWAP Bell inequality certifies the following:*

- *The dimension of Alice's and Bob's Hilbert spaces is a multiple of d, and we can write their Hilbert space as the tensor products $\mathcal{H}_A = \mathbb{C}^d \otimes \mathcal{H}_{A'}$, $\mathcal{H}_B = \mathbb{C}^d \otimes \mathcal{H}_{B'}$, where $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ are auxiliary Hilbert spaces of finite dimension;*

- *There exist local unitary transformations $U_A : \mathcal{H}_A \to \mathcal{H}_A$ and $U_B : \mathcal{H}_B \to \mathcal{H}_B$ such that*

$$U_B B_1 U_B^\dagger = Z_d \otimes \mathbb{1}_{B'}, \qquad U_B B_2 U_B^\dagger = T_d \otimes \mathbb{1}_{B'}, \tag{65}$$

$$U_A A_1 U_A^\dagger = (a_1^* Z_d + 2(a_1^*)^3 T_d) \otimes \mathbb{1}_{A'}, \qquad U_A A_2 U_A^\dagger = (a_1 Z_d - a_1^* T_d) \otimes \mathbb{1}_{B'}. \tag{66}$$

where $Z_d = diag[1,\omega,\dots,\omega^{d-1}]$ and $T_d = \sum_{i=0}^{d-1}\omega^{i+1/2}|i\rangle\langle i| - \frac{2}{d}\sum_{j,i=0}^{d-1}(-1)^{\delta_{i,0}+\delta_{j,0}}\omega^{(i+j+1)/2}|i\rangle\langle j|$.

- *Alice and Bob share a state $|\psi_{AB}\rangle$ which is unitarily equivalent to the maximally entangled pair of qudits*

$$U_A \otimes U_B|\psi_{AB}\rangle = |\phi_d^+\rangle \otimes |\tau_{A'B'}\rangle.$$

Note that Eqs. (65) fully characterize Bob's measurements, given that they are projective and $B_y^{(k)} = B_y^k$.

For the compiled SATWAP Bell inequality, a modification in the modeling of the quantum prover is necessary. Our focus, thus far, has primarily been on compiled games with binary outputs. The prover is initiated in some quantum state $|\psi\rangle$ and its action in the first round is described in the same way, with eqs. (36) and (37) still holding. However, a generalized k-th order decrypted observable now reads:

$$\begin{aligned}
\mathsf{A}_x^{(k)} &= \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)}\sum_{\mathsf{a}}\omega^{k\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}^\dagger\mathsf{M}_{\mathsf{a}|\mathsf{x}} && (67)\\
&= \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} A_{\mathsf{x}}^{(k)} && (68)
\end{aligned}$$

and the generalized decrypted correlator takes the form

$$\langle \mathsf{A}_x^{(k)}, B_y^{(l)}\rangle = \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x}\sum_{\mathsf{a}}\omega^{k\mathsf{Dec}(\mathsf{a})}\langle\psi_{\mathsf{a}|\mathsf{x}}|B_y^{(l)}|\psi_{\mathsf{a}|\mathsf{x}}\rangle, \tag{69}$$

with this value operationally giving the expectation value of ω^{ak+bl}, which will be directly used to asses the performance of the prover in the SATWAP game.

We generalize the modified moment matrix $\tilde{\mathcal{Q}}$ to include the expectation values of generalized observables. Recall that generalized observables are labeled not only by the input $x \in \mathsf{X}$ (or $y \in \mathsf{Y}$) but also by the degree $k \in$

$\{1, \ldots, d-1\}$ (or l). Every entry of the modified covariance matrix $\tilde{\mathcal{Q}}$ is labeled by two generalized observables, hence is a square matrix of dimension $(|\mathsf{X}| + |\mathsf{Y}|)(d-1)$. Hence, we define a generalization of the matrix $\tilde{\mathcal{Q}}$ as follows

$$\tilde{\mathcal{Q}} = \left[\begin{array}{c|c} \mathbb{1}_{(d-1)|\mathsf{X}|} & C \\ \hline C^T & S \end{array}\right] \tag{70}$$

where $\mathbb{1}_{(d-1)|\mathsf{X}|}$ is $(d-1)|\mathsf{X}| \times (d-1)|\mathsf{X}|$ identity matrix and

$$C = \sum_{x,y,k,l} \langle \mathrm{A}_x^{(d-k)}, B_y^{(l)} \rangle |(k-1)d + x\rangle\langle(l-1)d + y| \tag{71}$$

$$S = \mathop{\mathbb{E}}_{x \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}:\mathsf{Dec}(\mathsf{x})=x} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | B_y^{(d-l)} B_{y'}^{(l')} | \psi_{\mathsf{a}|\mathsf{x}} \rangle |(l-1)d + y\rangle\langle(l'-1)d + y'| \tag{72}$$

with $\langle \mathrm{A}_x^{(k)}, B_y^{(l)} \rangle$ being introduced in eq. (69).

As in 2.6.2, we define a linear operator $\tilde{\mathbb{E}}$ that maps every homogeneous degree-2 polynomial in the variables $\{A_x^{(k)}, B_y^{(l)}\}_{x,y,k,l}$ to linear combinations of elements of matrix $\tilde{\mathcal{Q}}$ in the following way

$$\tilde{\mathbb{E}}[A_x^{(d-k)} B_y^{(l)}] = C_{(k-1)d+x,(l-1)d+y}, \qquad \tilde{\mathbb{E}}[B_y^{(l)} \mathrm{A}_x^{(d-k)}] = C^T_{(l-1)d+y,(k-1)d+x} \tag{73}$$

$$\tilde{\mathbb{E}}[A_x^{(k)} A_{x'}^{(k')}] = \delta_{x,x'}\delta_{k,k'}, \qquad \tilde{\mathbb{E}}[B_y^{(l)} B_{y'}^{(l')}] = S_{(l-1)d+y,(l'-1)d+y'} \tag{74}$$

For $y = y'$, $l = l'$ or $x = x'$, $k = k'$ in eq. (50) we get a consistent mapping of identity

$$\tilde{\mathbb{E}}[A_x^{(d-k)} A_x^{(k)}] = \tilde{\mathbb{E}}[\mathbb{1}] = 1, \qquad \tilde{\mathbb{E}}[B_y^{(d-l)} B_y^{(l)}] = \tilde{\mathbb{E}}[\mathbb{1}] = S_{(l-1)d+y,(l-1)d+y} = 1. \tag{75}$$

With this formalism, we can prove a result equivalent to Theorem (3) for the quantum bound of the compiled SATWAP inequality. Let us first introduce the following lemma.

Lemma 11. *Let $P_{x,k} = (A_x^k)^\dagger - C_x^{(k)}$, where A_x^k is a generalised observable, and $C_x^{(k)}$ are linear sums of generalised observables defined in eq. (62). Then there exists a negligible function $\delta_{\mathrm{QHE}}(\cdot)$ such that we have $\tilde{\mathbb{E}}\left[(P_x^k)^\dagger P_x^k\right] \geq -\delta_{\mathrm{QHE}}(\kappa)$, where $\tilde{\mathbb{E}}[\cdot]$ is the pseudo-expectation map generalised above.*

Proof. The proof follows closely the arguments presented in the proof of Lemma 8, with the difference that generalised observables are not hermitian, and phases are also complex.

$$\begin{aligned}
\tilde{\mathbb{E}}\left[P_{x,k}^\dagger P_{x,k}\right] &= \tilde{\mathbb{E}}\left[(A_x^{(k)})^\dagger A_x^{(k)}\right] - \tilde{\mathbb{E}}\left[(A_x^{(k)})^\dagger C_x^{(k)}\right] - \tilde{\mathbb{E}}\left[(C_x^{(k)})^\dagger A_x^k\right] + \tilde{\mathbb{E}}\left[(C_x^{(k)})^\dagger C_x^{(k)}\right] \\
&= \tilde{\mathbb{E}}\left[A_x^{(d-k)} A_x^{(k)}\right] - \tilde{\mathbb{E}}\left[A_x^{(d-k)} C_x^{(k)}\right] - \tilde{\mathbb{E}}\left[C_x^{(d-k)} A_x^{(k)}\right] + \tilde{\mathbb{E}}\left[C_x^{(d-k)} C_x^{(k)}\right] \\
&= 1 - \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \omega^{(d-k)\mathsf{Dec}(\mathsf{a})} \langle \psi_{\mathsf{a}|\mathsf{x}} | C_x^{(k)} | \psi_{\mathsf{a}|\mathsf{x}} \rangle - \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \omega^{k\mathsf{Dec}(\mathsf{a})} \langle \psi_{\mathsf{a}|\mathsf{x}} | C_x^{(d-k)} | \psi_{\mathsf{a}|\mathsf{x}} \rangle \\
&+ \mathop{\mathbb{E}}_{i \in \mathsf{X}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(i)} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | C_x^{(d-k)} C_x^{(k)} | \psi_{\mathsf{a}|\mathsf{x}} \rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | \left(\mathbb{1} - \omega^{-k\mathsf{Dec}(\mathsf{a})} C_x^{(k)} - \omega^{k\mathsf{Dec}(\mathsf{a})} C_x^{(d-k)} + C_x^{(d-k)} C_x^{(k)} \right) | \psi_{\mathsf{a}|\mathsf{x}} \rangle \\
&\approx_{\delta_{\mathrm{QHE}}(\kappa)} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle \psi_{\mathsf{a}|\mathsf{x}} | \left(\omega^{k\mathsf{Dec}(\mathsf{a})} \mathbb{1} - C_x^{(k)} \right)^2 | \psi_{\mathsf{a}|\mathsf{x}} \rangle \geq 0
\end{aligned}$$

In the second and in the third line we used the linearity of the pseudo-expectation map over sums of generalised observables and the definitions stated above. In the fourth step we apply Lemma 7 to the last addend and we fix the index $i = x$, at the price of a negligible function $\delta_{\mathrm{QHF}}(\kappa)$. We can apply this lemma because $C_x^{(d-k)} C_x^{(k)}$ has a QPT-implementable block encoding, since is composed by linear sums and multiplications of QPT-implementable generalised observables (Corollaries 1 and 2). Finally, using linearity we can group all the terms inside of one average over $\mathsf{x} = \mathsf{Enc}(x)$; we rephrase this sum as an operator square, which is non-negative by definition. □

Theorem 4. *Let's consider the d-dimensional SATWAP Bell inequality, with quantum bound $(\beta_d^{SATWAP})_q$, and its compiled version through Kalai protocol. If d is polynomial w.r.t. the security parameter κ, then the quantum bound of the compiled SATWAP inequality is $(\beta_d^{SATWAP})_q + \theta(\kappa)$, where $\theta(\cdot)$ is a negligible function.*

Proof. Applying the map $\tilde{\mathbb{E}}$ to the shifted SATWAP operator given in eq. (64) gives :

$$\tilde{\mathbb{E}}\left[\beta_q \mathbb{1} - \mathcal{B}_d^{\text{SATWAP}}\right] = \frac{1}{2}\sum_{k=1}^{d-1}\left(\tilde{\mathbb{E}}\left[P_{1,k}^{\dagger}P_{1,k}\right] + \tilde{\mathbb{E}}\left[P_{2,k}^{\dagger}P_{2,k}\right]\right), \tag{76}$$

In Lemma 11 we proved that all elements in the sum on the r.h.s. are non-negative up to a negligible function, *i.e.*

$$\tilde{\mathbb{E}}\left[P_{x,k}^{\dagger}P_{x,k}\right] \approx_\delta \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^{\dagger}\left(\omega^{k\mathsf{Dec}(\mathsf{a})}\mathbb{1} - C_x^{(k)}\right)^2 \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \tag{77}$$

This implies that there exists a negligible function of the security parameter $\theta(\kappa)$ such that the maximal quantum score $\bar{\beta}_q$ in the compiled SATWAP inequality becomes

$$\bar{\beta}_q \leq 2(d-1) + \theta(\kappa). \tag{78}$$

□

Let us now explore self-testing properties, and assume that a QPT prover achieved the score $\bar{\beta}_q$ in the compiled SATWAP inequality. Given eq. (76), reaching the optimal quantum score implies

$$0 = \frac{1}{2}\sum_{k=1}^{d-1}\left(\tilde{\mathbb{E}}\left[P_{1,k}^{\dagger}P_{1,k}\right] + \tilde{\mathbb{E}}\left[P_{2,k}^{\dagger}P_{2,k}\right]\right). \tag{79}$$

By using eqs. (77) and (79) we get

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \langle\psi|\mathsf{M}_{\mathsf{a}|\mathsf{x}}^{\dagger}\left(\omega^{k\mathsf{Dec}(\mathsf{a})}\mathbb{1} - C_x^{(k)}\right)^2 \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \approx_\delta 0, \tag{80}$$

where we write δ as shorthand for δ_{QHE}. This further gives us

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \left\| C_x^{(k)}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle - \omega^{k\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \right\|^2 \approx_\delta 0, \tag{81}$$

further implying that for every k, every x decrypting to x, and every a

$$C_x^{(k)}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \approx_\delta \omega^{k\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle. \tag{82}$$

If we fix k' the previous relation implies

$$\begin{aligned}
\left[C_x^{(1)}\right]^{k'} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle &\approx_\delta \left[C_x^{(1)}\right]^{k'-1} C_x^{(1)}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{2\cdot\delta} \omega^{\mathsf{Dec}(\mathsf{a})}\left[C_x^{(1)}\right]^{k'-1} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{3\cdot\delta} \omega^{2\mathsf{Dec}(\mathsf{a})}\left[C_x^{(1)}\right]^{k'-2} \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\dots \\
&\approx_{k'\cdot\delta} \omega^{k'\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{(k'+1)\cdot\delta} C_x^{(k')}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle,
\end{aligned}$$

where in the second line we used eq. (82) for $k=1$, which we used successively until the last line where we used again eq. (82) for $k = k'$. By summing over a, and noting that $k' < d$ which is polynomially bounded in the security parameter κ we get:

$$\left[C_x^{(1)}\right]^{k}|\psi\rangle \approx_{O(\delta)} C_x^{(k)}|\psi\rangle. \tag{83}$$

Now we develop the following expression for an arbitrary k

$$\begin{aligned}
C_x^{(d-k)}C_x^{(k)}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle &\approx_\delta \omega^{k\mathsf{Dec}(\mathsf{a})}C_x^{(d-k)}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&\approx_{2\delta} \omega^{k\mathsf{Dec}(\mathsf{a})}\omega^{(d-k)\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&= \omega^{d\mathsf{Dec}(\mathsf{a})}\mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle \\
&= \mathsf{M}_{\mathsf{a}|\mathsf{x}}|\psi\rangle,
\end{aligned}$$

where for the first line we used eq. (82), for the second line we used the same equation by changing k to $d-k$, and the last line follows from $\omega^d = 1$. Again by summing over a we obtain

$$C_x^{(d-k)} C_x^{(k)} |\psi\rangle \approx_{O(\delta)} |\psi\rangle, \tag{84}$$

Thus, on the support of $|\psi\rangle$ the observables $C_x^{(k)}$ satisfy condition

$$\left[C_x^{(1)}\right]^k \approx_{O(\delta)} C_x^{(k)}, \qquad C_x^{(d-k)} C_x^{(k)} \approx_{O(\delta)} \mathbb{1}. \tag{85}$$

In [SSKA21] it is proven that these two equations for $O(\delta) = 0$ imply though Lemmas 1, 2, and 3 in the supplementary material therein that there exists a unitary U such that

$$U_B B_1^{(1)} U_B^\dagger = Z_d \otimes \mathbb{1}_{B'}, \qquad U_B B_2^{(1)} U_B^\dagger = T_d \otimes \mathbb{1}_{B'}, \tag{86}$$

with Z_d and T_d being given in Lemma 10. Since $B_1^{(1)}$ and $B_2^{(1)}$ are unitary we get $B_1^{(k)} = \left[B_1^{(1)}\right]^k$ and $B_2^{(k)} = \left[B_2^{(1)}\right]^k$. We conjecture that the derivation procedure is robust to noise, implying that in the case of reaching the optimal quantum violation of the compiled SATWAP inequality relations (86) hold up to a negligible function of the security parameter.

5 Computational self-test of any two binary measurements from a single prover

Let us consider first a family of correlation Bell inequalities introduced in [LMS+23], and further discussed in [BSB23]. The family of Bell inequalities is parameterized with three parameters μ, ν and χ, and the Bell operator is

$$\begin{aligned}\mathcal{B}_{\mu\nu\chi} = &\cos(\mu+\nu)\cos(\mu+\chi)(\cos(\chi)A_0 - \cos(\nu)A_1) \otimes B_0 \\ &+ \cos(\nu)\cos(\chi)(-\cos(\mu+\chi)A_0 + \cos(\mu+\nu)A_1) \otimes B_1\end{aligned} \tag{87}$$

The corresponding family of Bell inequalities involves the CHSH inequality (for $\mu = \chi = 0$ and $\nu = \pi$). A Bell inequality belonging to this family has quantum violations when $\cos(\mu+\chi)\cos(\mu+\nu)\cos(\nu)\cos(\chi) < 0$. Whenever this is the case, reaching the quantum bound

$$\beta_q = \pm \sin(\mu)\sin(\chi-\nu)\sin(\mu+\nu+\chi) \tag{88}$$

self-tests the maximally entangled pair of qubits [WBC23]. This property makes it a good candidate for our compilation procedure. The SOS decomposition of the shifted Bell operator is

$$\beta_q \mathbb{1} - \mathcal{B}_{\mu\nu\chi} = c_0 P_0^\dagger P_0 + c_1 P_1^\dagger P_1, \tag{89}$$

where

$$c_0 = -\frac{\cos(\chi)\cos(\mu+\chi)}{2\sin(\mu)}, \qquad c_1 = -\frac{\cos(\nu)\cos(\mu+\nu)}{2\sin(\mu)}$$

and

$$\begin{aligned}P_0 &= \sin(\mu)A_0 + \cos(\mu+\nu)B_0 - \cos(\nu)B_1 \\ P_1 &= \sin(\mu)A_1 + \cos(\mu+\chi)B_0 - \cos(\chi)B_1\end{aligned}$$

Given the form of the SOS decomposition (89), the optimal value of the compiled inequality $\bar{\beta}_q$ is the same as the quantum bound β_q given in (88) up to a negligible function. Taking the pseudo-expectation value of (89) we get

$$\beta_q - \bar{\beta} = c_0 \tilde{\mathbb{E}}\left[P_0^\dagger P_0\right] + c_1 \tilde{\mathbb{E}}\left[P_1^\dagger P_1\right] \tag{90}$$

As usual, we denote $\hat{B}_0 = (-\cos(\mu+\nu)B_0 + \cos(\nu)B_1)/\sin(\mu)$ and $\hat{B}_1 = -(\cos(\mu+\chi)B_0 + \cos(\chi)B_1)/\sin(\mu)$. If $\bar{\beta} = \beta_q - \varepsilon$, the equation above simply becomes

$$\varepsilon = c_0 \tilde{\mathbb{E}}\left[P_0^\dagger P_0\right] + c_1 \tilde{\mathbb{E}}\left[P_1^\dagger P_1\right]$$

where the two terms on the lhs don't have to be positive. Though, from the result of Lemma 8, we know that they must be positive up to a negligible function depending on the quantum homomorphic encryption scheme:

$$\tilde{\mathbb{E}}\left[P_x^\dagger P_x\right] \geq \underset{\mathsf{x}=\mathsf{Enc}(x)}{\mathbb{E}} \sum_{\mathsf{a}} \left\| \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 - \delta_{\mathrm{QHE}}(\kappa).$$

Using this bound on the previous equation we get the following:

$$\begin{aligned}\varepsilon + (c_0 + c_1)\delta_{\mathrm{QHE}}(\kappa) \geq & c_0 \underset{\mathsf{x}=\mathsf{Enc}(0)}{\mathbb{E}} \sum_{\mathsf{a}} \left\| \hat{B}_0 |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \\ & + c_1 \underset{\mathsf{x}=\mathsf{Enc}(1)}{\mathbb{E}} \sum_{\mathsf{a}} \left\| \hat{B}_1 |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2\end{aligned}$$

where now on the lhs we only have positive quantities. Hence, for all values of x we get this bound:

$$\underset{\mathsf{x}=\mathsf{Enc}(x)}{\mathbb{E}} \sum_{\mathsf{a}} \left\| \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \leq \frac{\varepsilon}{c_x} + \frac{c_0 + c_1}{c_x} \delta_{\mathrm{QHE}}(\kappa) \qquad \forall x \in \{0, 1\}. \tag{91}$$

As a pedagogical introduction, let us see what happens when the maximal quantum score is achieved in the noiseless case, *i.e.* $\varepsilon = 0$ and $\delta_{\mathrm{QHE}} = 0$. The equation above would imply that every addend is equal to zero:

$$\hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle = (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle, \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall \mathsf{a}.$$

When the quantum bound is saturated, the square of the hat operator $\hat{B}_x$ acts like identity on $|\psi_{\mathsf{a}|\mathsf{x}}\rangle$:

$$(\hat{B}_x)^2 |\psi_{\mathsf{a}|\mathsf{x}}\rangle = (-1)^{\mathsf{Dec}(\mathsf{a})} \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle = |\psi_{\mathsf{a}|\mathsf{x}}\rangle \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall \mathsf{a} \tag{92}$$

By the definition of $\hat{B}_0$, and assuming $B_0^2 = B_1^2 = \mathbb{1}$, the following is always true for every state:

$$\begin{aligned}(\hat{B}_0)^2 |\psi_{\mathsf{a}|\mathsf{x}}\rangle &= \left(\frac{\cos^2(\nu) + \cos^2(\nu + \mu)}{\sin^2(\mu)} \mathbb{1} - \frac{\cos(\nu)\cos(\nu + \mu)}{\sin^2(\mu)} \{B_0, B_1\} \right) |\psi_{\mathsf{a}|\mathsf{x}}\rangle \\ &= k_{\mathbb{1}} |\psi_{\mathsf{a}|\mathsf{x}}\rangle - k_{\{\}} \{B_0, B_1\} |\psi_{\mathsf{a}|\mathsf{x}}\rangle\end{aligned} \tag{93}$$

where in the second line we simply fixed a notation for the coefficients of the operators. Equations (92) and (93) together fix the value of the anti-commutator of Bob's observables when the maximal quantum score is achieved:

$$\{B_0, B_1\} |\psi_{\mathsf{a}|\mathsf{x}}\rangle = \frac{k_{\mathbb{1}} - 1}{k_{\{\}}} |\psi_{\mathsf{a}|\mathsf{x}}\rangle = 2\cos(\mu) |\psi_{\mathsf{a}|\mathsf{x}}\rangle \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall \mathsf{a}$$

where the second inequality is a simple trigonometric identity

$$\frac{k_{\mathbb{1}} - 1}{k_{\{\}}} = \frac{\cos^2(\nu) + \cos^2(\nu + \mu) - \sin^2(\mu)}{\sin^2(\mu)} \frac{\sin^2(\mu)}{\cos(\nu)\cos(\nu + \mu)} = 2\cos(\mu).$$

Since all observables are binary, this is a self-test. Indeed, Jordan's lemma ensures that B_0 and B_1 can be simultaneously block-diagonalised such that all blocks are either of size 2×2 or 1×1. In the same way like in [ŠBCB22], we embed every 1×1 into a Hilbert space of larger dimension. This operation does not affect the correlation probabilities, and it simplifies our analysis, as we work with a Jordan decomposition in which all blocks are of the size 2×2. Without loss of generalisation, we can apply a local unitary to the observable B_0 and bring it to Pauli's σ_x in every 2×2 block:

$$U B_0 U^\dagger = \sigma_x \otimes \sum_i |i\rangle\langle i|. \tag{94}$$

We can also safely bring all the 2×2 blocks of B_1 to the XZ plane of the Bloch sphere; by fixing the value of the anti-commutator, we get that B_1 has $\cos(\mu)\sigma_x + \sin(\mu)\sigma_z$ in every block. For every $\mu \neq 0$ we can find ν and χ such that the condition $\cos(\mu + \chi)\cos(\mu + \nu)\cos(\nu)\cos(\chi) < 0$ is satisfied, implying that the quantum bound is larger than the classical. This implies that we can perform a single-prover self-test of any two observables applied by Bob, *i.e.* for every μ there is a compiled XOR game whose maximal violation self-tests Bob's measurements implying:

$$U B_0 U^\dagger = \sigma_x \otimes \mathbb{1}, \qquad U B_1 U^\dagger = (\cos(\mu)\sigma_x + \sin(\mu)\sigma_z) \otimes \mathbb{1} \tag{95}$$

The noiseless assumption is unrealistic, both from a cryptographic and experimental point of view. Assuming a finite security parameter κ and small experimental deviations ϵ, we can still prove that the anti-commutator of Bob's observables is close to the noiseless value, obtaining a robust self-test for Bob's binary observables. Let's start considering Eq. (91) with $\mathsf{x} = \mathsf{Enc}(0)$, and open the sum over a:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \left[\sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| (\hat{B}_0 - \mathbb{1})|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| (\hat{B}_0 + \mathbb{1})|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right] \leq \frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0} \delta_{\mathrm{QHE}}(\kappa)$$

We call the vectors inside the norms as $|\Delta^{\pm}_{\mathsf{a}|\mathsf{x}}\rangle = (\hat{B}_0 \pm \mathbb{1})|\psi_{\mathsf{a}|\mathsf{x}}\rangle$, hence we can write:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \left[\sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| |\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right] \leq \frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0} \delta_{\mathrm{QHE}}(\kappa) \tag{96}$$

Consider again $\hat{B}_0$, its square is:

$$\begin{aligned}(\hat{B}_0)^2 &= \mathbb{1} + (\hat{B}_0 - \mathbb{1}) + \hat{B}_0(\hat{B}_0 - \mathbb{1}) = \mathbb{1} - (\hat{B}_0 + \mathbb{1}) + \hat{B}_0(\hat{B}_0 + \mathbb{1}) \\ &= k_{\mathbb{1}}\mathbb{1} - k_{\{\}}\{B_0, B_1\}\end{aligned}$$

where the first lines are trivial identities, and in the second line we rewrote Eq. (93). Rearranging the terms, and applying the observables on $|\psi_{\mathsf{a}|\mathsf{x}}\rangle$, we obtain the following formula for the anti-commutator of Bob's observables:

$$[2\cos(\mu)\mathbb{1} - \{B_0, B_1\}]\,|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \pm \frac{1}{k_{\{\}}} |\Delta^{\mp}_{\mathsf{a}|\mathsf{x}}\rangle + \frac{1}{k_{\{\}}} \hat{B}_0 |\Delta^{\mp}_{\mathsf{a}|\mathsf{x}}\rangle$$

where to find $2\cos(\mu)$ we used again the trigonometric identity above. We focus first on the equation with $|\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle$. We compute its norm squared, averaging over $\mathsf{x} = \mathsf{Enc}(0)$ and summing over $\mathsf{a} = \mathsf{Enc}(0)$

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| [2\cos(\mu)\mathbb{1} - \{B_0, B_1\}]\,|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 &= \frac{1}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle + \hat{B}_0|\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \\ &\leq \frac{1}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(0)} \left(\left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \left\| \hat{B}_0|\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right) \\ &\leq \frac{1}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(0)} \left(\left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \|\hat{B}_0\|^2 \left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right) \\ &= \frac{1 + \|\hat{B}_0\|^2}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2\end{aligned}$$

where we used Cauchy-Schwarz and the triangle inequality. Similarly, we can find a similar bound summing over $\mathsf{a} = \mathsf{Enc}(1)$ and using the decomposition of the anti-commutator with the vectors $|\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle$:

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| [2\cos(\mu)\mathbb{1} - \{B_0, B_1\}]\,|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 &= \frac{1}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| -|\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle + \hat{B}_0|\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \\ &\leq \frac{1 + \|\hat{B}_0\|^2}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| |\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2\end{aligned}$$

Now, putting together these two result we can bound the sum over a

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \left\| [2\cos(\mu)\mathbb{1} - \{B_0, B_1\}]\,|\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 &\leq \frac{1 + \|\hat{B}_0\|^2}{k^2_{\{\}}} \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \left[\sum_{\mathsf{a}=\mathsf{Enc}(0)} \left\| |\Delta^{-}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 + \sum_{\mathsf{a}=\mathsf{Enc}(1)} \left\| |\Delta^{+}_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \right] \\ &\leq \frac{1 + \|\hat{B}_0\|^2}{k^2_{\{\}}} \left(\frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0} \delta_{\mathrm{QHE}}(\kappa) \right) \\ &\leq \sin^2(\mu) \left[2\cos(\mu) + \frac{1}{\cos(\nu)\cos(\nu + \mu)} \right] \left(\frac{\varepsilon}{c_0} + \frac{c_0 + c_1}{c_0} \delta_{\mathrm{QHE}}(\kappa) \right)\end{aligned}$$

where in the second line we used the bound found in Eq. 96. The angles are fixed from the inequality, therefore in the last line we have some negligible functions in ϵ and κ multiplied by some constant factors depending on the angles. Therefore we proved that, on the support of the states used in the compiled game, the anti-commutator of Bob's observable is $2\cos(\mu)\mathbb{1}$ up to a negligible function $\eta_{anticomm}$:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \left\| [2\cos(\mu)\mathbb{1} - \{B_0, B_1\}] \, |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \leq \eta_{anticomm}(\epsilon, \kappa, \nu, \mu) \tag{97}$$

6 Computational self-test of three Pauli observables

The Elegant Bell inequality, first introduced in [Gis09], considers two parties and binary observables, with input sets $\mathsf{X} \in [4]$ and $\mathsf{Y} \in [3]$. The Bell operator has the form

$$\mathcal{B}^{el} = (A_1 + A_2 - A_3 - A_4) \otimes B_1 + (A_1 - A_2 + A_3 - A_4) \otimes B_2 + (A_1 - A_2 - A_3 + A_4) \otimes B_3$$

The quantum bound $\beta_q = 4\sqrt{3}$ self-tests a maximally entangled pair of qubits and maximally spread measurements for Alice and Bob (hence the elegance) [APVW16]. Specifically, Bob's three measurements form a set of mutually unbiased bases resembling an octahedron in the Bloch sphere, while Alice's four measurements form a dual structure, i.e. a cube.

This can be seen as an XOR game, therefore Theorem 3 applies and the quantum bound of the compiled game is preserved. In the following section we will proof that the self-testing properties of this game are also preserved by Kalai compilation. This is particularly interesting because the self-tested arrangement is not confined to a single plane on the Bloch sphere: is a triplet of MUB measurements in Bloch sphere.

The standard SOS decomposition for the shifted elegant Bell inequality in the nonlocal case is

$$\beta_q \mathbb{1} - \mathcal{B}^{el} = \frac{\sqrt{3}}{2} \sum_{i=1}^{4} P_i^2 \tag{98}$$

with the following definition for the polynomials P_i

$$P_1 = A_1 - \frac{B_1 + B_2 + B_3}{\sqrt{3}}, \qquad P_2 = A_2 - \frac{B_1 - B_2 - B_3}{\sqrt{3}},$$
$$P_3 = A_3 - \frac{-B_1 + B_2 - B_3}{\sqrt{3}}, \qquad P_4 = A_4 - \frac{-B_1 - B_2 + B_3}{\sqrt{3}}.$$

We use the standard notation $P_i = A_i - \hat{B}_i$. When the compiled game reaches the score $\bar{\beta} = \beta_q - \epsilon$, the following is true

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(x)} \sum_{\mathsf{a}} \left\| \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle \right\|^2 \leq \frac{2}{\sqrt{3}}\varepsilon + 4\delta_{\mathrm{QHE}}(\kappa) \qquad \forall x \tag{99}$$

As a pedagogical introduction we study first the noisiless case, with $\delta_{\mathrm{QHE}}(\kappa) = 0$ and $\varepsilon = 0$, implying that

$$\hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle - (-1)^{\mathsf{Dec}(\mathsf{a})} |\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0, \qquad \forall \mathsf{x} : \mathsf{Dec}(\mathsf{x}) = x, \forall x$$

Once again, this proves that the square of the hat operator acts like identity on $|\psi_{\mathsf{a}|\mathsf{x}}\rangle$:

$$(\hat{B}_x)^2 |\psi_{\mathsf{a}|\mathsf{x}}\rangle = (-1)^{\mathsf{Dec}(\mathsf{a})} \hat{B}_x |\psi_{\mathsf{a}|\mathsf{x}}\rangle = |\psi_{\mathsf{a}|\mathsf{x}}\rangle \tag{100}$$

The square of the hat operator can be completely characterized in terms of the anti-commutators of the observables, assuming their projectivity $B_1^2 = B_2^2 = B_3^2 = \mathbb{1}$. Let's consider $x = 1$, then

$$(\hat{B}_1)^2 = \mathbb{1} + \frac{1}{3}\big(\{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)$$

Considering all possible x and Eq. 100, we obtain the following system of equations :

$$\big(+\{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0$$
$$\big(-\{B_1, B_2\} + \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0$$
$$\big(-\{B_1, B_2\} - \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0$$
$$\big(+\{B_1, B_2\} - \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0$$

whose only solution is

$$\{B_1, B_2\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \{B_2, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = \{B_1, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle = 0 \tag{101}$$

This completely fix the three observales: they must be unitarely equivalent to the three Pauli's. See appendix C of [Kan17] for a formal proof of this statement.

To make the self-testing cryptographically and experimentally meaningful it needs to be robust to noise, *i.e.* we need to consider a non-null ε and $\delta_{\mathrm{QHE}}(\kappa)$. We want to prove that all the anti-commutators are still null up to a negligible function depending on the noise ε and the security parameter κ:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \left\|\{B_{y_1}, B_{y_2}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 \leq \eta(\epsilon, \kappa) \qquad \forall y_1 \neq y_2$$

Using similar tricks to the section before [i can expand, but it's trivial] we get the following system of equations:

$$\begin{aligned}
\mathop{\mathrm{E}}_{\mathsf{x}=\mathsf{Enc}(0)} \sum_{\mathsf{a}} \left\|\big(+\{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &\leq 9(1+\sqrt{3})f(\varepsilon) + \delta_{\mathrm{QHE}}(\kappa)\\
\mathop{\mathrm{E}}_{\mathsf{x}=\mathsf{Enc}(1)} \sum_{\mathsf{a}} \left\|\big(-\{B_1, B_2\} + \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &\leq 9(1+\sqrt{3})f(\varepsilon) + \delta_{\mathrm{QHE}}(\kappa)\\
\mathop{\mathrm{E}}_{\mathsf{x}=\mathsf{Enc}(2)} \sum_{\mathsf{a}} \left\|\big(-\{B_1, B_2\} - \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &\leq 9(1+\sqrt{3})f(\varepsilon) + \delta_{\mathrm{QHE}}(\kappa)\\
\mathop{\mathrm{E}}_{\mathsf{x}=\mathsf{Enc}(3)} \sum_{\mathsf{a}} \left\|\big(+\{B_1, B_2\} - \{B_2, B_3\} - \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 &\leq 9(1+\sqrt{3})f(\varepsilon) + \delta_{\mathrm{QHE}}(\kappa)
\end{aligned}$$

Even if the averages are over different values of x, we can change them all to be the same value $\bar{x}$, paying the price of an additional $\delta_{\mathrm{QHE}}(\kappa)$. We expand the definitions of the terms inside the norms. For every equation of the system we will have something like

$$\begin{aligned}
&\left\|\big(\{B_1, B_2\} + \{B_2, B_3\} + \{B_1, B_3\}\big)|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 =\\
&= \left\|\{B_1, B_2\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \left\|\{B_2, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \left\|\{B_3, B_1\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 +\\
&+ \langle\psi_{\mathsf{a}|\mathsf{x}}|\{\{B_1, B_2\}, \{B_2, B_3\}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle + \langle\psi_{\mathsf{a}|\mathsf{x}}|\{\{B_1, B_2\}, \{B_1, B_3\}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle + \langle\psi_{\mathsf{a}|\mathsf{x}}|\{\{B_1, B_3\}, \{B_2, B_3\}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle
\end{aligned}$$

with possibly different signs in the last line. We sum all of the inequalities; only the terms with the norm of the anti-commutators are going to survive, hence

$$4 \mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(\bar{x})} \sum_{\mathsf{a}} \left(\left\|\{B_1, B_2\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \left\|\{B_2, B_3\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 + \left\|\{B_3, B_1\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2\right) \leq 4\left(9(1+\sqrt{3})f(\varepsilon) + 2\delta_{\mathrm{QHE}}(\kappa)\right)$$

All the terms in the sum are positive, hence we obtain the desired bound for all the pairs of anti-correlators:

$$\mathop{\mathbb{E}}_{\mathsf{x}=\mathsf{Enc}(\bar{x})} \sum_{\mathsf{a}} \left\|\{B_{y_1}, B_{y_2}\}|\psi_{\mathsf{a}|\mathsf{x}}\rangle\right\|^2 \leq 9(1+\sqrt{3})f(\varepsilon) + 2\delta_{\mathrm{QHE}}(\kappa) \qquad \forall y_1 \neq y_2 \tag{102}$$

which is indeed the robust version of equation (101).

7 Open problems

Our findings reveal that the compilation procedure introduced in [KLVY23] effectively preserves the quantum bound of XOR games. However, it remains uncertain whether this preservation extends to generic nonlocal games. As demonstrated, the compilation of Bell inequalities is feasible, yet determining whether the quantum bound preservation holds for Bell inequalities not expressible as nonlocal games poses a challenge. In both scenarios, the complexity arises from the inability to find the quantum bound using a simple correlation matrix and the duality of semi-definite programming. Resolving this likely requires using the NPA hierarchy and employing moment matrices with numerous nonobservable elements. An additional open problem pertains to the quantum behavior of compiled games involving more than two players. Modeling a single quantum prover in such instances necessitates a rigorous characterization of sequential encrypted operations. Lastly, understanding the relationship between self-testing in standard nonlocal games and their compiled counterparts proves to be an instructive avenue for future exploration.

Acknowledgements

We thank Paul Hermouet, Dominik Leichtle, Mirjam Weilenmann, Jef Pauwels and Borivoje Dakić for insightful discussions. BB acknowledges support from the European Commission Horizon-CL4 program under grant agreement 101135288 for the EPIQUE project. IŠ acknowledge funding from PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030. ED acknowledges funding from the European Union's Horizon Europe research and innovation program under the grant agreement No 101114043 (QSNP).

References

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007. doi:10.1103/PhysRevLett.98.230501.

[ABOR00] William Aiello, Sandeep Bhatt, Rafail Ostrovsky, and S Raj Rajagopalan. Fast verification of any remote procedure call: Short witness-indistinguishable one-round proofs for NP. In *International Colloquium on Automata, Languages, and Programming*, pages 463–474. Springer, 2000. doi:10.1007/3-540-45022-X_39.

[AFDF+18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, 9(1):459, 2018. doi:10.1038/s41467-017-02307-4.

[AH12] Samson Abramsky and Lucien Hardy. Logical Bell inequalities. *Phys. Rev. A*, 85:062114, Jun 2012. doi:10.1103/PhysRevA.85.062114.

[AM16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, 2016. doi:10.1038/nature20119.

[APVW16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. *Physical Review A*, 93(4), April 2016. doi:10.1103/physreva.93.040102.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. doi:10.1103/RevModPhys.86.419.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

[BGK+23] Zvika Brakerski, Alexandru Gheorghiu, Gregory D. Kahanamoku-Meyer, Eitan Porat, and Thomas Vidick. Simple tests of quantumness also certify qubits. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 162–191. Springer, 2023. doi:10.1007/978-3-031-38554-4_6.

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014. doi:10.1145/2090236.2090262.

[Bra18] Zvika Brakerski. Quantum FHE (almost) as secure as classical. In *Annual International Cryptology Conference*, pages 67–95. Springer, 2018. doi:10.1007/978-3-319-96878-0_3.

[BSB23] Victor Barizien, Pavel Sekatski, and Jean-Daniel Bancal. Custom bell inequalities from formal sums of squares, 2023. arXiv:2308.08601.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on computing*, 43(2):831–871, 2014. doi:10.1109/FOCS.2011.12.

[CGL+02] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Physical review letters*, 88(4):040404, 2002. doi:10.1103/PhysRevLett.88.040404.

[CHSH69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880, 1969. doi:10.1103/PhysRevLett.23.880.

[CMM+24] David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang. A Computational Tsirelson's Theorem for the Value of Compiled XOR Games. Cryptology ePrint Archive, Paper 2024/348, 2024. URL: https://eprint.iacr.org/2024/348.

[Col07] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2007. doi:10.48550/arXiv.0911.3814.

[ECW20] Llorenç Escolà, John Calsamiglia, and Andreas Winter. All tight correlation Bell inequalities have quantum violations. *Phys. Rev. Res.*, 2:012044, Feb 2020. doi:10.1103/PhysRevResearch.2.012044.

[Fin82] Arthur Fine. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.*, 48:291–295, Feb 1982. doi:10.1103/PhysRevLett.48.291.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009. doi:10.1145/1536414.1536440.

[Gis09] Nicolas Gisin. *Bell Inequalities: Many Questions, a Few Answers*, pages 125–138. Springer Netherlands, Dordrecht, 2009. doi:10.1007/978-1-4020-9107-0_9.

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC '19. ACM, June 2019. doi:10.1145/3313276.3316366.

[Kan17] Jędrzej Kaniewski. Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95:062323, Jun 2017. doi:10.1103/PhysRevA.95.062323.

[KLVY23] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum Advantage from Any Non-local Game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1617–1628, 2023. doi:10.1145/3564246.3585164.

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D Rothblum. How to delegate computations: the power of no-signaling proofs. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 485–494, 2014. doi:10.1145/3456867.

[KŠT+19] Jędrzej Kaniewski, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum*, 3:198, 2019. doi:10.22331/q-2019-10-24-198.

[Lau09] Monique Laurent. Sums of squares, moment matrices and optimization over polynomials. *Emerging applications of algebraic geometry*, pages 157–270, 2009. doi:10.1007/978-0-387-09686-5_7.

[LMS+23] Thinh P. Le, Chiara Meroni, Bernd Sturmfels, Reinhard F. Werner, and Timo Ziegler. Quantum correlations in the minimal scenario. *Quantum*, 7:947, March 2023. doi:10.22331/q-2023-03-16-947.

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 332–338, 2018. doi:10.1109/FOCS.2018.00039.

[Mah23] Urmila Mahadev. Classical Homomorphic Encryption for Quantum Circuits. *SIAM Journal on Computing*, 52(6):FOCS18–189–FOCS18–215, 2023. doi:10.1137/18M1231055.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, 2004. doi:10.48550/arXiv.quant-ph/0307205.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007. doi:10.1103/PhysRevLett.98.010401.

[NW10] Miguel Navascués and Harald Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 466(2115):881–890, 2010. doi:10.1098/rspa.2009.0453.

[NZ23] Anand Natarajan and Tina Zhang. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification, 2023. doi:10.48550/arXiv.2303.01545.

[Ost16] Dimiter Ostrev. The structure of nearly-optimal quantum strategies for the non-local xor games. *Quantum Information & Computation*, 16(13-14):1191–1211, 2016. doi:10.26421/QIC16.13-14-6.

[PAB$^+$09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, apr 2009. doi:10.1088/1367-2630/11/4/045021.

[PAM$^+$10] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010. doi:10.1038/nature09008.

[RAD$^+$78] Ronald L Rivest, Len Adleman, Michael L Dertouzos, et al. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

[RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. doi:10.1145/359340.359342.

[SAT$^+$17] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119:040402, Jul 2017. doi:10.1103/PhysRevLett.119.040402.

[ŠB20] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020. doi:10.22331/q-2020-09-30-337.

[ŠBCB22] Ivan Šupić, Jean-Daniel Bancal, Yu Cai, and Nicolas Brunner. Genuine network quantum nonlocality and self-testing. *Physical Review A*, 105(2), February 2022. doi:10.1103/physreva.105.022206.

[SMA08] J. Silman, S. Machnes, and N. Aharon. On the relation between Bell's inequalities and nonlocal games. *Physics Letters A*, 372(21):3796–3800, 2008. doi:10.1016/j.physleta.2008.03.001.

[SSKA21] Shubhayan Sarkar, Debashis Saha, Jędrzej Kaniewski, and Remigiusz Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. *npj Quantum Information*, 7(1), October 2021. doi:10.1038/s41534-021-00490-3.

[TPKBA24] Armin Tavakoli, Alejandro Pozas-Kerstjens, Peter Brown, and Mateus Araújo. Semidefinite programming relaxations for quantum correlations, 2024. doi:10.48550/arXiv.2307.02551.

[Tsi87] Boris Tsirelson. Quantum analogues of the Bell inequalities. the case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987. doi:10.1007/BF01663472.

[VV14] Umesh Vazirani and Thomas Vidick. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014. doi:10.1103/PhysRevLett.113.140501.

[WBC23] Lewis Wooltorton, Peter Brown, and Roger Colbeck. Device-independent quantum key distribution with arbitrarily small nonlocality, 2023. arXiv:2309.09650.

[Weh06] Stephanie Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Phys. Rev. A*, 73:022110, Feb 2006. doi:10.1103/PhysRevA.73.022110.

Polylog-time- and constant-space-overhead fault-tolerant quantum computation with quantum low-density parity-check codes

Shiro Tamiya[1 4 *] Masato Koashi[1 2 †] Hayata Yamsaki[3 4 ‡]

[1] *Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

[2] *Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

[3] *Department of Physics, Graduate School of Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*

[4] *Nanofiber Quantum Technologies, Inc., 1-22-3 Nishiwaseda, Shinjuku-ku, Tokyo 169-0051,Japan.*

Abstract. A major challenge in fault-tolerant quantum computation (FTQC) is reducing space overhead, i.e., the large number of physical qubits per logical qubit, and time overhead, i.e., long physical gate sequences per logical gate. We prove that a protocol using finite-rate quantum LDPC codes with concatenated Steane codes achieves constant space overhead and polylogarithmic time overhead, even accounting for non-zero classical computation time. This protocol improves the time overhead upon constant-space-overhead protocols using quantum LDPC codes with polynomial time overhead and quasi-polylogarithmic time overhead using concatenated quantum Hamming codes. This result reveals the quantum LDPC code approach can achieve time-efficient FTQC while maintaining constant overhead, as well as the code-concatenation approach, and it underscores the need for a comprehensive investigation into the feasibility of physical implementation of the two approaches.

Keywords: Fault-tolerant quantum computation, Quantum error correction, Quantum LDPC codes, Quantum concatenated codes, Quantum expander codes, Steane code

1 Background

Quantum computation has promising potential for faster computation compared to classical computation [1, 2]. However, implementing quantum computation using physical qubits directly as qubits in an original circuit representing the computation may corrupt the results of the computation due to errors inherent in quantum devices. To address this problem, fault-tolerant quantum computation (FTQC) [3, 4] has been developed. FTQC enables the simulation of an original quantum circuit using the logical qubits of a quantum error-correcting code, rather than physical qubits. By employing techniques of quantum error correction, FTQC ensures accurate quantum computation even in the presence of errors that may accumulate as the size of the original circuit increases [3, 4].

Currently, there are two major FTQC schemes: one is a concatenated code scheme [5–7] and the other is a quantum low-density parity-check (LDPC) code scheme [8–19]. Both schemes have a threshold theorem [5, 6, 8, 20–26], which states that the failure probability of the fault-tolerant simulation can be arbitrarily suppressed, given that the physical error rate is below a certain threshold. However, conventional FTQC schemes, such as those using surface codes [10, 11] and concatenated Steane codes [6], require a substantial increase in the number of physical qubits per logical qubit, which scales polylogarithmically with the size of the original quantum circuit [6, 18]. This poses a challenge, as the number of physical qubits in quantum devices is limited, making the space overhead the primary obstacle to realizing FTQC. In addition to space overhead, time overhead, which refers to the ratio of the physical time step in simulating an original circuit to the time step in an original circuit, is also important to retain the speedups of quantum computation. The conventional FTQC schemes scale polylogarithmically in time overhead with the size of the original circuit [6, 18]. Reducing both space and time overhead in FTQC is of great interest from both practical and theoretical perspectives.

One of the main interests in the field of FTQC is how short a time overhead we can achieve while simultaneously maintaining a constant space overhead. In recent years, there have been advances in this problem. Reference [12] clarified the properties that a non-vanishing-rate quantum LDPC code must retain to achieve FTQC with a constant space overhead in combination with concatenated codes. Subsequently, Refs. [13, 27] showed that quantum expander codes [13, 28, 29] can be used as the quantum LDPC code for this protocol. Although this protocol keeps the space overhead constant, it sacrifices the parallelism of the gate; that is, this protocol has a limitation on the number of logical gates that can be performed per time step. As a result, sequential gate implementation was necessary for this protocol, leading to a polynomial increase in time overhead. More recently, Refs. [7, 30] resolved this bottleneck of constant-space-overhead protocols by developing a new protocol based on concatenated codes to achieve quasi-polylogarithmic time overhead while also achieving constant space overhead.

However, it still remains an open question whether it is

[*] shiro.tamiya01@gmail.com

[†] koashi@qi.t.u-tokyo.ac.jp

[‡] hayata.yamasaki@gmail.com

possible to design an even faster constant-space-overhead protocol that achieves polylogarithmic time overhead, which is shorter than the quasi-polylogarithmic time overhead and as fast as the conventional polylogarithmic-space-overhead protocols. This question relates to a trade-off relation between the space and time overheads in FTQC, originally raised in [12]. On the one hand, there exist fault-tolerant protocols where both the space overhead and time overhead are polylogarithmic [6, 18]. One the other hand, when space overhead is reduced to a constant, an ideal trade-off would be that the time overhead remains polylogarithmic, with only a higher degree polynomial, but existing constant-space-overhead protocols exhibit the polynomial or quasi-polylogarithmic time overheads [7, 12, 13, 27], resulting in apparently redundant time overhead. This issue highlights the challenge of understanding the trade-off relation of space and time overhead in FTQC.

2 Results

In this work, we demonstrate that FTQC can achieve a polylogarithmic time overhead while maintaining a constant space overhead, eliminating the redundant tradeoff between space overhead and time overhead. To achieve this goal, we analyze a hybrid fault-tolerant protocol that combines concatenated Steane code [6] and non-vanishing-rate quantum LDPC codes with an efficient decoding algorithm, in particular the quantum expander codes [13, 28, 29]. In our hybrid protocol, non-vanishing-rate quantum LDPC codes serve as registers to store and protect logical qubits, while concatenated codes serve to implement logical gate operations on logical qubits through gate teleportation [3, 31, 32] by preparing auxiliary encoded states of the non-vanishing-rate quantum LDPC codes.

Theorem 1 *Let $\{\mathrm{C}_n\}$ be a sequence of original circuits specified by an integer n. Each circuit C_n has width $W(n)$ and depth $D(n)$, where the size of C_n is polynomially bounded, i.e., $|\mathrm{C}_n| = O(W(n)D(n)) = O(\mathrm{poly}(n))$ as $n \to \infty$. Then, for all $\varepsilon > 0$, there exists a threshold $p_{\mathrm{th}} > 0$ and if the error rate $p < p_{\mathrm{th}}$, there exists a sequence of fault-tolerant circuits $\{\mathrm{C}_n^{\mathrm{FT}}\}$ and each circuit $\mathrm{C}_n^{\mathrm{FT}}$ has a width $W_{\mathrm{FT}}(n)$ and a depth $D_{\mathrm{FT}}(n)$ that satisfy*

$$\begin{aligned}\frac{W_{\mathrm{FT}}(n)}{W(n)} &= O(1),\\ \frac{D_{\mathrm{FT}}(n)}{D(n)} &= O\left(\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right),\end{aligned} \tag{1}$$

as $n \to \infty$, and $\mathrm{C}_n^{\mathrm{FT}}$ outputs the probability distribution that is close to that of C_n with total variation distance at most ε.

The formal statement of Theorem 1 and its proof is given in Sec. V E of the technical version and the definition of circuits and the noise model is given in Sec. III.

The summaries of our contributions are as follows.

1. *Construction of fault-tolerant protocol with higher parallelization of logical gates.*— Our crucial contribution for achieving polylogarithmic-time- and constant-space-overhead fault-tolerant protocol is demonstrating our fault-tolerant protocol can achieve the higher parallelism for executing logical gates than the existing constant-space-overhead protocols with quantum LDPC codes [3, 13, 27]. The existing protocols execute the logical gates sequentially. Specifically, they execute logical gates acting on $O(W(n)/\mathrm{polylog}(n))$ logical qubits at a single time step. However, taking into account advances in the analysis of error suppression by decoding algorithms [13, 27], we show that our protocol can increase parallelism to achieve a polylogarithmic time overhead while maintaining a constant space overhead.

2. *Identification of fault-tolerance conditions for quantum LDPC codes.*— We clarify the fault-tolerance conditions for quantum LDPC codes on gadgets that intend to perform logical operations acting on logical qubits in a quantum LDPC code. For details, see the techical version in Sec. V C. Unlike the fault-tolerance conditions for protocols based on concatenated codes [6, 7], the conditions do not require transversality, i.e., gadgets can be implemented by a tensor product of gates acting individually on each physical qubit, but require gadgets to have a constant depth and for the number of physical qubits through which errors can propagate via physical operations to be constant. These conditions contribute to the explicit construction of fault-tolerant protocols using quantum LDPC codes and show the existence of a threshold.

3. *Existence of threshold considering classical computation with non-negligible runtime.*— The existing analysis of the constant-space-overhead protocol with quantum LDPC codes assumes that classical computation, which is used in such as decoding algorithms and gate teleportation [13, 27, 33], can be performed instantaneously in zero time. However, in practice, the classical computation required to perform FTQC has a non-zero runtime that grows as the size of original circuits becomes large, which cannot be ignored in achieving a scalable physical implementation of FTQC. To address this issue, our analysis explicitly takes into account the nonzero runtime of classical computation in executing the protocol. For this purpose, we employ the constant-time decoding algorithms in Ref. [27]. Our contribution is to bound the runtime of all classical computations required to perform the fault-tolerant protocol (for details, see Sec. V D of the technical version). Remarkably, even when considering the runtime of classical computations, our constant-space-overhead protocol can exhibit polylogarithmic time overhead.

4. *A threshold analysis of fault-tolerant protocol for simulating open circuits.*—We provide a threshold analysis of fault-tolerant protocol using con-

catenated Steane code to implement open quantum circuits that do not end with measurements, as in Refs. [25, 34], whereas conventional analysis of FTQC with concatenated codes is applicable only to the circuits ending with measurements [6, 7]. Our formal proof is given in Sec. IV B of the technical version. In our protocol, this protocol is not used in isolation. It is integrated into the protocol with quantum LDPC codes in such a way that we use the concatenated Steane code to prepare encoded states of quantum LDPC codes in a fault-tolerant way. The threshold theorem for open circuits is used without an explicit proof in Refs. [12, 13, 27], but we prove the theorem based on our protocol and the local stochastic Pauli error model [3], to complete the full proof of the threshold theorem for the fault-tolerant protocol using quantum LDPC codes.

3 Conclusion

Our results show our protocol using non-vanishing-rate quantum LDPC codes with concatenated Steane codes attains both constant space and polylogarithmic time overheads. Our results represent a crucial step toward FTQC achieving significant quantum speedups with a feasibly bounded number of qubits and a negligibly small slowdown. Furthermore, we have resolved the issue of redundant spacetime trade-offs present in existing constant-space-overhead FTQC protocols. This work indicates promising potential for low-overhead FTQC using a hybrid approach of non-vanishing-rate quantum LDPC codes and concatenated codes.

References

[1] Ashley Montanaro. “Quantum algorithms: an overview”. In: *npj Quantum Information* 2.1 (Jan. 2016). ISSN: 2056-6387. DOI: 10.1038/npjqi.2015.23. URL: http://dx.doi.org/10.1038/npjqi.2015.23.

[2] Alexander M. Dalzell et al. *Quantum algorithms: A survey of applications and end-to-end complexities.* 2023. arXiv: 2310.03011 [quant-ph].

[3] Daniel Gottesman. “An introduction to quantum error correction and fault-tolerant quantum computation”. In: *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics.* Vol. 68. 2010, pp. 13–58.

[4] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[5] Dorit Aharonov and Michael Ben-Or. *Fault-Tolerant Quantum Computation With Constant Error Rate.* 1999. arXiv: quant-ph/9906129 [quant-ph].

[6] Panos Aliferis, Daniel Gottesman, and John Preskill. *Quantum accuracy threshold for concatenated distance-3 codes.* 2005. arXiv: quant-ph/0504218 [quant-ph].

[7] Hayata Yamasaki and Masato Koashi. “Time-Efficient Constant-Space-Overhead Fault-Tolerant Quantum Computation”. In: *Nature Physics* 20.2 (Jan. 2024), 247–253. ISSN: 1745-2481. DOI: 10.1038/s41567-023-02325-8. URL: http://dx.doi.org/10.1038/s41567-023-02325-8.

[8] A. Yu Kitaev. “Quantum computations: algorithms and error correction”. In: *Russian Mathematical Surveys* 52.6 (Dec. 1997), pp. 1191–1249. DOI: 10.1070/RM1997v052n06ABEH002155.

[9] A.Yu. Kitaev. “Fault-tolerant quantum computation by anyons”. In: *Annals of Physics* 303.1 (Jan. 2003), 2–30. ISSN: 0003-4916. DOI: 10.1016/s0003-4916(02)00018-0. URL: http://dx.doi.org/10.1016/S0003-4916(02)00018-0.

[10] S. B. Bravyi and A. Yu. Kitaev. *Quantum codes on a lattice with boundary.* 1998. arXiv: quant-ph/9811052 [quant-ph].

[11] Daniel Litinski. “A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery”. In: *Quantum* 3 (Mar. 2019), p. 128. ISSN: 2521-327X. DOI: 10.22331/q-2019-03-05-128. URL: http://dx.doi.org/10.22331/q-2019-03-05-128.

[12] Daniel Gottesman. “Fault-tolerant quantum computation with constant overhead”. In: *Quantum Info. Comput.* 14.15–16 (2014), 1338–1372. ISSN: 1533-7146.

[13] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. “Constant Overhead Quantum Fault-Tolerance with Quantum Expander Codes”. In: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS).* IEEE, Oct. 2018. DOI: 10.1109/focs.2018.00076. URL: http://dx.doi.org/10.1109/FOCS.2018.00076.

[14] Héctor Bombín. “Single-Shot Fault-Tolerant Quantum Error Correction”. In: *Phys. Rev. X* 5 (3 2015), p. 031043. DOI: 10.1103/PhysRevX.5.031043. URL: https://link.aps.org/doi/10.1103/PhysRevX.5.031043.

[15] Maxime A. Tremblay, Nicolas Delfosse, and Michael E. Beverland. “Constant-Overhead Quantum Error Correction with Thin Planar Connectivity”. In: *Phys. Rev. Lett.* 129 (5 2022), p. 050504. DOI: 10.1103/PhysRevLett.129.050504. URL: https://link.aps.org/doi/10.1103/PhysRevLett.129.050504.

[16] Christopher A Pattison, Anirudh Krishna, and John Preskill. “Hierarchical memories: Simulating quantum ldpc codes with local gates”. In: *arXiv preprint arXiv:2303.04798* (2023).

[17] Sergey Bravyi et al. “High-threshold and low-overhead fault-tolerant quantum memory”. In: *Nature* 627.8005 (2024), pp. 778–782.

[18] Austin G. Fowler et al. “Surface codes: Towards practical large-scale quantum computation”. In: *Physical Review A* 86.3 (Sept. 2012). ISSN: 1094-1622. DOI: 10.1103/physreva.86.032324. URL: http://dx.doi.org/10.1103/PhysRevA.86.032324.

[19] Nikolas P. Breuckmann and Jens Niklas Eberhardt. “Quantum Low-Density Parity-Check Codes”. In: *PRX Quantum* 2.4 (Oct. 2021). ISSN: 2691-3399. DOI: 10.1103/prxquantum.2.040101. URL: http://dx.doi.org/10.1103/PRXQuantum.2.040101.

[20] Emanuel Knill, Raymond Laflamme, and Wojciech H. Zurek. “Resilient quantum computation: error models and thresholds”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 454.1969 (Jan. 1998), 365–384. ISSN: 1471-2946. DOI: 10.1098/rspa.1998.0166. URL: http://dx.doi.org/10.1098/rspa.1998.0166.

[21] Ben W. Reichardt. *Fault-tolerance threshold for a distance-three quantum code*. 2005. arXiv: quant-ph/0509203 [quant-ph].

[22] Barbara M. Terhal and Guido Burkard. “Fault-tolerant quantum computation for local non-Markovian noise”. In: *Physical Review A* 71.1 (Jan. 2005). ISSN: 1094-1622. DOI: 10.1103/physreva.71.012336. URL: http://dx.doi.org/10.1103/PhysRevA.71.012336.

[23] Panos Aliferis and John Preskill. “Fault-tolerant quantum computation against biased noise”. In: *Phys. Rev. A* 78 (5 2008), p. 052331. DOI: 10.1103/PhysRevA.78.052331. URL: https://link.aps.org/doi/10.1103/PhysRevA.78.052331.

[24] Panos Aliferis and Barbara M. Terhal. *Fault-Tolerant Quantum Computation for Local Leakage Faults*. 2006. arXiv: quant-ph/0511065 [quant-ph].

[25] Panos Aliferis, Daniel Gottesman, and John Preskill. *Accuracy threshold for postselected quantum computation*. 2007. arXiv: quant-ph/0703264 [quant-ph].

[26] John Preskill. “Reliable quantum computers”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 454.1969 (Jan. 1998), 385–410. ISSN: 1471-2946. DOI: 10.1098/rspa.1998.0167. URL: http://dx.doi.org/10.1098/rspa.1998.0167.

[27] Antoine Grospellier. “Constant time decoding of quantum expander codes and application to fault-tolerant quantum computation”. Theses. Sorbonne Université, Nov. 2019. URL: https://theses.hal.science/tel-03364419.

[28] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. “Quantum Expander Codes”. In: *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*. 2015, pp. 810–824. DOI: 10.1109/FOCS.2015.55.

[29] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. “Efficient decoding of random errors for quantum expander codes”. In: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*. STOC ’18. ACM, June 2018. DOI: 10.1145/3188745.3188886. URL: http://dx.doi.org/10.1145/3188745.3188886.

[30] Satoshi Yoshida, Shiro Tamiya, and Hayata Yamasaki. *Concatenate codes, save qubits*. 2024. arXiv: 2402.09606 [quant-ph].

[31] E. Knill. *Scalable Quantum Computation in the Presence of Large Detected-Error Rates*. 2004. arXiv: quant-ph/0312190 [quant-ph].

[32] E. Knill. “Quantum computing with realistically noisy devices”. In: *Nature* 434.7029 (Mar. 2005), 39–44. ISSN: 1476-4687. DOI: 10.1038/nature03350. URL: http://dx.doi.org/10.1038/nature03350.

[33] Daniel Gottesman and Isaac L. Chuang. “Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations”. In: *Nature* 402.6760 (1999), pp. 390–393. ISSN: 1476-4687. DOI: 10.1038/46503. URL: https://doi.org/10.1038/46503.

[34] Matthias Christandl and Alexander Müller-Hermes. *Fault-tolerant Coding for Quantum Communication*. 2022. arXiv: 2009.07161 [quant-ph].

Technical version:
Polylog-time- and constant-space-overhead fault-tolerant quantum computation with quantum low-density parity-check codes

Technical version of "Polylog-time- and constant-space-overhead fault-tolerant quantum computation with quantum low-density parity-check codes" is organized as follows. In Sec. I, we present preliminaries for this work. In Sec. II, we describe the setting of FTQC. In Sec. III, we provide a rigorous analysis of the fault-tolerant protocol using concatenated Steane codes for implementing open quantum circuits (which do not terminate with measurements) to prepare encoded states of non-vanishing-rate quantum LDPC codes. In Sec. IV, using this protocol, we present and analyze the hybrid protocol using non-vanishing-rate quantum LDPC codes and concatenated Steane codes to achieve polylog-time and constant-space-overhead FTQC; in particular, we prove the threshold theorem for this protocol and bound its time and space overhead in Sec. IV E. Finally, in Sec. V, we conclude our work.

I. PRELIMINARIES

In this section, we present preliminaries used in our paper. In Sec. I A, we start with introducing the Pauli group and the Clifford group, along with their binary representations. In Sec. I B, we introduce the quantum error-correcting codes used in our fault-tolerant protocol.

A. Pauli group and Clifford group

We present the basics of the Pauli group and the Clifford group. The Pauli group is defined as follows.

Definition 1 (Pauli group)**.** Let X, Y, and Z be the Pauli operators defined as

$$X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y \coloneqq \mathrm{i}XZ = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}. \tag{1}$$

The Pauli group on n qubits, denoted by $\mathcal{P}_n$, consists of $2^n \times 2^n$ matrices in the form of

$$P = \alpha \bigotimes_{i=0}^{n-1} P_i, \tag{2}$$

where $\alpha \in \{\pm 1, \pm \mathrm{i}\}$ and $P_i \in \{I, X, Y, Z\}$. Here, I is an identity matrix with size 2×2 and $\mathrm{i} = \sqrt{-1}$. In particular, when specifying the dimension of the identity operator, the identity opeator with size $2^n \times 2^n$ is denoted by I_n. Also, let $\langle \mathrm{i}I_n \rangle$ be the center of the Pauli group $\mathcal{P}_n$, generated by $\mathrm{i}I_n$. The projective Pauli group is defined as the Pauli group where global phases are ignored, i.e.,

$$\tilde{\mathcal{P}}_n \coloneqq \mathcal{P}_n / \langle \mathrm{i}I_n \rangle, \tag{3}$$

where representatives of $\tilde{\mathcal{P}}_n$ are selected by fixing $\alpha = 1$.

The eigenvectors of the Pauli-Z operator serve as a particular basis for a qubit, which is referred to as the computational basis. This basis is denoted by $\{|0\rangle, |1\rangle\}$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of the Pauli-Z operator, corresponding to the eigenvalues $+1$ and -1, respectively. As a special case of projective measurement, we often use the measurement of the Pauli operator $P \in \mathcal{P}_n$ whose projective operators $\{\Pi_m\}_m$ associated with the measurement outcomes $m \in \{0, 1\}$ are defined as

$$\Pi_0 \coloneqq (I_n + P)/2, \;\; \Pi_1 \coloneqq (I_n - P)/2. \tag{4}$$

For a given Pauli operator $P \in \mathcal{P}_n$, the weight of P, denoted by $|P|$, is defined as the number of qubits on which P acts non-trivially, i.e.,

$$|P| \coloneqq \#\{i \in \{1, \ldots, n\} \colon P_i \neq I\}, \tag{5}$$

where P_i is given by (2).

The Clifford group is defined as the group whose elements map Pauli operators to Pauli operators under conjugation.

Definition 2 (Clifford group)**.** Let $\mathbb{U}(d)$ be the unitary group on the set $\mathbb{C}^d$ of complex vectors. The Clifford group on n qubits is the normalizer of the n-qubit Pauli group,

$$\mathcal{C}_n \coloneqq \{C \in \mathbb{U}(2^n) \mid CPC^\dagger \in \mathcal{P}_n, \forall P \in \mathcal{P}_n\}. \tag{6}$$

where $(\cdot)^\dagger$ represents the adjoint of $(\cdot)$. The elements of the Clifford group are called Clifford operators. Furthermore, the projective Clifford group is defined as

$$\tilde{\mathcal{C}}_n \coloneqq \mathcal{C}_n / \mathbb{U}(1), \tag{7}$$

where our analysis does not need to specify the representative of $\tilde{\mathcal{C}}_n$ while the representative of $\tilde{\mathcal{C}}_n / \tilde{\mathcal{P}}_n$ will be specified later in (14).

The symplectic representation of Pauli operators allows us to perform several calculations on Pauli operators using a binary vector. The definition of the symplectic representation of Pauli operators is as follows.

Definition 3. (Symplectic representation of Pauli operators)

Let $P = \bigotimes_{i=1}^n P_i \in \tilde{\mathcal{P}}_n$ be a Pauli operator. The mapping $\phi \colon \tilde{\mathcal{P}}_n \to \mathbb{F}_2^{2n}$ provides the symplectic representation of P. In this representation, P is mapped to a pair of row vectors $x, z \in \mathbb{F}_2^n$, denoted by $\phi(P) \coloneqq [x, z] \in \mathbb{F}_2^{2n}$, according to the following rules:

$$\text{if } P_i = I,\ \ x_i = 0 \text{ and } z_i = 0, \tag{8}$$
$$\text{if } P_i = X,\ x_i = 1 \text{ and } z_i = 0, \tag{9}$$
$$\text{if } P_i = Y,\ \ x_i = 1 \text{ and } z_i = 1, \tag{10}$$
$$\text{if } P_i = Z,\ x_i = 0 \text{ and } z_i = 1. \tag{11}$$

Since $\tilde{\mathcal{P}}_n \cong \mathbb{F}_2^{2n}$, when we ignore the global phase of the Pauli operator, the multiplication in two Pauli operators $P_1, P_2 \in \tilde{\mathcal{P}}_n$ can be calculated with their symplectic representation as

$$\phi(P_1) \oplus \phi(P_2), \tag{12}$$

where $\oplus$ represents the bitwise exclusive OR (XOR). Moreover, the multiplication in $P_1, P_2 \in \tilde{\mathcal{P}}_n$ can also be expressed as

$$P_1 P_2 = (-1)^{xz'^\top + x'z^\top} P_2 P_1, \tag{13}$$

where $\phi(P_1) = [x, z] \in \mathbb{F}_2^{2n}$, $\phi(P_2) = [x', z'] \in \mathbb{F}_2^{2n}$, and $z^\top$ represents the transpose of z. Thus, the commutator between two Pauli operators corresponds to $xz'^\top + x'z^\top$ in (13), which is defined as the symplectic inner product.

The conjugation of a Pauli operator in $\tilde{\mathcal{P}}_n$ by a Clifford operator in $\tilde{\mathcal{C}}_n$ is carried out in a way that maintains the symplectic inner product. From Refs. [1, 2], we have $\tilde{\mathcal{C}}_n/\tilde{\mathcal{P}}_n \cong \mathrm{Sp}(2n, \mathbb{F}_2)$, where the equivalence relation is defined by conjugation, and $\mathrm{Sp}(2n, \mathbb{F}_2)$ represents the group of $2n \times 2n$ symplectic matrices over $\mathbb{F}_2$. In addition, the corresponding $\Gamma \in \mathrm{Sp}(2n, \mathbb{F}_2)$ can be identified by mapping $[e_i, 0] \mapsto [x, z]$ and $[0, e_j] \mapsto [x', z']$, where e_i is the standard basis vector of $\mathbb{F}_2^n$ that has an entry 1 in the i-th column and 0 otherwise [2]. These facts provide the symplectic matrix $\gamma(C) \in \mathbb{F}_2^{2n\times 2n}$ of a representative of a Clifford operator $C \in \tilde{\mathcal{C}}_n/\tilde{\mathcal{P}}_n$ [2] as

$$\gamma(C) := \begin{bmatrix} \phi(CX_n^{(1)}C^\dagger)^\top & \cdots & \phi(CX_n^{(n)}C^\dagger)^\top & \phi(CZ_n^{(1)}C^\dagger)^\top & \cdots & \phi(CZ_n^{(n)}C^\dagger)^\top \end{bmatrix}, \tag{14}$$

where $X_n^{(i)} (Z_n^{(i)}) \in \tilde{\mathcal{P}}$ represents an n-qubit Pauli operator that acts as $X (Z)$ on the i-th qubit, and as I otherwise. The conjugation of a Pauli operator $P \in \tilde{\mathcal{P}}_n$ by a Clifford operator $C \in \tilde{\mathcal{C}}_n/\tilde{\mathcal{P}}_n$ can be calculated by multiplying the matrix $\gamma(C) \in \mathbb{F}_2^{2n\times 2n}$ with the vector $\phi(P) \in \mathbb{F}_2^{2n}$ from the right, i.e.,

$$\phi(P)\gamma(C). \tag{15}$$

The group $\tilde{\mathcal{C}}_n/\tilde{\mathcal{P}}_n$ is generated by the H operator, S operator, and CNOT operator defined as

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{16}$$

$$S := \begin{bmatrix} e^{-\mathrm{i}\frac{\pi}{4}} & 0 \\ 0 & e^{\mathrm{i}\frac{\pi}{4}} \end{bmatrix} = R_Z\left(\frac{\pi}{2}\right), \tag{17}$$

$$\mathrm{CNOT} := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{18}$$

where $R_Z(\theta) := e^{-\mathrm{i}\frac{\pi}{2}\theta Z} = \begin{bmatrix} e^{-\mathrm{i}\frac{\pi}{2}\theta} & 0 \\ 0 & e^{\mathrm{i}\frac{\pi}{2}\theta} \end{bmatrix}$. A Clifford operator $C \in \tilde{\mathcal{C}}_n/\tilde{\mathcal{P}}_n$ can be decomposed into 11 rounds in a sequence, where each round uses only one type of Clifford operator in the order of H, CNOT, S, CNOT, S, CNOT, H, S, CNOT, S, CNOT [3]. In this paper, the decomposed form is chosen as a representative of $\tilde{\mathcal{C}}_n/\tilde{\mathcal{P}}_n$.

B. Concatenated Steane codes and non-vanishing-rate quantum LDPC codes

In this section, we present basics of stabilizer codes that we will use in this paper. In Sec. I B 1, we introduce stabilizer codes and Calderbank-Shor-Steane (CSS) codes. In Sec. I B 2, we explain the Steane code as an important class of CSS codes and its code concatenation. In Sec. I B 3, we explain quantum LDPC codes.

1. *Stabilizer codes and Calderbank-Shor-Steane (CSS) codes*

A quantum error-correcting code $\mathcal{Q}$ with N physical qubits is a subspace $\mathcal{Q}$ of a 2^N-dimensional Hilbert space, i.e., $\mathcal{Q} \subseteq (\mathbb{C}^2)^{\otimes N}$, where $\mathbb{C}^2 = \mathrm{span}\{|0\rangle, |1\rangle\}$ represents a qubit. We consider a stabilizer code, which is specified by its stabilizer $\mathcal{S} \subset \mathcal{P}_N$, which is an Abelian subgroup of $\mathcal{P}_N$ satisfying $-I \notin \mathcal{S}$. The centralizer $C(\mathcal{S})$ consists of all Pauli operators that commute with all elements in $\mathcal{S}$. If $\mathcal{S}$ is generated by $N - K$ independent elements, then the corresponding space $\mathcal{Q}(\mathcal{S})$ is a 2^K-dimensional subspace that is invariant under the action of $\mathcal{S}$. Logical operators are elements of the set $C(\mathcal{S}) \setminus \mathcal{S}$. For each $k \in [1, \ldots, K]$, one can choose the associated logical X and Z operators in $C(\mathcal{S}) \setminus \mathcal{S}$ that obey the Pauli commutation relation. In this case, the subspace is isomorphic to a space of K qubits, which are called the *logical qubits*. We refer to the subspace $\mathcal{Q}(\mathcal{S})$ as the *code space* and a state of logical qubits as a *codeword*. The minimum number of physical qubits that any non-trivial logical operator acts upon is referred to as the *distance*. A stabilizer code $\mathcal{Q}(\mathcal{S})$ with the parameters of the number of physical qubits N, the number of logical qubits K, and distance D is denoted by an $[[N, K, D]]$ code. Furthermore, the rate R of the code $\mathcal{Q}(\mathcal{S})$ is defined as $R \coloneqq K/N$. We refer to physical qubits that form $\mathcal{Q}$ as *data qubits*.

A Calderbank-Shor-Steane (CSS) code [4, 5] is a stabilizer code that can be constructed from a pair of classical linear codes. A classical linear code with a block length n and dimension k is a linear subspace C of a vector space $\mathbb{F}_2^n$, where $\mathbb{F}_2 = \{0, 1\}$ is a finite field with 2 elements representing a bit. A linear code C is defined as the kernel of an $m \times n$ parity-check matrix H, i.e., $C = \{x \in \mathbb{F}_2^n : Hx^\top = 0\}$, where $m \geq n - k$ holds equality when H is full rank, and x is a row vector representing a codeword. In addition, a linear subspace of a vector space $\mathbb{F}_2^n$ spanned by the set of vectors that are orthogonal to all codewords in C is known as the dual code $C^\perp$ of C defined as $C^\perp \coloneqq \{d \in \mathbb{F}_2^n : d \oplus c = 0, \forall c \in C\}$. Given a pair of classical linear codes $C_X = \ker H_X$ and $C_Z = \ker H_Z$ with a block length N satisfying $C_Z^\perp \subseteq C_X$, we can define a parity-check matrix $H \in \mathbb{F}_2^{M \times 2N}$ of the CSS code as

$$H = \begin{bmatrix} H_X & 0 \\ 0 & H_Z \end{bmatrix}, \tag{19}$$

where $M = M_X + M_Z$. The parity-check matrix $H \in \mathbb{F}_2^{M \times 2N}$ of the CSS code gives the stabilizer group $\mathcal{S}$ of the code generated by $\{g_i\}_i$ such that

$$\begin{aligned} H_X^\top &= [\phi(g_0), \ldots, \phi(g_{M_X - 1})], \\ H_Z^\top &= [\phi(g_{M_X}), \ldots, \phi(g_{M-1})]. \end{aligned} \tag{20}$$

From the construction in (19), the stabilizer generators of the CSS code can be classified into Z-type generators of

$$g_m^Z \in \left\{ \bigotimes_i P_i \colon P_i \in \{I, Z\} \right\} \text{ for } m \in \{1, \ldots, M_Z\}, \tag{21}$$

and X-type generators of

$$g_{m'}^X \in \left\{ \bigotimes_i P_i \colon P_i \in \{I, X\} \right\} \text{ for } m' \in \{M_Z{+}1, \ldots, M\}. \tag{22}$$

The condition that these generators commute with each other is equivalent to $H_Z H_X^\top = 0$, which is guaranteed by the requirement of $C_Z^\perp \subseteq C_X$. The code space of the CSS codes $\mathcal{Q}$ is

$$\operatorname{span} \left\{ \sum_{y \in C_Z^\perp} |x \oplus y\rangle : x \in C_X \right\}, \tag{23}$$

the dimension of a CSS code is $K = k_X + k_Z - N$, where k_X and k_Z are the dimension of C_X and C_Z, respectively, and the distance of the code is $D = \min\{D_X, D_Z\}$, where $D_X = \min_{x \in C_X \setminus C_Z^\perp} |x|$, $D_Z = \min_{x \in C_Z \setminus C_X^\perp} |x|$, and $|x|$ is the Hamming weight of x.

2. *Concatenated Steane codes*

A $[[7, 1, 3]]$ Steane's 7-qubit code [5], or simply the Steane code, is a CSS code whose parity-check matrices H_X and H_Z are both $[7, 4, 3]$ Hamming code [6], i.e.,

$$H_Z = H_X = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}, \tag{24}$$

which satisfy $H_Z H_X^\top = 0$. The stabilizer generators of the Steane code are defined as

$$\begin{aligned} g_1^X &= X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I, \\ g_2^X &= I \otimes X \otimes X \otimes I \otimes X \otimes X \otimes I, \\ g_3^X &= I \otimes I \otimes X \otimes X \otimes I \otimes X \otimes X, \\ g_1^Z &= Z \otimes Z \otimes Z \otimes Z \otimes I \otimes I \otimes I, \\ g_2^Z &= I \otimes Z \otimes Z \otimes I \otimes Z \otimes Z \otimes I, \\ g_3^Z &= I \otimes I \otimes Z \otimes Z \otimes I \otimes Z \otimes Z, \end{aligned} \tag{25}$$

The logical Z and X operators of the Steane code acting on the logical qubit are described by the following operator acting on the 7 physical qubits, respectively,

$$\begin{aligned} I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes Z, \\ I \otimes I \otimes I \otimes I \otimes X \otimes X \otimes X. \end{aligned} \tag{26}$$

If a logical gate can be implemented by a tensor product of gates acting individually on each physical qubit, the logical gate is called *transversal*. Transversality is important in FTQC since the logical gate can be performed in a single time step without additional qubits and, more importantly, they inherently prevent error propagation occurring in the code. The feature of the Steane code is that the logical Clifford gates H, S, and CNOT can be executed transversally by $H^{\otimes 7}$, $(S^\dagger)^{\otimes 7}$, and CNOT$^{\otimes 7}$, respectively, as well as the logical Z and X.

A decoding algorithm for the Steane code is as follows: the CSS code corrects errors using two types of stabilizer generators, X-type generators and Z-type generators, independently. The X-type generators are used for correcting phase-flip (Z) errors and the Z-type generators are used for bit-flip (X) errors, respectively. In the following, we will focus on error correction using X-type generators. By definition, the X-type generator is derived from the parity-check matrix H_Z of the $[7, 4, 3]$ Hamming code in (24), and thus we can use the same decoding algorithm for the $[7, 4, 1]$ Hamming code. Suppose that a single-qubit Z error occurs, and the syndrome bits in $\sigma(E) = (s_1, s_2, s_3) \in \mathbb{F}_2^3$ are obtained, where the i-th element corresponds to the measurement outcome $m \in \{0,1\}$ of g_i in (25). Due to the properties of the Hamming code, the syndrome bits indicate the position of the qubit where the error occurred, given by a binary representation of

$$\tilde{i} = \sum_{i=1}^{3} s_i 2^{i-1}, \tag{27}$$

which gives the Z operator on the $\tilde{i}$-th qubit as the recovering operation.

The concatenated Steane codes [7, 8] are constructed by recursively replacing each qubit composed of a code with a logical qubit of the Steane code. First, at level L, we have a qubit to be encoded. For each $l \in \{L, \ldots, 1\}$, the code is obtained by replacing each physical qubit with a logical qubits of the Steane code. This recursive structure leads to the level-L concatenated Steane code, denoted by $\mathcal{Q}^{(L)}$, with parameters,

$$[[N = 7^L, K = 1, D = 3^L]]. \tag{28}$$

3. *Quantum LDPC codes*

A family of CSS codes with parameters $[[N_i, K_i, D_i]]$ indexed by an integer i is said to be an (r, c) quantum low-density parity-check (LDPC) code if the parity-check matrices of the CSS codes in the family have at most $r = O(1)$ non-zero elements in each row and at most $c = O(1)$ non-zero elements in each column as $i \to \infty$ and $N_i \to \infty$. That is, the X-type and Z-type stabilizer generators of the quantum LDPC codes have only $r = O(1)$ weights, and only a constant number $c = O(1)$ of stabilizer generators act nontrivially on each physical qubit of the quantum LDPC codes. If the rate R_i of a family of quantum LDPC codes converges to a finite positive value R as $i \to \infty$,

$$\lim_{i \to \infty} R_i = R > 0, \tag{29}$$

a code in the family is referred to as a *non-vanishing-rate* quantum LDPC code. Conversely, if the rate R converges to zero, a code in the family is referred to as a *vanishing-rate* quantum LDPC code.

Vanishing-rate quantum LDPC codes, such as surface codes [9–14] and color codes [15–18], are capable of executing most or all logical Clifford gates transversally [13, 14, 17–19]. However, a drawback of these codes is that the number of physical qubits required to protect a single logical qubit diverges asymptotically. In contrast, non-vanishing-rate quantum LDPC codes are advantageous since such codes can be used for constant-space-overhead FTQC as the rate converges to a non-zero value [20–22]. Although implementing logical Clifford gates transversally with non-vanishing-rate LDPC codes is challenging [23–26], these codes can implement logical gates by using gate teleportation if one can prepare required auxiliary encoded states in a fault-tolerant way.

II. SETTING OF FAULT-TOLERANT QUANTUM COMPUTATION

In this section, we present the setting of fault-tolerant quantum computation used in our work. We consider *original quantum circuits* composed of a finite set of quantum operations. In our setting, an original circuit is written in terms of the following quantum operations: $|0\rangle$-state preparation, Z-basis measurements, Pauli gates (X, Y, and Z), Clifford gates (H, S, and CNOT), non-Clifford gates ($T \coloneqq R_Z(\pi/4)$ and $T^\dagger$), and a wait operation I. The operations can be executed on all qubits simultaneously, and no more than one operation acts on a single qubit at any given time step. The total number of these time steps is referred to as the *depth* of the original circuit, and the maximum number of qubits, where maximization is taken over all time steps of the original circuit, is referred to as the *width*.

In this paper, we consider original circuits that start with the $|0\rangle$-state preparation and end with the Z-basis measurements, with no measurements included in the middle of the circuit [27]. Any stabilizer circuit has an equivalent circuit comprising 11 rounds in a sequence in the order of H, CNOT, S, CNOT, S, CNOT, H, S, CNOT, S, CNOT [3], or 9 rounds of CNOT, S, CNOT, S, H, S, CNOT, S, and CNOT [28]. The layer of the m-qubit stabilizer circuit given by both decompositions has an $O(m)$ depth and $O(m^2/\log(m))$ two-qubit gates [3, 28]. Thus, given any original circuit $\mathrm{C}_n^{\mathrm{org}}$ specified by an integer n with width $W(n)$ and depth $D(n)$, we can rewrite it into an original circuit that has the following form.

Assumption 1. *Let $\mathrm{C}_n^{\mathrm{org}}$ be an original circuit in the following form:*

- *A Clifford layer described by an $W(n)$-qubit stabilizer circuit with $O(W(n))$ depth, repeated $O(D(n))$ times*
- *Each Clifford layer is sandwiched between layers of single-depth circuits composed of T and $T^\dagger$ gates and $\mathbb{1}$, which we refer to as T-gate layers.*
- *The first Clifford layer is preceded by a single-depth layer circuit composed of $|0\rangle$-state preparations, rather than a T-gate layer. Similarly, the final Clifford layer is followed by a single-depth layer circuit composed of Z-basis measurements, instead of a T-gate layer.*

Note that because original circuits satisfying Assumption 1 do not contain measurements in the middle of the computation, the width of the original circuit remains unchanged.

The goal of FTQC is to simulate an original circuit $\mathrm{C}_n^{\mathrm{org}}$, i.e., sample from a probability distribution that is close to that of $\mathrm{C}_n^{\mathrm{org}}$ with the total variation distance at most $\varepsilon > 0$. To achieve this, we provide a fault-tolerant protocol that explicitly constructs a physical circuit with fault tolerance (referred to as a *fault-tolerant circuit*) described by physically implementable operations.

We assume that the physical circuit satisfies the following conditions. These conditions follow the convention of the previous works [8, 20, 21, 25, 29].

Assumption 2 (physical circuit)**.** *A physical circuit satisfies the following conditions:*

1. *Set of physical operations:*

   A physical circuit consists of physical operations including $|0\rangle$-state preparation, Z-basis measurement, Pauli gates X, Y, and Z, Clifford gates H, S, $S^\dagger$, and CNOT*, non-Clifford gates T and $T^\dagger$, and wait operation I. Each physical operation in a physical circuit is referred to as a physical location.*

2. *No geometrical constraint on CNOT gates:*

   We assume that the CNOT gate can be applied to an arbitrary pair of physical qubits at a single time step, regardless of the location of the two physical qubits as in neutral atom systems [30, 31], trapped-ion systems [32–34], and photonic systems [35–37].

3. *Parallel physical operations:*

   The physical operations can be performed simultaneously for all qubits in a single time step as long as each qubit is involved in only one operation at any given time. The depth of the physical circuit is determined by these time steps.

4. *Allocation of qubits and bits:*

   We allocate physical qubits via $|0\rangle$-state preparation and deallocate them through Z-basis measurement. Bits are allocated in a classical register to store the measurement outcomes. Once a classical computer receives the bits of the measurement outcomes, those bits are deallocated from a classical register. The number of physical qubits and bits at any given time are those that have been allocated previously and have not yet been deallocated.

5. *Ideal classical computation with non-negligible runtime:*

   For simplicity of our analysis, we assume that classical computation can be performed without faults. Additionally, during the classical computation, we assume that the wait operations on all allocated physical qubits are performed in the physical circuit. The depth of the wait operation is determined by the runtime of the classical computation. Specifically, the depth is limited to a value less than or equal to a constant multiple of the runtime of the classical computation.

The issue in quantum computing is that when executing these physical circuits during quantum computation, the circuits are subjected to noise that may impair the results of computation. When analyzing the impact of noise on FTQC with quantum LDPC codes, the conventional approach is to consider the local stochastic Pauli error model on a physical circuit [20–22], which is also used in this paper. This error model has the stochastic property, where a Pauli error is applied to a quantum state with probability p, and the state remains unchanged with probability $1-p$. It also satisfies the locality property, where the probability of an error occurring at any given set of locations decreases exponentially with the size of the set. However, it does not impose any other constraints; errors can exhibit correlations in both time and space and may be adversarially chosen to complicate fault-tolerant simulations.

Definition 4 (Local stochastic Pauli error model on a physical circuit)**.** Let C be a physical circuit, and L be a set of physical locations in C. Let a set of faulty locations be a random variable $F \subseteq L$, where a faulty location is defined as a physical location that leads to an error resulting from the imperfect physical operation at this location. We say that C is subjected to the local stochastic Pauli error model with parameter $p_{\mathrm{loc}} \in [0,1]$ if the following conditions hold.

1. For all $A \subseteq L$, the probability that F contains A satisfies

$$\mathbb{P}[F \supseteq A] \leq p_{\mathrm{loc}}^{|A|}. \tag{30}$$

2. The physical operations in F are associated with a Pauli operator chosen adversarially that represents an error as follows.

   - If a location in F is a $|0\rangle$-state preparation operation, a Pauli operator is applied to the qubit after the $|0\rangle$-state preparation is performed.
   - If a location in F is a gate operation (including Pauli gates, Clifford gates, non-Clifford gates, and a wait), a Pauli operator is applied to each qubit(s) after the corresponding gate operation is performed.
   - If a location in F is a Z-basis measurement operation, a bit flip or identity operation is applied to the measurement outcome.

   The physical locations in $L\backslash F$ behave in the same way as the case without faults.

In this paper, we assume a physical circuit is subjected to the local stochastic Pauli error model. We refer to a physical circuit that suffers from local stochastic Pauli errors as a *faulty* physical circuit.

Assumption 3. *A physical circuit* C *is subjected to the local stochastic Pauli error with parameter* $p_{\mathrm{loc}} \in [0,1]$.

For the faulty physical circuit to implement FTQC with a quantum LDPC code, we also define the local stochastic Pauli error model on a set of data qubits and syndrome bits of a block of a quantum LDPC code, denoted by V and W, respectively. For simplicity, we remove the distinction between V and W. That is, we consider the union $X \coloneqq V \cup W$ of the two sets, and we call each element of X a wire in a circuit.

Definition 5 (Local stochastic Pauli error model on wires)**.** Let V be a set of data qubits and W be a set of syndrome bits at a given time step of a physical circuit. Let $X \coloneqq V \cup W$ be a set of wires and $H \coloneqq F \cup G \subseteq X$ be a set of erroneous wires, where F is the set of erroneous wires in V and G in W. An error model is said to be the local stochastic Pauli error model on wires with parameter $p_{\mathrm{wire}} \in [0,1]$ if the following conditions are satisfied.

1. For any $U = S \cup T \subseteq X$, the probability that H contains U satisfies,

$$\mathbb{P}[H \supseteq U] \leq p_{\mathrm{wire}}^{|U|}. \tag{31}$$

2. A Pauli operator is applied to $F \subseteq V$, and bit flip or identity operations are applied to $G \subseteq W$.

In the case where the errors on the syndrome bits are not considered, an error model on data qubits is the local stochastic Pauli error model with parameter p_{data} if for all $S \subseteq V$, the following relations are satisfied.

1. For all $S \subseteq V$, the probability that $F \subseteq V$ contains S satisfies,

$$\mathbb{P}[F \supseteq S] \leq p_{\mathrm{data}}^{|S|}. \tag{32}$$

2. A Pauli operator is applied to $F \subseteq V$.

A fault-tolerant protocol provides a fault-tolerant circuit to simulate a given original circuit. The fault-tolerant protocol replaces qubits in an original circuit with logical qubits of a quantum error-correcting code. This process requires using multiple physical qubits per logical qubit for redundancy. At the same time, operations in an original circuit are replaced by logical operations acting on the logical qubits. Implementing these logical operations in a physical circuit requires additional time steps. This procedure incurs an overhead with respect to space and time. Let $W_{\mathrm{FT}}(n)$ represent the width and $D_{\mathrm{FT}}(n)$ represent the depth of a fault-tolerant circuit. Then, the space overhead is defined as the ratio of the width of the fault-tolerant circuit $W_{\mathrm{FT}}(n)$ to the width n of the corresponding original circuit,

$$\frac{W_{\mathrm{FT}}(n)}{W(n)}. \tag{33}$$

On the other hand, the time overhead is defined as the ratio of the depth $D_{\mathrm{FT}}(n)$ of the fault-tolerant circuit, including wait operations necessary for classical computation, to the depth $D(n)$ of the original circuit,

$$\frac{D_{\mathrm{FT}}(n)}{D(n)}. \tag{34}$$

For a target error ε, the fault-tolerant protocol is said to achieve a constant space overhead if the space overhead of the fault-tolerant circuit is

$$\frac{W_{\mathrm{FT}}(n)}{W(n)} = O(1), \tag{35}$$

as $n \to \infty$ and $\varepsilon \to 0$, and is said to achieve a polylogarithmic time overhead if the time overhead of the fault-tolerant circuit is

$$\frac{D_{\mathrm{FT}}(n)}{D(n)} = O\left(\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right) \tag{36}$$

as $n \to \infty$ and $\varepsilon \to 0$.

III. FAULT-TOLERANT PROTOCOL FOR OPEN QUANTUM CIRCUITS

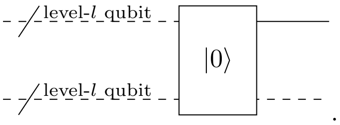
In this section, we explain a protocol based on concatenated Steane codes for simulating ideal quantum circuits that output a quantum state, rather than measurement outcomes. We refer to quantum circuits that output a quantum state as *open* quantum circuits, to distinguish them from *closed* quantum circuits that output measurement outcomes. The protocol will be used to simulate an original open circuit to produce an encoded state of a quantum LDPC code, and the encoded state is used for performing logical Clifford gates and logical T and $T^{\dagger}$ gates acting on logical qubits in a quantum LDPC code via gate teleportation [38, 39]. As discussed later in Sec. IV D, this protocol is not used in isolation. It is integrated into the protocol with quantum LDPC codes in such a way that we use the concatenated Steane code to prepare encoded states of quantum LDPC codes in a fault-tolerant way. The existing analysis [20–22] of the fault-tolerant protocol for quantum LDPC codes does not explicitly bound the error in preparing the encoded state, and one of our contributions here is to provide a thorough analysis including this part of the protocol to present a complete threshold theorem of the overall protocol.

A. Compilation from original open circuit to fault-tolerant circuit

For a given ideal open circuit, the protocol recursively constructs a level-l circuit ($l \in \{L, \ldots, 0\}$) consisting of elementary operations acting on level-l qubits. Here, a level-0 circuit is a physical circuit. We say that each elementary operation contained in the level-l circuit is a location of the level-l circuit. For the level-l circuit, we assume that at most one elementary operation can act on a single level-l qubit in a single time step. The depth of a level-l circuit is determined by the number of time steps. The set of elementary operations includes $|0\rangle$-state preparation operation, $|T\rangle$-state preparation operation, H-, S-, $S^\dagger$-, CNOT-, Pauli-gate operations, Z-basis measurement operation, and a wait operation. Here, $|T\rangle := TH|0\rangle$. We also define the T-gate abbreviation as a collection of the elementary operations to perform T gates by gate teleportation. For each elementary operation, we define the corresponding gadget that is a circuit to carry out the corresponding logical operation on a logical qubit of the Steane code. We also define an error-correction (EC) gadget, which is a circuit that performs error correction on a set of 7 qubits forming the Steane code, and a decoding interface, which is a circuit that performs the decoding operation to transform the logical state encoded in the Steane code consisting of the set of 7 qubits to the same state of an unencoded physical qubit.

The elementary operations and abbreviations are represented as in a diagram. In the diagram, the change from a dashed input line to a solid output line represents the allocation of a level-l qubit, while the change from a solid line to a dashed line represents deallocation. If both the input and output lines are dashed, it means that the corresponding level-l qubit is used as a workspace for performing elementary operations. The double output line represents the bits that the elementary operation outputs. The elementary operations are as follows.

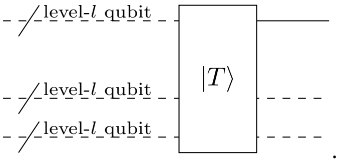
- $|0\rangle$-state preparation operation



(37)

The $|0\rangle$-state preparation operation allocates a single level-l qubit that is prepared in the state $|0\rangle$.

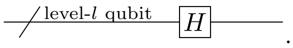
- $|T\rangle$-state preparation operation



(38)

The $|T\rangle$-state preparation operation allocates a single level-l qubit that is prepared in the state $|T\rangle$.

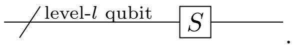
- H-gate operation



(39)

The H-gate operation applies the H gate to a level-l qubit.

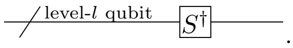
- S-gate operation



(40)

The S-gate operation applies the S gate to a level-l qubit.

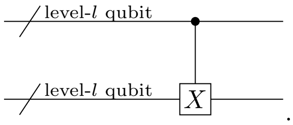
- $S^\dagger$-gate operation



(41)

The $S^\dagger$-gate operation applies the $S^\dagger$ gate to a level-l qubit.

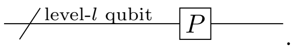
- CNOT-gate operation



(42)

The CNOT-gate operation applies the CNOT gate between two level-l qubits.

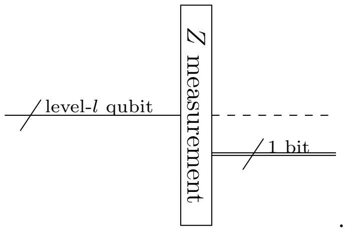
- Pauli-gate operation



(43)

The Pauli-gate operation applies the Pauli gate $P \in \mathcal{P}_1$ to a level-l qubit [40].

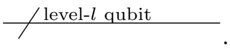
- Z-basis measurement operation



(44)

The Z-basis measurement operation performs the Z-basis measurement on a level-l qubit. It deallocates the level-l qubit and outputs a 1-bit measurement outcome.

- Wait operation

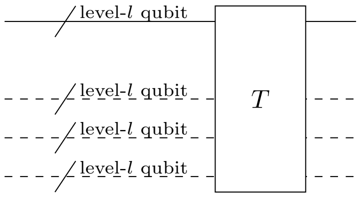


(45)

The wait operation applies an I operation to a level-l qubit, which is regarded as a special case of Pauli gates.

The T-gate abbreviation is denoted as follows:

- T-gate abbreviation

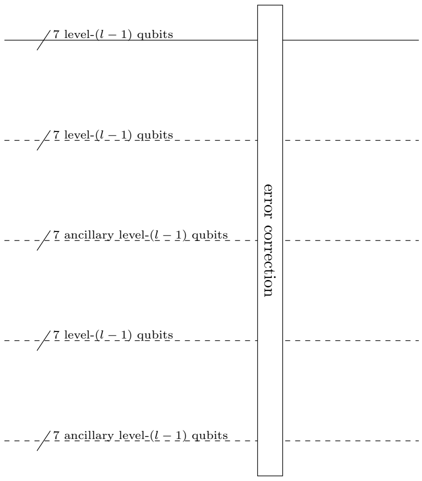


. (46)

The T-gate abbreviation performs the T-gate operation on a level-l qubit through gate teleportation.

In addition to the elementary operations and their corresponding gadgets, the EC gadget and the decoding interface are denoted as follows:

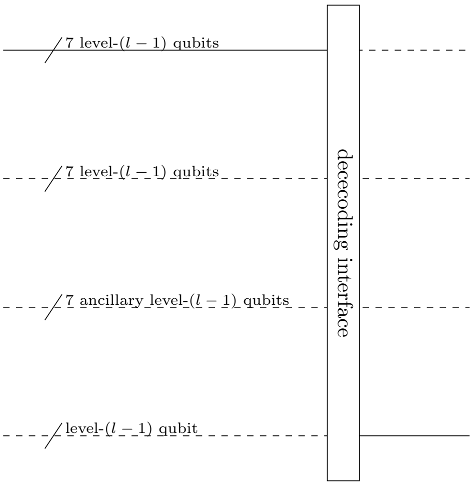
- EC gadget



. (47)

The EC gadget performs quantum error correction on a logical qubit consisting of 7 level-$(l-1)$ qubits, temporarily utilizing the other four sets of 7 level-$(l-1)$ qubits .

- Decoding interface



, (48)

A decoding interface performs the decoding operation from a logical qubit of the Steane code to an unencoded physical qubit.

The gadgets are carefully designed to satisfy the fault-tolerance conditions, which are presented in Appendix A, and their constructions are shown in Appendix B.

The procedure for compiling an original open circuit C that generates a quantum state $|\psi\rangle$ into a physical circuit, as shown in Fig. III A, is as follows. Given a target error $\delta > 0$ and an original circuit C, we first determine the concatenation level L such that the failure probability of the fault-tolerant simulation can be bounded by δ. Next, we compile the original circuit into a level-L circuit by replacing each operation in the original circuit with the corresponding elementary operation that acts on level-L qubits. As for the T and $T^\dagger$ gates in the original circuit, we replace a T gate with a T-gate abbreviation and a $T^\dagger$ gate with an $S^\dagger$-gate operation, followed by a T-gate abbreviation, respectively. In addition to each level-L qubit, we allocate $3+4=7$ auxiliary level-L qubits. Of these seven, the three auxiliary level-L qubits are used for elementary operations and the T-gate abbreviation. The other four registers are never explicitly used in the level-L circuit and not shown in Fig. III A, but these level-L qubits are used to provide workspaces for the EC gadget that will appear in the level-$(L-1)$ circuit. For each level $l \in \{L, L-1, \ldots, 1\}$, we recursively compile the level-l circuit into the corresponding level-$(l-1)$ circuit. For each level-l qubit in the level-l circuit, a set of seven level-$(l-1)$ qubits is allocated in the level-$(l-1)$ circuit, along with $3+4=7$ auxiliary level-$(l-1)$ qubits per set. As in the level-L case, three of these seven auxiliary level-$(l-1)$ qubits are used for abbreviations and elementary operations in the level-$(l-1)$ circuit. The remaining four level-$(l-1)$ qubits are never explicitly used in the level-$(l-1)$ circuit, but are used as workspaces for EC gadgets. This transformation involves replacing each elementary operation with the corresponding gadget and inserting an EC gadget between the gadgets. For simplicity of our analysis, we insert EC gadgets synchronously. This means that EC gadgets are executed only after all the gadgets for the elementary operations belonging to the same depth in the level-l circuit have been completed. Until the EC gadgets are finished, the gadgets corresponding to the elementary operations that belong to the next depth in the level-l circuit are not executed. To ensure synchronization, we incorporate wait operations after the previously completed gadgets. At this stage, the level-$(l-1)$ circuit outputs an encoded version of the quantum state $|\psi\rangle$, where each physical qubit of $|\psi\rangle$ is replaced by the 7 level-$(l-1)$ qubits forming the logical qubit of the Steane code. To obtain the unencoded state $|\psi\rangle$, we add the decoding interface to each logical qubit at the end of the level-$(l-1)$ circuit, i.e., an open circuit is always compiled into a circuit with decoding interface in the end, in place of measurements at the end of closed circuits.

By applying this procedure recursively, we obtain the

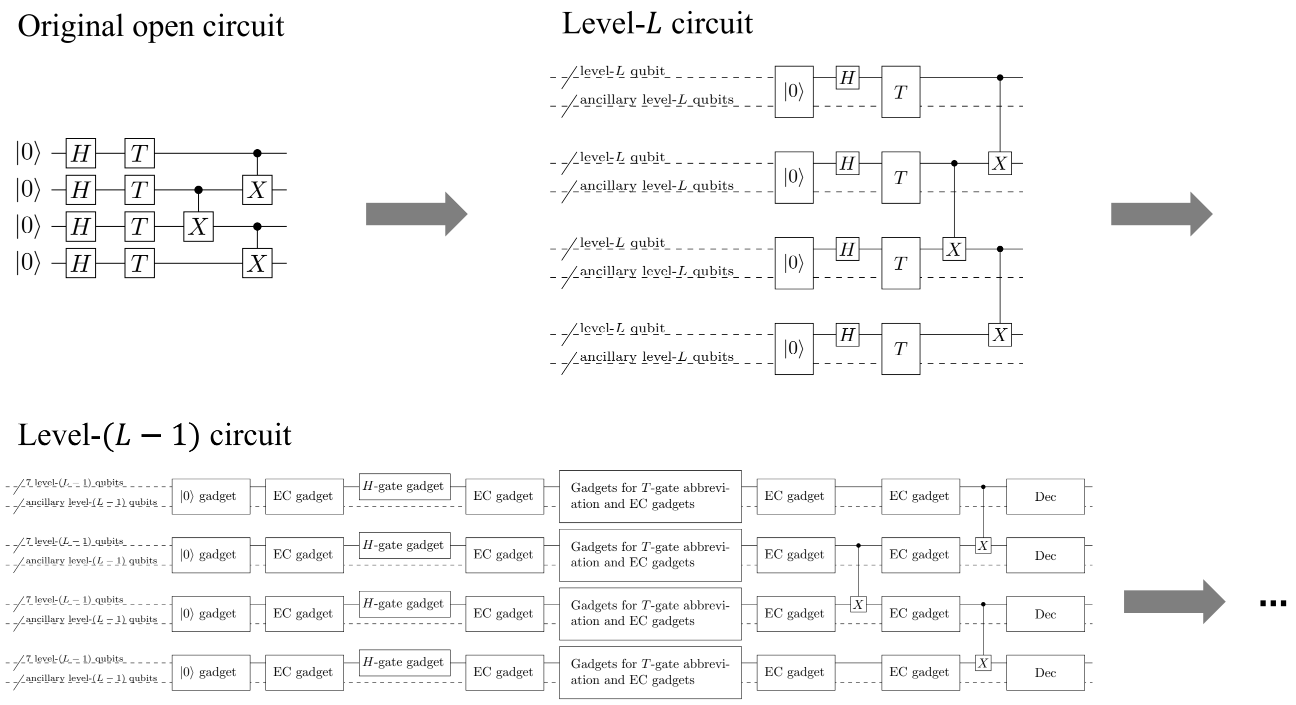


FIG. 1. Compilation procedure of our protocol for ideal open circuits. First, we compile an original open circuit into a level-L circuit that consists only of elementary operations on level-L qubits. Here, the T gate, which is implemented using gate teleportation, is an abbreviation of a sequence of elementary operations. For each level $l \in \{L, \ldots, 1\}$, we recursively compile the level-l circuit into the level-$(l-1)$ circuit by replacing each elementary operation with the corresponding gadget, inserting an EC gadget in between, and adding decoding interfaces, denoted by Dec, to every set of 7 level-$(l-1)$ qubits at the end of the level-$(l-1)$ circuit. In this way, we finally obtain a level-0 circuit, i.e., a physical circuit for an original open circuit.

level-0 circuit. However, in a level-0 circuit, Assumption 2 allows T and $T^\dagger$ gates to be implemented directly as physical operations, rather than gate teleportation using abbreviations of physical circuits. Thus, we replace T and $T^\dagger$ abbreviations in a level-0 circuit with the physical T and $T^\dagger$ gates, respectively, and elementary operations with the corresponding physical operations. As a result, the $3+4=7$ auxiliary level 0 qubits that are allocated for each level-0 qubit can be removed. After making these replacements, we finally obtain the level-0 circuit, i.e., physical circuit, denoted by $\mathrm{C}^{(L)}$, which is to be performed in quantum computation.

B. Threshold theorem for open circuits

In this section, we show the threshold theorem for simulating open circuits. Our approach is based on Ref. [41]. However, for open circuits we need a different treatment because the decoding interfaces are located at the end of the physical circuit. Thus, our proof is carried out by appropriately modifying the proof of the threshold theorem for closed circuits [41]. The threshold theorem for open circuits described below is used without an explicit proof in Refs. [20–22], but we prove the theorem based on our protocol and noise model, so as to complete the full proof of the threshold theorem for the fault-tolerant protocol using quantum LDPC codes. Although the threshold theorem for open circuits has been established in Ref. [42] as well, the noise model considered is the independent and ideally distributed (IID) Pauli error model, and thus the theorem in Ref. [42] is not applicable to our more general setting.

Theorem 6 (Threshold theorem for simulating open circuits with polylog-time and polylog-space overhead)**.** *Suppose that a physical circuit that satisfies Assumption 2 and 3 is subjected to a local stochastic Pauli error model. Let $\{\mathrm{C}_N\}$ be a sequence of original open circuits that produce a quantum state $|\psi_N\rangle$ specified by an integer N. Each circuit C_N has width $W(N)$ and depth $D(N)$ and $|\mathrm{C}_N|$ be the number of locations in C_N, where $|\mathrm{C}_N| \to \infty$ as $N \to \infty$. Let $\delta > 0$ be a constant. Suppose that we compile from the original open circuit C_N into a sequence of physical circuits $\tilde{\mathrm{C}}_N$ as explained in Sec. III A.*

Then, there exists a threshold $p_{\mathrm{loc}}^{\mathrm{th}} > 0$ and if $0 \leq p_{\mathrm{loc}} \leq p_{\mathrm{loc}}^{\mathrm{th}}/2$, the following statement holds for $N \to \infty$: there is a sequence of physical circuits $\tilde{\mathrm{C}}_N$ that produces $|\psi^{(N)}\rangle$ which is subjected to the local stochastic Pauli error with parameter $\tilde{p} \leq 2Mp_{\mathrm{loc}}$ with probability at least $1-\delta$, where M is a constant representing the number of loca-

tions in the decoding interface described in Sec. III B 1. Furthermore, $\tilde{\mathrm{C}}_N$ has width $\tilde{W}(N)$ and depth $\tilde{D}(N)$ such that

$$\begin{aligned} \frac{\tilde{W}(N)}{W(N)} &= O\left(\mathrm{polylog}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right), \\ \frac{\tilde{D}(N)}{D(N)} &= O\left(\mathrm{polylog}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right). \end{aligned} \tag{49}$$

To prove Theorem 6, the rest of this section is organized as follows. In Sec. III B 1, we present the construction of the decoding interface. In Sec. III B 2, we give the proof of Theorem. 6 based on the decoding interface explained in Sec. III B 1.

1. *Construction of the decoding interface*

The decoding interface is designed to map an encoded state of a logical qubit into the corresponding unencoded state of a physical qubit. Ideally, it behaves as the ideal decoder (50). The construction of the decoding interface is illustrated in Fig. III B 1. The interface is based on Knill's error correction [38, 39, 41, 42]. The interface uses auxiliary qubits that are in the state of a Bell state, with one side encoded in a logical state using an encoding circuit $U_{\mathrm{encode}}^{|\psi\rangle}$ as shown in Fig. 16 (b), in addition to the input logical state on which we want to decode. Then, a logical Bell measurement is performed on two sets of logical states. Based on the outcome of the 7-bit measurements in the transversal Z-basis, it is input to the decoding algorithm to calculate the outcome of the logical operator $\bar{Z}$. This classical computation is performed using the same procedure as explained in the Z-basis measurement gadget. The measurement outcome is then used to determine the correction operation for quantum teleportation. Once the Pauli correction operation is applied, the interface outputs a qubit in the desired state to be teleported.

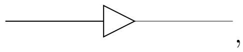
2. *Level reduction*

Next, to prove the threshold theorem, we consider the reduction of the level of a physical circuit $\mathrm{C}^{(L)}$. The reduction is carried out by replacing each Rec in $\mathrm{C}^{(L)}$ with an equivalent level-0 gate by moving the ideal decoder 7 from the end to the start in $\mathrm{C}^{(L)}$. The definition of the ideal decoder is as follows.

Definition 7 (Ideal decoder)**.** An ideal decoder is a combined non-fauly operation that consists of a syndrome measurement, followed by a recovery operation determined by the decoding algorithm using the result of the syndrome measurement, and ending with a decoding operation that maps an encoded state to the corresponding state of a physical qubit.

The ideal decoder is shown in the diagram as

- Ideal decoder



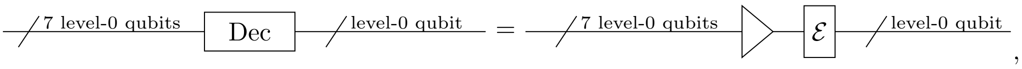
, (50)

where the bold line represents a logical qubit and the thin line represents an unencoded physical qubit.

Specifically, the proof in Ref. [41] is accomplished by recursively reducing the level of simulation by moving the ideal decoder from Z-basis measurement gadgets located at the end of a physical circuit to the front. By doing this, we obtain a level-reduced physical circuit $\mathrm{C}^{(L-1)}$ with a lower error parameter. For the concatenated code protocol for closed circuits, the level reduction procedure was established in Refs. [8, 41]. In contrast, the protocol for open circuits instructs the physical circuit to end with a decoding interface that is not fault-tolerant; a single fault could result in an error on the unencoded state. However, since the decoding interface is a stabilizer circuit [3], i.e., all operations in a stabilizer circuit are Clifford gates or Z-basis measurements, every faulty physical circuit can be transformed into the circuit that ideally executes the physical circuit and applies the Pauli error to the qubit at the final time step of the circuit. Under this transformation, due to the union bound, the output qubit is subjected to a local stochastic Pauli noise $\mathcal{E}$ with probability

$$\tilde{p} \leq M p_{\mathrm{loc}}, \tag{51}$$

where M is the number of locations in the decoding interface. Therefore, the decoding interface, denoted by Dec, can be transformed as follows.



, (52)

where the output level-0 qubit is subjected to the local stochastic Pauli noise $\mathcal{E}$ with parameter $\tilde{p} \leq M p_{\mathrm{loc}}$, which is a completely positive and trace-preserving (CPTP) map.

Using the ideal decoder obtained from the decoding interface as in (52), the rest of the level reduction procedure can be carried out similarly as in Ref. [41]. For simplicity, we refer to a level-0 circuit comprised of gadget followed

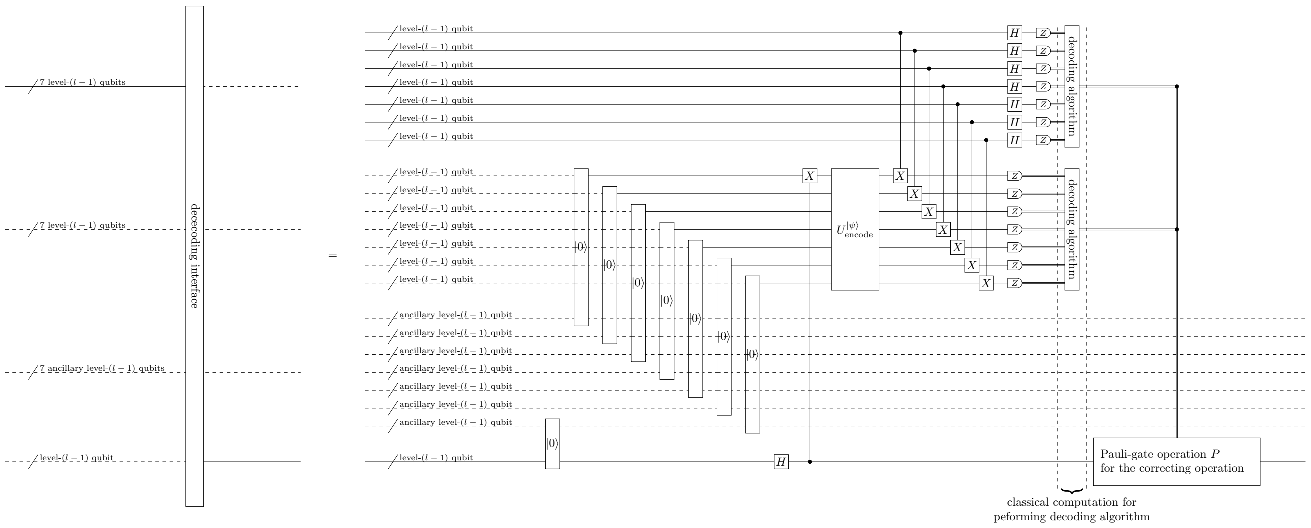

7 level-(l − 1) qubits
7 level-(l − 1) qubits
7 ancillary level-(l − 1) qubits
level-(l − 1) qubit
decoding interface
=
level-(l − 1) qubit
ancillary level-(l − 1) qubit
|0⟩
X
H
Z
$U^{|\psi\rangle}_{\text{encode}}$
decoding algorithm
decoding algorithm
Pauli-gate operation P
for the correcting operation
classical computation for
peforming decoding algorithm

FIG. 2. The level-$(l-1)$ circuit of the decoding interface.

by an EC gadget as a *rectangle* or *Rec*. Similarly, we call a level-0 circuit comprised of Rec, along with the preceding EC gadget, an *extended rectangle* or *ExRec*. If a gadget satisfies the fault-tolerance conditions as shown in Sec. A, then no single fault in any location of ExRec in $\mathrm{C}^{(L)}$ can cause a fault in the corresponding location in a level-1 circuit. Thus, if there is at most one fault in an ExRec in $\mathrm{C}^{(L)}$, then we can convert the Rec in $\mathrm{C}^{(L)}$ to the corresponding non-faulty level-0 operation. In contrast, if there are more than two faults in an ExRec in $\mathrm{C}^{(L)}$, the ExRec in $\mathrm{C}^{(L)}$ can be converted to an operation that acts on the corresponding non-faulty 0-operation followed by an error described by a Pauli operator. Using this relation, an ideal decoder can be reversed to convert all ExRecs in $\mathrm{C}^{(L)}$ to the corresponding level-0 operations, resulting in a physical circuit $\mathrm{C}^{(L-1)}$. Note that when the ideal decoder is moved from the end, the ideal decoder first encounters a truncated ExRec, i.e., a trailing EC gadget of a gadget is absent, but by adding an ideal trailing EC gadget to the gadget, we can apply the above procedure.

Therefore, if $\mathrm{C}^{(L)}$ is subjected to the local stochastic Pauli error model, a level-reduced circuit $\mathrm{C}^{(L-1)}$ is also subjected to the local stochastic Pauli error model, where the effective probability $p_{\mathrm{loc}}^{(1)}$ of faults occurring in $\mathrm{C}^{(L-1)}$ can be bounded by counting the number of locations in the largest ExRec, which is the one that contains the largest number of locations among all ExRecs as

$$p_{\mathrm{loc}}^{(1)} \leq A\left(p_{\mathrm{loc}}^{(0)}\right)^2, \tag{53}$$

where A is a constant representing the number of pairs of locations in the largest ExRec.

By applying this argument L times, we finally obtain a physical circuit $\mathrm{C}^{(0)}$ with parameter

$$p_{\mathrm{loc}}^{(L)} \leq p_{\mathrm{th}}\left(\frac{p_{\mathrm{loc}}^{(0)}}{p_{\mathrm{th}}}\right)^{2^L}, \tag{54}$$

where $p_{\mathrm{th}} := 1/A > 0$. Moreover, due to the union bound, the output qubits are subjected to a local stochastic Pauli error with parameter

$$\tilde{p} \leq M\sum_{l=0}^{L-1} p_{\mathrm{loc}}^{(l)} \leq M\sum_{l=0}^{\infty} p_{\mathrm{loc}}^{(l)} \leq \frac{Mp_{\mathrm{loc}}}{1-p_{\mathrm{loc}}/p_{\mathrm{loc}}^{\mathrm{th}}} \leq 2Mp_{\mathrm{loc}}, \tag{55}$$

where we used $p_{\mathrm{loc}}^{(0)} := p_{\mathrm{loc}}$ and $0 < p_{\mathrm{loc}} \leq p_{\mathrm{loc}}^{\mathrm{th}}/2$.

To achieve the target error δ, due to the union bound, it is sufficient to have $p_{\mathrm{loc}}^{(L)} \leq \delta/|\mathrm{C}_N|$. Therefore, using (54), we see that it suffices to have

$$L \geq \log_2 \log_{p_{\mathrm{loc}}^{\mathrm{th}}/p_{\mathrm{loc}}}\left(\frac{p_{\mathrm{loc}}^{\mathrm{th}}|\mathrm{C}_N|}{\delta}\right). \tag{56}$$

Therefore, to reduce the overhead of the protocol, we choose

$$L = \Theta\left(\log\left(\log\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right)\right). \tag{57}$$

This means that there exists a constant $c > 0$ such that $L \leq c\log_2\left(\log_{p_{\mathrm{loc}}^{\mathrm{th}}/p_{\mathrm{loc}}}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right)$ for large N.

Let w' be the maximum width and d' be the maximum depth of all gadgets for the elementary operations and the EC gadget. Since the compilation procedure has a recursive structure, we can obtain a physical circuit corresponding to operations in the original open circuit, except for the part of the decoding interfaces, with

$$\begin{aligned} W_{\mathrm{org}}(N) &= O\left(W(N)\times(w')^L\right) \\ &= O\left(W(N)\log^{\gamma_0}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right) \end{aligned} \tag{58}$$

and

$$D_{\mathrm{org}}(N) = O\left(D(N) \times (d')^L\right) = O\left(D(N) \log^{\gamma_1}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right), \tag{59}$$

where

$$\gamma_0 = c \log_2 w' \text{ and } \gamma_1 = c \log_2 d'. \tag{60}$$

In addition, a physical circuit corresponding to the decoding interface requires

$$D_{\mathrm{dec}}(N) = \sum_{l=1}^{L} (d'')^l = O\left(\log^{\gamma_2}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right), \tag{61}$$

where d'' is the depth of the decoding interface and $\gamma_2 = c \log_2 d''$. Thus, we have

$$\begin{aligned} \frac{\tilde{W}(N)}{W(N)} &= \frac{W_{\mathrm{org}}(N)}{W(N)} = O\left(\mathrm{polylog}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right), \\ \frac{\tilde{D}(N)}{D(N)} &= \frac{D_{\mathrm{org}}(N) + D_{\mathrm{dec}}(N)}{D(N)} = O\left(\mathrm{polylog}\left(\frac{|\mathrm{C}_N|}{\delta}\right)\right). \end{aligned} \tag{62}$$

From the above discussion, we conclude Theorem 6.

IV. DESCRIPTION OF POLYLOG-TIME CONSTANT-SPACE OVERHEAD PROTOCOL

In this section, we describe our fault-tolerant protocol that achieves polylog time and constant space overhead. We begin by explaining the compilation procedure of an original circuit into a fault-tolerant circuit in Sec. IV A. In Sec. IV B, we describe the construction of abbreviations for applying Clifford gates, and T- and $T^\dagger$-gates used in our protocol. Next, we specify the fault-tolerance conditions of gadgets for quantum LDPC codes in Sec. IV C, and the constructions of gadgets that satisfy the fault-tolerance conditions in Sec. IV D. Finally, we present the threshold theorem for our protocol in Sec. IV E.

A. Compilation of ideal quantum circuit into fault-tolerant quantum circuit

We present the compilation procedure for our fault-tolerant protocol that compiles an original quantum circuit into a fault-tolerant circuit to achieve the target error $\varepsilon > 0$ using a non-vanishing-rate CSS LDPC code $\mathcal{Q}$ in combination with the protocol with the concatenated Steane codes to simulate open circuits in Sec. III. Here, the (r, c) CSS LDPC code $\mathcal{Q}$ has parameters

$$[[N, K = \Theta(N), D = \Theta(N^\gamma)]], \tag{63}$$

where N represents the number of phyiscal qubits, K represents the number of logical qubits, D is the code distance, and $\gamma > 0$ is a constant. We choose N depending on ε and n so as to achieve the polylog-time- and constant-space-overhead fault-tolerant protocol.

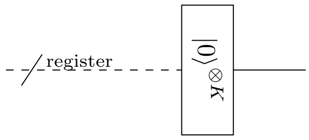
The compilation procedure consists of two steps: compiling the original circuit into an intermediate circuit and then compiling the intermediate circuit into a fault-tolerant circuit. In the compilation to the intermediate circuit, the qubits of the original circuit are grouped into registers, with each register containing at most K qubits, where K is the number of logical qubits of the quantum LDPC code $\mathcal{Q}$ in (63). Elementary operations for the quantum LDPC code will be specified as $|0\rangle^{\otimes K}$-state preparation, Clifford-state preparation operations, magic-state preparation operations, Pauli-gate operations, a CNOT-gate operation, a $Z^{\otimes K}$-measurement operation, a Bell-measurement operation, and wait operation. These elementary operations are defined as operations acting collectively on qubits in registers. By combining elementary operations, we will define abbreviations, including two-register Clifford-gate abbreviations and U_T-gate abbreviations. The intermediate circuits are described using these abbreviations and some of the elementary operations. For each elementary operation, we construct a physical circuit of the corresponding gadget that is intended to perform the corresponding logical operation acting on the logical qubits in a code block of $\mathcal{Q}$. Also, we construct an error-correcting (EC) gadget for quantum LDPC codes intended to carry out error correction on a code block of $\mathcal{Q}$ using a decoding algorithm. Here, the code $\mathcal{Q}$ must have an efficient decoding algorithm for the protocol to have a threshold, even when taking into account classical computation time. We will formally define an efficient decoding algorithm that the code $\mathcal{Q}$ should have in Sec. IV C. The gadgets are carefully designed to satisfy the fault-tolerance conditions described in Sec. IV C. The replacement of each abbreviation and elementary operation in the intermediate circuit with the corresponding gadget provides a fault-tolerant circuit for the original circuit.

1. *Compilation from original circuit to intermediate circuit*

As a first step in the compilation, we compile an original circuit into an intermediate circuit acting on K qubits within registers. First, we provide a list of elementary operations and abbreviations, along with corresponding diagrams, used in our protocol. In the diagram, a dashed input line changing to a solid output line indicates the allocation of a register, while a solid line changing to a dashed line indicates the deallocation. If both the input and output lines are dashed, the corresponding register is used as a workspace for performing elementary operations. A double output line represents the bits that the elementary operation outputs.

The elementary operations we will use are as follows.

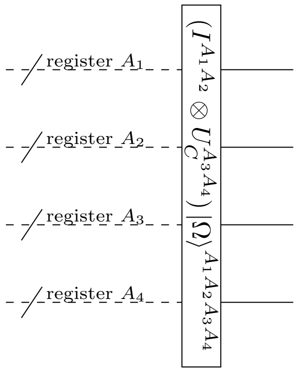
- $|0\rangle^{\otimes K}$-state preparation operation



. (64)

The $|0\rangle^{\otimes K}$-state preparation operation allocates a single register that is prepared in the state $|0\rangle^{\otimes K}$.

- Clifford-state preparation operations


register A_1
register A_2
register A_3
register A_4
$(I^{A_1A_2} \otimes U_C^{A_3A_4})\,|\Omega\rangle^{A_1A_2A_3A_4}$

. (65)

A Clifford-state preparation operation allocates four registers A_1, A_2, A_3, A_4 in the state

$$(I^{A_1A_2} \otimes U_C^{A_3A_4})\,|\Omega\rangle^{A_1A_2A_3A_4}, \tag{66}$$

where

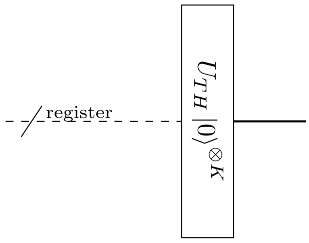
$$|\Omega\rangle^{A_1A_2A_3A_4} := |\Phi\rangle^{A_1A_3} \otimes |\Phi\rangle^{A_2A_4}, \tag{67}$$

$|\Phi\rangle^{A_iA_{i'}}$, which is a maximally entangled state between the registers A_i and $A_{i'}$, is given by

$$|\Phi\rangle^{A_iA_{i'}} = \frac{1}{\sqrt{2^K}} \sum_{m=0}^{2^K-1} |m\rangle^{A_i} \otimes |m\rangle^{A_{i'}}, \tag{68}$$

$I^{A_1A_2}$ is an identity operator acting on the qubits in the two registers A_1, and A_2 and $U_C^{A_3A_4}$ is an arbitrary Clifford operation acting on the qubits in the two registers A_3 and A_4.

- Magic-state preparation operations



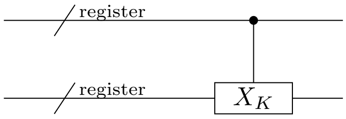
. (69)

A magic-state preparation operation allocates a single register in the state of

$$U_{TH}\,|0\rangle^{\otimes K}, \tag{70}$$

where U_{TH} is the tensor product of TH and I gates.

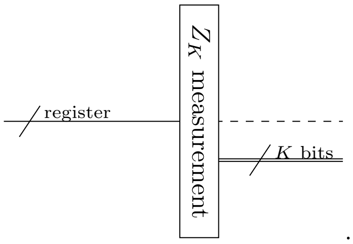
- CNOT-gate operation



. (71)

The CNOT-gate operation applies the CNOT$^{\otimes K}$ gates acting on the K qubits in the registers. Here, a controlled-X_K gate represents CNOT$^{\otimes K}$ gates on K qubits.

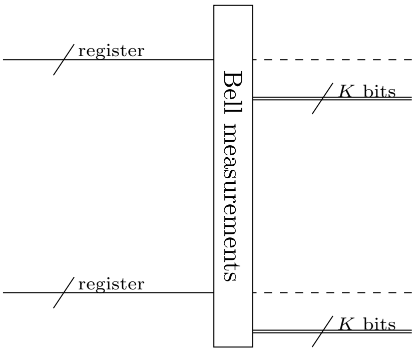
- Z_K-measurement operation



. (72)

The Z_K-measurement operation performs collective single-qubit measurements in Z basis of all K qubits contained in a register, deallocates the register, and outputs a K-bit string of the measurement outcomes. Here, Z_K represents this collective single-qubit Z-basis measurements on K qubits.

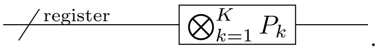
- Bell-measurement operation



. (73)

The Bell-measurement operation performs the Bell measurements on K pairs of qubits of a $X \otimes X$ operator and $Z \otimes Z$ operator, where each pair is shared by the two registers. It deallocates these registers and outputs a $2K$-bit string of the measurement outcomes. We assume that the upper register contains the K-bit string outcome of measurements of $X \otimes X$ operators and the lower register contains the outcome of measurements of $Z \otimes Z$ operators.

- Pauli-gate operations



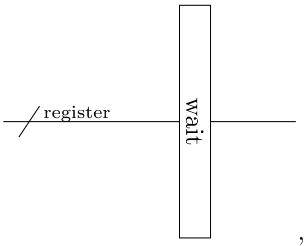
. (74)

A Pauli-gate operation performs a tensor product of arbitrary Pauli gates

$$\bigotimes_{k=1}^{K} P_k \in \tilde{\mathcal{P}}_K, \tag{75}$$

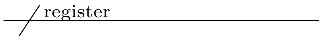
where $P_k \in \{I, X, Y, Z\}$ is a single-qubit Pauli operator acting on the k-th qubit in a register. As described below, Pauli-gate operations for quantum LDPC codes are performed by updating the Pauli frame in our protocol.

- Wait operations



, (76)

or simply

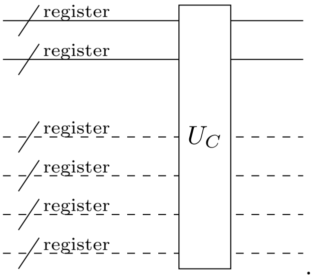


(77)

The wait operation performs the identity operator on a register, which is regarded as a special case of Pauli-gate operation.

In addition, the abbreviations are defined as follows. The explicit construction of the abbreviations (78) and (79) will be given in Sec. IV B.

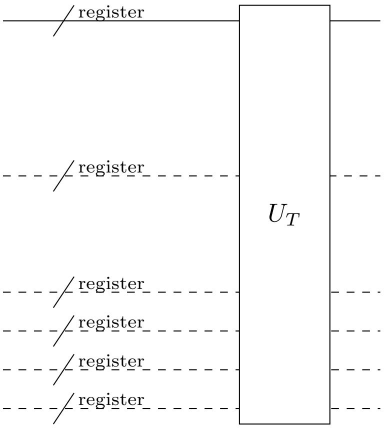
- Two-register Clifford-gate abbreviations



. (78)

A two-register Clifford-gate abbreviation applies an arbitrary Clifford operation U_C to two registers represented by solid lines. The four registers represented by dashed lines are used as workspaces.

- U_T-gate abbreviations



. (79)

A U_T-gate abbreviation applies the U_T operation to a register (solid line). Here, U_T is the tensor product of any combination of T, $T^\dagger$, and I. The five registers represented by dashed lines are used as workspaces.

Some of the elementary operations may take as input a bitstring that is determined during the execution of the quantum computation, and the specification of the elementary operation is determined on the fly by this input. Such elementary operations are called *on-demand* elementary operations. We also introduce on-demand abbreviations in a similar way. In the following, we list the on-demand elementary operations and abbreviations used in our protocol.

- On-demand Pauli gate operations

The Pauli-gate operations that are used for a correction operation required for gate teleportation in the two-register Clifford-gate abbreviation will be presented in Sec. IV B 1. The on-demand Pauli-gate operations receive a bitstring as a $2K$-bit vector of symplectic representation $\phi(P)$, where P is the K-qubit Pauli operator

$$P = \bigotimes_{k=1}^{K} P_k \in \tilde{\mathcal{P}}_K \tag{80}$$

to be applied by updating the Pauli frame as discussed in more detail below.

- On-demand two-register Clifford-gate abbreviations

The two-register Clifford-gate abbreviations used for correction operations for the gate teleportation in the U_T-gate abbreviations will be presented in

Sec IV B 2. The Clifford gate $U_C \in \tilde{\mathcal{C}}_{2K}/\tilde{\mathcal{P}}_{2K}$ we use in the U_T-gate abbreviations has the form of a tensor product of $2K$ single-qubit Clifford gates,

$$U_C = \bigotimes_{k=1}^{2K} C_k, \tag{81}$$

where $C_k \in \tilde{\mathcal{C}}_1/\tilde{\mathcal{P}}_1$ is an arbitrary single-qubit Clifford operator that acts on the k-th qubit of the first register for $k \in \{1, \ldots, K\}$ and on the $(k-K)$-th qubit of the second register for $k \in \{K+1, \ldots, 2K\}$. Thus, the on-demand abbreviations receive a bitstring as $2K$ symplectic matrices of size 2×2 of C_k as in (14).

- On-demand Clifford-state preparation

  The Clifford-state preparation operation is invoked by the on-demand two-register Clifford-gate abbreviation. The on-demand Clifford-state preparations receive bits as a $2K \times 2K$ binary matrix representing U_C.

It is essential for our protocol to perform on-demand Pauli operations classically by tracking and updating the *Pauli frame* of a quantum state [39, 43, 44]. The Pauli frame of a state relative to a specific reference state at a given time is defined as a Pauli operator

$$P_\mathrm{F} \in \tilde{\mathcal{P}}_K, \tag{82}$$

such that applying P_F to a state returns the reference state. We refer to a Pauli frame used in circuits described by elementary operations as a *elementary* Pauli frame. Note that we will also define a physical Pauli frame later in (86), which is used for physical circuits and is different from the elementary one. During the execution of quantum computation, for each register, we store a Pauli frame as a bitstring

$$\phi(P_\mathrm{F}) \in \mathbb{F}_2^{2K}. \tag{83}$$

We choose the reference state as the *corrected* state that would be obtained if the correction operation in the two-register Clifford-gate abbreviation to perform gate teleportation were applied to qubits, and the Pauli frame is tracked for the *uncorrected* state with no correction operation applied. The advantage of using Pauli frames is that it eliminates the need to physically implement on-demand Pauli operations. This means that there is no need to convert them into Pauli gadgets as described in the physical circuit, thereby eliminating the classical computation required to determine the physical Pauli-gate operation for performing a logical Pauli-gate operation and avoiding the errors that arise from physically applying the Pauli gates.

In the compilation prior to starting the execution of quantum computation, elementary operations (and abbreviations) that are not on-demand, i.e., do not require classical input, are called scheduled operations (and abbreviations) and are distinguished from on-demand ones. All scheduled elementary operations and abbreviations are determined during compilation, independently of on-demand operations, and are remain unchanged during the execution of quantum computation. This reduces the time overhead of waiting for classical computations during the execution.

In constructing an intermediate circuit, we require it shold be represented only by abbreviations (including the two-register Clifford-gate abbreviations (78), the U_T-gate abbreviations (79)), the $|0\rangle^{\otimes K}$-state preparation operation (64), the Z_K-measurement operation (72), and the wait operation (76). For simplicity, we refer to these elementary operations and abbreviations as intermediate operations. We compile the original circuit into the intermediate circuit using the following procedure. First, n qubits in the original circuit are divided into

$$\kappa(n) := \lceil n/K \rceil \tag{84}$$

registers, where each register contains at most K qubits, and $\lceil \cdot \rceil$ represents the ceiling function. For each of these registers, we also allow the intermediate circuit to use five auxiliary registers that can be allocated and used as workspace for the abbreviations. Next, we replace the operations in the original circuit with the corresponding intermediate operations. The $|0\rangle$-state preparations at the beginning of the original circuit are replaced with $|0\rangle^{\otimes K}$-state preparations. We replace the Z-basis measurements at the end of the original circuit with Z_K-measurement operations. We replace a T-gate layer in the original circuit with U_T-gate abbreviations. We replace each Clifford layer of Clifford gates in the original circuit with two-register Clifford-gate abbreviations. Even if an arbitrarily long sequence of Clifford gates acts on qubits located in the same register of the intermediate circuit, the Clifford gates can be collectively replaced with a single use of a two-register Clifford-gate abbreviation. However, we assume the intermediate circuit can perform at most one intermediate operation per register per time step, where the total number of time steps defines the depth of the intermediate circuits. Under this construction, if a one-depth part of the original circuit contains multiple Clifford gates acting on qubits in different pairs of registers, the corresponding part of the intermediate circuit requires two-register Clifford-gate abbreviations placed in series, as described in Sec. IV E. After replacing operations in the original circuit with intermediate operations, we limit the maximum number of non-trivial intermediate operations (i.e., operations other than the wait operation) that can be applied in parallel at a single time step, denoted by

$$L(n), \tag{85}$$

which will turn out to be able to be chosen as (199) later in our analysis. At the same time step, we insert wait operations for all registers where a non-trivial intermediate operation is not applied. Progressing beyond the existing analyses [20–22] with $L(n) = \Theta(W(n)/\mathrm{poly}(n))$, we

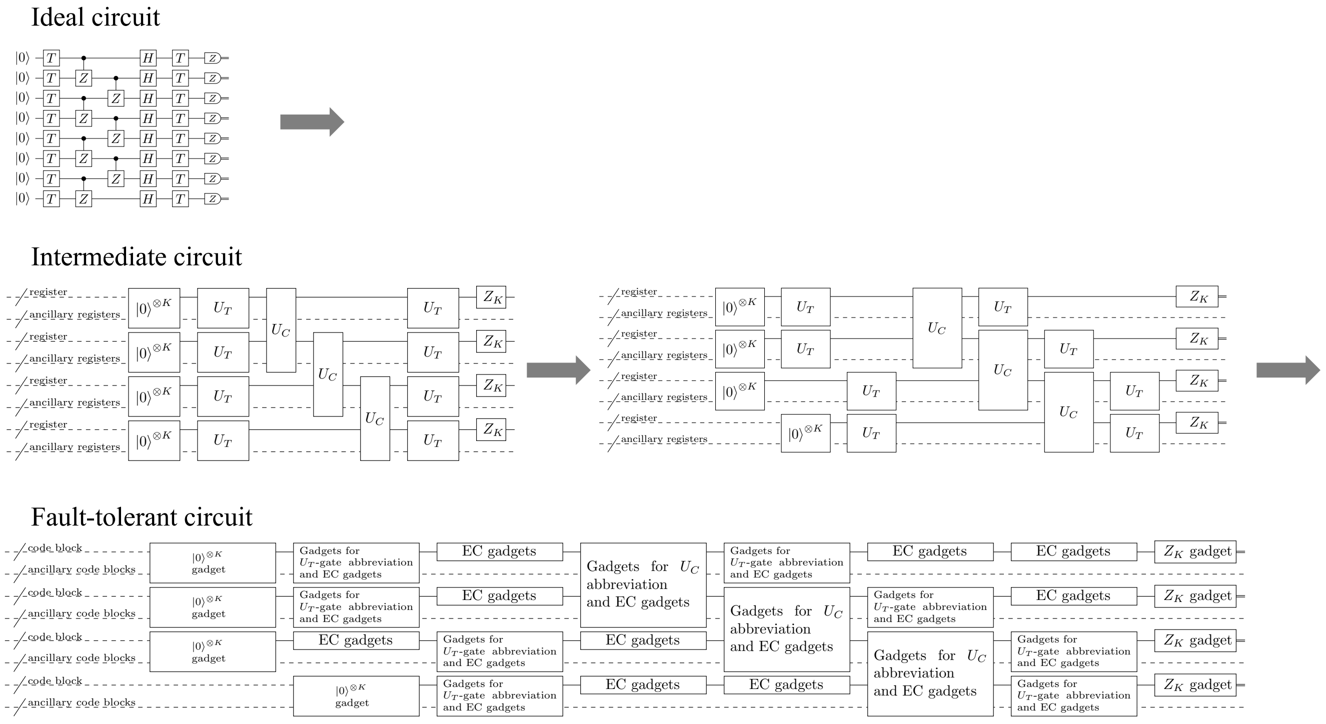


FIG. 3. Compilation procedure of our fault-tolerant protocol. First, we compile an original circuit into an intermediate circuit that consists only of intermediate operations acting on registers. Here, the two-register Clifford-gate abbreviation U_C and the U_T-gate abbreviation, which are implemented via gate teleportation, are described by a sequence of elementary operations. Then, we limit the number of intermediate operations each time step to achieve constant-space overhead. Finally, we compile the intermediate circuit with reduced parallelism into a fault-tolerant circuit by replacing each elementary operation with the corresponding gadget, inserting an EC gadget in between.

will rigorously show that $L(n) = \Theta(W(n)/\mathrm{polylog}(n))$ to prove that polylogarithmic time overhead is achievable.

2. *Compilation from intermediate circuit to fault-tolerant circuit*

As the next step in the compilation, we compile an intermediate circuit into a fault-tolerant circuit. In this step, all elementary operations in the intermediate circuit are replaced with corresponding gadgets, consisting only of physical operations.

The construction of gadgets will be described in Sec. IV D. Each gadget consists of a *quantum* part and a *classical* part. The quantum part is described by physical operations that need to be applied to the data qubits, whereas the classical part involves the necessary classical computations for executing the gadget. During the execution of the classical part, the wait operations act on the data qubits in the same way as the quantum part.

For the EC gadget, a Pauli recovery operation takes as an input bitstring that is determined by a decoding algorithm during the execution of the quantum computation, and the specification of the EC gadget is determined on the fly by this input. In this paper, the Pauli recovery operation can also be performed as a classical part by tracking Pauli frames, as well as the on-demand Pauli operation of a two-register Clifford gate abbreviation. Apart from the elementary Pauli frame in (82), we also define a *physical* Pauli frame, which is a Pauli frame for physical circuits. This physical Pauli frame

$$P_{\mathrm{F}} \in \tilde{\mathcal{P}}_N \tag{86}$$

is stored for each code block, individually. We choose the reference state as the *recovered* state that would be obtained if a recovery operation were applied to the physical qubits, and the Pauli frame is tracked for the *unrecovered* state with no recovery operation applied. The advantage of using the Pauli-frame technique is that it eliminates the need to physically implement recovery operations and simplifies the proof of the threshold theorem of the overall protocol, as explained in Sec. IV E.

Compilation from intermediate circuits to fault-tolerant circuits involves the following procedures performed sequentially for each intermediate operation within the same time step. For a given time step, if an intermediate operation is an abbreviation, the abbreviation is expanded into elementary operations (left unchanged if an intermediate operation is already an elementary operation). Next, elementary operations within the same time step in the intermediate circuit are replaced with corresponding gadgets, and EC gadgets are inserted between elementary operations. At this point, the same intermediate operation has a different circuit depth when replaced by a physical circuit. Therefore, wait operations are inserted for synchronization, so that EC gadgets should be inserted at a constant time interval from the completion of the execution of the physical circuit of the intermediate operation that finishes earlier until the completion of the execution of the intermediate operation belonging to the same time step with the greatest depth of the physical circuit. By performing this procedure at all time steps of the intermediate circuit, a fault-tolerant quantum circuit is finally obtained.

B. Construction of abbreviations

In the following, we explain the construction of abbreviations. In Sec. IV B 1, we present the construction of two-register Clifford-gate abbreviations (78). In Sec. IV B 2, we present the construction of U_T-gate abbreviations (79).

1. *Two-register Clifford-gate abbreviations*

The two-register Clifford-gate abbreviations are used to apply multiple Clifford gates acting on the same pair of registers. The construction of the abbreviations is shown in Fig. 4.

The abbreviation is based on a gate teleportation protocol [39, 45, 46]. In the beginning, we have the two registers A_1 and A_2 on which we want to perform the Clifford operation U_C, and the four auxiliary registers A_3, A_4, A_5, A_6 in the state

$$|\Psi_{U_C}\rangle^{A_3A_4A_5A_6} = (I^{A_3A_4} \otimes U_C^{A_5A_6})\,|\Omega\rangle^{A_3A_4A_5A_6}\,, \quad (87)$$

which is prepared by the Clifford-state preparation operation (65). After preparing the auxiliary states, we perform the Bell-measurement operation (73) on two pairs of registers A_1, A_3 and A_2, A_4. These Bell measurements output the pair of $2K$-bit outcomes as

$$(x^{A_1A_3}, z^{A_1A_3}) \in \mathbb{F}_2^{2K} \text{ and } (x^{A_2A_4}, z^{A_2A_4}) \in \mathbb{F}_2^{2K}, \quad (88)$$

where the K-bit string x' represents the outcomes of the measurements of $X \otimes X$, and the K-bit string z' represents the outcomes of the measurements of $Z \otimes Z$. From the $4K$-bit outcomes, we calculate the correction operation $P_{\text{corr}} \in \tilde{\mathcal{P}}_{2K}$ for the gate teleportation in the form of

$$P_{\text{corr}} := U_C^{A_5A_6}\left(\bigotimes_{k=1}^{K} P_k^{A_5} \otimes \bigotimes_{l=1}^{K} P_l^{A_6}\right)\left(U_C^{A_5A_6}\right)^{\dagger}, \quad (89)$$

where $P_k^{B_j} \in \{I, X, Y, Z\}$ with $j \in \{5, 6\}$ is a Pauli operator acting on the k-th qubit in the register B_j. From the $4K$-bit measurement outcome of the Bell measurements, the corresponding correction operation in (89) can be calculated via multiplication of the symplectic matrix $\gamma(U_C^{A_5A_6}) \in \mathbb{F}_2^{4K\times 4K}$ from the right of the row vector of the symplectic representation of $\phi\left(\left(\bigotimes_{k=1}^{K} P_k^{A_5} \otimes \bigotimes_{l=1}^{K} P_l^{A_6}\right)\right) \in \mathbb{F}_2^{4K}$ as

$$\phi(P_{\text{corr}}) = \phi\left(\left(\bigotimes_{k=1}^{K} P_k^{A_5} \otimes \bigotimes_{l=1}^{K} P_l^{A_6}\right)\right)\gamma(U_C^{A_5A_6}). \quad (90)$$

The resulting $4K$-dimensional row vector of (90) is used as an input bitstring to specify the on-demand Pauli-gate operation for the correction operation. Using $O(K^2)$ parallel processes, this classical computation can be performed within a runtime of

$$O(\log(K)). \quad (91)$$

The wait operations (76) are performed during this classical computation. Then, the Pauli-gate operation (89) for the correcting operation is applied to the registers A_5, A_6 completing this abbreviation.

However, by using the Pauli frame technique, we can avoid the need to perform an on-demand Pauli operation directly on physical qubits. Specifically, when on-demand Pauli operations are physically applied, there is no need to compute physical Pauli operations such that on-demand Pauli operations are performed as logical operations, which takes runtime $O(\log N)$ as explained in Appendix C. Instead, we can simply store the on-demand Pauli operation as an elementary Pauli frame in a classical register. Let

$$P_{\mathrm{F}}^{A_1} \in \tilde{\mathcal{P}}_K \text{ and } P_{\mathrm{F}}^{A_2} \in \tilde{\mathcal{P}}_K \quad (92)$$

be an elementary Pauli frame of the registers A_1 and A_2, respectively, at the time just before the abbreviation and

$$(x'^{A_1A_3}, z'^{A_1A_3}) \in \mathbb{F}_2^{2K} \text{ and } (x'^{A_2A_4}, z'^{A_2A_4}) \in \mathbb{F}_2^{2K} \quad (93)$$

be the measurement outcomes of the Bell measurement operation obtained from the uncorrected state, where the K-bit string x' represents the measurement outcomes of $X \otimes X$ operators, and the K-bit string z' represents the measurement outcomes of the $Z \otimes Z$ operators. The classical computer receives an input bitstring as the symplectic representation

$$\phi(P_{\mathrm{F}}^{A_1}) \in \mathbb{F}_2^{2K} \text{ and } \phi(P_{\mathrm{F}}^{A_2}) \in \mathbb{F}_2^{2K}, \quad (94)$$

and the pair of $2K$-bit strings $(x'^{A_1A_3}, z'^{A_1A_3})$ and $(x'^{A_2A_4}, z'^{A_2A_4})$ in (93). Then, the classical computer outputs a bitstring of the symplectic representation of the elementary Pauli frame

$$\phi(P_{\mathrm{F}}^{A_5}) \in \mathbb{F}_2^{2K} \text{ and } \phi(P_{\mathrm{F}}^{A_6}) \in \mathbb{F}_2^{2K}, \quad (95)$$

where $P_{\mathrm{F}}^{A_5}$, $P_{\mathrm{F}}^{A_6}$ are Pauli frames of the registers A_5 and A_6, respectively, at the final step of the abbreviation and

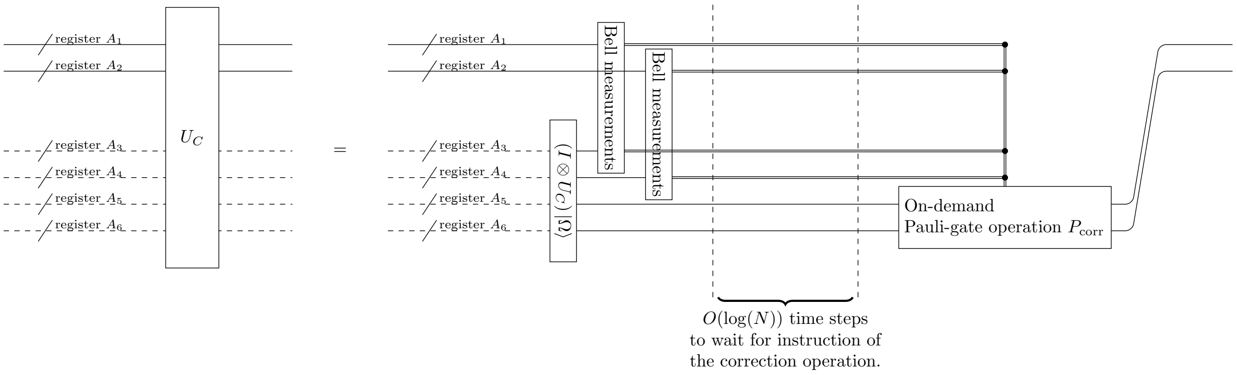


FIG. 4. The construction of the two-register Clifford-gate abbreviations (78) to perform a Clifford gate U_C applied to the two registers A_1, A_2.

provide the input for the subsequent abbreviation. To this end, we first modify the measurement outcomes (93) to (88) based on the input Pauli frame (92). For registers A_1 and A_3, this modification can be performed by taking a sum for $i \in [1, \ldots, K]$ as

$$x_i^{A_1A_3} = x_i'^{A_1A_3} \oplus \left(\phi\left(P_{\mathrm{F}}^{A_1}\right)\right)_{i+K} \oplus \left(\phi\left(P_{\mathrm{F}}^{A_2}\right)\right)_{i+K}, \tag{96}$$

and

$$z_i^{A_1A_3} = z_i'^{A_1A_3} \oplus \left(\phi\left(P_{\mathrm{F}}^{A_1}\right)\right)_{i} \oplus \left(\phi\left(P_{\mathrm{F}}^{A_2}\right)\right)_{i}. \tag{97}$$

Similarly, the same procedure can be applied to the registers A_2 and A_4. Using $O(K)$ parallel processes, the modification can be performed with runtime $O(1)$. Next, based on the modified measurement outcomes $(x^{A_1A_3}, z^{A_1A_3})$, $(x^{A_2A_4}, z^{A_2A_4})$, the classical computation for determining the Pauli correction operation (89) is performed as already explained above. This classical computation can be performed within runtime $O(\log K)$. The Pauli correction operation gives the elementary Pauli frames in (95) to be passed as the next input of the abbreviation,

$$\phi(P_{\mathrm{F}}^{A_5}) = \left((\phi(P_{\mathrm{corr}}))_{[1:K]}, (\phi(P_{\mathrm{corr}}))_{[2K+1:3K]}\right), \tag{98}$$

and

$$\phi(P_{\mathrm{F}}^{A_6}) = \left((\phi(P_{\mathrm{corr}}))_{[K:2K+1]}, (\phi(P_{\mathrm{corr}}))_{[3K+1:4K]}\right), \tag{99}$$

where $(\phi(P_{\mathrm{corr}}))_{[j:k]}$ represents a binary row vector consisting of the elements from the j-th to the k-th position of the original binary row vector $\phi(P_{\mathrm{corr}})$. Using $O(K)$ parallel processes, these computations can be performed within runtime $O(1)$. Therefore, the classical computation for calculating (95) from (94) can be performed with runtime $O(1)$.

As a result, the depth of the whole abbreviation is bounded by

$$O(\log K), \tag{100}$$

where the dominant part is the classical computation for calculating (90).

2. U_T-gate abbreviation

The U_T-gate abbreviation is used to apply the U_T gate, which is the tensor product of T, $T^\dagger$ and I acting on the qubits in a register. The construction of the U_T-gate abbreviation is shown in Fig. 5.

The U_T-gate abbreviation is also based on the gate teleportation protocol [39, 45, 46]. At the beginning of the gate teleportation protocol, we have the register A_1 containing the qubits on which we want to perform the gate U_{TH}, and the auxiliary register A_2 in the state

$$|\Psi_{U_{TH}}\rangle = U_{TH}\,|0\rangle^{\otimes K}, \tag{101}$$

which is prepared by the magic-state preparation operation (69). After preparing the auxiliary register A_2, we perform the CNOT-gate operation (71), followed by the Z_K-measurement operation (72). This Z_K-measurement operation outputs a K-bit string as

$$z \in \mathbb{F}_2^K. \tag{102}$$

From the K-bit measurement outcomes, a Clifford gate SX for the correction operation is applied to the qubits on which U_T has non-trivial support. At this point, T has been applied to the qubits where $T^\dagger$ is to be performed. Thus, an additional Clifford gate $S^\dagger$ needs to be applied to the qubit to perform $T^\dagger$. To implement these Clifford gates, we use a two-register abbreviation to perform $U_{\mathrm{corr}} \in \tilde{\mathcal{C}}_{2K}/\tilde{\mathcal{P}}_{2K}$ as in (78) that acts non-trivially only on the register A_2. Specifically, U_{corr} is expressed as a tensor product involving pairs of single-qubit Clifford gate $SX \otimes I$ and $I \otimes I$. Using the K-bit string of measurement outcome, we calculate the correction operation as

$$U_{\mathrm{corr}} = \bigotimes_{k=1}^{2K} C_k, \tag{103}$$

where $C_k \in \tilde{\mathcal{C}}_1/\tilde{\mathcal{P}}_1$ is either SX or I. This correction operation is performed with the on-demand Clifford-gate abbreviation (81), whose input consists of $2K$ symplectic matrices in (14) of size 2×2 which are either

$$\gamma(SX) \text{ or } \gamma(I). \tag{104}$$

Subsequently, this input is loaded into an on-demand two-register Clifford-gate abbreviation to execute the correction operation. Using $O(K)$ parallel processes, the runtime of classical computation to generate the input to the on-demand abbreviation can be bounded by $O(1)$.

Unlike the two-register Clifford-gate abbreviation, even if we utilize the Pauli frame technique, the correction operation of Clifford gate must be performed. If a Clifford correction operation were stored classically and a subsequent measurement operation contained in a next abbreviation was executed, it would be impossible to deterministically obtain the modified measurement results that would have been achieved with the application of the correction operation. When we utilize the Pauli frame technique, we have an elementary Pauli frame

$$P_{\mathrm{F}}^{A_1} \in \tilde{\mathcal{P}}_K \tag{105}$$

at the time just before the abbreviation and measurement outcomes

$$z' \in \mathbb{F}_2^K \tag{106}$$

of the Z_K-measurement operation obtained from the uncorrected state. The classical computer takes an input bitstirng of the symplectic representation

$$\phi(P_{\mathrm{F}}^{A_1}) \in \mathbb{F}_2^{2K} \tag{107}$$

and the K-bit string z' (106). Then, the classical computer outputs a bitstring of the symplectic representation of the elementary Pauli frame

$$\phi({P'}_{\mathrm{F}}^{A_1}) \in \mathbb{F}_2^{2K} \tag{108}$$

at the final step of the abbreviation and provide the input of the subsequent abbreviation. To this end, we modify the measurement outcomes (106) to (102) based on the input Pauli frame. The modification of the measurement outcomes z' (106) is performed by taking a sum for $i \in [1, \ldots, K]$ as

$$z_i = {z'}_i \oplus (\phi({P'}_{\mathrm{F}}^{A_1}))_i. \tag{109}$$

Using $O(K)$ parallel processes, this modification can be performed within runtime $O(1)$. Then, based on the modified measurement outcomes z_i, the classical computation for determining the Clifford correction operation is performed as already explained above. The elementary Pauli frame (108) to be passed to the next input of the abbreviation is calculated for each $i \in [1, \ldots, K]$

$$\phi(({P'}_{\mathrm{F}}^{A_1})_i) = \gamma(C_i)\phi(({P'}_{\mathrm{F}}^{A_1})_i). \tag{110}$$

Using $O(K)$ parallel processes, this classical computation can be performed with runtime $O(1)$. Therefore, the classical computations for calculating (108) from (107) can be performed with runtime $O(1)$ using $O(K)$ parallel processes.

As a result, the depth of the U_T-gate abbreviation is bounded by

$$O(\log K), \tag{111}$$

where the dominant part is the depth of the on-demand two-register Clifford-gate abbreviation.

C. Conditions of fault-tolerant gadgets on quantum LDPC codes

In this section, we define the fault-tolerance condition for gadgets for quantum LDPC codes. Before we provide the definition, we introduce a property of the decoding algorithm that is required for constructing our protocol.

The decoding algorithm used for quantum LDPC codes needs to consider cases where the syndrome bits may be erroneous, due to noise in the circuits used to measure the syndrome bits. Here, we consider a CSS LDPC code obtained from a pair of classical linear codes, $C_X = \ker H_X$ and $C_Z = \ker H_Z$, where $H_X \in \mathbb{F}_2^{M_Z \times N}$ and $H_Z \in \mathbb{F}_2^{M_Z \times N}$ are parity-check matrices. Let $e = \phi(E) \in \mathbb{F}_2^{2N}$ be a symplectic representation of a Pauli error $E \in \mathcal{P}_N$ on data physical qubits, and $\Delta = (\Delta_X, \Delta_Z) \in \mathbb{F}_2^M$ be errors on syndrome bits. The ideal syndrome bits

$$\sigma = (\sigma_X, \sigma_Z) \in \mathbb{F}_2^M \tag{112}$$

for the error $e \in \mathbb{F}_2^{2N}$ is given by

$$\sigma_X = H_Z e_X \quad \text{and} \quad \sigma_Z = H_X e_Z. \tag{113}$$

However, the ideal syndrome bits $\sigma \in \mathbb{F}_2^M$ can be corrupted by syndrome errors $\Delta \in \mathbb{F}_2^M$, resulting in noisy syndrome bits

$$\tilde{\sigma} = (\tilde{\sigma}_X, \tilde{\sigma}_Z) \in \mathbb{F}_2^M \tag{114}$$

which is given by

$$\tilde{\sigma}_X = \sigma_X \oplus \Delta_X \quad \text{and} \quad \tilde{\sigma}_Z = \sigma_Z \oplus \Delta_Z. \tag{115}$$

Using the noisy syndrome $\tilde{\sigma}$, the decoding algorithm calculates the recovery operation $R \in \mathcal{P}_N$ with the symplectic representation $r = \phi(R)$.

In the analysis of the decoding algorithm, the local stochastic Pauli error model for the pair (e, Δ) is used, which is defined as follows:

Definition 8 (Local stochastic Pauli error model on data qubits and syndrome bits)**.** Let V be the set of physical qubits and $W_{X(Z)}$ be the set of $X(Z)$-type stabilizer generators. Let $e = (e_X, e_Z) \in \mathbb{F}_2^{2N}$ be a Pauli error, $\Delta = (\Delta_X, \Delta_Z) \in \mathbb{F}_2^M$ be syndrome bit errors. Let

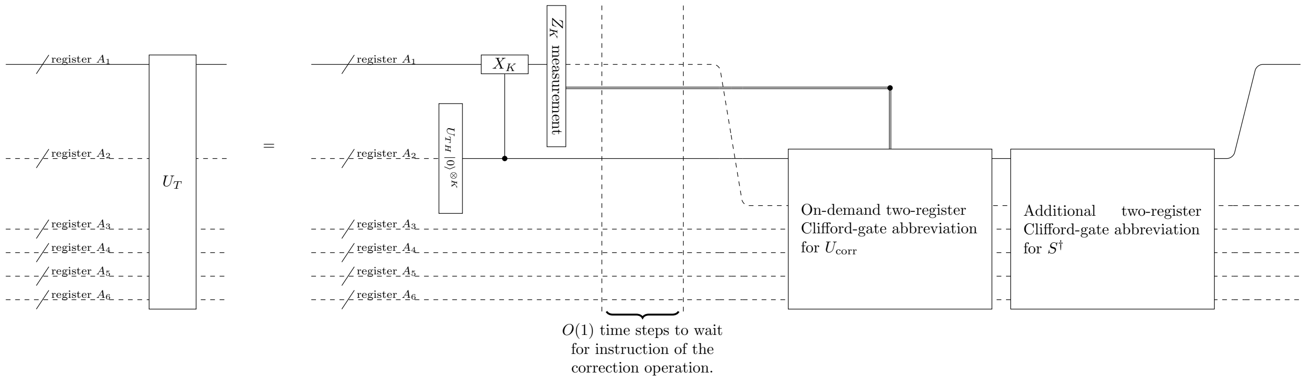

register A_1
register A_2
register A_3
register A_4
register A_5
register A_6
U_T
=
register A_1
register A_2
register A_3
register A_4
register A_5
register A_6
$U_{TH}\,|0\rangle^{\otimes K}$
X_K
Z_K measurement
On-demand two-register Clifford-gate abbreviation for U_{corr}
Additional two-register Clifford-gate abbreviation for $S^\dagger$
$O(1)$ time steps to wait for instruction of the correction operation.

FIG. 5. The construction of the U_T-gate abbreviation (79) to perform a U_T gate on the register A_1.

$\mathrm{supp}(e_{X(Z)}) \subseteq V$ be the support of a $X(Z)$-type Pauli error and $\mathrm{supp}(\Delta_{X(Z)}) \subseteq W_{Z(X)}$ be the support of errors on syndrome bits. We say that errors (e, Δ) follow the local stochastic Pauli error model with parameters $(p_{\mathrm{data}}, p_{\mathrm{synd}})$ if for all $S \subseteq V$, $T \subseteq W_Z$, and $T' \subseteq W_X$, the following relations are satisfied.

$$\begin{aligned}\mathbb{P}\left[S \subseteq \mathrm{supp}(e_X) \text{ and } T \subseteq \mathrm{supp}(\Delta_X)\right] &\leq p_{\mathrm{data}}^{|S|} p_{\mathrm{synd}}^{|T|}, \\ \mathbb{P}\left[S \subseteq \mathrm{supp}(e_Z) \text{ and } T \subseteq \mathrm{supp}(\Delta_Z)\right] &\leq p_{\mathrm{data}}^{|S|} p_{\mathrm{synd}}^{|T|}\end{aligned} \tag{116}$$

In particular, when the errors on the syndrome bits are not considered, we say that errors follow a local stochastic Pauli error model with parameter p_{data} if for all $S \subseteq V$, the errors satisfy

$$\mathbb{P}\left[S \subseteq \mathrm{supp}(e_X)\right] \leq p_{\mathrm{data}}^{|S|} \text{ and } \mathbb{P}\left[S \subseteq \mathrm{supp}(e_Z)\right] \leq p_{\mathrm{data}}^{|S|}. \tag{117}$$

Quantum expander codes [20, 47] and quantum Tanner codes [48], which are important classes of CSS LDPC codes, each have their own decoding algorithms [20, 22, 49] such that when $\Delta \neq 0$, they can deduce a recovery operation to suppress the residual error $e^{\mathrm{re}} \in \mathbb{F}_2^{2N}$ on data physical qubits,

$$e^{\mathrm{re}} := e \oplus r. \tag{118}$$

An intriguing property of these decoding algorithms is the *single-shot* property [20, 22]. A decoding algorithm with the single-shot property works by using noisy syndrome bits $\tilde{\sigma}$, where these noisy syndrome bits are obtained from a *single* round of syndrome measurements for each stabilizer generator [20, 22, 49–53]. Using these syndrome bits obtained from the single syndrome extraction, existing single-shot decoding algorithms for finite-quantum LDPC codes [20, 22, 49] run in an iterative way, i.e., they repeat T internal loops, to output a final estimate of a recovery operation $r := r^{(T)}$. Each of the T loops can be executed with a runtime of $O(1)$, using $O(N)$ parallel processes. For each iteration $t \in [1, \ldots, T]$, the algorithm computes a temporally deduced recovery operation $r^{(t)} \in \mathbb{F}_2^{2N}$. The decoding algorithm requires that for all t, the support of the residual error, derived by using $r^{(t)} \in \mathbb{F}_2^{2N}$, should be less than or equal to the code distance D. Formally, the definition of the single-shot decoding algorithm for non-vanishing-rate quantum LDPC codes is as follows:

Definition 9 (Single-shot decoding algorithm)**.** Let $\{\mathcal{Q}_i\}_i$ be a family of CSS LDPC codes where $\mathcal{Q}_i$ is an $[[N_i, K_i, D_i]]$ code with $N_i \to \infty$ for $i \to \infty$. Let $e = (e_X, e_Z) \in \mathbb{F}_2^{2N}$ be a Pauli error, $\Delta = (\Delta_X, \Delta_Z) \in \mathbb{F}_2^M$ be syndrome bits error, and $\tilde{\sigma} = (\tilde{\sigma}_X, \tilde{\sigma}_Z) \in \mathbb{F}_2^M$ be noisy syndrome bits. For $P = \{X, Z\}$, a decoding algorithm returns the recovery operation $r_P^{(t)} \in \mathbb{F}_2^{2N}$ at each iteration $t \in \{1, \ldots, T\}$, and the final output of the recovery operation is denoted by $r_P := r_P^{(T)}$. A decoding algorithm for $\{\mathcal{Q}_i\}_i$ is said to be single-shot if, for $i \to \infty$ and for

$$u_P := e_P \oplus r_P^{(1)} \oplus \cdots \oplus r_P^{(T)}, \tag{119}$$

there exist positive constants a and b such that

$$|u_P| \leq a|e_P|_{\mathrm{R}} + b|\Delta_P| \leq D, \tag{120}$$

and then given the noisy syndrome bits $\tilde{\sigma}_P \in \mathbb{F}_2^{M_P}$ the algorithm can find a recovering operation $r_P \in \mathbb{F}_2^N$ after T steps that satisfy

$$|e_P + r_P|_{\mathrm{R}} \leq \alpha|e_P|_{\mathrm{R}} + \beta|\Delta_P|, \tag{121}$$

with

$$\alpha = 2^{-\Omega(T)}, \quad \beta = O(1). \tag{122}$$

Moreover, each iteration of the decoding algorithm can be performed within runtime $O(1)$ by using $O(N)$ parallel processes. Here $|\cdot|_{\mathrm{R}}$ denotes the stabilizer-reduced weight defined to be the minimum weight of a stabilizer-equivalent error to $e_P \in \mathbb{F}_2^N$, i.e.,

$$|e_P|_{\mathrm{R}} := \min_{g' \in C^\perp} |e_P + g'|. \tag{123}$$

In the analysis of this work, we consider the local stochastic Pauli error model on the data qubits and the syndrome bits. Under this model, the weight of errors typically scales linearly in the number of physical qubits N contained in a code $\mathcal{Q}$. It appears that a code with code distance $D = \Omega(N)$ would be required to correct errors of linear weight. However, when one uses quantum LDPC codes under the stochastic error model, there are cases where errors can be corrected with a high probability when the error parameter is below a threshold error parameter [20–22, 54] as $N \to \infty$. This is feasible because, at sufficiently low error rates, typical linear weight errors occurring in quantum LDPC codes tend to form small, separate clusters of errors that are independently correctable by using a single-shot decoding algorithm. In the following, we define two decoding algorithms that quantum LDPC codes should have: the single-shot decoding algorithm with thresholds for reducing residual errors and the decoding algorithm with threshold for recovering logical information, where these algorithms are designed to correct local stochastic Pauli errors on wires with high probability if an error parameter is below a certain threshold value. The quantum expander code has both of these decoding algorithms while it is currently unknown whether the quantum Tanner code may also have these decoding algorithms satisfying the required properties for error suppression.

Both decoding algorithms, which reduce errors and correct errors, are performed iteratively. The runtime of the classical computation depends on the number of iterations within each algorithm. It is important to note that the runtime of each loop does not grow as $N \to \infty$ when parallel processes are used. These decoding algorithms work in different situations and play different roles in our fault-tolerant protocol. Specifically, the single-shot decoding algorithm for reducing errors is capable of finding a recovery operation to keep the residual error small even if the syndrome bits are noisy, and thus we will utilize the algorithm in the EC gadget to keep the residual error small in the code block. On the other hand, the decoding algorithm for correcting errors is capable of recovering the logical state only when the syndrome bit errors are absent, and thus, we will use the algorithm in the Z_K-measurement gadget and the Bell-measurement gadget to obtain the measurement outcomes of the logical qubits in $\mathcal{Q}$. To summarize, we define the single-shot decoding algorithm for reducing errors and the decoding algorithm for correcting errors as follows.

Definition 10 (Single-shot decoding algorithm with thresholds for reducing errors)**.** Let $\{\mathcal{Q}_i\}_i$ be a family of CSS LDPC codes where $\mathcal{Q}_i$ is an $[[N_i, K_i, D_i]]$ code with $N_i \to \infty$ and $D_i \to D$ as $i \to \infty$ and $\{\mathcal{Q}_i\}_i$. Let $e = (e_X, e_Z) \in \mathbb{F}_2^{2N}$ be the data qubit errors and $\Delta = (\Delta_X, \Delta_Z) \in \mathbb{F}_2^M$ be the syndrome bit errors that are local stochastic with parameters $(p_{\text{data}}, p_{\text{synd}})$. A single-shot decoding algorithm with thresholds for $\{\mathcal{Q}_i\}_i$ has thresholds $p_{\text{dec}}^{\text{th}} > 0$, and if $p_{\text{data}} \leq p_1 < p_{\text{dec}}^{\text{th}}$, $p_{\text{synd}} \leq p_2 < p_{\text{dec}}^{\text{th}}$, for $P \in \{X, Z\}$, a single-shot decoding algorithm returns a recovery operation $r_P \in \mathbb{F}_2^{2N}$ from the noisy syndrome bits $\tilde{\sigma}$ (114) that are obtained from a single round of syndrome measurements for each stabilizer generator after T internal loops, with probability at least

$$1 - e^{-\Omega(D)}, \tag{124}$$

such that there exists a bit sequence e'_P satisfying

$$e'_P \oplus e_P \oplus r_P \in C_P^{\perp}, \tag{125}$$

where $e_P^{'}$ follows the local stochastic Pauli error model with parameter $p_{\text{data}}^{\text{re}}$ satisfying

$$p_{\text{data}}^{\text{re}} \leq p_1^{c(T)}, \tag{126}$$

where $c(T)$, which is referred to as an error suppression parameter, is a monotonically increasing function with respect to T. Each round of iteration can be executed with a runtime of $O(1)$, using $O(N)$ parallel processes.

If the decoding algorithm fails to return recovery operations r_P for both $P \in \{X, Z\}$ satisfying (125), then we say that the decoding algorithm fails.

Definition 11 (Decoding algorithm with threshold for correcting errors)**.** Let $\{\mathcal{Q}_i\}_i$ be a family of CSS LDPC codes where $\mathcal{Q}_i$ is an $[[N_i, K_i, D_i]]$ code with $N_i \to \infty$ and $D_i \to D$ as $i \to \infty$. Let $e = (e_X, e_Z) \in \mathbb{F}_2^{2N}$ be the data qubit error and $\Delta = (\Delta_X, \Delta_Z) \in \mathbb{F}_2^M$ be the syndrome bit errors that are local stochastic with parameters $(p_{\text{data}}, p_{\text{synd}})$. Suppose the syndrome bit errors are absent, i.e., $p_{\text{synd}} = 0$. A decoding algorithm has a threshold $p'^{\text{th}}_{\text{dec}} > 0$ and if $p_{\text{data}} < p'^{\text{th}}_{\text{dec}}$, for each $P \in \{X, Z\}$, the decoding algorithm returns a recovery operation $r_P \in \mathbb{F}_2^{2N}$ from the syndrome bits $\sigma \in \mathbb{F}_2^M$ as in (112) after $T = O(\log N)$ internal loops, such that the residual error $e^{\text{re}} := e \oplus r$ satisfies

$$e_P \oplus r_P \in C_P^{\perp}, \tag{127}$$

with probability at least

$$1 - e^{-\Omega(D)}. \tag{128}$$

Each loop can be executed with a runtime of $O(1)$, using $O(N)$ parallel processes.

To the best of our knowledge, the family of quantum expander codes with $D = \Theta(\sqrt{N})$ is the only non-vanishing-rate quantum LDPC code that satisfies the requirements in Defs. 10 and 11. Specifically, the small-set-flip decoding algorithm for the quantum expander codes can work as both the single-shot decoding algorithm for reducing errors with thresholds in Def. 10 and the decoding algorithm for correcting errors in Def. 11 [20, 22]. More recently, Ref. [49] showed that the family of quantum Tanner codes with $D = \Theta(N)$ also has a single-shot decoding algorithm, but there is no proof that the bounds on the error parameter of a residual error under the local stochastic error model as in (126). Although it is conceivable that quantum Tanner codes could also achieve polylogarithmic time and constantspace overhead FTQC based on our protocol, we leave the rigious proof as an open work. To summarize, we make the following assumption about the families of non-vanishing-rate quantum LDPC codes that can be used in our protocol.

Assumption 4. *A family of non-vanishing-rate CSS LDPC codes $\{\mathcal{Q}_i\}_i$ where $\mathcal{Q}_i$ is an $[[N_i, K_i, D_i]]$ code with $N_i \to \infty$ and $D_i \to D = \Theta(N^\gamma)$ with $0 < \gamma \leq 1$ for $i \to \infty$ has a decoding algorithm that can serve as both the single-shot decoding algorithm for reducing errors with thresholds in Def. 10 and the decoding algorithm for correcting errors with threshold in Def. 11.*

In order for the fault-tolerant protocol using quantum LDPC codes to exhibit fault tolerance, gadgets must be designed so that errors caused by faults occurring in a gadget do not propagate too much even when the code block size N of $\mathcal{Q}$ increases, i.e., $i \to \infty$. To achieve this, we define the following fault-tolerance conditions that each type of gadget must satisfy.

The definition of fault tolerance of the state-preparation gadgets, including the gadget of the $|0\rangle^{\otimes K}$-state preparation operation (64), the gadgets of the Clifford-state preparation operations (65), and the gadgets of the magic-state preparation operations (69), is as follows.

Definition 12 (Fault-tolerance conditions of the state preparation gadgets for quantum LDPC codes)**.** Let C be a physical circuit of a state-preparation gadget. A state-preparation gadget C is fault-tolerant if, for $i \to \infty$, the gadget successfully prepare a desired state with any target probability of at least $1 - \delta$, and data qubits at the final step of C are subjected to the local stochastic error model on data qubits with parameter

$$Mp_{\mathrm{loc}}, \tag{129}$$

where $M = O(1)$ is a constant. We say that δ is the failure probability of a state-preparation gadget.

The definition of fault tolerance of the gate gadgets, including a gadget of the CNOT-gate operation (71), the measurement gadgets, including the gadget of the Z_K-measurement operation (72) and the gadget of the Bell-measurement operation (73), and the EC gadgets are defined as follows:

Definition 13 (Fault-tolerance conditions of gate, measurement, EC gadgets for quantum LDPC codes)**.** Let C be a physical circuit of a gadget. Let L be the set of locations in C, and $X_{\mathrm{in}}, X_{\mathrm{out}}$ be the set of wires at the first and final time step of C, respectively. A wire $x \in X$ at a given time step is *connected* to another wire $x' \in X'$ at a different time step if a Pauli operator acting at x can propagate to and affect x' through physical operations. Then, let us define a bipartite graph

$$G = (L, R, E) \tag{130}$$

of C, where the i-th vertex $l_i \in L$ corresponds to the i-th wire $x_i^{\mathrm{in}} \in X_{\mathrm{in}}$, the j-th vertex $r_i \in R$ corresponds to the j-th wire $x_j^{\mathrm{out}} \in X_{\mathrm{out}}$, and an edge $e \in E$ has the endpoints $l_i \in L$ and $r_j \in R$ if and only if $x_i^{\mathrm{in}} \in X_{\mathrm{in}}$ and $x_j^{\mathrm{out}} \in X_{\mathrm{out}}$ are connected. We say that a gadget is fault-tolerant if for $i \to \infty$, C satisfies the following conditions.

1. The maximum degree of a vertex in G of C is constant.

2. The depth of the quantum part of C is constant.

By constructing gadgets that satisfy the fault-tolerance conditions in Defs. 12 and 13, we will show in Sec. IV E that if the physical error rate is below a certain threshold, the failure probability of fault-tolerant simulations can be arbitrarily suppressed.

D. Construction of fault-tolerant gadgets

In this section, we present the construction of the gadgets that satisfy the fault-tolerance conditions in Defs. 12 and 13.

1. Z_K-measurement gadget

The construction of the Z_K-measurement gadget is shown in Fig. 6 (a). The gadget is implemented by transversal Z-basis measurements of the physical operation, followed by the classical computation for performing the decoding algorithm in Def. 11. The transversal measurements give N-bit measurement outcomes

$$z \in \mathbb{F}_2^N, \tag{131}$$

where z_i corresponds to the measurement outcome of the Z-basis measurement on the i-th physical qubit and is subjected to errors.

From $z \in \mathbb{F}_2^N$, we need to estimate the K-bit logical measurement outcomes

$$\bar{z} \in \mathbb{F}_2^K, \tag{132}$$

where $\bar{z}_i$ corresponds to the measurement outcome of the logical $\bar{Z}_i$ operator on the i-th logical qubits. This can be done in the following steps:

1. From $z \in \mathbb{F}_2^N$, we calculate the syndrome bits

$$\sigma_X \in \mathbb{F}_2^{M_Z} \tag{133}$$

of the Z-type generators by using the relation,

$$(\sigma_X)_i := \bigoplus_{j \in \mathrm{supp}(g_i^Z)} z_j, \tag{134}$$

where g_i^Z is the i-th Z-type stabilizer generator, and $\mathrm{supp}(g_i^Z)$ represents the set of indices of the

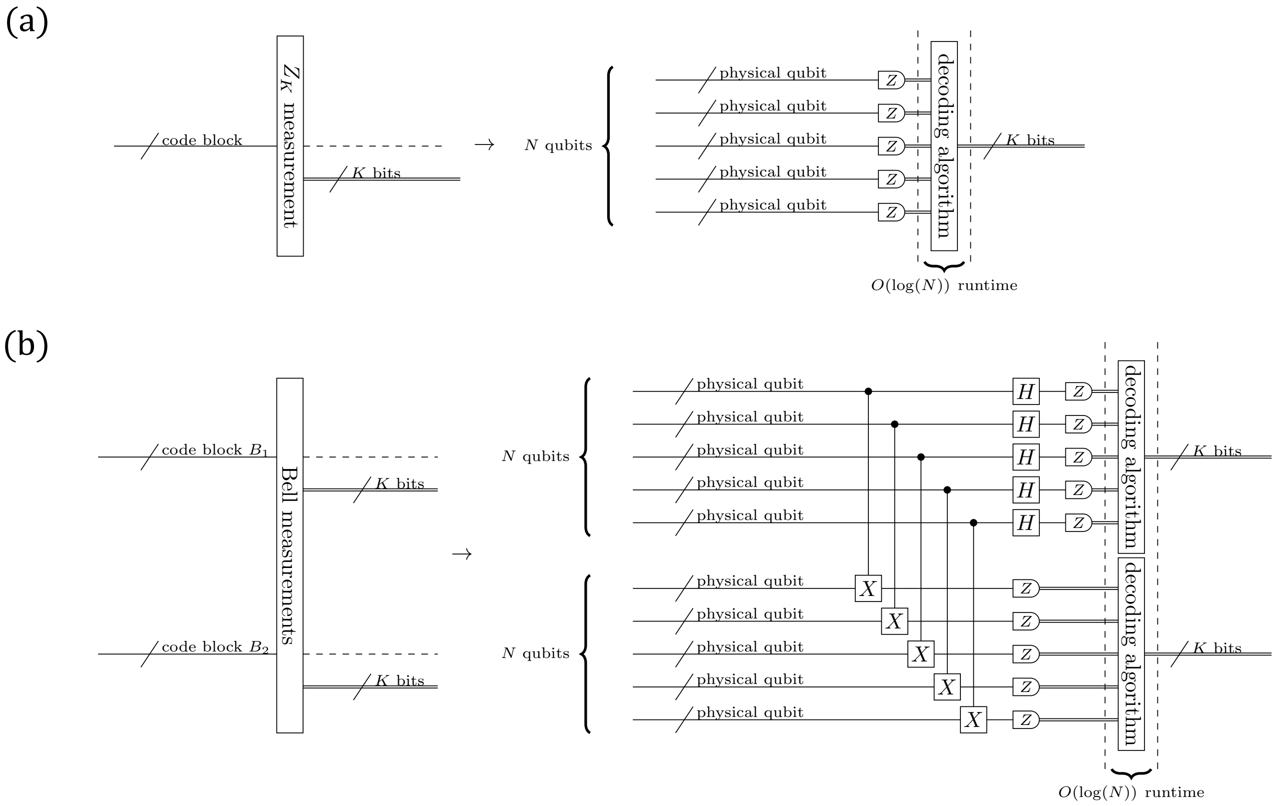


FIG. 6. (a) The physical circuit of the gadget of the Z_K-measurement operation (72) and (b) the physical circuit of the gadget of the Bell-measurement operation (73)

physical qubits on which g_i^Z acts nontrivially. Here, the syndrome bits σ_X (133) are calculated classically, and thus there are no syndrome bit errors. Using $M_Z = O(N)$ parallel processes, we can compute the syndrome bits σ_X (133) within runtime $O(\log N)$ since we use the CSS LDPC code $\mathcal{Q}$, and thus $|g_i^Z| = O(1)$ as $N \to \infty$.

2. We perform the decoding algorithm in Def. 11 that takes as input the syndrome bits $\sigma_X \in \mathbb{F}_2^{M_Z}$ and outputs the recovery operation $r_X \in \mathbb{F}_2^N$. Then, the corrected bitstring $\tilde{z} \in \mathbb{F}_2^N$ are obtained as for all $i \in [1, \ldots, N]$

$$\tilde{z}_i := z_i \oplus (r_X)_i. \tag{135}$$

Since there are no syndrome bit errors, the decoding algorithm can correct the data error. A decoding algorithm for correcting errors with threshold in Def. 11 can be performed within runtime $O(\log(N))$, and calculating (135) for all i can also be performed within runtime $O(1)$ using $O(N)$ parallel processes.

3. We calculate the measurement outcomes $\bar{z} \in \mathbb{F}_2^K$ of the logical operators as for all $i \in [1, \ldots, K]$

$$\bar{z}_i := \bigoplus_{j \in \mathrm{supp}(\bar{Z}_i)} \tilde{z}_j, \tag{136}$$

where $\bar{Z}_i$ is the logical-Z operator acting on the i-th logical qubit, and $\mathrm{supp}(\bar{Z}_i)$ represents the set of indices of the physical qubits on which $\bar{Z}_i$ acts nontrivially. Using $DK = O(N^2)$ parallel processes, we can compute (136) for all i within runtime $O(\log N)$ since $|\bar{Z}_i| = \Theta(D) = \Theta(N^\gamma)$ with $0 < \gamma \leq 1$ as $N \to \infty$.

Therefore, using $O(N^2)$ parallel processes, the classical part of the gadget can be performed within runtime

$$O(\log(N)). \tag{137}$$

For the Pauli-frame technique, we require additional classical computation. Let

$$P_{\mathrm{F}} \in \mathbb{F}_2^N \tag{138}$$

be a Pauli frame at the final step of the previous gadget and

$$z' \in \mathbb{F}_2^N \tag{139}$$

be the outcomes of the transversal Z-basis measurements obtained from the unrecovered state. The classical computer takes as input as the symplectic representation $\phi(P_{\mathrm{F}})$ and the measurement outcomes $z' \in \mathbb{F}_2^N$ of an unrecovered state and outputs the measurement outcomes $z \in \mathrm{F}_2^N$ of an recovered state as in (131). This calculation is performed for all $i \in [1, \ldots, N]$

$$z_i = z'_i \oplus (\phi(P_{\mathrm{F}}))_i \,. \tag{140}$$

Using $O(N)$ parallel processes, this additional computation can be performed within runtime $O(1)$.

The width of the quantum part in the gadget is bounded by

$$O(N), \tag{141}$$

and the depth of the quantum part is bounded by

$$O(1). \tag{142}$$

From the transversality and constant depth of the quantum part in the gadget, the gadget satisfies the fault-tolerance condition in Def. 13. The runtime of the classical part of the gadget can be bounded by runtime

$$O(\log N). \tag{143}$$

2. *Bell-measurement gadget*

The construction of the Bell-measurement gadget is shown in Fig. 6 (b). The gadget is implemented by the transversal CNOT gates between the controlled block B_1 and the target block B_2, the transversal H gates on B_1, followed by the transversal Z-basis measurements on B_1 and B_2. The transversal measurements on B_1 and B_2 yield a pair of N-bit strings of measurement outcomes, respectively, as

$$(x, z) \in \mathbb{F}_2^{2N} \tag{144}$$

where $x \in \mathbb{F}_2^N$ represents the outcomes from B_1 and $z \in \mathbb{F}_2^N$ represents those from B_2. Here, x_i and z_i correspond to the measurement outcome of the $X_i \otimes X_i$ and $Z_i \otimes Z_i$ operators, respectively, on N pairs of physical qubits. From $(x, z) \in \mathbb{F}_2^{2N}$, we deduce a pair of K-bit string of logical measurement outcomes as

$$(\bar{x}, \bar{z}) \in \mathbb{F}_2^{2K}, \tag{145}$$

where $\bar{x}_i$ and $\bar{z}_i$ correspond to the measurement outcomes of $\bar{X}_i \otimes \bar{X}_i$ and $\bar{Z}_i \otimes \bar{Z}_i$, respectively, on K pairs of logical qubits. To obtain K-bit outcomes of $\bar{z} \in \mathbb{F}_2^K$ from the noisy measurement outcomes $z \in \mathbb{F}_2^N$, we follow the procedure as described for the case of the Z_K-measurement gadget. The K-bit outcomes of $\bar{x} \in \mathbb{F}_2^K$ can also be estimated by replacing the Z-basis with the X-basis and performing the presented procedure since we consider the CSS code.

Based on the Pauli-frame technique, we require additional classical computation. Let

$$P_{\mathrm{F}}^{B_1} \otimes P_{\mathrm{F}}^{B_2} \in \mathbb{F}_2^{2N} \tag{146}$$

be a Pauli frame at the final step of the previous gadget and

$$(x', z') \in \mathbb{F}_2^{2N} \tag{147}$$

be the outcomes of transversal Z-basis measurements obtained from the unrecovered state, where $x' \in \mathbb{F}_2^N$ and $z' \in \mathbb{F}_2^N$ correspond to the outcomes from B_1 and B_2, respectively. The classical computation takes as input the symplectic representation $\phi(P_{\mathrm{F}}^{B_1} \otimes P_{\mathrm{F}}^{B_2})$ and the measurement outcomes $z' \in \mathbb{F}_2^N$ and outputs the measurement outcomes $z \in \mathrm{F}_2^N$ of a recovered state as in (144). This calculation is performed for all $i \in [1, \ldots, N]$

$$z_i = z'_i \oplus \left(\phi(P_{\mathrm{F}}^{B_1})\right)_i \oplus (\phi(P_{\mathrm{F}}^{B_2}))_i, \tag{148}$$

and

$$x_i = x'_i \oplus \left(\phi(P_{\mathrm{F}}^{B_1})\right)_{i+N} \oplus \left(\phi(P_{\mathrm{F}}^{B_2})\right)_{i+N} . \tag{149}$$

Using $O(N)$ parallel processes, this additional computation can be performed within runtime $O(1)$.

The width of the quantum part in the gadget is bounded by

$$O(N), \tag{150}$$

and the depth of the quantum part is bounded by

$$O(1). \tag{151}$$

The same analysis as in the Z-measurements gadget bounds the runtime of the classical part of the Bell-measurement gadget as

$$O(\log N). \tag{152}$$

From the transversality and constant depth of the quantum part in the gadget, the gadget satisfies the fault-tolerance conditions in Def. (13).

3. *CNOT-gate operation gadget*

The CNOT-gate gadget is designed to perform the logical CNOT gate between logical qubits in different code blocks B_1, B_2. The construction of the gadget is shown in Fig. 7. The gadget is implemented by transversal CNOT-gate operations of the physical operations.

For the Pauli-frame technique, we require additional classical computation for updating the physical Pauli frame. Let $P_{\mathrm{F}}^{B_1} \in \tilde{P}_N$ and $P_{\mathrm{F}}^{B_2} \in \tilde{P}_N$ be a physical Pauli frame at the final step of the previous gadget. The classical computation takes the two $2N$-bit strings as input, which represent the symplectic representation of the

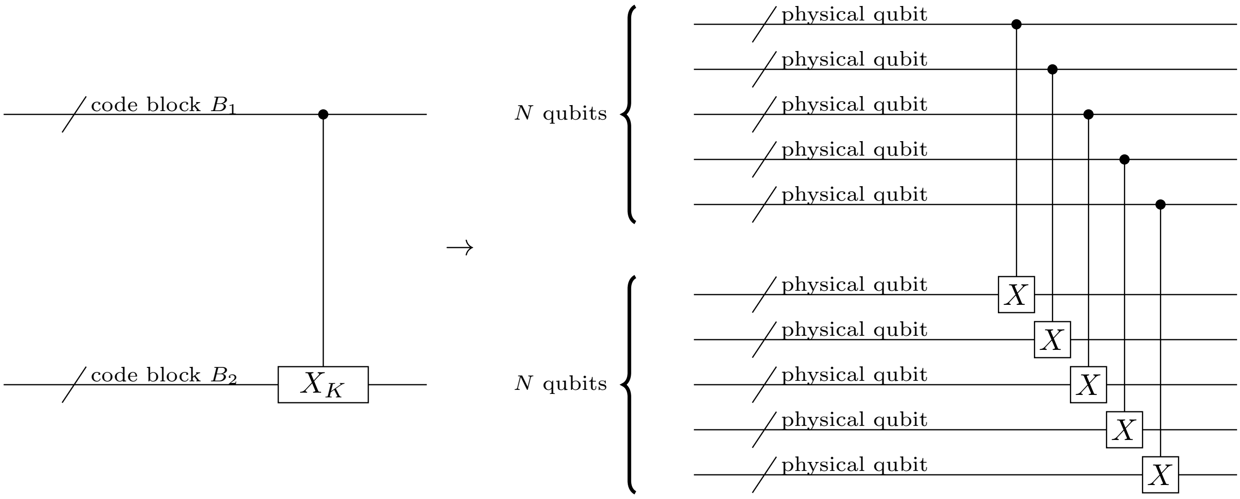


FIG. 7. The physical circuit of the gadget of the CNOT-gate operation (71).

Pauli frames, $\phi(P_{\mathrm{F}}^{B_1}) \in \mathbb{F}_2^{2N}$ and $\phi(P_{\mathrm{F}}^{B_2}) \in \mathbb{F}_2^{2N}$. The computation outputs two $2N$-bit strings representing the symplectic representation of the Pauli frames ${P'}_{\mathrm{F}}^{B_1} \in \tilde{P}_N$ and ${P'}_{\mathrm{F}}^{B_2} \in \tilde{P}_N$ at the final time step of this gadget. The updated Pauli frames can be calculated for $i \in [1, \ldots, N]$ as

$$\left(\phi\left({P'}_{\mathrm{F}}^{B_1}\right)\right)_i = \left(\phi(P_{\mathrm{F}}^{B_1})\right)_i \oplus \left(\phi(P_{\mathrm{F}}^{B_2})\right)_{i+N}, \tag{153}$$

and

$$\left(\phi\left({P'}_{\mathrm{F}}^{B_2}\right)\right)_i = \left(\phi(P_{\mathrm{F}}^{B_1})\right)_i \oplus \left(\phi(P_{\mathrm{F}}^{B_2})\right)_i. \tag{154}$$

Using $O(N)$ parallel processes, this calculation can be performed within runtime $O(1)$.

Therefore, the depth of the gadget is

$$O(1), \tag{155}$$

and the width is

$$O(N). \tag{156}$$

Due to the transversality and constant depth of the quantum part in the gadget, the gadget satisfies the fault-tolerance conditions in Def. 13.

4. $|0\rangle^{\otimes K}$-state preparation gadget

The $|0\rangle^{\otimes K}$-state preparation gadget is designed to prepare the code block initialized in the logical state $|\overline{0}\rangle^{\otimes K}$ encoded in the quantum LDPC code.

A physical circuit $\tilde{U}_{\mathrm{encode}}$ of this gadget is generated by the protocol for open circuits, as explained in Sec. III. In the gadget, the protocol simulates an original open circuit U_{encode} as shown in Fig. 8 (a) that encodes an arbitrary K-qubits state $|\psi\rangle$ into a logical state $|\overline{\psi}\rangle$ encoded in $\mathcal{Q}$ with parameters (63) as

$$U_{\mathrm{encode}}(|\psi\rangle \otimes |0\rangle^{\otimes(N-K)}) = |\overline{\psi}\rangle. \tag{157}$$

For stabilizer codes, there exists such encoding circuit U_{encode} described by a stabilizer circuit [55]. Furthermore, any n-qubit stabilizer circuit has an equivalent stabilizer circuit that has $O(n^2/\log n)$ one- or two-qubit gates and $O(n)$ depth [3, 28]. This gives the encoding circuit U_{encode} with width

$$O(N), \tag{158}$$

depth

$$O(N), \tag{159}$$

and locations

$$O(N^2/\log N). \tag{160}$$

From Theorem 6, there exists a physical circuit $\tilde{U}_{\mathrm{encode}}$ to output $|\overline{0}\rangle^{\otimes K}$ with probability at least $1-\delta$, where the data qubits of $|\overline{0}\rangle^{\otimes K}$ are subjected to the local stochastic Pauli error model with parameter at most $2Mp_{\mathrm{loc}}$ with $M = O(1)$, where M is the number of locations in the decoding interface in Sec. III B 1. Thus, the gadgets satisfy the fault-tolerance condition in Def. 12.

As a result, if we take $\delta = O(\varepsilon/\mathrm{poly}(n))$, due to (158), (159), and $|U_{\mathrm{encode}}| = O(N^2/\log N)$ in (160), both the width and the depth of the physical circuit $\tilde{U}_{\mathrm{encode}}$ are bounded by

$$O\left(N\mathrm{polylog}\left(\frac{|U_{\mathrm{encode}}|}{\delta}\right)\right) = O\left(N\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right), \tag{161}$$

where ε is the target error probability of the protocol based on the quantum LDPC code.

5. Clifford-state preparation gadget

The Clifford-state preparation gadgets are designed to prepare the four code blocks B_1, B_2, B_3, and B_4 initialized in the logical state $\left|\overline{\Psi_{U_C}}\right\rangle^{B_1B_2B_3B_4}$ of $\mathcal{Q}$, where

$$|\Psi_{U_C}\rangle^{A_1A_2A_3A_4} = (I^{A_1A_2} \otimes U_C^{A_3A_4})(|\Phi\rangle^{A_1A_3} \otimes |\Phi\rangle^{A_2A_4}). \tag{162}$$

Here, $|\Phi\rangle^{A_iA_{i'}}$ is a maximally entangled state between the registers A_i and $A_{i'}$ as

$$|\Phi\rangle^{A_iA_{i'}} = \frac{1}{\sqrt{2^K}} \sum_{m=0}^{2^K-1} |m\rangle^{A_i} \otimes |m\rangle^{A_{i'}}. \tag{163}$$

A physical circuit $\tilde{V}$ of this gadget is also generated by the protocol for open circuits, as explained in Sec. III. The protocol simulates the ideal open circuit V as shown in Fig. 8 (b) that consists of a circuit to generate the state $|\Psi_{U_C}\rangle$, followed by the parallel use of encoding circuits U_{encode} as in (157) for preparing $\left|\overline{\Psi_{U_C}}\right\rangle$. Since the original circuit V consists of the Clifford gates, V has an equivalent stabilizer circuit [3, 28] with width

$$O(N), \tag{164}$$

depth

$$O(N), \tag{165}$$

and locations

$$O(N^2/\log N). \tag{166}$$

From Theorem 6, there exists a physical circuit $\tilde{V}$ outputting $\left|\overline{\Psi_{U_C}}\right\rangle^{B_1B_2B_3B_4}$ with probability at least $1-\delta$, where the data qubits are subjected to the local stochastic Pauli error model with the parameter at most $2Mp_{\mathrm{loc}}$ with $M = O(1)$. Therefore, the gadgets satisfy the fault-tolerance condition in Def. 12.

As a result, if we take $\delta = O(\varepsilon/\mathrm{poly}(n))$, due to (164), (165), and $|V| = O(N^2/\log N)$ in (166), both the width and the depth of the physical circuit $\tilde{V}$ are bounded by

$$O\left(N\mathrm{polylog}\left(\frac{|V|}{\delta}\right)\right) = O\left(N\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right), \tag{167}$$

where ε is the target error probability of the protocol based on the quantum LDPC code.

6. Magic-state preparation gadget

The magic-state preparation gadgets are designed to prepare the code block initialized in the logical state $\left|\overline{\Psi_{U_{TH}}}\right\rangle$ of $\mathcal{Q}$, where

$$|\Psi_{U_{TH}}\rangle = U_{TH}\,|0\rangle^{\otimes K}. \tag{168}$$

Here, U_{TH} is the tensor product of TH gate or the I gate, where TH is applied to the logical qubits to which T gate or $T^\dagger$ gate will be applied using the U_T-gate abbreviation explained in Sec. IV B 2.

A physical circuit $\tilde{W}$ of this gadget is also generated by the protocol for open circuits, as explained in Sec. III. The protocol simulates the ideal open circuit W as shown in Fig. 8 (c) that consists of a circuit to generate the state $|\Psi_{U_{TH}}\rangle$, followed by the encoding circuit U_{encode} for creating the encoded state $\left|\overline{\Psi_{U_{TH}}}\right\rangle$.

Since the original circuit W consists of constant-depth gates TH, followed by Clifford gates U_{encode}, W has width

$$O(N), \tag{169}$$

depth

$$O(N), \tag{170}$$

and locations

$$O(N^2/\log N). \tag{171}$$

From Theorem 6, there exists a physical circuit $\tilde{W}$ outputting $\left|\overline{\Psi_{U_{TH}}}\right\rangle$ with probability at least $1-\delta$, where the data qubits are subjected to the local stochastic Pauli error model with parameter at most $2Mp_{\mathrm{loc}}$ with $M = O(1)$. Thus, the gadgets satisfy the fault-tolerance condition in Def. 12.

As a result, if we take $\delta = O(\varepsilon/\mathrm{poly}(n))$, due to (169), (170), and $|W| = O(N^2/\log N)$ in (171), both the width and the depth of the physical circuit $\tilde{W}$ are bounded by

$$O\left(N\mathrm{polylog}\left(\frac{|W|}{\delta}\right)\right) = O\left(N\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right), \tag{172}$$

where ε is the target error probability of the protocol based on the quantum LDPC code.

7. Error-correction gadget

An EC gadget is designed to keep residual errors in the code block small using the decoding algorithm in Def. 10. For each code block, $N - K = O(N)$ auxiliary physical qubits are used to perform the syndrome measurement. Each auxiliary physical qubit is assigned to a corresponding stabilizer generator. We perform the circuit as shown in Fig. 9 to measure a specific stabilizer generator and obtain the syndrome bits,

$$\tilde{\sigma} = (\tilde{\sigma}_X, \tilde{\sigma}_Z) \in \mathbb{F}_2^{N-K}, \tag{173}$$

as in (114).

The measurements of all generators make up the syndrome measurement circuit of the EC gadget as shown in Fig. 10. Note that Ref. [21] uses Shor's error correction [56], which utilizes a cat state consisting of multiple qubits for each stabilizer generator, where the number

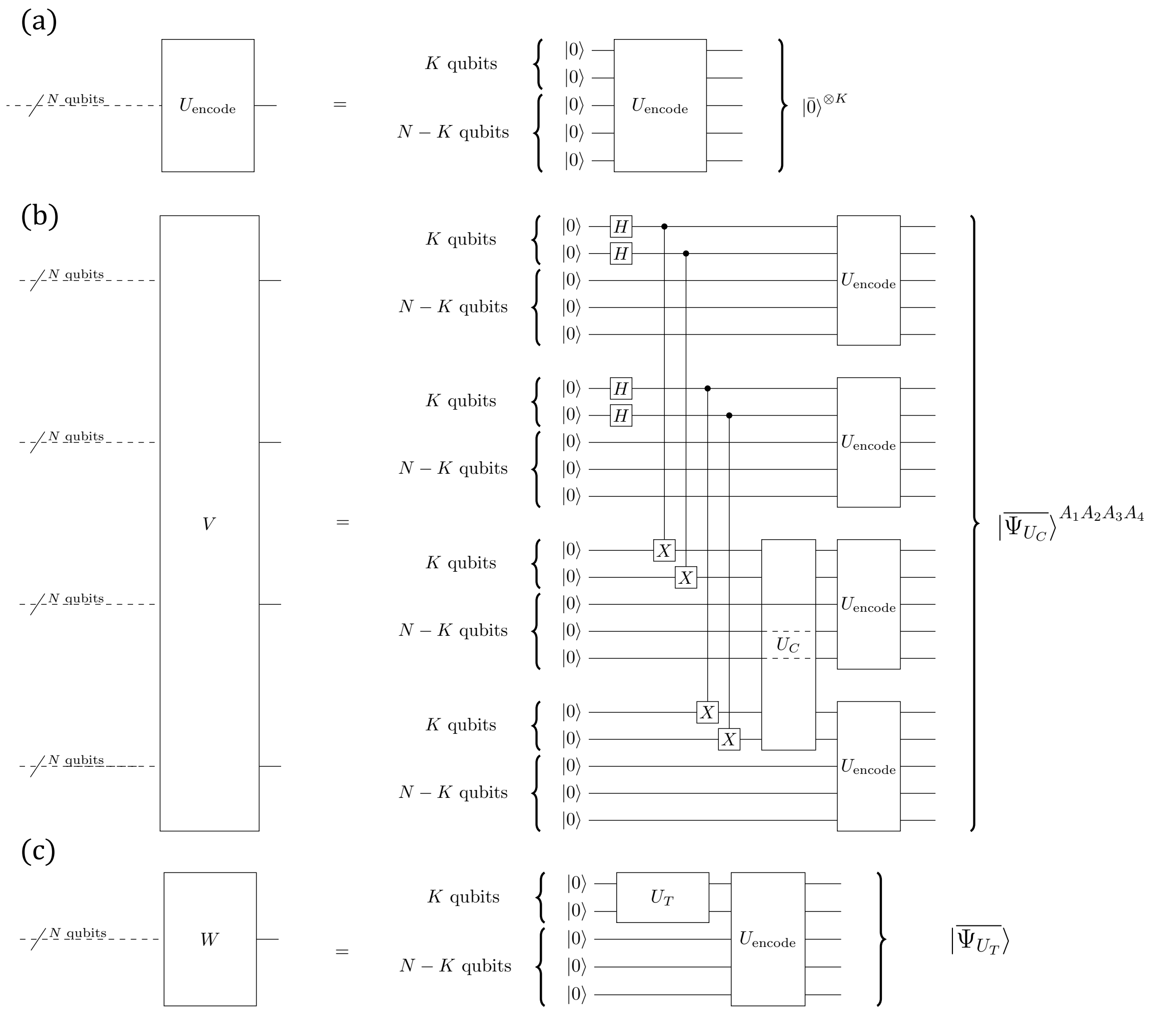


FIG. 8. (a) An original open circuit U_{encode} to create an encoded state of $|0\rangle^{\otimes K}$, (b) an original open circuit V to create an encoded state of $|\Psi_{U_C}\rangle$ and (c) an original open circuit W to create an encoded state of $|\Psi_{U_T}\rangle$. A physical circuit of the state-preparation gadgets are obtained from the protocol for simulating open circuits, as explained in Sec. III

of qubits in the cat state corresponds to the weights of the stabilizer generator. However, the EC gadgets only need to satisfy our fault-tolerance conditions in Def. 13; therefore, a single auxiliary physical qubit per stabilizer generator is sufficient. Using the noisy syndrome bits $\tilde{\sigma}$, a single-shot decoding algorithm with thresholds in Def. 10 with T internal loops deduces the recovery operation, and then the recovery operation is applied to the data qubits in the EC gadget to keep the residual error on the data qubits small. Here, we choose T to satisfy

$$c(T) > 2\Delta^{\text{synd}}, \tag{174}$$

where $c(T)$ is a monotonically increasing function, meaning that $T = O(1)$, and $\Delta^{\text{synd}} = O(1)$ is the maximum degree in (130) of the syndrome measurement circuit. The condition of (174) is required to show the existence of a threshold in our protocol, as will be explained in Lemma 16.

If we use the Pauli frame, the EC gadget consists of the syndrome measurement circuit to extract syndrome bits of unrecovered data qubits,

$$\tilde{\sigma}' = (\tilde{\sigma}'_X, \tilde{\sigma}'_Z) \in \mathbb{F}_2^{N-K}, \tag{175}$$

followed by the classical computation for modifying the syndrome bits to obtain the syndrome bits $\tilde{\sigma}$ of recovered data qubits as in (173) based on an input physical Pauli frame (more specifically, the syndrome bits that would be obtained if an ideal recovery operation would be applied to the data qubits at the next time step of a syndrome measurement circuit) and performing the decoding algorithm. During the modification of the syndrome bits and the execution of the decoding algorithm, the wait operation is performed on the data qubits. If we have a physical Pauli frame at the final time step of a previous

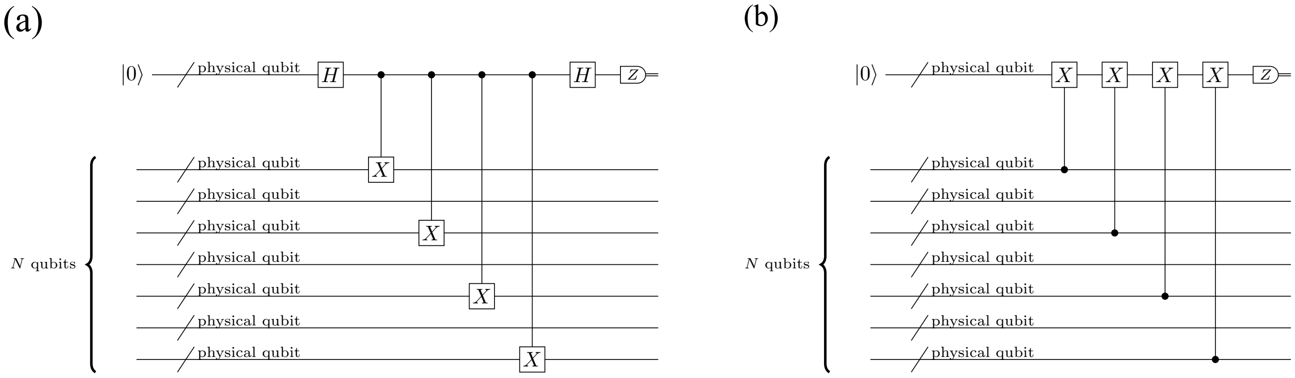


FIG. 9. The circuit for measuring the X-type stabilizer generator (a) and the Z-type stabilizer generator (b). The CNOT gate's support corresponds to the stabilizer generator's support. The syndrome measurement circuit is the circuit for measuring all stabilizer generators, each of which consists of the circuit shown in this figure.

gadget

$$P_{\mathrm{F}} \in \tilde{\mathcal{P}}_N, \tag{176}$$

we calculate the recovered syndrome bits as in (173) in the following way. First, a classical computer receives bitstrings $\tilde{\sigma}' \in \mathbb{F}_2^{N-K}$ and $\phi(P_{\mathrm{F}}) \in \mathbb{F}_2^{2N}$ as input. Considering how the physical Pauli frame P_{F} propagates through the syndrome circuit, the modification of the syndrome bits corresponding to the Z-type stabilizer generators is executed as, for $i \in [0,\ldots,M_Z-1]$,

$$(\tilde{\sigma}_X)_i = (\tilde{\sigma}'_X)_i \oplus \left(\bigoplus_{j\in\mathrm{supp}(g_i^Z)} (\phi(P_{\mathrm{F}}))_j \right), \tag{177}$$

and for the syndrome bits corresponding to the X-type stabilizer generators, that is, for $i \in [0,\ldots,M_X-1]$,

$$(\tilde{\sigma}_Z)_i = (\tilde{\sigma}'_Z)_i \oplus \left(\bigoplus_{j\in\mathrm{supp}(g_i^X)} (\phi(P_{\mathrm{F}}))_{j+N} \right). \tag{178}$$

This classical computation can be performed in runtime $O(1)$, using $O(N)$ parallel processes. Using recovered syndrome bits $\tilde{\sigma}$, a single-shot decoding algorithm with thresholds in Def. 10 with $T = O(1)$ internal loops deduces the recovery operation, and then the recovery operation $R \in \tilde{\mathcal{P}}_N$ updates the physical Pauli frame as for $i \in [1,\ldots,N]$

$$(\phi(P'_{\mathrm{F}}))_i = (\phi(R))_i \oplus (\phi(P_{\mathrm{F}}))_i\,. \tag{179}$$

The update of the physical Pauli frame can be performed in runtime $O(1)$ with $O(N)$ parallel processes.

Recall that each code block is encoded with a nonvanishing-rate (r,c) quantum LDPC code. The measurements can be performed in parallel for generators that act on disjoint data qubits; thus, the depth of the quantum part of the syndrome measurement is bounded by

$$O(rc) = O(1). \tag{180}$$

In addition, the width of the quantum part of the syndrome measurement circuit is bounded by

$$O(N+M) = O(N+(N-K)) = O(N), \tag{181}$$

where $M = N-K$ is the number of auxiliary physical qubits for measuring stabilizer generators. The runtime of the classical part is bounded by

$$O(1). \tag{182}$$

Since the width of the gadget is $O(N)$, even if the gadgets are executed for all code blocks simultaneously, it does not pose an obstacle in constructing the constant-space overhead fault-tolerant protocol. Even if the classical part of the gadget is included, the EC gadget is fault-tolerant in the sense of Def. 13 because the depth of the gadget is constant. From the property of quantum LDPC codes and the constant depth of the quantum part in the gadget, the EC gadgets satisfy the fault-tolerance conditions, as shown in Def. 13.

E. Threshold theorem

In the following, we prove the threshold theorem of our protocol.

Theorem 14. *(Fault-tolerant quantum computation with polylogarithmic time and constant space overhead). Let $\{\mathrm{C}_n^{\mathrm{org}}\}$ be a sequence of original closed circuits as described in Assumption 1 specified by an integer n, and $\mathrm{C}_n^{\mathrm{org}}$ has width $W(n)$ and depth $D(n)$, where*

$$|\mathrm{C}_n^{\mathrm{org}}| = O(W(n)D(n)) = O(\mathrm{poly}(n)), \tag{183}$$

as $n\to\infty$. Suppose that we compile an original circuit $\mathrm{C}_n^{\mathrm{org}}$ into a physical circuit $\mathrm{C}_n^{\mathrm{FT}}$ that is subjected to a local stochastic Pauli error with parameter $p_{\mathrm{loc}} > 0$ as described in Sec. IV A. The gadgets are constructed as described in Sec. IV D, i.e., state-preparation, gate, and

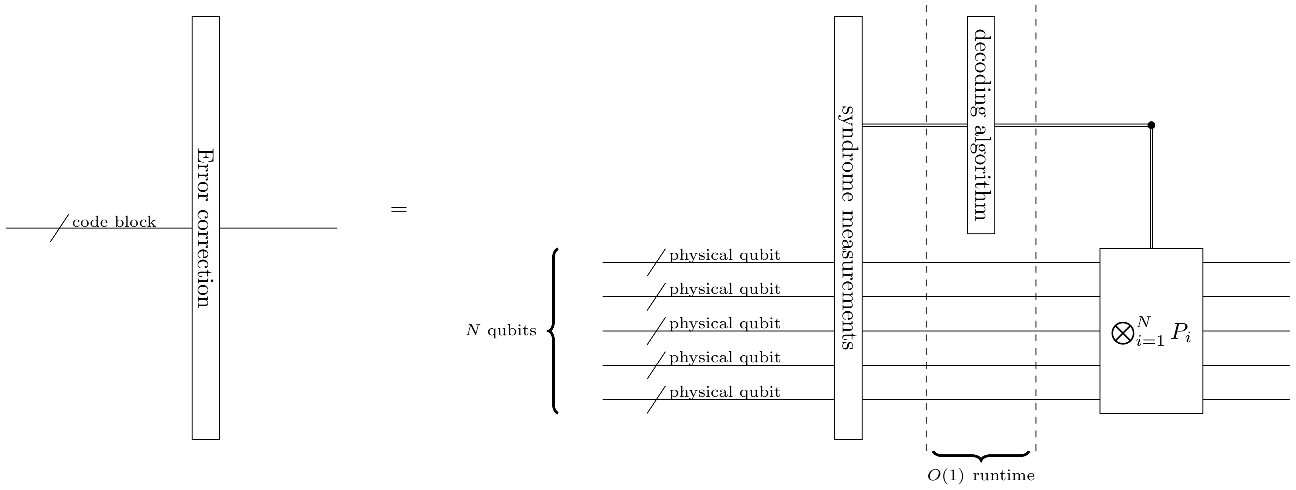


FIG. 10. A physical circuit of the EC gadget. The classical part of the gadget consists of modifying the syndrome bits based on an input Pauli frame and performing the decoding algorithm.

measurement, EC gadgets satisfy the fault-tolerance conditions in Defs. 12 and 13, where each code block is based on a non-vanishing-rate quantum CSS LDPC code

$$\mathcal{Q} \tag{184}$$

with parameters

$$[[N, K = \Theta(N), D = \Theta(N^{\gamma})]] \tag{185}$$

satisfying Assumption 4, i.e., a single-shot decoding algorithm for reducing errors in Def. 10 has a threshold $p_{\mathrm{dec}}^{\mathrm{th}} > 0$ *and a decoding algorithm for correcting errors in Def. 11 has threshold* $p'^{\mathrm{th}}_{\mathrm{dec}} > 0$.

Let $p_{\mathrm{loc}}^{\mathrm{th}} > 0$ *be a threshold of the concatenated-code protocol to simulate open circuits as explained in Sec. III B. Then, for all* $\varepsilon > 0$*, there exists a threshold* $q_{\mathrm{loc}}^{\mathrm{th}} > 0$ *and if* $0 \leq p_{\mathrm{loc}} < \min\{q_{\mathrm{loc}}^{\mathrm{th}}, p_{\mathrm{loc}}^{\mathrm{th}}/2\}$*, the following statement holds: there exists a sequence of physical circuits* $\{\mathrm{C}_n^{\mathrm{FT}}\}$*, where* $\mathrm{C}_n^{\mathrm{FT}}$ *has width* $W_{\mathrm{FT}}(n)$ *and depth* $D_{\mathrm{FT}}(n)$ *such that*

$$\begin{aligned} \frac{W_{\mathrm{FT}}(n)}{W(n)} &= O(1), \\ \frac{D_{\mathrm{FT}}(n)}{D(n)} &= O\left(\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right), \end{aligned} \tag{186}$$

as $n \to \infty$*, and* $\mathrm{C}_n^{\mathrm{FT}}$ *outputs the probability distribution that is close to that of* $\mathrm{C}_n^{\mathrm{org}}$ *with total variation distance at most* ε.

In the following, we will show that there exists a threshold based on the fault-tolerant construction of the gadgets presented in Sec. IV D. Next, we will show that our protocol achieves a constant space overhead and a polylogarithmic time overhead.

First, we fix the parameters of the protocol. We choose the number of physical qubits N of $\mathcal{Q}$ in (184) as

$$N = \Theta\left(\log^{\alpha}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right), \tag{187}$$

where $\alpha > 1/\gamma$ is a constant, the number of registers κ as

$$\kappa(n) \coloneqq \frac{W(n)}{K} = \Theta\left(\frac{W(n)}{\log^{\alpha}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)}\right). \tag{188}$$

Let $\delta > 0$ be the failure probability of a state-preparation gadget, and we choose the probability as

$$\delta = O\left(\frac{\varepsilon}{|\mathrm{C}_n^{\mathrm{org}}|^2}\right). \tag{189}$$

We consider a sequence of original open circuits $\{\mathrm{C}_N^{\mathrm{prep}}\}$ to prepare $|0\rangle^{\otimes K}$, Clifford, and magic states encoded in $\mathcal{Q}$ in (184), as explained in Secs. IV D 4, IV D 5, and IV D 6, respectively. Here, N corresponds to the number of physical qubits in (187), and $\mathrm{C}_N^{\mathrm{prep}}$ has width

$$W_{\mathrm{prep}}(N) = O(N) \tag{190}$$

as in (158), (164), and (169), depth

$$D_{\mathrm{prep}}(N) = O(N) \tag{191}$$

as in (159), (165), (170), and locations

$$|\mathrm{C}_N^{\mathrm{prep}}| = O(N^2/\log N) \tag{192}$$

as in (160), (166), (171). From Theorem 6, we have a corresponding sequence of physical circuits $\{\tilde{\mathrm{C}}_N^{\mathrm{prep}}\}$ with

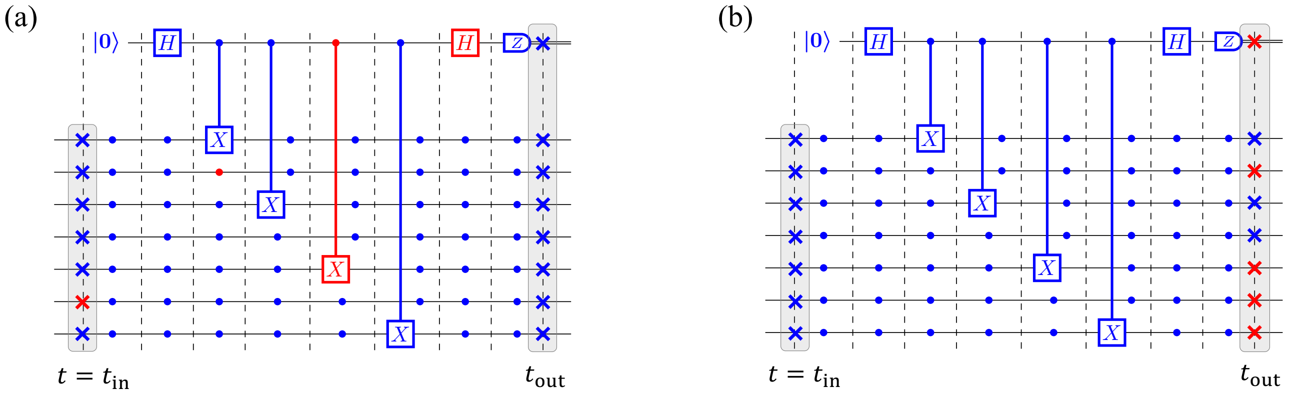


FIG. 11. A set of input wires, X_{in}, at time step $t = t_{\text{in}}$ and output wires, X_{out}, at time step $t = t_{\text{out}}$, along with a set of locations L of a physical circuit for measuring X-type stabilizer generators, as shown in Fig. 9. (a) Each cross represents a wire in X_{in} or X_{out}, where a red cross indicates an erroneous wire, and each operation (with a wait operation represented by a circle) represents a location in L, where a red operation indicates a faulty location. (b) A possible equivalent non-faulty circuit can be obtained by propagating Pauli errors that occurred in the erroneous wires at $t = t_{\text{in}}$ and Pauli errors that occurred due to the faulty locations in (a), where these errors result in erroneous wires that correspond to the red crosses at $t = t_{\text{out}}$.

width $\tilde{W}_{\text{prep}}(N)$ and depth $\tilde{D}_{\text{prep}}(N)$. The prepared states are subjected to the local stochastic Pauli error with parameter

$$\tilde{p} \leq M' p_{\text{loc}}, \tag{193}$$

where M' is defined as

$$M' := 2M, \tag{194}$$

and M is a constant representing the number of locations in the decoding interface as explained in Sec. III B 1. Moreover, the width of the physical circuits satisfies

$$\frac{\tilde{W}_{\text{prep}}(N)}{W_{\text{prep}}(N)} = O\left(\log^{\gamma_1}\left(\frac{|\mathrm{C}_N^{\text{prep}}|}{\delta}\right)\right) \tag{195}$$

$$= O\left(\log^{\gamma_1}\left(\frac{|\mathrm{C}_n^{\text{org}}|}{\varepsilon}\right)\right), \tag{196}$$

where we use (187), (192), and (189), and $\gamma_1 > 0$ is a constant. Similarly, the depth of the physical circuits satisfies

$$\frac{\tilde{D}_{\text{prep}}(N)}{D_{\text{prep}}(N)} = O\left(\log^{\gamma_2}\left(\frac{|\mathrm{C}_N^{\text{prep}}|}{\delta}\right)\right) \tag{197}$$

$$= O\left(\log^{\gamma_2}\left(\frac{|\mathrm{C}_n^{\text{org}}|}{\varepsilon}\right)\right), \tag{198}$$

where $\gamma_2 > 0$ is a constant. Then, we choose the number of non-trivial intermediate operations $L(n)$ in (85) that we apply in a one-depth part of an intermediate circuit as

$$L(n) = \Theta\left(\frac{W(n)}{\log^{\alpha+\gamma_1}\left(\frac{|\mathrm{C}_n^{\text{org}}|}{\varepsilon}\right)}\right). \tag{199}$$

We begin with obtaining a bound on the error parameter on output wires of a faulty physical circuit C. Let

$$X_{\text{in}} \tag{200}$$

be a set of input wires at the first step of C,

$$X_{\text{out}} \tag{201}$$

be a set of output wires at the final step of C, and

$$L \tag{202}$$

be a set of locations in C as shown in Fig. 11. As stated in Lemma 15, the output wires X_{out} in (201) undergo the local stochastic Pauli error model if the locations L in (202) and the input wires X_{in} in (200) also undergo the local stochastic Pauli error model. The lemma provides an upper bound on the error parameter p'_{wire} of the output wires, given the error parameters p_{wire} and p_{loc} of X_{in} and C, respectively. This bound is obtained by considering possible configurations of erroneous input wires in X_{in} and faulty locations in L that can produce erroneous wires in X_{out}. For simplicity, we denote the union of X_{in} and L by

$$\tilde{L} := X_{\text{in}} \cup L. \tag{203}$$

In addition, for a given set $U \subseteq X_{\text{out}}$,

$$A(U) \subseteq \tilde{L} \tag{204}$$

denotes the set of locations or wires of input wires that are connected to at least one wire in U. Similarly, for a given set $\tilde{R} \subseteq \tilde{L}$,

$$B(\tilde{R}) \subseteq X_{\text{out}} \tag{205}$$

denotes a set of wires that connect to at least one location or one input wire in $\tilde{R}$.

Lemma 15. *Suppose we have a physical stabilizer circuit* C *that undergoes the local stochastic Pauli error model with parameter p_{loc}, and input wires X_{in} in* (200) *and output wires X_{out} in* (201) *of* C *that undergo to the local stochastic Pauli error model with parameter p_{wire} and p'_{wire}, respectively. Let G be a bipartite graph of* C *as in* (130)*, where Δ be the maximum degree of a vertex of G and d be the depth of* C*.*

Then, output wires X_{out} undergo the local stochastic Pauli error model with parameter p'_{wire} satisfying

$$p'_{\text{wire}} \leq \frac{2^{d\Delta} q^{1/\Delta}}{1-q}, \tag{206}$$

where $q \coloneqq \max\{p_{\text{wire}}, p_{\text{loc}}\}$.

Proof. For any $U \subseteq X_{\text{out}}$ and $\tilde{R} \subseteq \tilde{L}$, we have

$$|A(U)| \leq d\Delta|U|, \quad |B(\tilde{R})| \leq \Delta|\tilde{R}|. \tag{207}$$

Given a set of the union of erroneous input data qubits and faulty locations, denoted by $\tilde{F} \subseteq \tilde{L}$, the set of erroneous wires $H \subseteq X$ satisfies $H = B(\tilde{F})$. Then, we have

$$\begin{aligned}\mathbb{P}[H \supseteq U] \leq& \mathbb{P}\left[\exists \tilde{R} \subseteq A(U) \colon \tilde{F} \supseteq \tilde{R}, B(\tilde{R}) = U\right] \\ \leq& \sum_{r \geq |U|/\Delta} \left[\sum_{\tilde{R} \subseteq A(U) \colon |\tilde{R}| = r} \mathbb{P}[\tilde{F} \supseteq \tilde{R}]\right] \\ \leq& \sum_{r \geq |U|/\Delta} \binom{|A(U)|}{r} q^r.\end{aligned}$$

Using the upper bound for the binomial coefficient

$$\binom{|A(U)|}{r} \leq 2^{|A(U)|}, \tag{208}$$

and $|A(U)| \leq d\Delta|U|$, we have

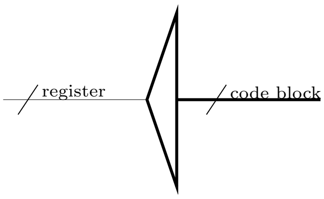
$$\begin{aligned}\mathbb{P}[H \supseteq U] \leq& 2^{d\Delta|U|} \sum_{r \geq |U|/\Delta} q^r \\ \leq& \left(\frac{2^{d\Delta} q^{1/\Delta}}{1-q}\right)^{|U|}.\end{aligned}$$

Moreover, since a physical circuit C is a stabilizer circuit, there exists a Pauli operator that represents errors on the set of fautly wires H. Therefore, the set of wires is subjected to the local stochastic Pauli error model on wires with parameter

$$p_{\text{wire}} \leq \frac{2^{d\Delta} q^{1/\Delta}}{1-q}. \tag{209}$$

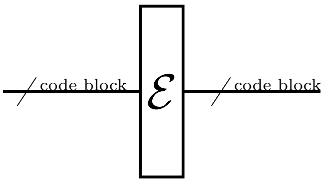
□

Next, we show that there exists a positive threshold value with respect to p_{loc}, and if p_{loc} is below the threshold, we can probabilistically transform a gadget with trailing EC gadget(s) into the corresponding elementary operation. When p_{loc} is sufficiently low, due to the fault-tolerance conditions in Defs. 12 and 13 and Lemma 15, propagation of errors between EC gadgets is suppressed, allowing EC gadgets to keep the error rate low in the code blocks. The transformations are described by the following diagrams. Let



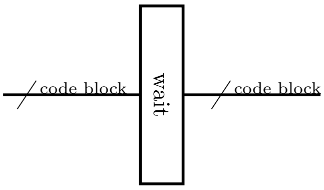
(210)

be an ideal encoder from K qubits in a register to K logical qubits of a code block $\mathcal{Q}$,



(211)

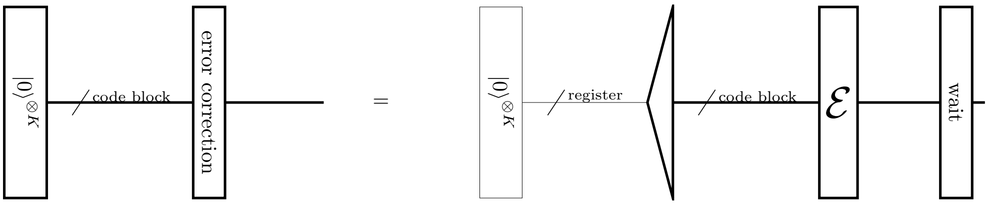
be a local stochastic Pauli noise $\mathcal{E}$, which is a CPTP map, acting on data qubits, and



(212)

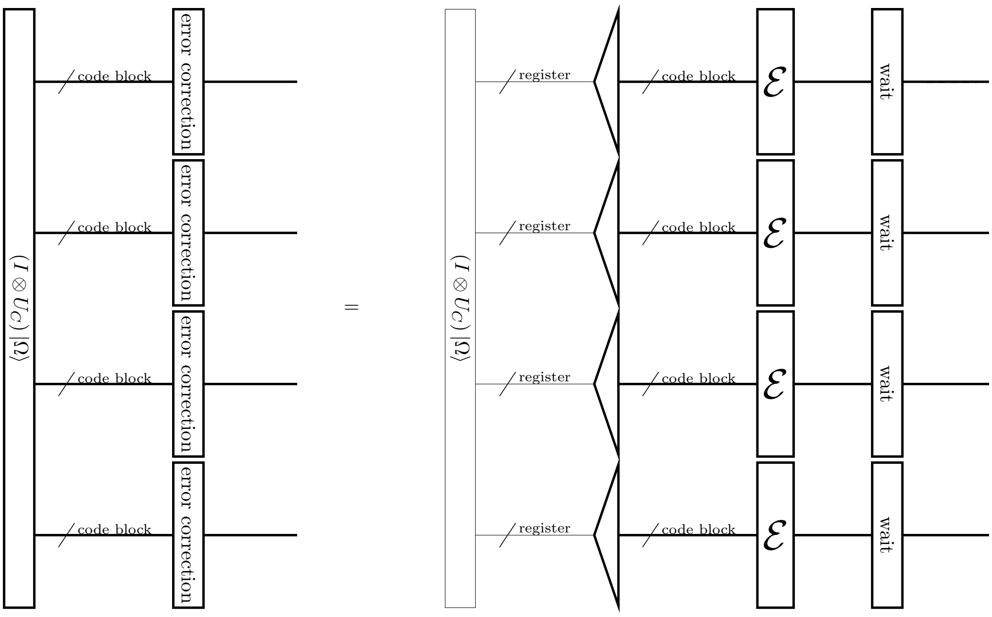
be a wait operation during performing classical computation in an EC gadget. Here, the box surrounded by a bold line represents a gadget. Then, each gadget can be transformed as follows.

1. state-preparation gadgets
   - $|0\rangle^{\otimes K}$-state preparation gadget



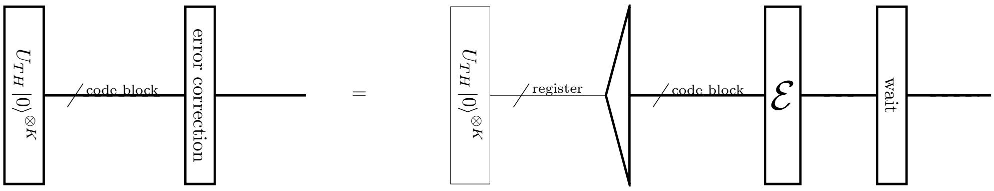
, (213)

- Clifford-state preparation gadgets


$(I \otimes U_C)\,|\Omega\rangle$
code block
error correction
=
$(I \otimes U_C)\,|\Omega\rangle$
register
code block
$\mathcal{E}$
wait

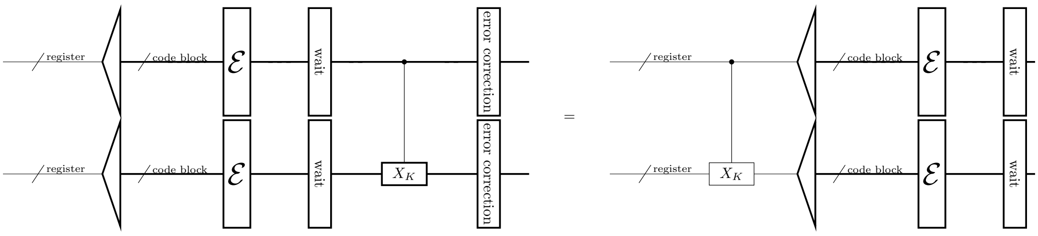
, (214)

- magic-state preparation gadgets


$U_{TH}\,|0\rangle^{\otimes K}$
code block
error correction
=
$U_{TH}\,|0\rangle^{\otimes K}$
register
code block
$\mathcal{E}$
wait

, (215)

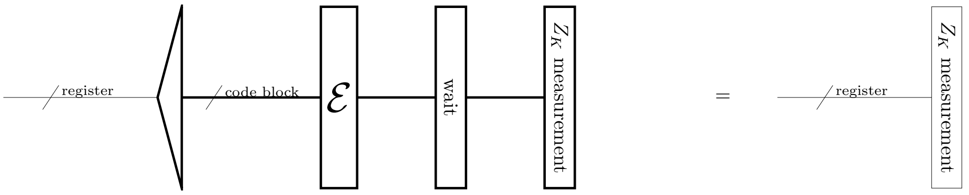
2. gate gadget
   - CNOT-gate gadget



, (216)

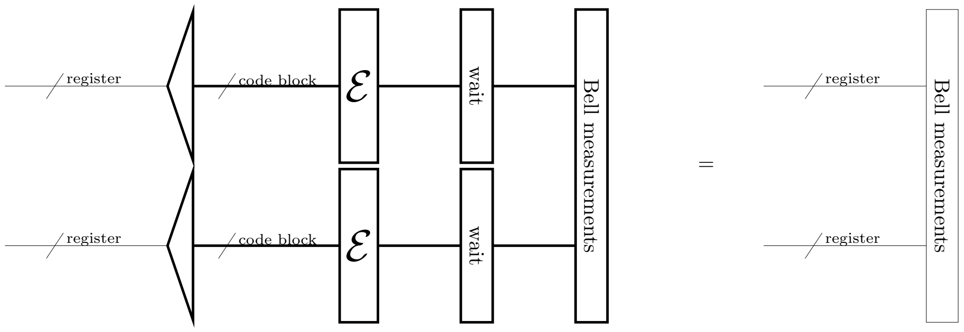
3. measurement gadgets

- Z_K-measurement gadget



, (217)

- Bell-measurement gadget



. (218)

From Lemma 16, we can probabilistically transform a sequence of gadgets into a corresponding sequence of elementary operations from the state-preparation gadgets to the measurement gadgets as in (213), (214), (215), (216), (217), and (218) by pushing the ideal encoder (210) forward.

Lemma 16. *Suppose that we have a physical circuit* C *that undergoes the local stochastic Pauli error model with parameter* p_{loc}*, and we have a single-shot decoding algorithm for reducing errors in Def. 10 with threshold* $p_{\mathrm{dec}}^{\mathrm{th}} > 0$ *and a decoding algorithm for correcting errors in Def. 11 with threshold* ${p'}_{\mathrm{dec}}^{\mathrm{th}} > 0$*. We have a sequence of gadgets, starting with the state-preparation gadgets and ending with the measurement gadgets, with the EC gadget inserted between each gadget. Suppose the state-preparation, gate, measurement, and EC gadgets satisfy the fault-tolerance conditions in Defs. 12 and 13.*

Then, there exists a threshold $q_{\mathrm{loc}}^{\mathrm{th}} > 0$*, and if* $p_{\mathrm{loc}} < \min\{q_{\mathrm{loc}}^{\mathrm{th}}, p_{\mathrm{loc}}^{\mathrm{th}}/2\}$*, each gadget with trailing EC gadget(s) can be transformed into the corresponding elementary operation as in (213), (214), (215), (216), (217), and (218) with probability at least*

$$1 - \Omega(\varepsilon / |\mathrm{C}_n^{\mathrm{org}}|^2). \tag{219}$$

Moreover, the parameter of the local stochastic Pauli noise $\mathcal{E}$ *in (213), (214), (215), (216), (217), and (218) is bounded by*

$$p_{\mathrm{data}} \leq M' p_{\mathrm{loc}}, \tag{220}$$

where $M' \coloneqq 2M$ *in (194).*

Proof. Let $\mathrm{C}^{\mathrm{synd}}$ be the syndrome measurement circuit in the EC gadget with a maximum degree $\Delta^{\mathrm{synd}} = O(1)$ and depth $d^{\mathrm{synd}} = O(1)$, and $\mathrm{C}^{\mathrm{wait}}$ be a circuit of wait operations for classical computation in the EC gadget with a maximum degree $\Delta^{\mathrm{wait}} = 1$ and depth $d^{\mathrm{wait}} = T = O(1)$ as in Def. 13.

First, we consider the transformation of state-preparation gadgets, i.e., the $|0\rangle^{\otimes K}$-state preparation (213), the Clifford-state preparation gadgets (214) and the magic-state preparation gadgets (215). From Theorem 6, the data qubits at the final step of the state-preparation gadgets are subjected to the local Pauli stochastic error model with parameter $p_{\mathrm{data}} \leq M' p_{\mathrm{loc}}$. By applying Lemma 15 to $\mathrm{C}^{\mathrm{synd}}$, the wires at the final step of $\mathrm{C}^{\mathrm{synd}}$ are subjected to the local stochastic Pauli error model with parameter

$$p_{\mathrm{wire}} \leq \frac{2^{d^{\mathrm{synd}} \Delta^{\mathrm{synd}}} (M' p_{\mathrm{loc}})^{1/\Delta^{\mathrm{synd}}}}{1 - M' p_{\mathrm{loc}}}. \tag{221}$$

Since the function $f(x) = x/(1-x)$ for $x \in [0,1)$ is monotonically increasing, by lowering p_{loc}, we have p_{loc} such that

$$\frac{2^{c_1^{\mathrm{synd}}} (M' p_{\mathrm{loc}})^{1/\Delta^{\mathrm{synd}}}}{1 - M' p_{\mathrm{loc}}} < p_{\mathrm{dec}}^{\mathrm{th}}. \tag{222}$$

With p_{loc} satisfying (222), due to (126), a residual error is applied after a recovery operation to data qubits that are subjected to the local stochastic Pauli error model with parameter

$$p_{\mathrm{data}} \leq \left(\frac{2^{d^{\mathrm{synd}} \Delta^{\mathrm{synd}}} (M' p_{\mathrm{loc}})^{1/\Delta^{\mathrm{synd}}}}{1 - M' p_{\mathrm{loc}}} \right)^{c(T)}, \tag{223}$$

where $c(T)$ is an error suppression parameter of a decoding algorithm (126), and $T = O(1)$ is the number of iterations of the decoding algorithm, determined by (174). Under this choice, there is a positive value of p_{loc} that satisfies

$$p_{\mathrm{data}} \leq \left(\frac{2^{d^{\mathrm{synd}} \Delta^{\mathrm{synd}}} (M' p_{\mathrm{loc}})^{1/\Delta^{\mathrm{synd}}}}{1 - M' p_{\mathrm{loc}}} \right)^{c(T)} \leq M' p_{\mathrm{loc}}, \tag{224}$$

and after the ideal encoding circuit is moved to the final step of the trailing syndrome measurement circuit using the Pauli frame, the parameter of the residual Pauli noise $\mathcal{E}$ can be bounded by

$$M' p_{\mathrm{loc}}. \tag{225}$$

Due to the union bound taking into account the failure probability of the single-shot decoding algorithm for reducing errors in Def. 10 and the failure probability of a state-preparation gadget in Def. 12, this transformation fails with probability at most

$$\begin{aligned} \exp(-\Omega(D)) + \delta &= \exp(-\Omega(N^{\gamma})) + \delta \\ &= O\left(\frac{\varepsilon}{|\mathrm{C}_n^{\mathrm{org}}|^2} \right), \end{aligned} \tag{226}$$

where we use (187) and (189).

Next, we consider the transformation of the gate gadget, i.e., the CNOT-gate gadget (216). Here, we consider a circuit $\mathrm{C}^{\mathrm{CNOT}}$ of the CNOT-gate gadget with a maximum degree $\Delta^{\mathrm{CNOT}} = 2$ and depth $d^{\mathrm{CNOT}} = O(1)$. Then, by applying Lemma 15 to a sequence of $\mathrm{C}^{\mathrm{wait}}$, $\mathrm{C}^{\mathrm{CNOT}}$ and $\mathrm{C}^{\mathrm{synd}}$, the parameters of the wire in the final step of the syndrome measurement circuit are suppressed, taking into account the wait operation during the classical part of the previous EC gadget as

$$p_{\mathrm{wire}} \leq \frac{2^{(d^{\mathrm{synd}} \Delta^{\mathrm{synd}} + d^{\mathrm{CNOT}} \Delta^{\mathrm{synd}} + \Delta^{\mathrm{CNOT}} \Delta^{\mathrm{synd}} T)} (M' p_{\mathrm{loc}})^{1/(\Delta^{\mathrm{CNOT}} \Delta^{\mathrm{synd}})}}{1 - M' p_{\mathrm{loc}}} =: p_{\mathrm{wire}}^{\mathrm{CNOT}}. \tag{227}$$

If we have p_{loc} such that

$$p_{\mathrm{wire}} \leq p_{\mathrm{wire}}^{\mathrm{CNOT}} \leq p_{\mathrm{dec}}^{\mathrm{th}}, \tag{228}$$

then, since we choose T such that $c(T) > 2\Delta^{\mathrm{synd}}$ as in (174), there is a positive value of p_{loc} satisfying

$$p_{\mathrm{data}} \leq \left(p_{\mathrm{wire}}^{\mathrm{CNOT}} \right)^{c(T)} \leq M' p_{\mathrm{loc}}, \tag{229}$$

after the ideal encoding circuit is moved to the final step of the syndrome measurement circuit, we can again bound p_{data} at the final step of the syndrome measurement circuit as

$$p_{\mathrm{data}} \leq M' p_{\mathrm{loc}}. \tag{230}$$

Under the condition that the previous decoding algorithm succeeds, the single-shot decoding algorithm for reducing errors in Def. 10 fails with probability at most

$$\exp(-\Omega(D)) = O\left(\frac{\varepsilon}{|\mathrm{C}_n^{\mathrm{org}}|^2} \right), \tag{231}$$

where we use (185).

Finally, we consider the transformation of the measurement gadgets, i.e., the Z_K-measurement gadget (217) and the Bell-measurement gadget (218). Here, we consider a circuit C^{Z_K} of the Z_K-measurement gadget with a maximum degree $\Delta^{Z_K} = 1$ and depth $d^{Z_K} = O(1)$ and a circuit $\mathrm{C}^{\mathrm{Bell}}$ of the Bell-measurement gadget with a maximum degree $\Delta^{\mathrm{Bell}} = 2$ and depth $d^{\mathrm{Bell}} = O(1)$. By applying Lemma 15 to C^{Z_K}, the parameter of the local stochastic Pauli error at the final time of the quantum part is bounded by

$$p_{\mathrm{data}} \leq \frac{2^{(d^{Z_K} \Delta^{Z_K} + d^{\mathrm{wait}} \Delta^{Z_K})} (M' p_{\mathrm{loc}})^{1/\Delta^{Z_K}}}{1 - M' p_{\mathrm{loc}}} =: p_{\mathrm{wire}}^{Z_K}. \tag{232}$$

If we have p_{loc} such that

$$p_{\mathrm{data}} \leq p_{\mathrm{wire}}^{Z_K} \leq p'^{\mathrm{th}}_{\mathrm{dec}}, \tag{233}$$

then the decoding algorithm in Def. 11 fails to return the measurement results of the logical operators with probability at most

$$\exp(-\Omega(D)) = O\left(\frac{\varepsilon}{|\mathrm{C}_n^{\mathrm{org}}|^2} \right), \tag{234}$$

where we use (185). For the Bell-measurement gadget $\mathrm{C}^{\mathrm{Bell}}$, by applying Lemma 15, the parameter of the local stochastic Pauli error at the final time is bounded by

$$p_{\mathrm{data}} \leq \frac{2^{(d^{\mathrm{Bell}} \Delta^{\mathrm{Bell}} + d^{\mathrm{wait}} \Delta^{\mathrm{Bell}})} (M' p_{\mathrm{loc}})^{1/\Delta^{\mathrm{Bell}}}}{1 - M' p_{\mathrm{loc}}} =: p_{\mathrm{loc}}^{\mathrm{Bell}}. \tag{235}$$

If we have p_{loc} such that

$$p_{\mathrm{data}} \leq p_{\mathrm{loc}}^{\mathrm{Bell}} \leq p'^{\mathrm{th}}_{\mathrm{dec}}, \tag{236}$$

then the decoding algorithm in Def. 11 fails to return the measurement results of the logical operators with probability at most

$$\exp(-\Omega(D)) = O\left(\frac{\varepsilon}{|\mathrm{C}_n^{\mathrm{org}}|^2}\right), \tag{237}$$

where we use (185). Therefore, (222), (224), (227), (228), (233), and (235) determine the threshold $q_{\mathrm{loc}}^{\mathrm{th}} > 0$ of the overall protocol. □

If an error parameter is below the threshold, we can transform a sequence of gadgets into a sequence of elementary operations using Lemma 16. Note that even without the Pauli frame technique, since each gadget is a stabilizer circuit, a faulty physical circuit can be transformed into a physical circuit without faulty locations where Pauli errors are applied on wires just before the Z-basis measurements in syndrome measurement circuits. Then, the above argument holds without modification.

Finally, we show that our fault-tolerant protocol can achieve an arbitrary target error $\varepsilon > 0$ with a polylogarithmic time and constant space overhead.

We begin by bounding the depth of the physical circuit $\mathrm{C}_n^{\mathrm{FT}}$ compiled from $\mathrm{C}_n^{\mathrm{org}}$. We replace the operations in the original circuit with the intermediate operations for each one-depth part of the original circuit. For the Clifford layer, a single use of the two-register Clifford-gate abbreviation allows the simultaneous application of an arbitrarily long sequence of Clifford gates to a single pair of different registers. However, since a single register contains multiple qubits, even if the ideal quantum circuit could perform a different two-qubit Clifford gate in a single depth, the two-register Clifford-gate abbreviation cannot perform a different pair of two-qubit Clifford gates in a single depth.

To bound the depth of the intermediate circuit required for performing all combinations of the two-qubit Clifford gates in a one-depth part of the Clifford layer of $\mathrm{C}_n^{\mathrm{org}}$, we obtain the combinations of two-qubit Clifford abbreviations that can be executed simultaneously from a solution of the following edge coloring problem. We consider an undirected graph $G = (V, E)$, where each vertex in V corresponds to one of the registers, and each edge in E connects vertices representing registers on which a two-qubit Clifford gate acts in a single-depth part of the Clifford layer (if the gate acts on the same register, the edge forms a self-loop). To simplify the analysis, we additionally define a graph G' by removing all self-loops from G. In the graph G', when each pair of adjacent edges is assigned a different color such that no two neighboring edges have the same color, the two-qubit Clifford gates assigned to each color are implemented as one-depth executable two-qubit Clifford-gate abbreviations in the intermediate circuit. Since each register has K qubits, a qubit in a register can be connected to at most K qubits in other registers by a two-qubit Clifford gate. In this case, since G' is a simple graph and the degree of G' is at most K, G' is $(K+1)$-edge colorable [57, 58]. Thus, G is $(K+2)$-edge colorable because adding another color allows all self-loops to be colored with this color. Note that the algorithm for constructing the $(K+1)$-edge coloring of G' can be performed in polynomial time with respect to the number of vertices and edges [59], and therefore the computation of the $(K+2)$-edge coloring of G can also be performed efficiently. Thus, any possible combination of Clifford gates can be performed in each one-depth part of the original circuit by using two-qubit Clifford abbreviations of up to $(K+2)$-depth in the intermediate circuit. For a T-gate layer, we can perform the T, $T^\dagger$, and I gate in a single-depth part by using a single use of the U_T-gate abbreviation (the same for a single-depth layer of Z-basis-measurement operations, and $|0\rangle$-state-prepration operations).

In the following, by counting the number of EC gadgets in the fault-tolerant circuit, we show that the error probability of our protocol can be suppressed to ε. Subsequently, we demonstrate that our protocol achieves a constant space overhead and a polylogarithmic time overhead. We restrict the number of non-trivial intermediate operations $L(n)$ that we apply in a one-depth part of the intermediate circuit to (199). The intermediate circuit compiled from a one-depth part of the original circuit has depth

$$(K+2) \times \frac{\kappa(n)}{L(n)} = \Theta\left(\log^{\alpha+\gamma_1}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right), \tag{238}$$

where we use (185), (187), (188), and (199). If we replace all the elementary operations contained in the intermediate operation with the corresponding gadget, then the depth of a physical circuit compiled from a one-depth part of the intermediate circuit is bounded by

$$\begin{aligned} O(\tilde{D}_{\mathrm{prep}}(N)) &= O\left(D_{\mathrm{prep}}(N)\log^{\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right) \\ &= O\left(\log^{\alpha+\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right), \end{aligned} \tag{239}$$

where the dominant parts are the state-preparation gadgets as explained in Secs. IV D 4, IV D 5, and IV D 6, and we use (187), (190), and (198). Thus, the physical circuit compiled from the original circuit has depth $D_{\mathrm{FT}}(n)$ bounded by

$$\begin{aligned} &D_{\mathrm{FT}}(n) \\ &= O\left(D(n)\log^{\alpha+\gamma_1}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\log^{\alpha+\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right) \\ &= O\left(D(n)\log^{2\alpha+\gamma_1+\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right) \end{aligned} \tag{240}$$

where we use (238) and (239). Since we allocate five auxiliary registers for each register, the number of EC gadgets in the physical circuit is bounded by

$$
\begin{aligned}
&6\kappa(n) \times O\left(D(n)\log^{2\alpha+\gamma_1+\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right) \\
&\quad = O\left(W(n)D(n)\log^{\alpha+\gamma_1+\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right).
\end{aligned}
\tag{241}
$$

Therefore, the total error probability of the fault-tolerant protocol can be bounded by

$$
\begin{aligned}
&O\left(W(n)D(n)\log^{\alpha+\gamma_1+\gamma_2}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right) \times O\left(\frac{\varepsilon}{|\mathrm{C}_n^{\mathrm{org}}|^2}\right) \\
&= O(\varepsilon),
\end{aligned}
\tag{242}
$$

where we use (183) and (219) in Lemma 16.

Next, the width of a physical circuit compiled from a single non-trivial intermediate operation is bounded by

$$
\begin{aligned}
O(\tilde{W}_{\mathrm{prep}}(N)) &= O\left(W_{\mathrm{prep}}(N)\log^{\gamma_1}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right) \\
&= O\left(\log^{\alpha+\gamma_1}\left(\frac{|\mathrm{C}_n^{\mathrm{org}}|}{\varepsilon}\right)\right),
\end{aligned}
\tag{243}
$$

where the dominant parts are the state-preparation gadgets, as explained in Secs. IV D 4, IV D 5, and IV D 6, and we use (187), (188), and (199). Thus, the width of the physical circuit can be bounded by

$$
\begin{aligned}
&W_{\mathrm{FT}}(n) \\
&= O\left(\tilde{W}_{\mathrm{prep}}(N) \times L(n) + (N + (N-K)) \times (\kappa(n) - L(n))\right) \\
&= O(W(n)),
\end{aligned}
\tag{244}
$$

where $N-K$ is the number of auxiliary physical qubits for measuring stabilizer generators in a EC gadget as explained in Sec. IV D 7, and we use (183), (185), (187), (188), and (199), and (243). Therefore, the fault-tolerant protocol can achieve the constant-space overhead as

$$
\frac{W_{\mathrm{FT}}(n)}{W(n)} = O(1). \tag{245}
$$

On the other hand, the depth $D_{\mathrm{FT}}(n)$ of $\mathrm{C}_n^{\mathrm{FT}}$ is bounded by (240). Therefore, the fault-tolerant protocol can achieve the polylog-time overhead as

$$
\frac{D_{\mathrm{FT}}(n)}{D(n)} = O\left(\mathrm{polylog}\left(\frac{n}{\varepsilon}\right)\right), \tag{246}
$$

where we use (183). From the above discussion, we conclude Theorem 14.

V. CONCLUSION

In this work, we present a hybrid fault-tolerant protocol that combines concatenated codes for gate operations with a non-vanishing-rate quantum LDPC code (in particular, the quantum expander codes [20, 60, 61]) for state preservation. Our protocol achieves polylogarithmic time overhead while maintaining constant space overhead. Thus, our protocol improves the time overhead of existing constant-space-overhead protocols, i.e., the protocols based on non-vanishing-rate quantum LDPC codes [20–22], as well as the protocol based on concatenated quantum Hamming codes [25]. This improvement is achieved by increasing the parallelism for executing logical gates from $O(W(n)/\mathrm{poly}(n))$ to $O(W(n)/\mathrm{polylog}(n))$, improving on Ref. [21], due to advances in the analysis of error suppression by decoding algorithms [20, 22]. Moreover, we show that our protocol has a threshold even when accounting for the runtime of classical computation required to perform the fault-tolerant circuit, whereas existing analyses of protocols for quantum LDPC codes assume that such classical computation can be instantaneous [20–22]. Our protocol eliminates redundant spacetime trade-offs present in existing constant-space-overhead FTQC protocols [20–22, 25].

These results highlight that the quantum LDPC code approach can achieve time-efficient FTQC while maintaining a constant space overhead, as well as the code-concatenation approaches [25, 26]. Our work contributes to the fundamental understanding of low-overhead FTQC, and more importantly, it underscores the need for a comprehensive investigation to determine which of the two approaches holds more promise for future physical implementations of FTQC.

ACKNOWLEDGMENTS

S.T. was supported by JST [Moonshot R&D][Grant Number JPMJMS2061], JSPS KAKENHI Grant Number 23KJ0521, and FoPM, WINGS Program, the University of Tokyo. H.Y. acknowledges JST PRESTO Grant Number JPMJPR201A, JPMJPR23FC, JSPS KAKENHI Grant Number JP23K19970, and MEXT Quantum Leap Flagship Program (MEXT QLEAP) JPMXS0118069605, JPMXS0120351339. The quantum circuits shown in this paper are drawn using QPIC [62].

[1] N. de Beaudrap, A linearized stabilizer formalism for systems of finite dimension, Quantum Information and Computation **13**, 73–115 (2013).

[2] N. Rengaswamy, R. Calderbank, H. D. Pfister, and S. Kadhe, Synthesis of logical clifford operators via symplectic geometry, in *2018 IEEE International Symposium*

on Information Theory (ISIT) (IEEE, 2018).

[3] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, Physical Review A **70**, 10.1103/physreva.70.052328 (2004).

[4] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Physical Review A **54**, 1098 (1996).

[5] A. Steane, Multiple particle interference and quantum error correction, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **452** (1996).

[6] R. W. Hamming, Error detecting and error correcting codes, The Bell System Technical Journal **29**, 147 (1950).

[7] E. Knill and R. Laflamme, Concatenated quantum codes (1996), arXiv:quant-ph/9608012 [quant-ph].

[8] P. Aliferis, D. Gottesman, and J. Preskill, Quantum accuracy threshold for concatenated distance-3 codes (2005), arXiv:quant-ph/0504218 [quant-ph].

[9] A. Kitaev, Fault-tolerant quantum computation by anyons, Annals of Physics **303**, 2–30 (2003).

[10] S. B. Bravyi and A. Y. Kitaev, Quantum codes on a lattice with boundary (1998), arXiv:quant-ph/9811052 [quant-ph].

[11] D. Litinski, A game of surface codes: Large-scale quantum computing with lattice surgery, Quantum **3**, 128 (2019).

[12] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation, Physical Review A **86**, 10.1103/physreva.86.032324 (2012).

[13] M. Vasmer and D. E. Browne, Three-dimensional surface codes: Transversal gates and fault-tolerant architectures, Physical Review A **100**, 10.1103/physreva.100.012312 (2019).

[14] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, Topological quantum memory, Journal of Mathematical Physics **43**, 4452–4505 (2002).

[15] H. Bombin and M. A. Martin-Delgado, Topological quantum distillation, Physical Review Letters **97**, 10.1103/physrevlett.97.180501 (2006).

[16] H. Bombin and M. A. Martin-Delgado, Exact topological quantum order in $d = 3$ and beyond: Branyons and brane-net condensates, Phys. Rev. B **75**, 075103 (2007).

[17] A. Kubica and M. E. Beverland, Universal transversal gates with color codes: A simplified approach, Physical Review A **91**, 10.1103/physreva.91.032330 (2015).

[18] H. Bombin, Gauge color codes: Optimal transversal gates and gauge fixing in topological stabilizer codes (2015), arXiv:1311.0879 [quant-ph].

[19] H. Bombin, Clifford gates by code deformation, New Journal of Physics **13**, 043005 (2011).

[20] O. Fawzi, A. Grospellier, and A. Leverrier, Constant overhead quantum fault-tolerance with quantum expander codes, in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2018).

[21] D. Gottesman, Fault-tolerant quantum computation with constant overhead, Quantum Info. Comput. **14**, 1338–1372 (2014).

[22] A. Grospellier, *Constant time decoding of quantum expander codes and application to fault-tolerant quantum computation*, Theses, Sorbonne Université (2019).

[23] A. Krishna and D. Poulin, Fault-tolerant gates on hypergraph product codes, Physical Review X **11**, 10.1103/physrevx.11.011023 (2021).

[24] A. O. Quintavalle, P. Webster, and M. Vasmer, Partitioning qubits in hypergraph product codes to implement logical gates, Quantum **7**, 1153 (2023).

[25] H. Yamasaki and M. Koashi, Time-efficient constant-space-overhead fault-tolerant quantum computation, Nature Physics **20**, 247–253 (2024).

[26] S. Yoshida, S. Tamiya, and H. Yamasaki, Concatenate codes, save qubits (2024), arXiv:2402.09606 [quant-ph].

[27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[28] D. Maslov and M. Roetteler, Shorter stabilizer circuits via bruhat decomposition and quantum circuit transformations, IEEE Transactions on Information Theory **64**, 4729–4738 (2018).

[29] P. Aliferis, D. Gottesman, and J. Preskill, Accuracy threshold for postselected quantum computation (2007), arXiv:quant-ph/0703264 [quant-ph].

[30] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, J. P. Bonilla Ataides, N. Maskara, I. Cong, X. Gao, P. Sales Rodriguez, T. Karolyshyn, G. Semeghini, M. J. Gullans, M. Greiner, V. Vuletić, and M. D. Lukin, Logical quantum processor based on reconfigurable atom arrays, Nature **626**, 58–65 (2023).

[31] Q. Xu, J. P. Bonilla Ataides, C. A. Pattison, N. Raveendran, D. Bluvstein, J. Wurtz, B. Vasić, M. D. Lukin, L. Jiang, and H. Zhou, Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays, Nature Physics 10.1038/s41567-024-02479-z (2024).

[32] S. A. Moses, C. H. Baldwin, M. S. Allman, R. Ancona, L. Ascarrunz, C. Barnes, J. Bartolotta, B. Bjork, P. Blanchard, M. Bohn, J. G. Bohnet, N. C. Brown, N. Q. Burdick, W. C. Burton, S. L. Campbell, J. P. Campora, C. Carron, J. Chambers, J. W. Chan, Y. H. Chen, A. Chernoguzov, E. Chertkov, J. Colina, J. P. Curtis, R. Daniel, M. DeCross, D. Deen, C. Delaney, J. M. Dreiling, C. T. Ertsgaard, J. Esposito, B. Estey, M. Fabrikant, C. Figgatt, C. Foltz, M. Foss-Feig, D. Francois, J. P. Gaebler, T. M. Gatterman, C. N. Gilbreth, J. Giles, E. Glynn, A. Hall, A. M. Hankin, A. Hansen, D. Hayes, B. Higashi, I. M. Hoffman, B. Horning, J. J. Hout, R. Jacobs, J. Johansen, L. Jones, J. Karcz, T. Klein, P. Lauria, P. Lee, D. Liefer, S. T. Lu, D. Lucchetti, C. Lytle, A. Malm, M. Matheny, B. Mathewson, K. Mayer, D. B. Miller, M. Mills, B. Neyenhuis, L. Nugent, S. Olson, J. Parks, G. N. Price, Z. Price, M. Pugh, A. Ransford, A. P. Reed, C. Roman, M. Rowe, C. Ryan-Anderson, S. Sanders, J. Sedlacek, P. Shevchuk, P. Siegfried, T. Skripka, B. Spaun, R. T. Sprenkle, R. P. Stutz, M. Swallows, R. I. Tobey, A. Tran, T. Tran, E. Vogt, C. Volin, J. Walker, A. M. Zolot, and J. M. Pino, A race-track trapped-ion quantum processor, Phys. Rev. X **13**, 041052 (2023).

[33] C. Ryan-Anderson, J. G. Bohnet, K. Lee, D. Gresh, A. Hankin, J. P. Gaebler, D. Francois, A. Chernoguzov, D. Lucchetti, N. C. Brown, T. M. Gatterman, S. K. Halit, K. Gilmore, J. A. Gerber, B. Neyenhuis, D. Hayes, and R. P. Stutz, Realization of real-time fault-tolerant quantum error correction, Phys. Rev. X **11**, 041058 (2021).

[34] L. Egan, D. M. Debroy, C. Noel, A. Risinger, D. Zhu, D. Biswas, M. Newman, M. Li, K. R. Brown, M. Cetina, and C. Monroe, Fault-tolerant operation of a quantum error-correction code (2021), arXiv:2009.11482 [quant-

ph].

[35] J. E. Bourassa, R. N. Alexander, M. Vasmer, A. Patil, I. Tzitrin, T. Matsuura, D. Su, B. Q. Baragiola, S. Guha, G. Dauphinais, K. K. Sabapathy, N. C. Menicucci, and I. Dhand, Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer, Quantum **5**, 392 (2021).

[36] D. Litinski and N. Nickerson, Active volume: An architecture for efficient fault-tolerant quantum computers with limited non-local connections (2022), arXiv:2211.15465 [quant-ph].

[37] H. Yamasaki, K. Fukui, Y. Takeuchi, S. Tani, and M. Koashi, Polylog-overhead highly fault-tolerant measurement-based quantum computation: all-gaussian implementation with gottesman-kitaev-preskill code (2020), arXiv:2006.05416 [quant-ph].

[38] E. Knill, Scalable quantum computation in the presence of large detected-error rates (2004), arXiv:quant-ph/0312190 [quant-ph].

[39] E. Knill, Quantum computing with realistically noisy devices, Nature **434**, 39–44 (2005).

[40] In our protocol for the concatenated code, we apply the Pauli gates directly rather than updating the Pauli frame for simplicity of the presentation. It would also be possible to use the updates of Pauli frame here. By contrast, in the protocol for the quantum LDPC code, we always apply Pauli gates by updating the Pauli frame, which is convenient for bounding the error rate right after each decoding of the quantum LDPC code.

[41] D. Gottesman, An introduction to quantum error correction and fault-tolerant quantum computation, in *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, Vol. 68 (2010) pp. 13–58.

[42] M. Christandl and A. Müller-Hermes, Fault-tolerant coding for quantum communication (2022), arXiv:2009.07161 [quant-ph].

[43] D. P. DiVincenzo and P. Aliferis, Effective fault-tolerant quantum computation with slow measurements, Physical Review Letters **98**, 10.1103/physrevlett.98.020501 (2007).

[44] C. Chamberland, P. Iyer, and D. Poulin, Fault-tolerant quantum computing in the pauli or clifford frame with slow error diagnostics, Quantum **2**, 43 (2018).

[45] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature **402**, 390 (1999).

[46] E. Knill, Scalable quantum computing in the presence of large detected-error rates, Phys. Rev. A **71**, 042322 (2005).

[47] A. Leverrier, J.-P. Tillich, and G. Zemor, Quantum expander codes, in *2015 IEEE 56th Annual Symposium on Foundations of Computer Science* (IEEE, 2015).

[48] A. Leverrier and G. Zemor, Quantum tanner codes, in *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Los Alamitos, CA, USA, 2022) pp. 872–883.

[49] S. Gu, E. Tang, L. Caha, S. H. Choe, Z. He, and A. Kubica, Single-shot decoding of good quantum ldpc codes, Communications in Mathematical Physics **405**, 85 (2024).

[50] E. T. Campbell, A theory of single-shot error correction for adversarial noise, Quantum Science and Technology **4**, 025006 (2019).

[51] H. Bombín, Single-shot fault-tolerant quantum error correction, Phys. Rev. X **5**, 031043 (2015).

[52] A. Kubica and M. Vasmer, Single-shot quantum error correction with the three-dimensional subsystem toric code, Nature Communications **13**, 10.1038/s41467-022-33923-4 (2022).

[53] B. J. Brown, N. H. Nickerson, and D. E. Browne, Fault-tolerant error correction with the gauge color code, Nature Communications **7**, 12302 (2016).

[54] A. A. Kovalev and L. P. Pryadko, Fault tolerance of quantum low-density parity check codes with sublinear distance scaling, Physical Review A **87**, 10.1103/physreva.87.020304 (2013).

[55] R. Cleve and D. Gottesman, Efficient computations of encodings for quantum error correction, Phys. Rev. A **56**, 76 (1997).

[56] P. W. Shor, Fault-tolerant quantum computation (1997), arXiv:quant-ph/9605011 [quant-ph].

[57] V. G. Vizing, On an estimate of the chromatic class of a p-graph, Diskret. Analiz. **3**, 25 (1964).

[58] J. Bondy and U. Murty, *Graph Theory*, 1st ed. (Springer Publishing Company, Incorporated, 2008).

[59] E. Arjomandi, An efficient algorithm for colouring the edges of a graph with $\delta + 1$ colours, INFOR: Information Systems and Operational Research **20**, 82 (1982).

[60] A. Leverrier, J.-P. Tillich, and G. Zémor, Quantum expander codes, in *2015 IEEE 56th Annual Symposium on Foundations of Computer Science* (2015) pp. 810–824.

[61] O. Fawzi, A. Grospellier, and A. Leverrier, Efficient decoding of random errors for quantum expander codes, in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC ' 18 (ACM, 2018).

[62] qpic, `https://github.com/qpic/qpic` (2016).

[63] G. Hayato, Minimizing resource overheads for fault-tolerant preparation of encoded states of the steane code, Scientific Reports **6**, 10.1038/srep19578 (2016).

[64] R. Chao and B. W. Reichardt, Quantum error correction with only two extra qubits, Phys. Rev. Lett. **121**, 050502 (2018).

[65] C. Chamberland and A. W. Cross, Fault-tolerant magic state preparation with flag qubits, Quantum **3**, 143 (2019).

Appendix A: Conditions of fault-tolerant gadgets on concatenated Steane codes

In this section, we provide the fault-tolerance conditions for concatenated Steane codes [29, 41]. For the argument, we introduce the notion of r-filter. The r-filter is a mathematical object used for analysis and does not correspond to any physical operation during quantum computation. The r-filter is used to ensure that the weight of an error occurring on a codeword at a given time is not too large. It is defined as follows:

Definition 17 (r-filter)**.** An r-filter is a projector onto the subspace spanned by all states of the form $E\left|\bar{\psi}\right\rangle$, where $E \in \mathcal{P}_N$ with a weight of at most r and $\left|\bar{\psi}\right\rangle \in \mathcal{Q}$ is a codeword. If the ideal syndrome bits of an encoded state were hypothetically obtained and the syndrome bits indicate a Pauli error with a weight of at most r, then the

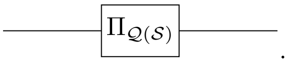
r-filter leaves the encoded state unchanged. Conversely, if the indicated error exceeds the weight r, the r-filter rejects the encoded state, terminating the computation.

Reference [41] provides the definition for $[[N, 1, 2t+1]]$ codes where $0 \leq r \leq t$. However, for the Steane code with $t = 1$, we can easily interpret the r-filter for $r = 0, 1$. The 0-filter is defined as a projector onto the code space, i.e.,

$$\Pi_{\mathcal{Q}} := \prod_i \frac{I + g_i}{2}, \tag{A1}$$

where $\{g_i\}_i$ is a set of stabilizer generators as given in (25). The 0-filter is illustrated in the diagram as,

- 0-filter



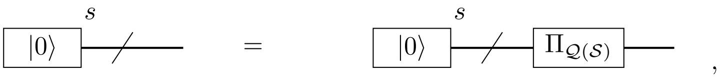
(A2)

The 1-filter for the Steane code becomes the identity operator I acting on the whole Hilbert space because all the $X(Z)$-type errors that appear in the Steane code can be decomposed into logical $X(Z)$ errors plus weight-1 $X(Z)$ errors. The 1-filter is not shown in the diagram because it is trivial.

Then, the fault-tolerance conditions for preparation, gate, and measurement gadgets are presented below with diagrams using ideal decoder in Def. 7 and the 0-filter in Def. 17. In the diagrams, an operation surrounded by thin lines and acting on thin wires represents a non-fauly operation. The variable s shown in the upper right of a gadget represents the number of faults in the gadget.

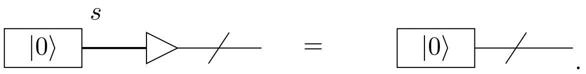
The $|0\rangle$-state preparation gadget is fault-tolerant if it satisfies

prep A: when $s = 0$



(A3)

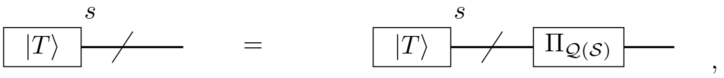
prep B: when $s = 0, 1$



(A4)

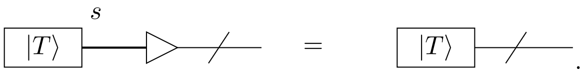
Also, the $|T\rangle$-state preparation gadget is fault-tolerant if it satisfies

prep A: when $s = 0$



(A5)

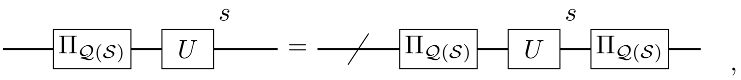
prep B: when $s = 0, 1$



(A6)

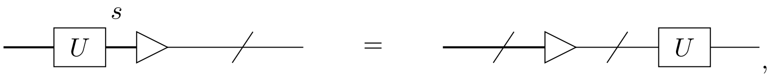
The Pauli-, H-, and S-gate gadgets are fault-tolerant if they satisfy the following conditions, with each gate denoted by U:

gate A: when $s = 0$


$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
s
=
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
s
$\Pi_{\mathcal{Q}(\mathcal{S})}$
,

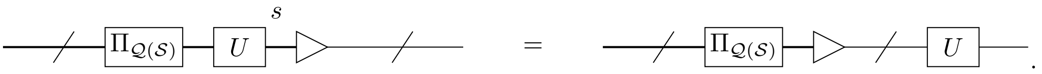
(A7)

gate B: when $s = 0$



(A8)

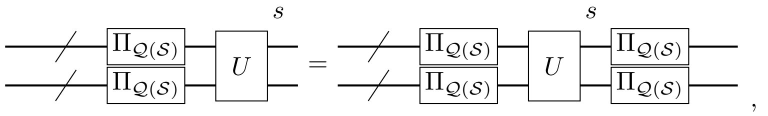
and when $s = 0, 1$


$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
s
=
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
.

(A9)

The CNOT-gate gadget is fault-tolerant if it satisfies, with the CNOT-gate denoted by U,

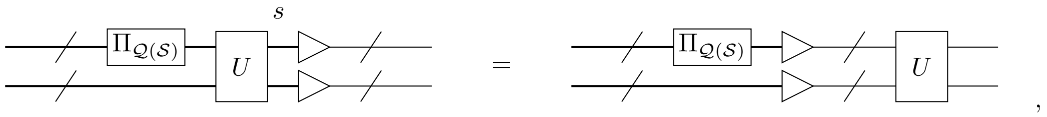
gate A: when $s = 0$



s
$\Pi_{\mathcal{Q}(\mathcal{S})}$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
$=$
s
$\Pi_{\mathcal{Q}(\mathcal{S})}$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
$\Pi_{\mathcal{Q}(\mathcal{S})}$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
,

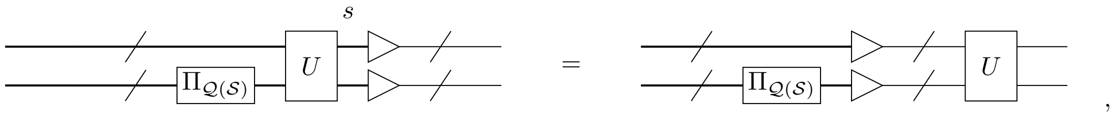
(A10)

gate B: when $s = 0$



s
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
$=$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
,

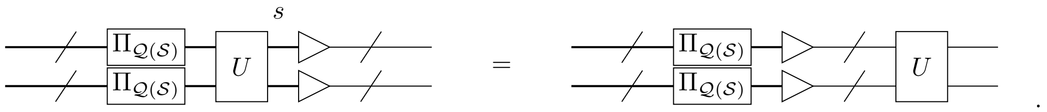
(A11)



s
U
$\Pi_{\mathcal{Q}(\mathcal{S})}$
$=$
U
$\Pi_{\mathcal{Q}(\mathcal{S})}$
,

(A12)

and when $s = 0, 1$

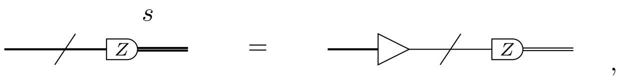


s
$\Pi_{\mathcal{Q}(\mathcal{S})}$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
$=$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
U
.

(A13)

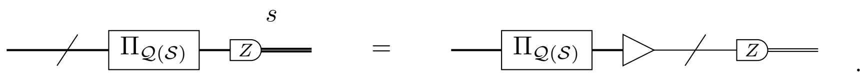
The Z-basis measurement gadget is fault-tolerant if it satisfies

meas A: when $s = 0$



(A14)

meas B: when $s = 0, 1$

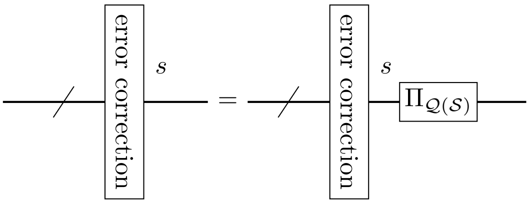


s
$\Pi_{\mathcal{Q}(\mathcal{S})}$
Z
$=$
$\Pi_{\mathcal{Q}(\mathcal{S})}$
Z
.

(A15)

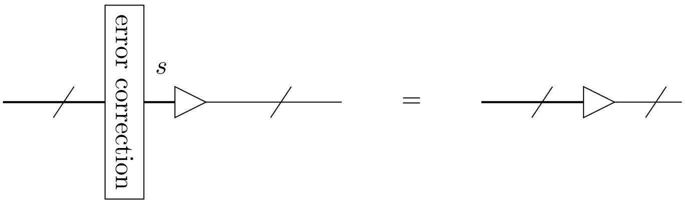
The EC gadget is fault-tolerant if it satisfies

ec A: when $s = 0$



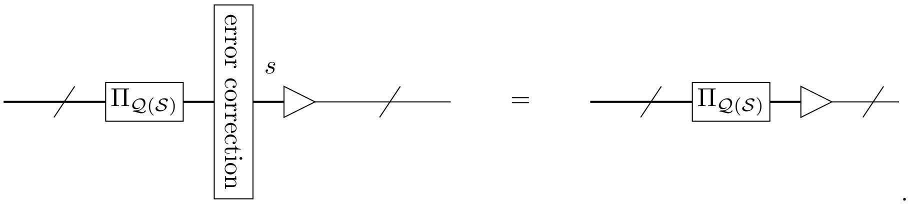
, (A16)

ec B: when $s = 0$



, (A17)

and when $s = 0, 1$


$\Pi_{\mathcal{Q}(\mathcal{S})}$
error correction
s
=
$\Pi_{\mathcal{Q}(\mathcal{S})}$

. (A18)

Appendix B: Construction of abbreviations and gadgets

In this section, we present the explicit construction of an abbreviation and gadgets that satisfy the fault-tolerance condition presented from (A3) to (A18).

1. T-gate abbreviation

The construction of the T-gate abbreviation is shown in Fig. 12. The abbreviation is based on gate teleportation. Implementation is assisted by a single auxiliary qubit in the state $|T\rangle$ from the $|T\rangle$-state preparation gadget. We subsequently perform the CNOT-gate gadget followed by the Z-basis measurement. To implement the T gate, a Clifford gate SX for the correction operation is applied to the qubit if the measurement outcome is $m = 1$.

2. Z-basis measurement gadget

The Z-basis measurement gadget is constructed as shown in Fig. 13. The gadget is implemented by transversal Z-basis measurements, followed by the execution of the decoding algorithm by classical computation.

We present the explicit procedure for performing the Z-basis measurement. Specifically, we give the procedure for calculating the measurement outcome $\bar{z} \in \{0, 1\}$ of the Pauli operator Z on a level-l qubit from the noisy measurement outcomes $z_i \in \mathbb{F}_2$ of Z_i on the i-th level-$(l-1)$ qubits for $i \in \{1, \ldots, 7\}$. The procedure is as follows:

1. We measure the 7 level-$(l-1)$ qubits on the Z-basis. The outcomes are $z \in \mathbb{F}_2^7$, where each bit $z_i \in \mathbb{F}_2$ is the noisy measurement outcome on the i-th level-$(l-1)$ qubit.

2. We calculate the syndrome bits $\sigma_X \in \mathbb{F}_2^3$ of the Z-type generators from the 7-bit outcomes of the Z-basis measurement of the level-$(l-1)$ qubits by using the relation,

$$(\sigma_X)_i = \bigoplus_{j \in \mathrm{supp}(g_i^Z)} z_j, \tag{B1}$$

where $\mathrm{supp}(g_i^Z)$ denotes the set of qubit indices where g_i^Z has non-trivial support.

3. We execute the decoding algorithm (27) which takes the syndrome bits $\sigma_X \in \mathbb{F}_2^3$ as input and outputs the recovery operation of an X-type Pauli operator, denoted by $\hat{F} \in \mathcal{P}_N$. Then, the corrected

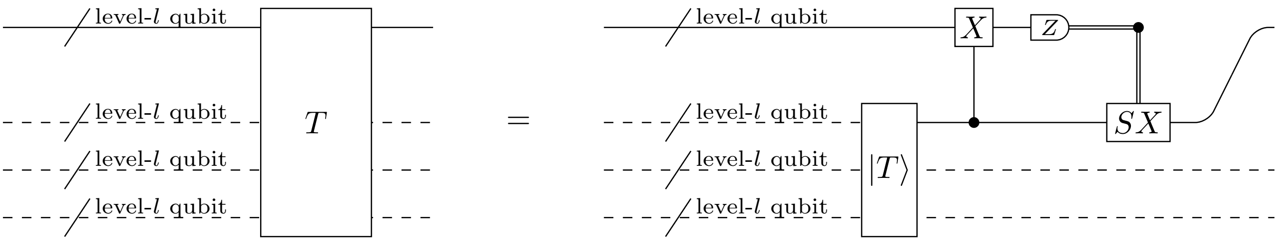


FIG. 12. The level-l circuit of the T-gate abbreviation for performing the T gate through gate teleportation.

bits $\tilde{z} \in \mathbb{F}_2^7$ are obtained for $i \in \{1, \ldots, 7\}$ as

$$\tilde{z}_i := z_i \oplus (\phi(\hat{F}))_i, \tag{B2}$$

where $(\phi(\hat{F}))_j$ represents the j-th element of the row vector $\phi(\hat{F})$.

4. We calculate the noiseless measurement outcome $\bar{z} \in \mathbb{F}_2$ of Z on the level-l qubit as

$$\bar{z} := \bigoplus_{i \in \mathrm{supp}(\bar{Z})} \tilde{z}_i, \tag{B3}$$

where $\bar{Z}$ is the logical-Z operator of the Steane code as given in (26), and $\mathrm{supp}(\bar{Z})$ denotes the set of indices of the physical qubits on which the logical-Z operator acts nontrivially.

The fault tolerance of the Z-basis measurement gadget defined as in (A14) and (A15) is ensured by transversality.

3. Gate gadgets

The constructions of the Pauli-, H-, S-, $S^\dagger$ and CNOT-gate gadgets are shown in Fig. 14. The Pauli-, H-, S-, $S^\dagger$- and CNOT-gate gadgets are implemented by the transversal Pauli, H, $S^\dagger$, S and CNOT gates acting on the level-$(l-1)$ qubits, respectively. The fault tolerance of the gate gadgets defined as (A7), (A8), (A9), (A10), (A11), (A12) and (A13) is ensured by transversality.

4. $|0\rangle$-state preparation gadget

The construction of the $|0\rangle$-state preparation gadget is shown in Fig. 15 (a). We first prepare 7 qubits in the state $|0\rangle^{\otimes 7}$ using the $|0\rangle$-state preparation operations. Then, we use an encoding circuit $U_{\mathrm{encode}}^{|0\rangle}$ to transform the state $|0\rangle^{\otimes 7}$ into the logical state of $|0\rangle$. The encoding circuit $U_{\mathrm{encode}}^{|0\rangle}$ is shown in Fig. 15 (b), presented in Ref. [63].

The issue here is that the encoding circuit is non-fault-tolerant, meaning a single fault occurring during the encoding circuit may lead to an error with a weight greater than one by the end of the encoding circuit. Thus, verification is essential to detect such errors, ensuring that the $|0\rangle$-state preparation gadget satisfies the fault-tolerance conditions specified in (A3) and (A4). In the verification process, the gadget executes the same encoding circuit $U_{\mathrm{encode}}^{|0\rangle}$ to prepare another set of 7 qubits in the logical state of $|0\rangle$. Subsequently, the gadget performs the transversal CNOT gate targeting the newly prepared qubits. This is followed by the transversal Z-basis measurements on these qubits. From these Z-basis measurements, we obtain the syndrome bits for all Z-type stabilizer generators in (25) and the measurement outcome of the logical Z operator on the level-l qubit in (26) through classical computation described in the Z-basis measurement gadget. These are crucial for detecting badly propagated X-type errors. The verification passes if and only if all the syndrome bits are trivial and the measurement outcome m of the logical Z operator is $m = 0$. If verification fails, the gadget discards the resulting state and repeats the encoding circuit $U_{\mathrm{encode}}^{|0\rangle}$ without verification in the second run. Note that the detection of the Z-type errors is unnecessary for verifying $|0\rangle$ since multiple Z-type errors at the end of the encoding circuit may lead to a logical Z error but do not transform the state, i.e., $Z|0\rangle = |0\rangle$.

We check that the above gadget construction satisfies the fault-tolerance condition defined in (A3) and (A4). In the case where $s = 0$, i.e., no fault occurs during the gadget, the gadget successfully outputs 7 qubits in the logical state of $|0\rangle$, and thus the conditions (A3) and (A4) are satisfied. Next, we discuss the case where $s = 1$, i.e., only a single fault occurs in the gadget. If the verification succeeds, the gadget successfully outputs 7 qubits in the logical state of $|0\rangle$ in the first run. If the verification fails in the first run, i.e., an error is detected, then the gadget discards the resulting state. Then, the gadget restarts and executes the encoding circuit to prepare 7 qubits in the logical state of $|0\rangle$ in the second run without verification. In this scenario, since a single fault occurred in the first run, no fault occurred during the part for preparing 7 qubits in the logical state of $|0\rangle$ in the second run, given that we consider the condition where $s = 1$. Therefore, the fault-tolerance conditions (A3) and (A4) of the gadget are satisfied.

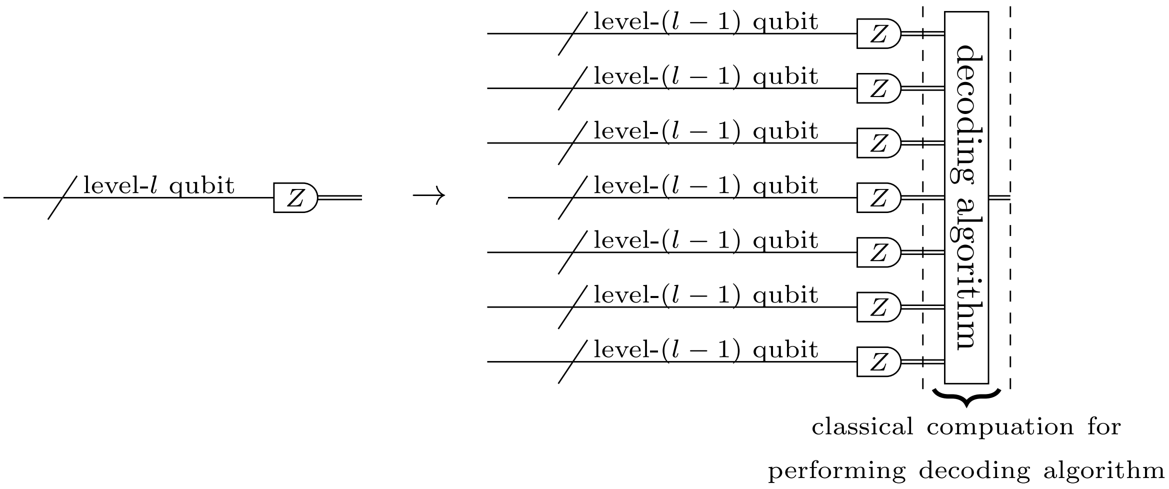


FIG. 13. The level-$(l-1)$ circuit of the Z-basis measurement gadget. The gadget is implemented by transversal Z-basis measurements, followed by the decoding algorithm.

5. $|T\rangle$-state preparation gadget

The $|T\rangle$-state preparation gadget is constructed as shown in Fig. 16 (a). The gadget starts with the preparation of the logical state of $|T\rangle := TH|0\rangle$ from the 7 qubits in the state $|T\rangle \otimes |0\rangle^{\otimes 6}$. We utilize the non-fault-tolerant encoding circuit $U_{\text{encode}}^{|\psi\rangle}$ to transform an arbitrary state $|\psi\rangle$ into an logical state of $|\psi\rangle$, as shown in Fig. 16 (b), presented in Ref. [63]. A single fault that occurs during or before the encoding circuit $U_{\text{encode}}^{|\psi\rangle}$ leads to an error with a weight greater than one, as well as for the $|0\rangle$-state preparation gadget. Thus, verification is essential to detect such errors for the $|T\rangle$-state preparation gadget to satisfy the fault-tolerance conditions given by (A5) and (A6). For verification, we perform a measurement of the operator $TXT^\dagger$, followed by error detection. The measurement of the operator $TXT^\dagger$ is needed for verification, since the $|T\rangle$ state we want to prepare is stabilized by the operator $TXT^\dagger$, i.e.,

$$TXT^\dagger|T\rangle = |T\rangle \tag{B4}$$

Since $TXT^\dagger = SX$ is a Clifford operator, we can measure the logical operator $TXT^\dagger$ by performing transversal measurements of $T^\dagger XT = S^\dagger X$. This measurement can be performed with controlled $T^\dagger XT$ gates controlled by the auxiliary A as shown in Fig. 16. The auxiliary qubit is measured to obtain the measurement outcome of the operator $T^\dagger XT$. If the measurement outcome of the operator $TXT^\dagger$ is $m = 1$, indicating that the state is projected onto the state orthogonal to $|T\rangle$, then we consider the verification to be failed, and the gadget discards the state. To measure the logical operator $TXT^\dagger$ in a fault-tolerant way, we additionally use a qubit as the flag qubit [64, 65], where the flag qubit corresponds to the auxiliary qubit B in Fig. 16. A single fault on the auxiliary qubit A may result in an error with a weight greater than one on the code block, which consists of the 7 qubits. However, in such a case, if the measurement outcome of the auxiliary qubit B, serving as the flag qubit, is $m = 1$ in the Z basis, the verification is deemed to have failed, and the gadget discards the state. To verify that the state is in the code subspace, we perform error detection at the end of $|T\rangle$-state preparation gadget based on the gate teleportation as shown in Fig. 16. If at least one non-trivial syndrome bit is detected during the execution of the gate teleport protocol, then we consider the verification to be failed, and the gadget discards the state. Therefore, the verification is successful only if the measurement outcome m of $TXT^\dagger$ is $m = 0$, the measurement outcome m of the flag qubit is $m = 0$, and all the syndrome bits obtained during the gate teleportation protocol are trivial. If the verification fails, the gadget discards the resulting state at the point of failure. Afterwards, the gadget repeats the encoding circuit to prepare the logical state $|T\rangle$ without verification in the second run.

We show that the $|T\rangle$-state preparation gadget satisfies the fault-tolerance condition defined by (A5) and (A6). If $s = 0$, indicating no fault in the gadget, the gadget successfully outputs the logical state $|T\rangle$, satisfying conditions (A5) and (A6) are satisfied. Next, we consider the case where $s = 1$, indicating a single fault in the gadget, and show that condition (A6) is satisfied. We divide the $|T\rangle$-state preparation gadget, which may cause a single fault, into three parts: (1) preparing the logical state of $|T\rangle$, (2) measuring the logical operator $TXT^\dagger$, and (3) error detection. Here, we show that the fault-tolerance condition is satisfied if a single fault occurs in any of the three parts.

1. A fault occurs during the preparation of the logical state $|T\rangle$.

   In this scenario, since we assume that only a single

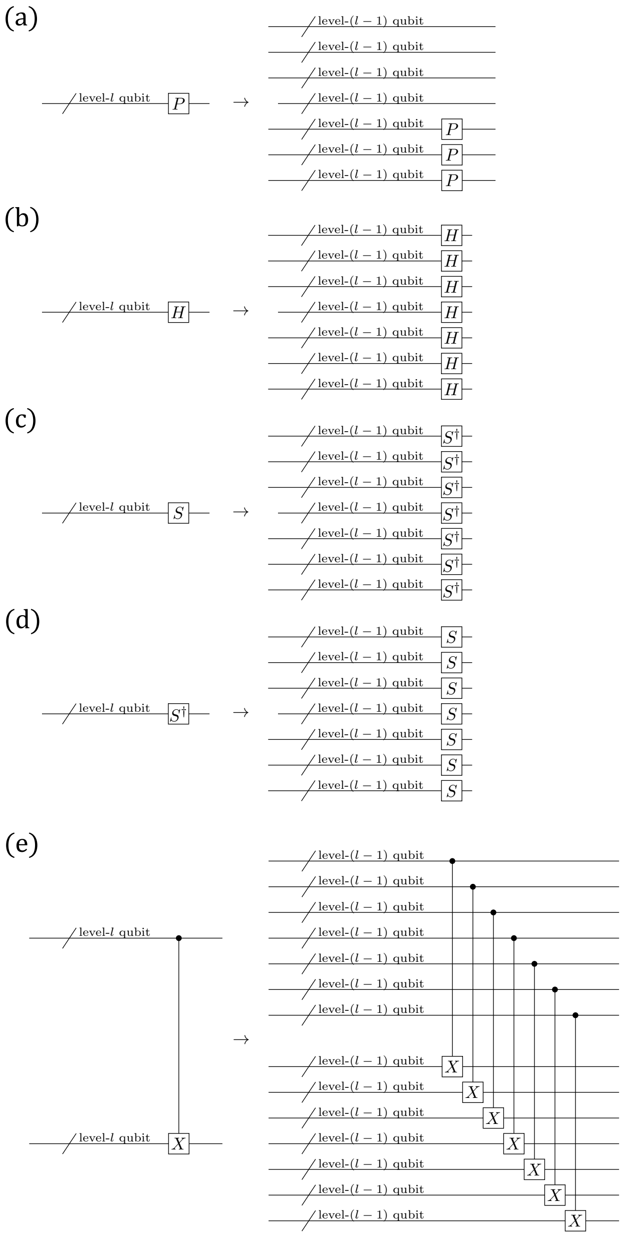


FIG. 14. A level-$(l-1)$ circuit of the Pauli-gate gadget (a), the H-gate gadget (b), the S-gate gadget (c), the $S^\dagger$-gate gadget (d), and the CNOT-gate gadget (e).

fault occurs during the gadget, the measurement of the operator $TXT^\dagger$ and the error detection are performed ideally. If the verification succeeds, the gadget successfully outputs the logical state $|T\rangle$. If the verification fails, the gadget discards the state obtained in the first run and then re-executes the encoding circuit in the second run. In this second run, the gadget outputs the logical state $|T\rangle$ without further verification because a single fault occurred in the first run. After completing the encoding circuit in the second run, the gadget successfully outputs the logical state $|T\rangle$. With this gadget construction, the condition (A6) is satisfied.

2. A fault occurs during the measurement of the logical operator $TXT^\dagger$.

   In this case, since there is no fault in the first part (i) of the gadget, the encoding circuit outputs the logical state $|T\rangle$. The problem arises when a single fault occurs in the auxiliary qubit A, as the fault-induced error may propagate to the code block of 7 qubits, resulting in an error with a weight greater than one. However, even if such a fault occurs, the error resulting from the fault is also propagated to the auxiliary qubit B, causing a measurement outcome of $m = 1$, which can be detected through verification. For example, if a fault occurs on the auxiliary qubit A, resulting in a Pauli-X or -Y error, this error affects the code block, leading to an error with multiple weights. Subsequently, this error propagates to the auxiliary qubit B through the CNOT gates, resulting in a measurement outcome of $m = 1$ on qubit B. Therefore, a Pauli error that produces an error with multiple weights on the code block can be effectively detected through the verification process. If the verification process fails, the gadget discards the state obtained from the first run and performs the encoding circuit again in the second run without verification. This construction of the gadget ensures that the condition (A6) is satisfied.

3. A fault occurs during error detection.

   Since there are no faults in (i) and (ii) of the gadget, the state before executing the error detection is a logical state of $|T\rangle$. If a single fault occurs that can be detected by the error detection procedure, the gadget discards the state. In the second run, it executes the encoding circuit again, satisfying the condition (A6). Even if a single fault occurs that is cannot be detected through error detection, from (A18), the condition (A6) is also satisfied.

Therefore, the fault tolerance of the $|T\rangle$-state preparation gadget defined as (A5) and (A6) is satisfied.

6. Error-correction gadget

The error-correction gadget is constructed as in Fig. 17. This gadget is based on Knill's error correction [38, 39, 41]. The gadget uses two sets of 7 auxiliary qubits initialized to the logical state of $|0\rangle$ using the $|0\rangle$-state preparation gadget, in addition to the input 7 qubits on which we want to perform error correction. By using these two sets of 7 auxiliary qubits, we perform quantum teleportation of the input level-l qubit. The two 7-bit outcomes from the Z-basis measurements are fed

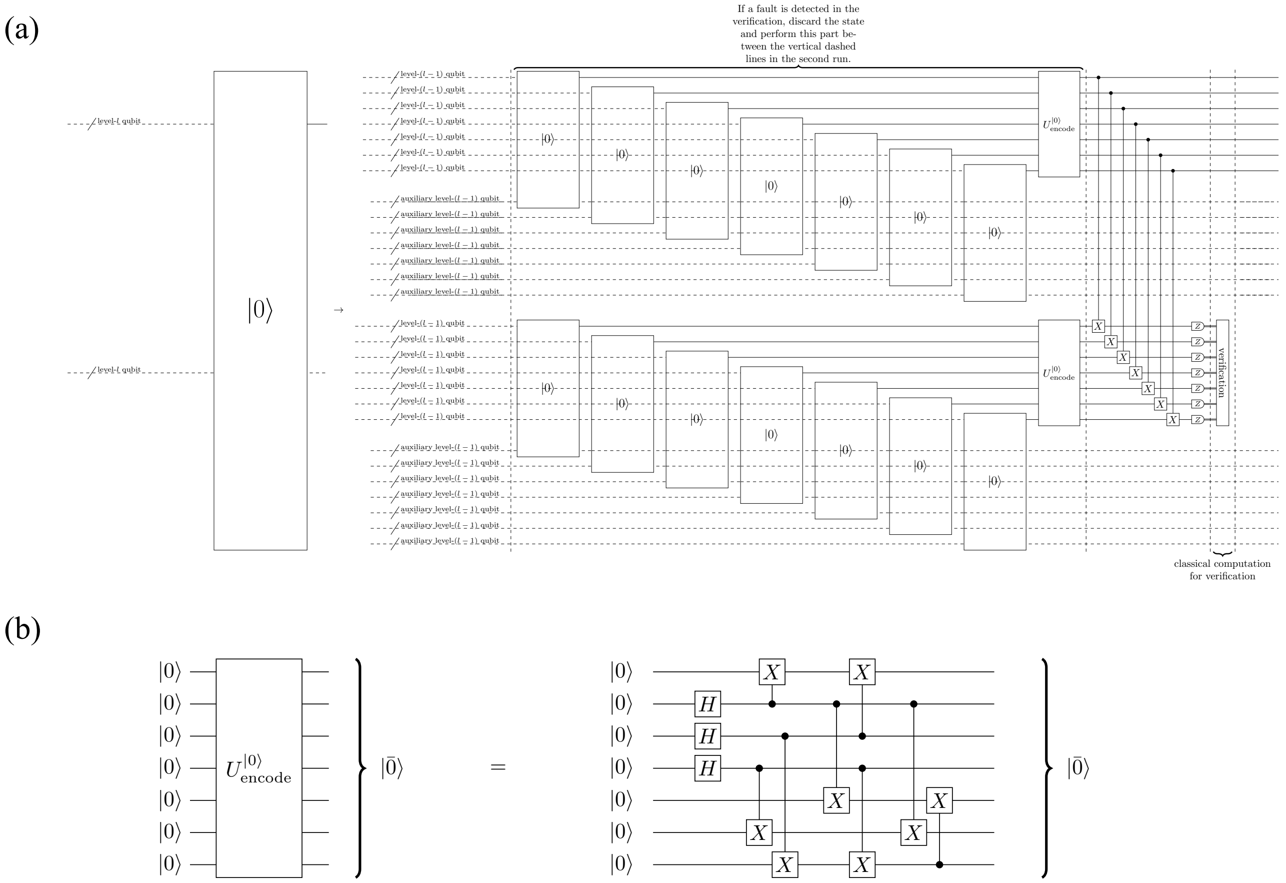

(a)
If a fault is detected in the verification, discard the state and perform this part between the vertical dashed lines in the second run.
level-l qubit
level-l qubit
$|0\rangle$
→
level-(l − 1) qubit
auxiliary level-(l − 1) qubit
$|0\rangle$
$U_{\text{encode}}^{|0\rangle}$
X
Z
verification
classical computation for verification
(b)
$|0\rangle$
$U_{\text{encode}}^{|0\rangle}$
$|\bar{0}\rangle$
=
H
X
$|\bar{0}\rangle$

FIG. 15. (a) The level-$(l-1)$ circuit of the $|0\rangle$-state preparation gadget. (b) The encoding circuit $U_{\text{encode}}^{|0\rangle}$ for preparing the logical state $|\bar{0}\rangle$ of the Steane code from $|0\rangle^{\otimes 7}$ presented in Ref. [63].

to the decoding algorithm to calculate the measurement outcomes of the logical Z, which is the same procedure explained in the Z-basis measurement gadget. The measurement outcome is used to decide the correction operation for the quantum teleportation. The fault tolerance of the EC gadget defined by conditions (A16), (A17), and (A18) follows from transversality.

Appendix C: Pauli-gate gadgets for quantum LDPC codes

The Pauli-gate gadget for quantum LDPC codes is intended to perform a logical operation $\bar{P}$ acting on logical qubits in a code block of a Pauli-gate operation

$$P = \bigotimes_{k=1}^{K} P_k \in \tilde{\mathcal{P}}_K \tag{C1}$$

as in (75), where $P_k \in \{I, X, Y, Z\}$ is a Pauli operator acting on the k-th qubit. The construction of the gadget is shown in Fig. 18.

A logical Pauli operator $\bar{P}_k$ of P_k in (C1) is described as a tensor product of a N-qubit Pauli operator acting on physical qubits; thus, $\bar{P}$ can be described by a N-qubit Pauli operator as

$$\bar{P} = \bigotimes_{k=1}^{K} \bar{P}_k = \bigotimes_{k=1}^{K} \bigotimes_{n=1}^{N} P_{n,k} \in \tilde{\mathcal{P}}_N, \tag{C2}$$

where $\bar{P}_k = \bigotimes_{n=1}^{N} P_{n,k}$, and $P_{n,k} \in \{I, X, Y, Z\}$ is a Pauli operator acting on the n-th physical qubit.

When we perform a on-demand Pauli-gate gadget (80) for executing a two-register Clifford-gate abbreviation (78), we require an on-demand calculation of (C2). A classical computer receives a bitstring of a $2K$-bit string of the symplectic representation of a K-qubit Pauli operator $P \in \tilde{\mathcal{P}}_K$ in (C1) and outputs a $2N$-bit string of the symplectic representation of $\bar{P} \in \tilde{\mathcal{P}}_N$ in (C2). The runtime for calculating (C2) can be bounded in the following. Based on the input $2K$-bit string, we obtain K $2N$-bit strings, where the k-th $2N$-bit string is the symplectic representation of $\bar{P}_k$. Here, calculating (C2) corresponds to taking a sum of the K bitstrings as in (12). Thus, if for $n \in \{1, \ldots, N\}$, each n-th bit can be calculated simultaneously with $O(N)$ parallel processes, and the sums of the n-th positions of the K bitstrings

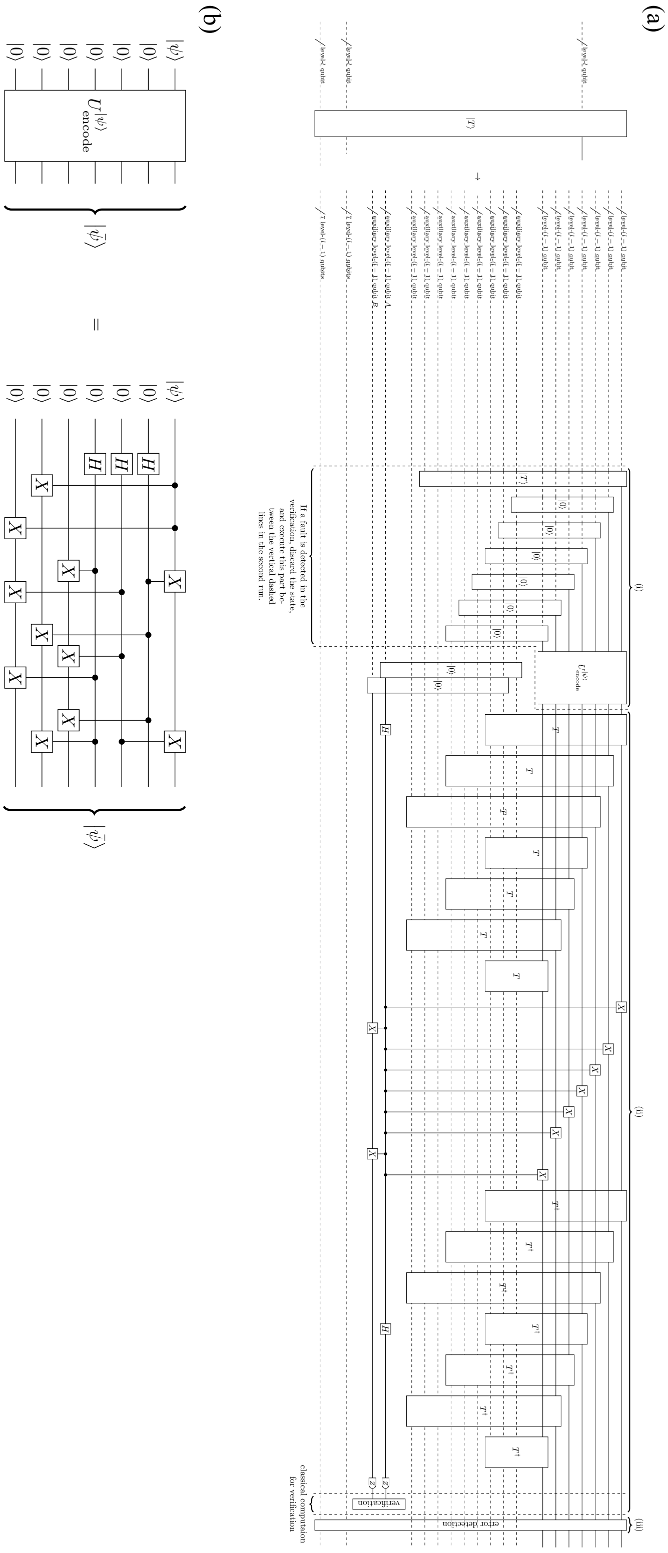

(a)
level-l qubit
level-(l − 1) qubit
|T⟩
|0⟩
$U^{|\psi\rangle}_{\text{encode}}$
T
T†
X
H
verification
error detection
If a fault is detected in the verification, discard the state, and execute this part between the vertical dashed lines in the second run.
classical computation for verification
(i)
(ii)
(iii)
(b)
|ψ⟩
|0⟩
=
$|\bar{\psi}\rangle$

FIG. 16. (a) The level-$(l-1)$ circuit of the $|T\rangle$-state preparation gadget. (b) The encoding circuit $U^{|\psi\rangle}_{\text{encode}}$ for preparing the logical state $|\bar{\psi}\rangle$ of the Steane code from $|\psi\rangle^{\otimes 7}$ presented in Ref. [63].

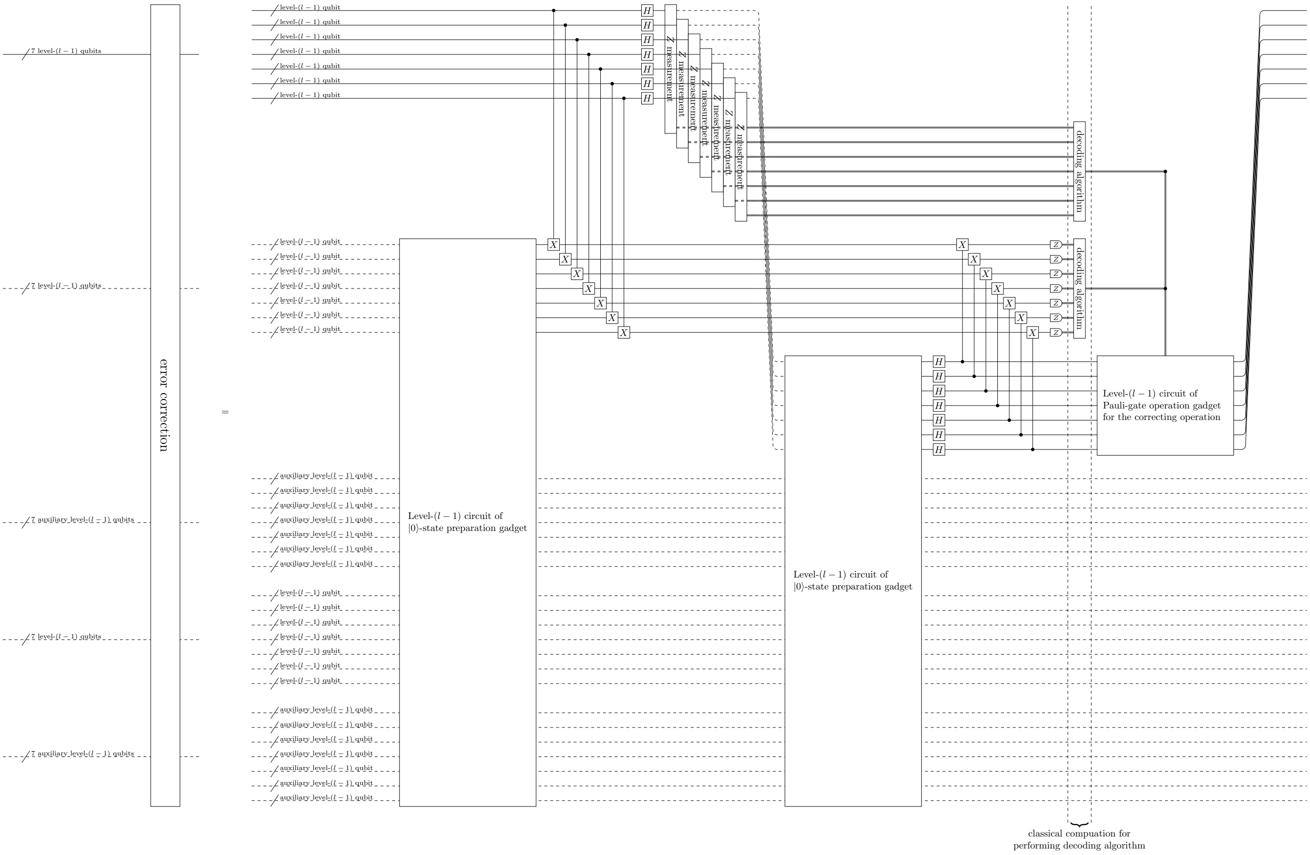

7 level-$(l-1)$ qubits
7 level-$(l-1)$ qubits
7 auxiliary level-$(l-1)$ qubits
7 level-$(l-1)$ qubits
7 auxiliary level-$(l-1)$ qubits
error correction
=
level-$(l-1)$ qubit
auxiliary level-$(l-1)$ qubit
H
X
Z
Z measurement
decoding algorithm
decoding algorithm
Level-$(l-1)$ circuit of $|0\rangle$-state preparation gadget
Level-$(l-1)$ circuit of $|0\rangle$-state preparation gadget
Level-$(l-1)$ circuit of Pauli-gate operation gadget for the correcting operation
classical compuation for performing decoding algorithm

FIG. 17. The level-$(l-1)$ circuit of the EC gadget.

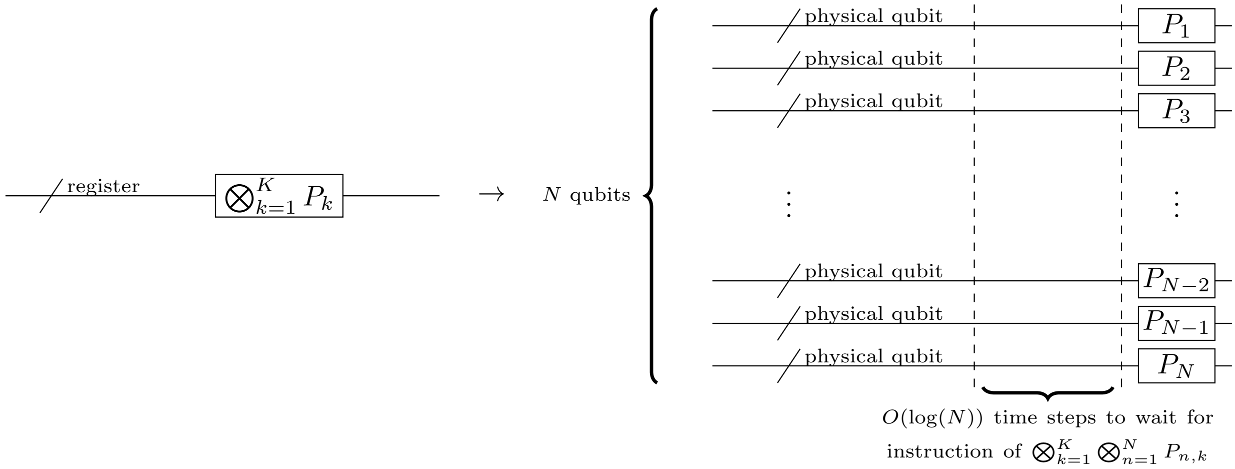


FIG. 18. A physical circuit of the gadget of the on-demand Pauli gate operation (80), where $P_i \in \{I, X, Y, Z\}$ for $i \in \{1, \ldots, N\}$ is a Pauli operator.

are computed with $O(K)$ parallel processes, i.e., using $O(NK) = O(N^2)$ parallel processes in total, we can perform this calculation in runtime

$$O(\log(N)). \tag{C3}$$

Therefore, the depth of the gadget is bounded by

$$O(\log N), \tag{C4}$$

where the dominat part is time steps to wait for calculating (C3), and the width of the gadget is bounded by

$$O(N). \tag{C5}$$

Experimental quantum kernel estimation enhanceed by single photons

Zhenghao Yin[1 2 *] Iris Agresti[1] Giovanni de Felice[3] Douglas Brown[3]
Alexis Toumi[3] Ciro Pentangelo[4 5] Simone Piacentini[5] Andrea Crespi[4 5]
Francesco Ceccarelli[5] Roberto Osellame[5] Bob Coecke[3] Philip Walther[1 6]

[1] *University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), Boltzmanngasse 5, Vienna A-1090, Austria*

[2] *University of Vienna, Faculty of Physics, Vienna Doctoral School of Physics (VDSP), Boltzmanngasse 5, Vienna A-1090, Austria*

[3] *Quantinuum, 17 Beaumont Street, Oxford OX1 2NA, UK*

[4] *Dipartimento di Fisica, Politecnico di Milano, piazza L. Da Vinci 32, 20133 Milano, Italy*

[5] *Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), piazza L. Da Vinci 32, 20133 Milano, Italy*

[6] *Christian Doppler Laboratory for Photonic Quantum Computer, Faculty of Physics, University of Vienna, 1090 Vienna, Austria*

Abstract. Quantum machine learning using qubit system attracts extreme research interest during the last decade, as it is does not require fault-tolerant quantum computer at the noisy intermediate-scale quantum era. In general, the theoretical and experimental works so far focus on universal quantum computation theory and solid state systems, for example superconducting qubits and trapped ions. Meanwhile, photon featuring long coherent time and convenient operation, has not been well studied in the term quantum machine learning. Here, we propose the quantum kernel estimation based on boson nature which is fundamental for other quantum machine learning protocols. In our experiment, we demonstrate the quantum kernel estimation using quantum interference which is extinct in photonic systems. Furthermore, we benchmark our methods with other classical kernel methods showing quantum kernel can outperform classical kernel methods at some datasets.

Keywords: quantum machine learning, quantum optics, integrated photonic circuits

1 Introduction

Quantum machine learning is potential advantageous in noisy quantum computers, for example variational quantum estimation for quantum Quantum approximate optimization algorithm for factorization, and quantum kernel estimation for classification. Besides, quantum kernel methods can map data points in the original space, which are hard to recognize, to a high-dimensional *feature space*. This nonlinear mapping can extract data features effectively and help the machine learning tasks. Once the suitable mapping is performed, it is possible to identify the hyperplane through a support vector machine [1] (SVM), according to the inner product of the mapped data. Such a hybrid classical-quantum model would benefit from the quantum feature maps that utilize the evolution of quantum systems, which can be hard to simulate on classical computers, and hence outsource the hardest part of the computation to the quantum hardware.

In this paper, we give an experimental demonstration of quantum kernel estimation, where data points are mapped in the feature space through the unitary evolution of two-boson Fock states (see Fig. 1). Such encoding can arbitrarily tune the dimension of the feature space and provide enough of a non-linearity to achieve a high classification accuracy with data which are only non-linearly classifiable. Furthermore, we show that for given tasks, this algorithm leads to an enhancement in the performance of quantum kernels with respect to their classical counterparts.

2 Photonic quantum kernel estimation

A kernel method relies on a function that maps N input data points x_i, from a space $\mathcal{X} \subseteq \mathbb{R}^d$ into a feature space $\mathcal{H}$. Here, d is the dimension of each data point. This is done through a feature map $\Phi : \mathcal{X} \to \mathcal{H}$. Then, a SVM can be used to produce a *prediction* function $f_K : \mathcal{X} \to \mathbb{R}$ as $f_K(x) = \sum_i \alpha_i K(x, x_i)$, where these α_i coefficients are obtained by solving a linear optimization problem. The inputs of the optimization are the labels y and the matrix obtained by computing the pairwise distances between data points is $K_{i,j} = K(x_i, x_j) = \langle \Phi(x_j) | \Phi(x_i) \rangle$, the so-called *Gram matrix*.

In this work, we implement a quantum version of the kernel method by sampling from the output probability distribution arising from the unitary evolution of a Fock input state. The pairwise distances are estimated between data points, which belong to a class y taking values $+1$ or -1. This process is depicted in Fig. 1a. Therefore, our feature map plugs the data that needs to be classified into the free parameters defining a unitary evolution applied to a fixed Fock state of dimension m and whose sum of occupational numbers is n: $x \mapsto |\Phi(x)\rangle = U_x|\psi\rangle$. Here, $|\psi\rangle$ is the encoding state which is free to choose. Then, as shown in Fig. 1c, the pairwise inner products of the feature points are experimentally evaluated, as $|\langle\psi|U(x_i)^\dagger U(x_j)|\psi\rangle|^2$. Such unitaries can be effectively implemented by a programmable photonic circuit

[*] zhenghao.yin@univie.ac.at

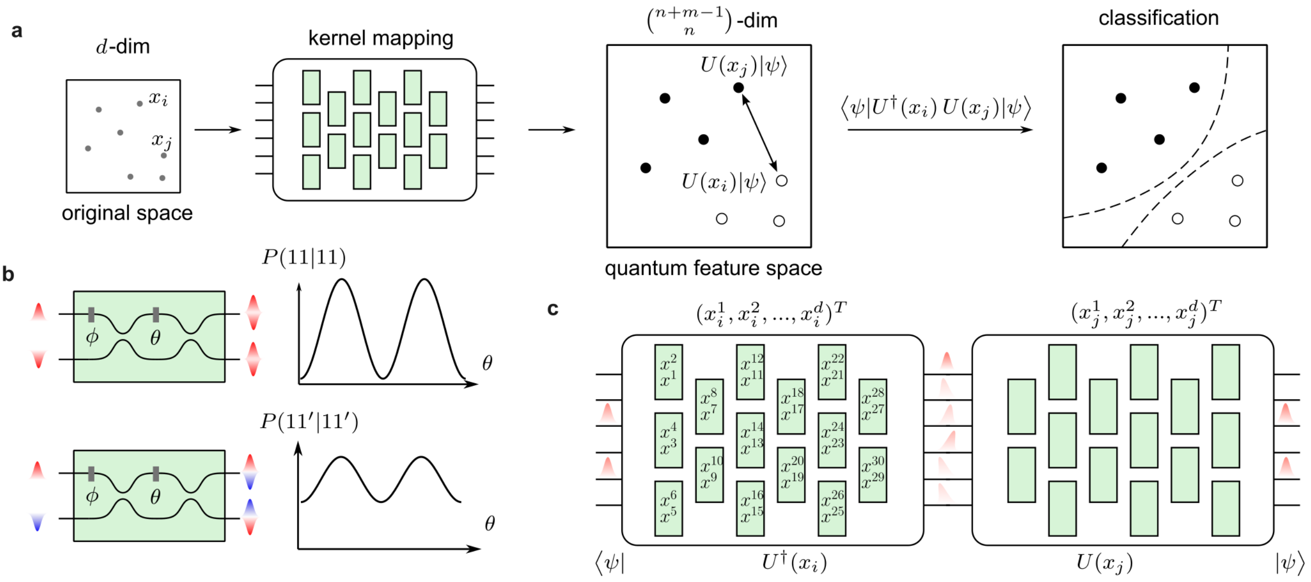


Figure 1: **Photonic quantum kernel estimation.** **a**. The photonic quantum kernel maps each data point x_i to be classified from a d-dimensional space into a quantum state $|\Phi\rangle_i$, living in a Hilbert feature space. In detail, the classical data x_i is encoded into a unitary evolution $U(x_i)$ applied on a fixed input state $|\psi\rangle$. After mapping all the data points in the dataset, we perform the classification finding the hyperplane best separating the classes, i.e. through a classical support vector machine (SVM). **b.** Pairs of indistinguishable photons and distinguishable photons show a different behavior when injected in a Mach-Zehnder interferometer (MZI). **c.** Estimation of the inner product of two data points x_i and x_j by encoding them in two unitaries $U(x_i)$ and $U(x_j)$.

consisting of an array of Mach-Zehnder interferometers (MZIs)[2]. At this point, the SVM finds the hyperplane separating the training data points through the aforementioned optimization process [3, 4] and, at the end, the binary classification of unknown points x is given by the following relation:

$$y = \text{sign}\left(\sum_{i=1}^{N} \alpha_i y_i K(x, x_i)\right) \tag{1}$$

where α_i are, as before, the coefficients optimized in the training process and y_i is the class of the i-th point in the training. This model is defined *implicitly*, as the labels are assigned by weighted inner products of the encoded data points [5, 6, 7, 8, 9, 10, 11, 12, 13].

If the Fock state contains indistinguishable bosons, they will exhibit quantum interference, as shown in Fig. 1b. In this case, the output probability distribution is given by the permanents of sub-matrices of the matrix representing the unitary evolution of the input [14]. More specifically, considering an input configuration s, the probability of detecting the output configuration t is given by $|\text{per}(U_{s,t})|^2/\Pi_i^m s_i!\Pi_i^m t_i!$. Here, per$(\cdot)$ denotes the permanent matrix operation, s_i and t_i are the occupational numbers at the i-th mode and $U_{s,t}$ is the sub-matrix obtained by selecting the rows/columns corresponding to the occupied modes of the input/output Fock states. On the other hand, if the bosons are distinguishable, they will not exhibit quantum interference. In this case the probability will amount to $\text{per}(|U_{s,t}|^2)/\Pi_i^m s_i!\Pi_i^m t_i!$.

3 Experiment and Results

In our experiment, we adopt a programmable integrated photonic processor containing laser-written waveguides and 27 thermal phase phases shifters as shown in Fig .2a. By arranging the Mach-Zehnder interferometer, it is able to perform any arbitrary 6x6 unitary matrices. The two photons are generated by a ppKTP nonlinear crystal and yield 97% on-chip indistinguishability. After evolution on the chip, all the output photons are detected by 6 superconducting nanowire single photon detectors and sequentially recorded in 15 different coincidence counting.

We test the performance of two photonic kernels in several different configurations. Firstly, we consider two different inputs, $|1,1,0,0,0,0\rangle$ and $|0,0,1,1,0,0\rangle$. Second, we are able to tune the indistinguishability to implement the quantum kernel and the coherent kernel.

For both input states, we test datasets of four different sizes: 40, 60, 80 and 100. We use the setup depicted in Fig.2a to evaluate all of the pairwise products between the unitaries $U(x_i)^\dagger U(x_j)$. Hence, $|\langle\psi|U(x_i)^\dagger U(x_j)|\psi\rangle|^2$ is given by the probability of detecting the photons on the same modes from which they were injected.

For each dataset, we use 2/3 of the data points for the training of the SVM, and the remaining 1/3 as a test set. The accuracy is defined as the number of correctly classified points over the total size of the test set. Let us note that values lower than 0.5 indicate that the model was not able to learn the features of the training set and generalize to unknown data.

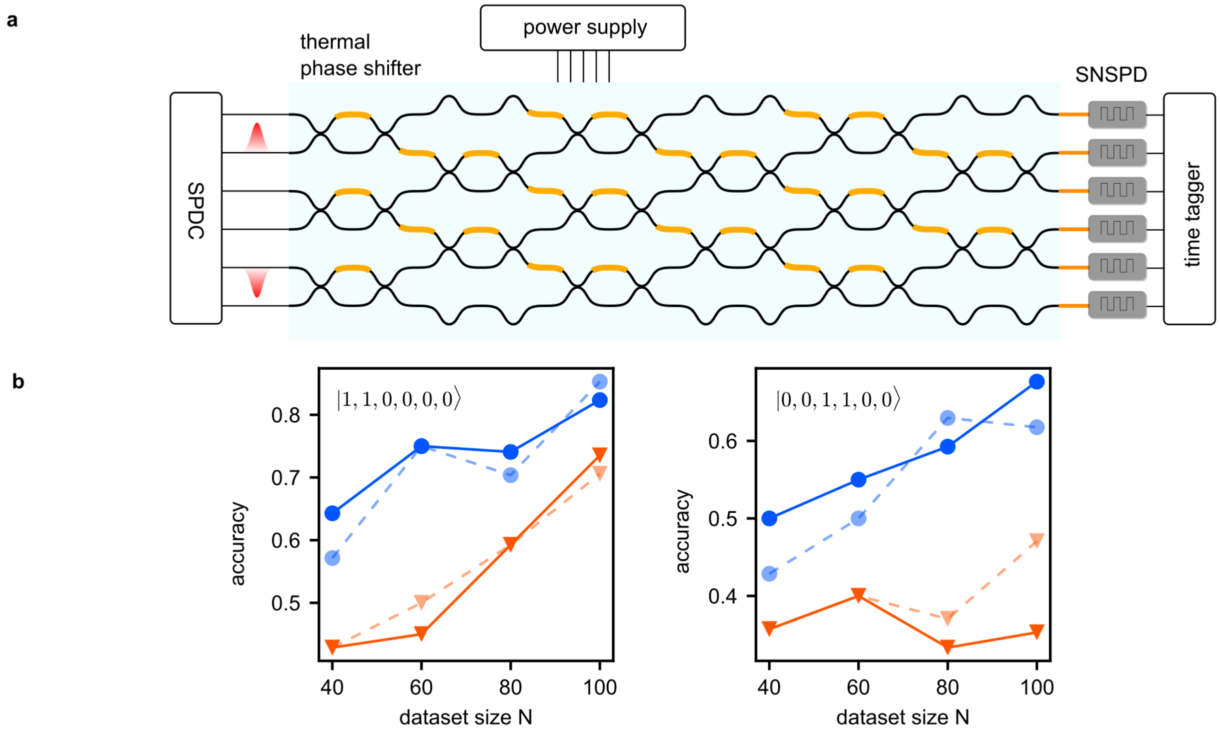


Figure 2: **Implementation of photonic quantum kernel estimation. a.** Experimental setup consisting of two parts, the off-chip single photon source and the programmable integrated photonic processor. **b.** We tested our method on datasets of different sizes (40, 60, 80, 100) and for two different input states ($|1,1,0,0,0,0\rangle$ and $|0,0,1,1,0,0\rangle$) respectively.

In Fig. 2b, we show the test accuracies obtained by injecting two input states for four different dataset sizes, where the quantum kernel performs significantly better than the coherent kernel at both experiments. The dashed lines indicate the results of numerical simulations, while the solid lines indicate experimental results.

4 Discussion

In this work, we show the first experimental demonstration of quantum kernel estimation, based on the unitary evolution of Fock states through an integrated photonic processor. In our implementation, data is mapped into a feature space by encoding it into the evolution of a fixed two-photon input state over six modes. The sampled output distribution is then fed into an SVM, which performs the classification. To achieve this, we adopt an integrated photonic processor realized by femtosecond laser writing in a borosilicate glass substrate [15].

Our method can find a wide range of promising near-term applications in quantum machine learning tasks such as information retrieval, natural language processing and medical image classification [16, 17, 18, 19], where kernel methods have been proposed a foundational keystone [20]. Our experimental results demonstrate that our quantum-enhanced kernels can outperform classical ones on datasets resulting from quantum observations, it also opens the door to hybrid methods where photonic processors are used to enhance the performance of deep neural networks.

References

[1] Cortes, C. & Vapnik, V. Support-vector networks. *Machine learning* **20**, 273–297 (1995).

[2] Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walsmley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460 (2016). ArXiv: 1603.08788.

[3] Boser, B. E., Guyon, I. M. & Vapnik, V. N. A training algorithm for optimal margin classifiers. In *Proceedings of the fifth annual workshop on Computational learning theory*, 144–152 (1992).

[4] Vapnik, V. *The nature of statistical learning theory* (Springer science & business media, 1999).

[5] Schuld, M. Supervised quantum machine learning models are kernel methods. *arXiv preprint arXiv:2101.11020* (2021).

[6] Lloyd, S., Schuld, M., Ijaz, A., Izaac, J. & Killoran, N. Quantum embeddings for machine learning 1–11 (2020). ArXiv: 2001.03622.

[7] Kübler, J. M., Buchholz, S. & Schölkopf, B. The Inductive Bias of Quantum Kernels (2021). ArXiv:2106.03747 [quant-ph, stat].

[8] Bartkiewicz, K. *et al.* Experimental kernel-based quantum machine learning in finite feature

space. *Scientific Reports* **10**, 1–9 (2020). ArXiv: 1906.04137 Publisher: Nature Publishing Group UK ISBN: 0123456789.

[9] Huang, H. Y., Kueng, R. & Preskill, J. Information-Theoretic Bounds on Quantum Advantage in Machine Learning. *Physical Review Letters* **126**, 190505 (2021). ArXiv: 2101.02464 Publisher: American Physical Society.

[10] Kusumoto, T., Mitarai, K., Fujii, K., Kitagawa, M. & Negoro, M. Experimental quantum kernel trick with nuclear spins in a solid. *npj Quantum Information* **7**, 94 (2021).

[11] Haug, T., Self, C. N. & Kim, M. Quantum machine learning of large datasets using randomized measurements. *arXiv preprint arXiv:2108.01039* (2021).

[12] Schölkopf, B. & Smola, A. J. *Learning with kernels: support vector machines, regularization, optimization, and beyond* (MIT press, 2002).

[13] Jerbi, S. *et al.* Quantum machine learning beyond kernel methods. *Nature Communications* **14**, 517 (2023).

[14] Scheel, S. Permanents in linear optical networks. *arXiv preprint quant-ph/0406127* (2004).

[15] Pentangelo, C. *et al.* High-fidelity and polarization-insensitive universal photonic processors fabricated by femtosecond laser writing. *Nanophotonics* (2024). Publisher: De Gruyter.

[16] Wang, X., Du, Y., Luo, Y. & Tao, D. Towards understanding the power of quantum kernels in the NISQ era. *Quantum* **5**, 531 (2021).

[17] Yu, C.-H., Gao, F., Wang, Q.-L. & Wen, Q.-Y. Quantum algorithm for association rules mining. *Physical Review A* **94**, 042311 (2016).

[18] Lorenz, R., Pearson, A., Meichanetzidis, K., Kartsaklis, D. & Coecke, B. QNLP in Practice: Running Compositional Models of Meaning on a Quantum Computer. *ArXiv e-prints* (2021). 2102.12846.

[19] Landman, J. *et al.* Quantum Methods for Neural Networks and Application to Medical Image Classification. *Quantum* **6**, 881 (2022).

[20] Schuld, M. & Petruccione, F. Quantum Models as Kernel Methods. In Schuld, M. & Petruccione, F. (eds.) *Machine Learning with Quantum Computers*, Quantum Science and Technology, 217–245 (Springer International Publishing, Cham, 2021).

Experimental quantum-enhanced kernels on a photonic processor

Zhenghao Yin,[1, 2, *] Iris Agresti,[1, †] Giovanni de Felice,[3] Douglas Brown,[3] Alexis Toumi,[3] Ciro Pentangelo,[4, 5] Simone Piacentini,[5] Andrea Crespi,[4, 5] Francesco Ceccarelli,[5] Roberto Osellame,[5] Bob Coecke,[3] and Philip Walther[1, 6, ‡]

[1] *University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), Boltzmanngasse 5, Vienna A-1090, Austria*
[2] *University of Vienna, Faculty of Physics, Vienna Doctoral School of Physics (VDSP), Boltzmanngasse 5, Vienna A-1090, Austria*
[3] *Quantinuum, 17 Beaumont Street, Oxford OX1 2NA, UK*
[4] *Dipartimento di Fisica, Politecnico di Milano, piazza L. Da Vinci 32, 20133 Milano, Italy*
[5] *Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), piazza L. Da Vinci 32, 20133 Milano, Italy*
[6] *Christian Doppler Laboratory for Photonic Quantum Computer, Faculty of Physics, University of Vienna, 1090 Vienna, Austria*

In recent years, machine learning has had a remarkable impact on standard computation, with applications ranging from scientific to everyday-life scopes. Meanwhile, as the complexity of the addressed task grows, energy consumption and computational power requirements become a bottleneck. In this context, it has been shown that quantum (or quantum-inspired) computation might lower the amount of required resources. However, whether such enhancements can be achieved with state-of-the-art quantum technologies and for practically relevant tasks is still an open question. Here, we demonstrate a kernel method on a photonic integrated processor to perform a binary classification task, by exploiting quantum interference. We benchmark our protocol against standard algorithms and show that it outperforms them for the given tasks. A significant improvement with respect to standard algorithms is shown, even in a regime that does not display quantum interference and exploits only the coherence of single photons. This implies that we do not need entangling gates and can readily raise the dimension of our system through additional circuit modes and/or injected photons. Our result opens the way to more efficient computing algorithms and for the formulation of tasks where quantum effects enhance the effectiveness of standard methods.

INTRODUCTION

The past decades have witnessed a swift development of technologies based on quantum mechanical phenomena, which have opened up new perspectives in a wide spectrum of applications. These range from the realization of a global-scale quantum communication network, the Quantum Internet [1, 2], to the simulation of quantum systems [3], to quantum computing [4]. In particular, the interest towards the last field has been fueled by some milestone discoveries, such as Shor's factorization and Grover's search algorithm [5, 6], which have promised that quantum processors can outperform their classical counterparts. However, a clear advantage of quantum computation has been experimentally demonstrated only recently and on different computational tasks, boson sampling [7–12] and random circuit sampling [13], which do not have clear practical applications.

Given these premises, it is crucial to investigate the tasks in which quantum computing can bring added value and enhance the operation of classical computers. Moreover, the question is whether this can be achieved for problems that are now within the reach of state-of-art technology, where only noisy intermediate-scale quantum computers are available [14, 15]. In this context, a flurry of interest has been devoted to the open question of whether the new paradigm of quantum computing can have an impact on machine learning [16–18], which has revolutionized classical computation, granting new possibilities and changing our everyday lives, from email filtering to artificial intelligence. The two main directions that have been investigated are, on one side, whether quantum computation could improve the efficiency of the learning process, allowing us to find better optima with the need of a lower number of inquiries [19–22] and, on the other, how quantum behaviours can enhance the expressivity of the input encoding, exploiting correlations between variables that are hard to reproduce through classical computation [23, 24]. In particular, regarding the latter aspect, a straightforward application of quantum computing on kernel models has become evident. Kernel methods are widely used tools in machine learning [25, 26], that base their functioning on the fact that patterns for data points, which are hard to recognize in their original space, can become easy to identify once nonlinearly mapped to a (high-dimensional) *feature space*. Once the suitable mapping is performed, it is possible to identify the hyperplane which best separates the classes of feature data points, through a support vector machine [27] (SVM), according to the inner product of the mapped data. Let us note that the only part of the

[*] zhenghao.yin@univie.ac.at
[†] iris.agresti@univie.ac.at
[‡] philip.walther@univie.ac.at

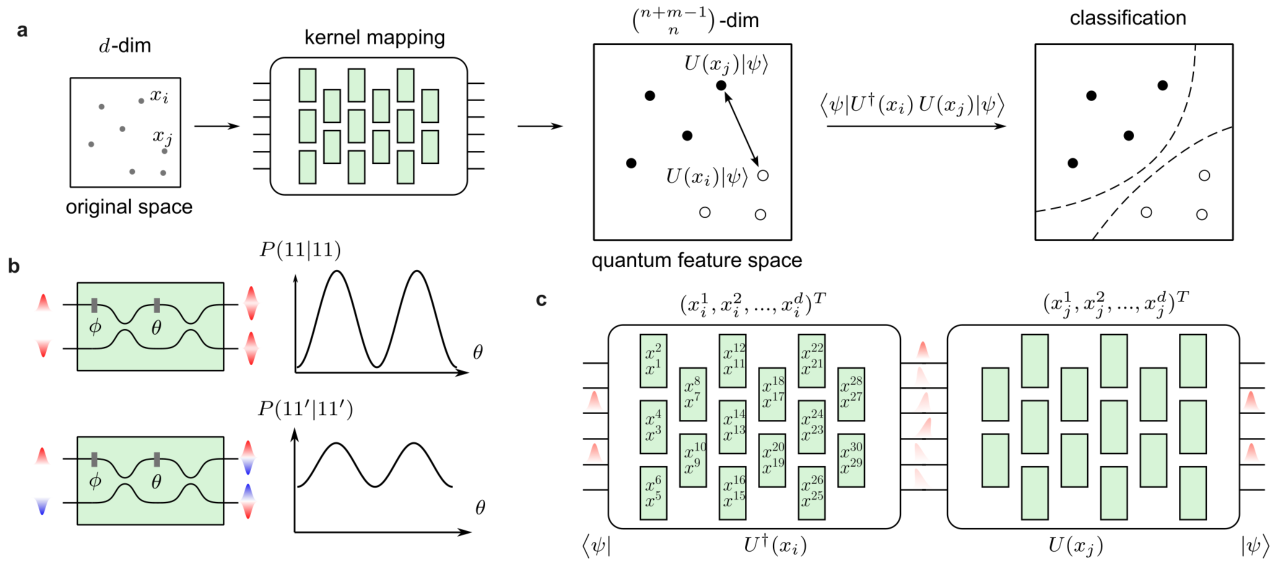

a
d-dim
x_i
x_j
original space
kernel mapping
$\binom{n+m-1}{n}$-dim
$U(x_j)|\psi\rangle$
$U(x_i)|\psi\rangle$
quantum feature space
$\langle\psi|U^\dagger(x_i)\,U(x_j)|\psi\rangle$
classification
b
ϕ
θ
$P(11|11)$
θ
$P(11'|11')$
θ
c
$(x_i^1, x_i^2, ..., x_i^d)^T$
$(x_j^1, x_j^2, ..., x_j^d)^T$
x^1 x^2 x^3 x^4 x^5 x^6 x^7 x^8 x^9 x^{10} x^{11} x^{12} x^{13} x^{14} x^{15} x^{16} x^{17} x^{18} x^{19} x^{20} x^{21} x^{22} x^{23} x^{24} x^{25} x^{26} x^{27} x^{28} x^{29} x^{30}
$\langle\psi|$
$U^\dagger(x_i)$
$U(x_j)$
$|\psi\rangle$

FIG. 1. **Photonic quantum kernel estimation. a**. The photonic quantum kernel maps each data point x_i to be classified from a d-dimensional space into a quantum state $|\Phi\rangle_i$, living in a Hilbert feature space. In detail, the classical data x_i is encoded into a unitary evolution $U(x_i)$ applied on a fixed input state $|\psi\rangle$. This implies $|\Phi\rangle_i = U(x_i)|\psi\rangle$. After mapping all the data points in the dataset, from the inner pairwise products, we perform the classification finding the hyperplane best separating the classes, i.e. through a classical support vector machine (SVM), according to Eq. (1). **b.** Pairs of indistinguishable photons and distinguishable photons show a different behaviour when injected in a Mach-Zehnder interferometer (MZI). Here, input states 11 and 11$'$ indicate, respectively, two indistinguishable and distinguishable photons being injected in the circuit and being detected at the output modes. **c.** Estimation of the inner product of two data points x_i and x_j by encoding them in two unitaries $U(x_i)$ and $U(x_j)$. The inner product $\langle\phi_j|\phi_i\rangle$ amounts to $\langle\psi|U^\dagger(x_i)U(x_j)|\psi\rangle$. This is equivalent to projecting the evolved state $U^\dagger(x_j)U(x_i)|\psi\rangle$ onto $|\psi\rangle$. Each box represents a programmable MZI with two free parameters (namely a beam splitter with tunable reflectivity and phase), as shown in **b**.

model that is trained is the SVM, whose training and resulting classification can be performed efficiently, once the inner products are available. Hence, an interesting question is whether using a quantum apparatus to perform the data mapping and evaluate the inner products among the resulting feature points can lead to an enhanced performance. Such a hybrid classical-quantum model would benefit, on one hand, from the quantum feature maps that result from the evolution of quantum systems (which can be hard to simulate on classical computers) and, on the other, it would outsource the hardest part of the computation to the quantum hardware. This question was theoretically answered in the affirmative by [28], where a machine learning task inspired by cryptography was constructed that is provably hard for classical computers to learn and can be solved efficiently with a quantum kernel. However, the implementation of this task remains far out of reach for current experimental capabilities. Moreover, a risk that one encounters in quantum kernel estimation is that, once the feature space is too large, all data points are mapped into orthogonal states, resulting in an ineffective classification. Hence, a moderately-sized quantum feature space can prove more suitable, to preserve the similarity among data belonging to the same class.

In this paper, we give an experimental demonstration of quantum kernel estimation, where data points are mapped in the feature space through the unitary evolution of two-boson Fock states (see Fig. 1). Such encoding allows us to arbitrarily tune the dimension of the feature space and, even for relatively small dimensions, it provides enough of a non-linearity to achieve a high classification accuracy with data which are only non-linearly classifiable.

Furthermore, we show that for given tasks, this algorithm leads to an enhancement in the performance of quantum kernels with respect to their classical counterparts. These tasks were selected by maximizing the so-called *geometric difference*, which measures the separation in performance between a pair of kernels [29]. To experimentally demonstrate this method, we exploit a photonic platform and, in particular, an integrated photonic processor [30] where we inject two-boson Fock states to map the data to be classified (see Fig. 1a). This photonic platform is particularly suitable for this task, as it allows us to encode and manipulate our input data with high fidelity.

To benchmark our enhanced performance, we compare

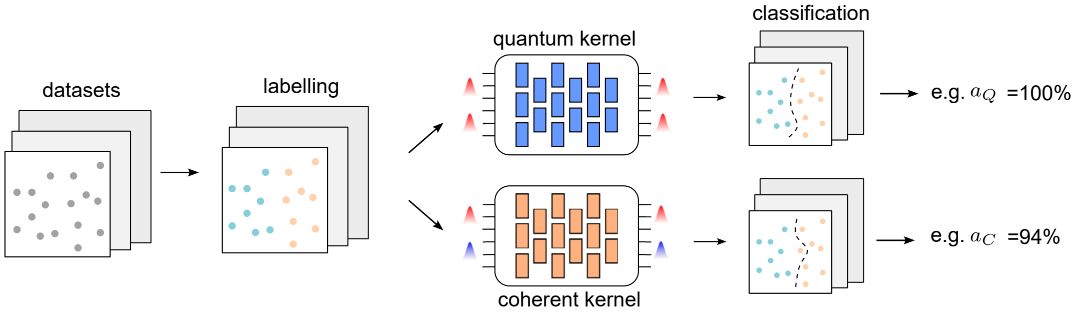


FIG. 2. **Classification tasks for photonic kernel methods.** The datasets are randomly generated and consist in d-dimensional vectors, with entries between 0 and 1. Then, we randomly assign labels to each point as belonging to class +1 or -1 and we test the ability of our photonic kernels, displaying and not displaying quantum interference (respectively indicated as *quantum kernel* and *coherent kernel*), to correctly classify the data. This is quantified by the accuracy of our models, which we indicate as a_Q and a_C.

our classification accuracies to the case in which the photonic inputs display no quantum interference, that is using distinguishable photons [31]. We also compare to conventional kernels, including Gaussian and polynomial kernels [25], optimizing their performance by using a grid search over their hyperparameters. We show that for given tasks, both the photonic kernels, with and without quantum interference, outperform standard methods.

PHOTONIC QUANTUM KERNEL ESTIMATION

A kernel method relies on a function that maps N input data points x_i, on which we wish to perform binary classification, from a space $\mathcal{X} \subseteq \mathbb{R}^d$ into a feature space $\mathcal{H}$. Here, d is the dimension of each data point. This is done through a feature map $\Phi : \mathcal{X} \to \mathcal{H}$. Then, a SVM can be used to produce a *prediction* function $f_K : \mathcal{X} \to \mathbb{R}$ as $f_K(x) = \sum_i \alpha_i K(x, x_i)$, where these α_i coefficients are obtained by solving a linear optimization problem. The inputs of the optimization are the labels y and the matrix obtained by computing the pairwise distances between data points is $K_{i,j} = K(x_i, x_j) = \langle\Phi(x_j)|\Phi(x_i)\rangle$, the so-called *Gram matrix* (for further information about kernel methods, see Supplementary Note 1).

In this work, we implement a quantum version of the kernel method, in which the aforementioned pairwise distances between data points, which belong to a class y taking values +1 or −1, are estimated by sampling from the output probability distribution arising from the unitary evolution of a Fock input state. This process is depicted in Fig. 1a. Therefore, our feature map plugs the data that needs to be classified into the free parameters defining a unitary evolution applied to a fixed Fock state of dimension m and whose sum of occupational numbers is n: $x \mapsto |\Phi(x)\rangle = U_x|\psi\rangle$. Here, $|\psi\rangle$ is the encoding state which is free to choose. Then, as shown in Fig. 1c, the pairwise inner products of the feature points are experimentally evaluated, as $|\langle\psi|U(x_i)^\dagger U(x_j)|\psi\rangle|^2$. Such unitaries can be effectively implemented by a programmable photonic circuit consisting of an array of Mach-Zehnder interferometers (MZIs)[32]. Hence, the dimension of the feature Hilbert space $\mathcal{H}$ will be $\binom{n+m-1}{n}$. At this point, the SVM finds the hyperplane separating the training data points through the aforementioned optimization process [33, 34] and, at the end, the binary classification of unknown points x is given by the following relation:

$$y = \text{sign}\left(\sum_{i=1}^{N} \alpha_i y_i K(x, x_i)\right) \quad (1)$$

where α_i are, as before, the coefficients optimized in the training process and y_i is the class of the i-th point in the training. This model is defined *implicitly*, as the labels are assigned by weighted inner products of the encoded data points [35–43].

If the Fock state contains indistinguishable bosons, they will exhibit quantum interference, as shown in Fig. 1b. In this case, the output probability distribution, which in general is hard to compute on classical processors, is given by the permanents of sub-matrices of the matrix representing the unitary evolution of the input [44]. More specifically, considering an input configuration s, the probability of detecting the output configuration t is given by $|\text{per}(U_{s,t})|^2/\Pi_i^m s_i!\Pi_i^m t_i!$. Here, per($\cdot$) denotes the permanent matrix operation, s_i and t_i are the occupational numbers at the i-th mode and $U_{s,t}$ is the sub-matrix obtained by selecting the rows/columns corresponding to the occupied modes of the input/output Fock states. On the other hand, if the bosons are distinguishable, they will not exhibit quantum interference and their output distribution is always efficiently computable [7, 10, 11, 45]. In this case the probability will amount to per($|U_{s,t}|^2$)$/\Pi_i^m s_i!\Pi_i^m t_i!$.

In the following, we will refer to a kernel implemented with indistinguishable bosons as a *quantum kernel*, K_Q, and with distinguishable ones as a *coherent kernel*, K_C.

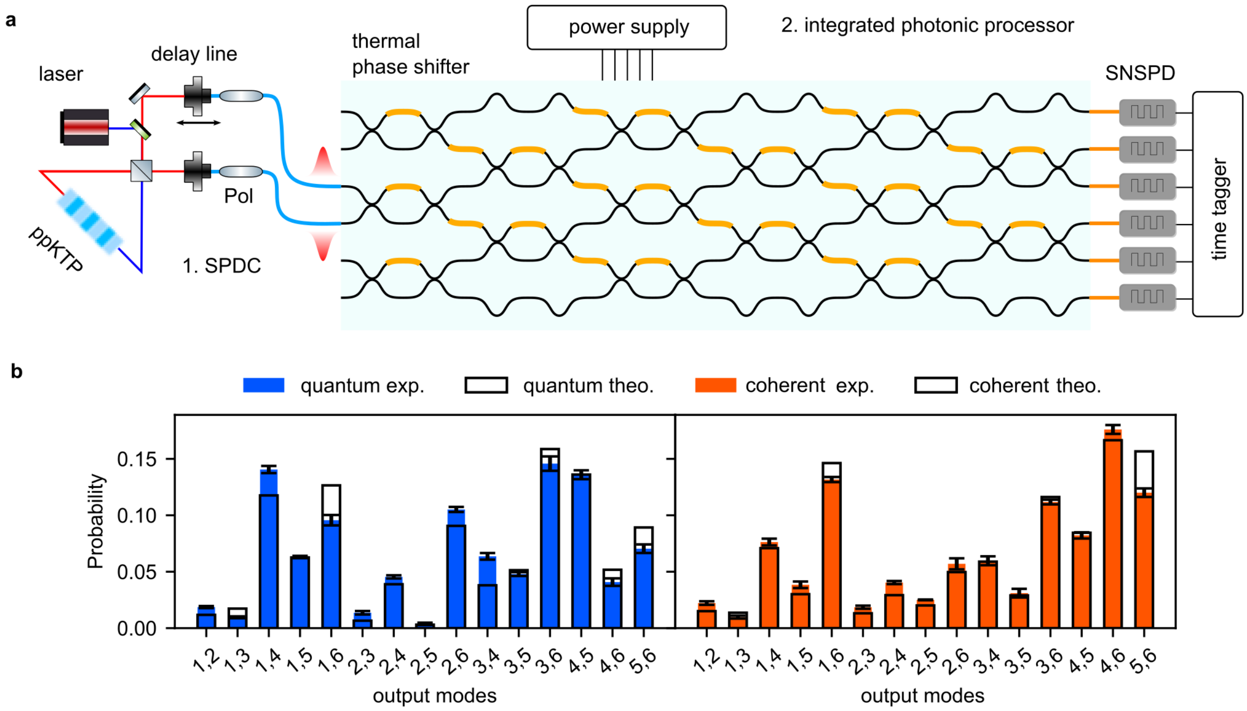


FIG. 3. **Implementation of photonic quantum kernel estimation. a.** Experimental setup consisting of two parts, the off-chip single photon source and the programmable integrated photonic processor. The frequency degenerate photons are generated by a type-II spontaneous parametric down-conversion source. Afterwards, the two photons are made indistinguishable in their polarization and arrival time. Then, we inject these photons in two modes of an integrated photonic processor with 6 input/output modes [30]. Detection is performed by superconducting nanowire single-photon detectors (SNSPDs). The degree of indistinguishability can then be tuned through a delay line, changing their relative temporal delay. **b.** Probability distribution of photon detection events. We show two instances of the experimental photon detection probability, compared to the theoretical calculation. The quantum and coherent kernel measurements are obtained respectively by injecting two indistinguishable and distinguishable photons into the third and fourth modes of the circuits, i.e. $|0,0,1,1,0,0\rangle$. The x axis shows all the circuit channels which output two photons simultaneously. Thus, all 15 possible photon detection configurations are accessible.

CLASSIFICATION TASK

To select a classification task that would benefit from the described model, we use a quantifier called the *geometric difference* [29], which compares two kernels K_a and K_b, which we will denote as $g_{a,b}$. Given a set of data points $\{x_i | x_i \in \mathcal{X}\}$ without any labels, the geometric difference provides the binary labels $\{y_i\}$ that maximise the expected difference in prediction error between two kernels – in our case, we consider K_Q and K_C, as depicted in Fig. 2. Therefore, we obtain this optimal labelling by solving the following minimisation problem:

$$y^\star = \arg\min_{y\in\mathbb{R}^d}\left(\frac{s_{K_Q}(y)}{s_{K_C}(y)}\right) \qquad (2)$$

where $s_K(y) = y^T K y$ is the model complexity of the pair K and y, i.e. the number of features that the model needs to make accurate predictions (see the Supplementary Note 2). To saturate the following inequality [29]:

$$\exists y \quad \cdot \quad s_{K_C}(y) \quad \leq \quad g^2_{CQ}\, s_{K_Q}(y) \qquad (3)$$

we take $y^T K_C^{-1} y = g^2_{CQ} y^T K_Q^{-1} y$, and obtain the relation

$$g_{CQ} = \sqrt{\left\|\sqrt{K_Q}\,(K_C)^{-1}\sqrt{K_Q}\right\|_\infty} \qquad (4)$$

where $\|\cdot\|_\infty$ denotes the spectral norm and g_{CQ} is the so-called *geometric difference.*

We can now use Eq. (4) to generate the classification task that, given a pair of kernels K_Q, K_C and a set of data points $\{x_i\}$, produces the labels $\{y_i\}$ that maximise the difference in prediction error bound. This can be done through the following procedure: (i) evaluate the Gram matrices K_Q and K_C over a set of non-labelled data points $\{x_i\}$; (ii) compute the positive definite matrix $M = \sqrt{K_Q}\,(K_C)^{-1}\sqrt{K_Q}$; (iii) compute the eigenvalues and eigenvectors of M by spectral decomposition; (iv) find the maximum eigenvalue g and its corresponding eigenvector v; (v) assign the labels $y = \sqrt{K_Q}v$. From a practical point of view, we start with the two aforementioned kernels, K_C and K_Q, and then, by maximizing the geometric difference, we find the tasks for which the latter brings an enhanced accuracy of the classification. For more details regarding the algorithm to define the classification task, see the Supplementary Note 4. Let us note that the implemented tasks constitute instances of problems that can be naturally implemented with high accuracy on our quantum platform. As such they constitute a first stepping stone towards the identification of practical tasks for which quantum machine learning can enhance the performance of classical models.

EXPERIMENT

Our experimental setup consists of two parts, a single-photon source generating the input states and a programmable integrated photonic processor depicted in Fig. 3a. First, to generate the input state, we use a type II spontaneous parametric down-conversion source, which generates frequency degenerate single-photon pairs at 1546 nm in a periodically poled K-titanyl phosphate crystal. The two photons are then made indistinguishable in their polarization and arrival time, respectively, via wave retarders and a delay line, which we also use to tune the degree of indistinguishability of the generated photons.

For the implementation of photonic kernels, which map our input data to a feature space, we require an apparatus able to perform arbitrary unitary transformations on a given input state. As mentioned before, our feature map sends each data point x_i onto the state resulting from the evolution $U(x_i)$ of a fixed input Fock state $|\psi\rangle$. Then, for the application of the SVM, which finds the best hyperplane separating the data, we need to evaluate the inner products between all of the points x_i, x_j in the feature space, which amounts to $\langle\psi|U(x_i)^\dagger U(x_j)|\psi\rangle$. This implies that, if we take $|\psi\rangle$ as a Fock state of n photons over m modes, the inner product $\langle\Phi(x_i)|\Phi(x_j)\rangle$ is given by projecting the evolved state $U(x_i)^\dagger U(x_j)\,|\psi\rangle$ onto $|\psi\rangle$.

To this aim, we employ an integrated photonic processor [30] fabricated on a borosilicate glass substrate, in which optical waveguides are inscribed through femtosecond laser writing [46–48]. The circuit features six input/output modes and it is based on a rectangular mesh of 15 programmable MZIs [32], as depicted in Fig. 3a. Each interferometer is equipped with two thermal phase shifters [49] in order to provide tunable reflectivity and phase. By properly choosing the values of the phase shifters, such arrangement allows us to perform any unitary transformation on the input photon states. Given this property, our device is also referred to as a universal photonic processor. Design, fabrication and calibration of the integrated photonic circuit are described in [30].

Specifically, the data were encoded in the values of the phase shifts, as follows: $x_i = (x_i^1, x_i^2, ..., x_i^{30}) \rightarrow \theta_i = (2\pi x_i^1, 2\pi x_i^2, ..., 2\pi x_i^{30})$, where θ_i are the phase shifts introduced by the phase shifters of a universal interferometer. This implies that, in principle, we would need a sequence of two of such circuits (as in the scheme of Fig. 1c), to first implement $U^\dagger(x_i)$ and then $U(x_j)$ on our inputs. However, in our implementation, we adopt only one universal circuit and directly implement the unitary corresponding to the product $U(x_i)^\dagger U(x_j)$. This reduces the experimental complexity and the propagation losses within the circuit itself.

At the output, detection is performed by superconducting nanowire single-photon detectors (SNSPDs). Due to the fact that these detectors are not photon-number resolving, we post-select the output events to those featuring two detectors clicking the *collision-free* events (see Supplemental Information Note 3). To test the role of quantum interference in the accuracy of the classification, we tune the indistinguishability of the two photons by changing their relative temporal delay. An instance of the probability distribution of the same unitary is shown in Fig. 3b, indicating the high experiment fidelity. The optimal classification task is chosen for each data set according to the algorithm explained in the previous section.

RESULTS

We test the performance of two photonic kernels in several different configurations. Firstly, we consider two different inputs, $|\psi_L\rangle = |1,1,0,0,0,0\rangle$ and $|\psi_C\rangle = |0,0,1,1,0,0\rangle$. This amounts to either injecting the photons into the first two modes or the central two modes. Second, we are able to tune the indistinguishability to implement the quantum kernel and the coherent kernel (see Supplementary Note 5). The maximal achieved indistinguishability between the photons is 0.9720±0.0044, by measuring the on-chip Hong-Ou-Mandel interference [50].

For both input states, we test datasets of four different sizes: 40, 60, 80 and 100. We then use the setup depicted in Fig.3a to implement all of the pairwise products between the unitaries $U(x_i)^\dagger U(x_j)$. Hence, $|\langle\psi|U(x_i)^\dagger U(x_j)|\psi\rangle|^2$ is given by the probability of detecting the photons on the same modes from which they were injected.

For each size N, we perform $N(N-1)/2$ unitaries to compute all of the inner products. The distance between the unitaries experimentally realized and the target ones can be estimated as $\sum_i \sqrt{P_i^{\text{theo}} \cdot P_i^{\text{exp}}}$, where P_i^{exp} is the experimental detection frequency for the i-th output configuration, while P_i^{theo} is the one estimated based on the theory[51]. The mean fidelity of all datasets is

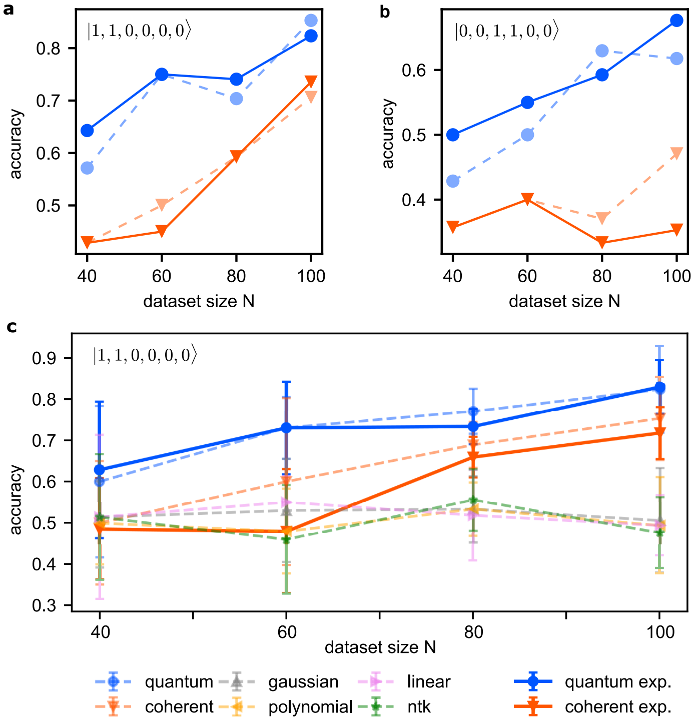


FIG. 4. **Experimental classification accuracies. a-b.** We tested our method on datasets of different sizes (from 40 to 200) and for two different input states ($|1,1,0,0,0,0\rangle$ and $|0,0,1,1,0,0\rangle$) respectively. For each dataset, 2/3 of the datapoints were used for training the support vector machine (SVM) and 1/3 for test. **c.** The average classification accuracies on 5 different sets for the quantum kernel (blue curves) and the coherent (orange curve) kernel, along with the following computational kernels: Gaussian (grey curve), polynomial (yellow) and linear (purple). The dashed line indicates the results of numerical simulations, while the solid ones the experimental results. The error bar shows the standard deviation of the classification accuracies on 5 datasets for all the kernels.

0.9816±0.0148 and 0.9934±0.0048, for the quantum kernel and coherent kernel respectively (for additional details regarding intermediate degrees of indistinguishability, see Supplementary Note 5). For each dataset, we use 2/3 of the data points for the training of the SVM, and the remaining 1/3 as a test set. The accuracy is defined as the number of correctly classified points over the total size of the test set. Let us note that values lower than 0.5 indicate that the model was not able to learn the features of the training set and generalize to unknown data.

In Fig. 4a and b, we show the test accuracies obtained by injecting two input states for four different dataset sizes, where the quantum kernel performs significantly better than the coherent kernel at both experiments. In Fig. 4c, we report the average test accuracy obtained for five different datasets with the same size, varying the dataset sizes from 40 to 100 as well. Moreover, the results obtained with the quantum kernel (blue curves) and the coherent kernel (orange curve) are compared with the following numerical kernels: Gaussian (grey curve), polynomial (yellow) and linear (purple). For the latter three kernel methods, we consider the maximal accuracy obtained by optimizing their hyperparameters (for further details, please see the Supplemental Information Note 4). Although the task is built only comparing the performance of the kernels based on indistinguishable and distinguishable photons, the obtained accuracy is higher also than commonly used classical kernels [25, 26]. The dashed lines indicate the results of numerical simulations, while the solid lines indicate experimental results.

DISCUSSION

In this work, we show the first experimental demonstration of quantum kernel estimation, based on the unitary evolution of Fock states through an integrated photonic processor. In our implementation, data is mapped into a feature space by encoding it into the evolution of a fixed two-photon input state over six modes. The sampled output distribution is then fed into an SVM, which performs the classification. To achieve this, we adopt an integrated photonic processor realized by femtosecond laser writing in a borosilicate glass substrate [30]. It is noteworthy that, although our apparatus only features linear optical elements, i.e. phase shifters and beam splitters, the chosen encoding produces a sufficient nonlinearity to achieve high accuracy in the classification of non-linearly separable datasets. This constitutes a difference of our method from implementations on superconducting qubits platforms, where entangling gates are typically needed for quantum kernel estimation [29, 52]. Furthermore, in our case, it is not necessary to increase the dimension of the feature Hilbert space to achieve a good accuracy. This is a crucial feature which allows us to avoid the typical difficulty of quantum kernels whereby all data points are encoded in orthogonal states, leading to null inner products and, therefore, to an ineffective classification [53]. Another novelty of our approach lies on the fact that we are not using the photonic platform to reproduce classical kernels, as in [54], because our kernel function is given by the natural evolution of bosons through a quantum circuit.

The task we implement is artificially designed by arbitrarily assigning binary labels to randomly generated data points, which we encode in the phase shifts introduced by an optical circuit. To assign the labels, we exploit as our metric the so-called *geometric difference*. This allows us to select the task for which the presence of quantum interference yields a better classification accuracy with respect to the case where the photons constituting the input state are fully distinguishable (and hence no interference is displayed). Despite the fact that the geometric difference compares the performance of a pair of kernels (in our case kernels implemented with indistinguishable versus distinguishable bosons), the selected tasks are performed significantly better by both the bosonic kernels than commonly used kernels, such as the Gaussian, polyonomial and linear ones. Our results indicate that, for these tasks, a kernel estimation performed on photonic hardware enhances the overall performance, even for medium-size problems, which are reachable by the state-of-art of quantum technologies. Moreover, the possibility of using distinguishable bosons to have a (smaller) performance enhancement represents an intriguing possibility, as it circumvents the difficulty of single photons states generation. This strategy can prove especially convenient to reduce the impact of photon losses on the experimental time required to collect significant statistics.

Despite being overshadowed by deep neural networks, kernels are still widely used in a large number of tasks, due to their simplicity, and ability to learn from small datasets [55, 56]. Indeed, they have also had a recent revival in classical machine learning, where they have been used as a theoretical framework that subsumes state-of-the-art neural network architectures such as transformers [57?]. Another recent trend, consists in merging neural networks and kernels, by introducing kernel-like layers inside the structure of neural networks. Notable examples are attention modules in natural language processing, and Hopfield layers [58].

Our method can find a wide range of promising near-term applications in quantum machine learning tasks such as information retrieval, natural language processing and medical image classification [59–62], where kernel methods have been proposed a foundational keystone [63]. Our experimental results demonstrate that our quantum-enhanced kernels can outperform classical ones on datasets resulting from quantum observations, it also opens the door to hybrid methods where photonic processors are used to enhance the performance of deep neural networks.

Moreover, these results open the way for further investigations related to the non-linearities that can be achieved through photonic platforms [64, 65], which are crucial elements for machine learning purposes and, in particular, for neuromorphic computation models, such as *reservoir computing* [66, 67]. This may be of particular importance when considering difficulties related to energy consumption, as it has been proved that partially optical networks can be adopted to reduce the overall energy requirements with respect to electronic ones [68]. In addition, we envisage further studies related to the combination of this kind of non-linearity with those brought by the implementation of feedback loops, as in the case of quantum memristor [69] and the exploitation of quantum interference in the implementation of feature maps.

ACKNOWLEDGEMENTS

The authors would like to thank Anna Pearson for her active involvement in the first stages of this project. This research was funded by the European Union Horizon 2020 and Horizon Europe research and innovation programme under grant agreement No 899368 (EPIQUS), and the Marie Skłodowska-Curie grant agreement No 956071 (AppQInfo), and the QuantERA II Programme under Grant Agreement No 101017733 (PhoMemtor). I.A. acknowledges financial support from the Österreichischer Wissenschaftsfonds FWF, through the ”Early-Stage Program: Research – Innovation – Training” post-doctoral fellowship No ESP 205-N (PREQUrSOR). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them. Further funding was received from the Austrian Science Fund (FWF) through BeyondC (F7113). Research Group 5 (FG5) and I 6002-N,; and from the Austrian Federal Ministry for Digital and Economic Affairs, the National Foundation for Research, Technology and Development and the Christian Doppler Research Association. G.d.F would like to thank Konstantinos Meichanetzidis and Tommaso Salvatori for insightful discussions on the project. The integrated photonic processor was partially fabricated at PoliFAB, the micro- and nanofabrication facility of Politecnico di Milano (https://www.polifab.polimi.it/). C.P., F.C. and

R.O. wish to thank the PoliFAB staff for the valuable technical support. For the purpose of open access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

AUTHOR CONTRIBUTIONS

Z.Y. and I.A. designed and conducted the experiment and G.d.F., D.B. and A.T. developed the theory and algorithm. C.P., S.P., A.C. and F.C. conducted the design, fabrication and calibration of the integrated photonic processor. Z.Y., I.A. and G.d.F. wrote the first draft of the manuscript. R.O., B.C. and P.W. supervised the whole project. All authors discussed the results and reviewed the manuscript.

COMPETING INTERESTS

F.C. and R.O. are cofounders of the company Ephos. The authors declare that they have no other competing interests.

[1] Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).

[2] Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018).

[3] Georgescu, I. M., Ashhab, S. & Nori, F. Quantum simulation. *Reviews of Modern Physics* **86**, 153 (2014).

[4] Nielsen, M. A. & Chuang, I. L. Quantum computation and quantum information. *Phys. Today* **54**, 60 (2001).

[5] Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, 124–134 (Ieee, 1994).

[6] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 212–219 (1996).

[7] Aaronson, S. & Arkhipov, A. The Computational Complexity of Linear Optics. *Proceedings of the 43rd annual ACM symposium on Theory of computing - STOC '11* **9**, 333 (2010). URL http://portal.acm.org/citation.cfm?doid=1993636.1993682. ArXiv: 1011.3245 Publisher: ACM Press Place: New York, New York, USA ISBN: 9781450306911.

[8] Zhong, H.-S. *et al.* Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).

[9] Madsen, L. S. *et al.* Quantum computational advantage with a programmable photonic processor. *Nature* **606**, 75–81 (2022).

[10] Tillmann, M. *et al.* Experimental boson sampling. *Nature Photonics* **7**, 540–544 (2013). ArXiv: 1212.2240.

[11] Broome, M. A. *et al.* Photonic Boson Sampling in a Tunable Circuit. *Science* **339**, 794–798 (2013). URL https://www.science.org/doi/abs/10.1126/science.1231440. Publisher: American Association for the Advancement of Science.

[12] Crespi, A. *et al.* Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nature Photonics* **7**, 545–549 (2013). URL https://www.nature.com/articles/nphoton.2013.112. Number: 7 Publisher: Nature Publishing Group.

[13] Arute, F. *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).

[14] Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 1–20 (2018). ArXiv: 1801.00862.

[15] Brooks, M. Before the quantum revolution. *Nature* **574**, 19–21 (2019).

[16] Biamonte, J. *et al.* Quantum machine learning. *Nature* **549**, 195–202 (2017).

[17] Wittek, P. *Quantum machine learning: what quantum computing means to data mining* (Academic Press, 2014).

[18] Dunjko, V. & Briegel, H. J. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics* **81**, 074001 (2018).

[19] Neven, H., Denchev, V. S., Rose, G. & Macready, W. G. Training a large scale classifier with the quantum adiabatic algorithm. *arXiv preprint arXiv:0912.0779* (2009).

[20] Rebentrost, P., Mohseni, M. & Lloyd, S. Quantum support vector machine for big data classification. *Physical review letters* **113**, 130503 (2014).

[21] Leifer, M. S. & Poulin, D. Quantum graphical models and belief propagation. *Annals of Physics* **323**, 1899–1946 (2008).

[22] Saggio, V. *et al.* Experimental quantum speed-up in reinforcement learning agents. *Nature* **591**, 1–12 (2021). URL http://dx.doi.org/10.1038/s41586-021-03242-7. Publisher: Springer US.

[23] Boixo, S. *et al.* Characterizing quantum supremacy in near-term devices. *Nature Physics* **14**, 595–600 (2018).

[24] Gan, B. Y., Leykam, D. & Angelakis, D. G. Fock state-enhanced expressivity of quantum machine learning models. *EPJ Quantum Technology* **9**, 16 (2022).

[25] Shawe-Taylor, J. & Cristianini, N. *Kernel methods for pattern analysis* (Cambridge university press, 2004).

[26] Hofmann, T., Schölkopf, B. & Smola, A. J. Kernel methods in machine learning (2008).

[27] Cortes, C. & Vapnik, V. Support-vector networks. *Machine learning* **20**, 273–297 (1995).

[28] Liu, Y., Arunachalam, S. & Temme, K. A rigorous and robust quantum speed-up in supervised machine learning. *Nature Physics* **17**, 1013–1017 (2021). URL http://dx.doi.org/10.1038/s41567-021-01287-z. ArXiv: 2010.02174 Publisher: Chapman and Hall/CRC ISBN: 9780429297595.

[29] Huang, H. Y. *et al.* Power of data in quantum machine learning. *Nature Communications* **12** (2021). URL http://dx.doi.org/10.1038/s41467-021-22539-9. ArXiv: 2011.01938 Publisher: Springer US.

[30] Pentangelo, C. *et al.* High-fidelity and polarization-insensitive universal photonic processors fabricated by femtosecond laser writing. *Nanophotonics* (2024). URL https://www.degruyter.com/document/doi/10.1515/nanoph-2023-0636/html. Publisher: De Gruyter.

[31] Renema, J. J. *et al.* Efficient Classical Algorithm for Boson Sampling with Partially Distinguishable Photons. *Physical Review Letters* **120**, 220502 (2018). URL https://doi.org/10.1103/PhysRevLett.120.220502. Publisher: American Physical Society.

[32] Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walsmley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460 (2016). ArXiv: 1603.08788.

[33] Boser, B. E., Guyon, I. M. & Vapnik, V. N. A training algorithm for optimal margin classifiers. In *Proceedings of the fifth annual workshop on Computational learning theory*, 144–152 (1992).

[34] Vapnik, V. *The nature of statistical learning theory* (Springer science & business media, 1999).

[35] Schuld, M. Supervised quantum machine learning models are kernel methods. *arXiv preprint arXiv:2101.11020* (2021).

[36] Lloyd, S., Schuld, M., Ijaz, A., Izaac, J. & Killoran, N. Quantum embeddings for machine learning 1–11 (2020). URL http://arxiv.org/abs/2001.03622. ArXiv: 2001.03622.

[37] Kübler, J. M., Buchholz, S. & Schölkopf, B. The Inductive Bias of Quantum Kernels (2021). URL http://arxiv.org/abs/2106.03747. ArXiv:2106.03747 [quant-ph, stat].

[38] Bartkiewicz, K. *et al.* Experimental kernel-based quantum machine learning in finite feature space. *Scientific Reports* **10**, 1–9 (2020). URL https://doi.org/10.1038/s41598-020-68911-5. ArXiv: 1906.04137 Publisher: Nature Publishing Group UK ISBN: 0123456789.

[39] Huang, H. Y., Kueng, R. & Preskill, J. Information-Theoretic Bounds on Quantum Advantage in Machine Learning. *Physical Review Letters* **126**, 190505 (2021). URL https://doi.org/10.1103/PhysRevLett.126.190505. ArXiv: 2101.02464 Publisher: American Physical Society.

[40] Kusumoto, T., Mitarai, K., Fujii, K., Kitagawa, M. & Negoro, M. Experimental quantum kernel trick with nuclear spins in a solid. *npj Quantum Information* **7**, 94 (2021).

[41] Haug, T., Self, C. N. & Kim, M. Quantum machine learning of large datasets using randomized measurements. *arXiv preprint arXiv:2108.01039* (2021).

[42] Schölkopf, B. & Smola, A. J. *Learning with kernels: support vector machines, regularization, optimization, and beyond* (MIT press, 2002).

[43] Jerbi, S. *et al.* Quantum machine learning beyond kernel methods. *Nature Communications* **14**, 517 (2023).

[44] Scheel, S. Permanents in linear optical networks. *arXiv preprint quant-ph/0406127* (2004).

[45] Spagnolo, N. *et al.* General Rules for Bosonic Bunching in Multimode Interferometers. *Physical Review Letters* **111**, 130503 (2013). URL https://link.aps.org/doi/10.1103/PhysRevLett.111.130503. Publisher: American Physical Society.

[46] Davis, K. M., Miura, K., Sugimoto, N. & Hirao, K. Writing waveguides in glass with a femtosecond laser. *Optics letters* **21**, 1729–1731 (1996).

[47] Osellame, R., Cerullo, G. & Ramponi, R. (eds.) *Femtosecond Laser Micromachining: Photonic and Microfluidic Devices in Transparent Materials*, vol. 123 of *Topics in Applied Physics* (Springer, Berlin, Heidelberg, 2012). URL https://link.springer.com/10.1007/978-3-642-23366-1.

[48] Corrielli, G., Crespi, A. & Osellame, R. Femtosecond laser micromachining for integrated quantum photonics. *Nanophotonics* **10**, 3789–3812 (2021). URL https://www.degruyter.com/document/doi/10.1515/nanoph-2021-0419/html?lang=en. Publisher: De Gruyter.

[49] Ceccarelli, F. *et al.* Low power reconfigurability and reduced crosstalk in integrated photonic circuits fabricated by femtosecond laser micromachining. *Laser & Photonics Reviews* **14**, 2000024 (2020).

[50] Hong, C.-K., Ou, Z.-Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Physical review letters* **59**, 2044 (1987).

[51] Scheel, S. Permanents in linear optical networks (2004). URL http://arxiv.org/abs/quant-ph/0406127. ArXiv: quant-ph/0406127.

[52] Havlíček, V. *et al.* Supervised learning with quantum-enhanced feature spaces. *Nature* **567**, 209–212 (2019).

[53] Liu, Y., Choudhary, A., Marpaung, D. & Eggleton, B. J. Integrated microwave photonic filters. *Advances in Optics and Photonics* **12**, 485 (2020).

[54] Bartkiewicz, K. *et al.* Experimental kernel-based quantum machine learning in finite feature space. *Scientific Reports* **10**, 12356 (2020).

[55] Lee, J. *et al.* Finite versus infinite neural networks: an empirical study. *Advances in Neural Information Processing Systems* **33**, 15156–15172 (2020).

[56] Radhakrishnan, A., Ruiz Luyten, M., Prasad, N. & Uhler, C. Transfer learning with kernel methods. *Nature Communications* **14**, 5570 (2023).

[57] Jacot, A., Gabriel, F. & Hongler, C. Neural tangent kernel: Convergence and generalization in neural networks. *Advances in neural information processing systems* **31** (2018).

[58] Ramsauer, H. *et al.* Hopfield networks is all you need. *arXiv preprint arXiv:2008.02217* (2020).

[59] Wang, X., Du, Y., Luo, Y. & Tao, D. Towards understanding the power of quantum kernels in the NISQ era. *Quantum* **5**, 531 (2021). URL https://quantum-journal.org/papers/q-2021-08-30-531/.

[60] Yu, C.-H., Gao, F., Wang, Q.-L. & Wen, Q.-Y. Quantum algorithm for association rules mining. *Physical Review A* **94**, 042311 (2016). URL https://link.aps.org/doi/10.1103/PhysRevA.94.042311.

[61] Lorenz, R., Pearson, A., Meichanetzidis, K., Kartsaklis, D. & Coecke, B. QNLP in Practice: Running Compositional Models of Meaning on a Quantum Computer. *ArXiv e-prints* (2021). 2102.12846.

[62] Landman, J. *et al.* Quantum Methods for Neural Networks and Application to Medical Image Classification. *Quantum* **6**, 881 (2022). URL https://quantum-journal.org/papers/q-2022-12-22-881/.

[63] Schuld, M. & Petruccione, F. Quantum Models as Kernel Methods. In Schuld, M. & Petruccione, F. (eds.) *Machine Learning with Quantum Computers*, Quantum Science and Technology, 217–245 (Springer International Publishing, Cham, 2021). URL https://doi.org/10.1007/978-3-030-83098-4_6.

[64] Denis, Z., Favero, I. & Ciuti, C. Photonic kernel machine learning for ultrafast spectral analysis. *Physical Review Applied* **17**, 034077 (2022).

[65] Spagnolo, M. *et al.* Experimental photonic quantum memristor. *Nature Photonics* **16**, 318–323 (2022).

[66] Govia, L., Ribeill, G., Rowlands, G. & Ohki, T. Nonlinear input transformations are ubiquitous in quantum reservoir computing. *Neuromorphic Computing and Engineering* **2**, 014008 (2022).

[67] Innocenti, L. *et al.* Potential and limitations of quantum extreme learning machines. *Communications Physics* **6**, 118 (2023).

[68] Hamerly, R., Bernstein, L., Sludds, A., Soljačić, M. & Englund, D. Large-scale optical neural networks based on photoelectric multiplication. *Physical Review X* **9**, 021032 (2019).

[69] Spagnolo, M. *et al.* Experimental photonic quantum memristor. *Nature Photonics* **16**, 318–323 (2022).

METHODS

The two photon input states are generated by a type-II spontaneous parametric down-conversion source, which generates frequency degenerate single-photon pairs at 1546 nm via a periodically poled K-titanyl phosphate (ppKTP) crystal. Afterwards, the two photons are made indistinguishable in their polarization, which is rotated through paddles, and arrival time, through a delay line, which we use also to tune the degree of indistinguishability of the generated photons. Then, we inject these photons in two modes of an integrated photonic processor with 6 input/output modes [30]. This circuit features 27 thermal phase shifters and its architecture follows the rectangular scheme presented in [32], to implement arbitrary unitary evolution on any input Fock state. The current source is supplied to each phase shifter independently to avoid electrical crosstalk. In the end, detection is performed by superconducting nanowire single-photon detectors (SNSPDs) housed in a 1K cryostat. We postselect the detected events to the cases in which two detectors click simultaneously in a temporal window of 1 ns. A time tagger with a 15.63 ps resolution is used to process the real-time coincidence counting for all 15 postselection patterns.

DATA AVAILABILITY

The data supporting this study's findings are available from the project page (https://github.com/dapingQ/PhoQuKs), containing detailed explanations of all the datasets.

CODE AVAILABILITY

The code scripts analyzing the study is available from the project page (https://github.com/dapingQ/PhoQuKs).

Heisenberg-limited adaptive gradient estimation for multiple observables

Kaito Wada[1] * Naoki Yamamoto[1 2] † Nobuyuki Yoshioka[3 4 5] ‡

[1] *Department of Applied Physics and Physico-Informatics, Keio University, Hiyoshi 3-14-1, Kohoku, Yokohama 223-8522, Japan*

[2] *Quantum Computing Center, Keio University, Hiyoshi 3-14-1, Kohoku, Yokohama 223-8522, Japan*

[3] *Department of Applied Physics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

[4] *Theoretical Quantum Physics Laboratory, RIKEN Cluster for Pioneering Research (CPR), Wako-shi, Saitama 351-0198, Japan*

[5] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

Abstract. In quantum mechanics, measuring a general observable involves statistical uncertainty, which can be reduced by averaging samples. Minimizing the number of samples is crucial in future quantum computing, especially when we desire to explore numerous observables in large systems. This work presents an adaptive extension of the quantum gradient estimation algorithm to estimate the expectation values of M observables within root mean squared error ε using $\mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M)$ queries to a state preparation oracle. That is, the method achieves Heisenberg-limited scaling $\mathcal{O}(\varepsilon^{-1})$ and the sublinear scaling with M, offering a resource-efficient implementation with space overhead of $\mathcal{O}(M)$ and avoiding numerical instability in quantum signal processing techniques for large-scale tasks.

Keywords: Quantum computation, Quantum metrology, Observable estimation

1 Overview and summary

Achieving quantum enhancement in the estimation of unknown parameters is a fundamental goal in quantum technology. In particular, the gap between the standard quantum limit (SQL) and the Heisenberg limit (HL) in such estimation tasks has been getting a significant focus since the late 20th century. The SQL represents the scaling of measurement counts as $\mathcal{O}(1/\varepsilon^2)$ for target accuracy ε, while the HL scales as $\mathcal{O}(1/\varepsilon)$ due to quantum uncertainty relations that are usually quantified by a natural metric called the mean squared error (MSE). The HL can theoretically be reached using entanglement or coherence in quantum probes without noise [14, 15], while its experimental verification has not been realized for a long time until the quantum phase estimation procedure by Higgins *et al.* with use of a novel adaptive measurement [19].

The quest for quantum-enhanced measurement extends to multiple observables, a topic crucial for various applications of quantum computing like quantum simulation [26, 1, 8, 13, 3, 39], quantum machine learning [4, 25, 20], and quantum finance [33, 6]. Although modified amplitude estimation algorithms [34, 37, 36] can individually achieve HL scaling for multiple observables, we here seek a protocol that achieves both the HL scaling and the sublinear scaling with respect to M in estimating all of M observables. Some approaches based on the gradient estimation [22] have reported nearly Heisenberg-limited scaling with logarithmic corrections [35, 21], but no method has yet achieved ultimate precision scaling as defined by the HL. Specifically, existing works often rely on confidence intervals to quantify the estimation error, which do not bound the worst-case scenario as effectively as MSE. As well known in the field of quantum metrology [15, 18], the MSE successfully bounds other measures of uncertainty [2], while the converse does not hold in general. Considering that any quantum algorithm to estimate observables queries the state preparation oracle whose complexity usually scales with the target system size, it is crucial to design an estimation algorithm that achieves the Heisenberg-limited scaling in terms of MSE.

Driven by such a situation, we make a significant contribution to multiple observables estimation of number M with root MSE of ε. Concretely, we explicitly construct an adaptive estimation scheme as summarized as Algorithm 1 that satisfies the following features (each correspond to Theorem 1, 2, and 3, respectively):

- *Heisenberg-limited scaling with sublinear scaling on M.* The proposed method achieves the pure HL scaling with root MSE ε as $\mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M)$ in query to the state preparation. Also, this scaling indicates a nearly quadratic improvement regarding M, compared to the (modified) quantum amplitude estimation [5, 24, 32, 34, 37, 36].

- *Constant space overhead.* The quantum circuits in the proposed scheme require additional $\mathcal{O}(M)$ qubits, which is independent of ε.

- *Robustness in high-precision regime.* When the high precision $\varepsilon \ll 1$ is required, the quantum circuits in our method have at most $\mathcal{O}(\log(1/\varepsilon))$ parameterized gates for QSVT [13], which can be tuned by $\mathcal{O}(\text{polylog}(1/\varepsilon))$ classical computation, while the previous method [35] requires to tune $\mathcal{O}(1/\varepsilon)$ gates with $\mathcal{O}(\text{poly}(1/\varepsilon))$ classical computation. This significant reduction in classical compu-

*wkai1013keio840@keio.jp

†yamamoto@appi.keio.ac.jp

‡nyoshioka@ap.t.u-tokyo.ac.jp

Table 1: The development of quantum phase estimation (QPE) and quantum gradient estimation (QGE).

	Phase estimation	Gradient estimation
Non-adaptive • Large space overhead • SQL $\mathcal{O}(1/\varepsilon^2)$	Textbook style [31]	Jordan, Gilyén *et al.* [22, 12]
Adaptive (or Iterative) • Constant space overhead • HL $\mathcal{O}(1/\varepsilon)$	Higgins *et al.* [19, 18]	Our work
Further applications of the HL scheme	[23, 11, 10, 17]	Future work

tation allows us to avoid the numerical instability problem [16, 7, 9, 38, 30] that spoils the quantum enhancement.

In our algorithm, we sample from an $\mathcal{O}(M + \log_2 d)$-qubit circuit with an alternating sequence of a global interaction to encode the expectation values of target observables and a controlled rotation over the target $\log_2 d$-qubit system (and some ancillary system). The global interaction and the total circuit length are adaptively adjusted to read out the expectation values in high resolution, keeping the space overhead small. Then, we classically process the samples similarly to the adaptive phase estimation algorithms [18, 23, 11] and use the processing results to construct the next quantum circuit. The sublinear scaling on M comes from the spectral amplification process [27, 13] embedded in the global interaction. Importantly, the proposed algorithm is the first adaptive extension of quantum gradient estimation [22, 12], which allows us to evaluate the M-dimensional gradient of a real scalar function $f(\boldsymbol{x})$ on $\mathbb{R}^M$ with sublinear scaling on M; see Table 1 for the comparison with phase estimation algorithms.

We remark that the classical computation in the third point is required for the circuit construction, especially for quantum signal processing (QSP) [29, 28]. QSP provides a systematic way to operate a 1-qubit system under a wide range of polynomial functions of degree n, using $\mathcal{O}(n)$ parameterized quantum gates. In the framework of QSP (or its extension QSVT [13]), we need to tune the parameterized gates classically for a desired polynomial. Although finding this parameter for a degree-n polynomial can be achieved in $\mathcal{O}(\mathrm{poly}(n))$ classical computation time, it exhibits numerical instability for large n, posing a central challenge in the practical application of QSVT [30]. In the previous method for multiple observables estimation [35], the number of parameterized gates is given by $n = \tilde{\mathcal{O}}(\sqrt{M}/\varepsilon)$, leading to a quite large runtime in classical computation e.g., $\sim M/\varepsilon^2$ [sec] when we use the method in Ref. [9] (assuming it works in such a large n). In contrast, our method requires tuning only $\mathcal{O}(\sqrt{M}\log(M/\varepsilon))$ gates under a certain condition by partially using a special polynomial whose parameters are analytically derived.

Algorithm 1 Adaptive observables estimation

```
Input: $\log_2 d$-qubit state preparation unitary $U_\psi$; observables $\{O_j\}_{j=1}^M$ with the spectral norm $\|O_j\| \le 1$ such that $M > \mathcal{O}(\log d)$ holds; confidence parameter $c \in (0, 3/8(1+\pi)^2]$; target root MSE $\varepsilon \in (0,1)$.
Set a fixed precision parameter $p := 3$ and temporal estimates $\tilde{u}_j^{(0)} := 0$ for all $j$.
for $q = 0, 1, ..., q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$ do
    Measure $\mathcal{O}(\log M/\delta^{(q)})$ approximate copies of the probing state $|\Upsilon(q)\rangle$ in Eq. (1) after $p$-qubit inverse quantum Fourier transformations.
    Here, $\delta^{(q)} := c/8^{q_{\max}-q}$ is a failure probability.
    Set the coordinate-wise median of the measurement outputs as $g_j^{(q)}$.
    Update $\tilde{u}_j^{(q+1)} := \tilde{u}_j^{(q)} + \pi 2^{-q} g_j^{(q)}$
    Truncate $\tilde{u}_j^{(q+1)}$ in $[-1, 1]$
end for
return final estimates $\tilde{u}_j := \tilde{u}_j^{(q_{\max}+1)}$
```

2 Main idea of algorithm

Let us state the concrete problem setup and provide the main idea of the proposed algorithm (see Algorithm 1 for the pseudocode). We consider estimating quantum expectation values of given d-dimensional M Hermitian operators $\{O_j\}_{j=1}^M$ ($\|O_j\| \le 1$) regarding a quantum state $|\psi\rangle$, which is prepared by a state preparation oracle U_ψ. Here, the observables are assumed to be accessed by some block-encoding unitaries. The key idea of the proposed scheme is to adaptively prepare the following *probing state*, from which the approximated expectation values can be extracted via gradient estimation algorithm [22]:

$$|\Upsilon(q)\rangle := \frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x} \in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^q \pi^{-1} \langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle} |\boldsymbol{x}\rangle \tag{1}$$

where $q = 0, 1, \cdots, \lceil \log_2(1/\varepsilon) \rceil$ denotes a iteration step, p denotes a fixed precision parameter, $\langle O_j \rangle := \langle \psi | O_j | \psi \rangle$ and G_p^M is a set of 2^{pM} grid points in $\mathbb{R}^M$. In the technical manuscript, we will show that $p = 3$ is sufficient for our algorithm to successfully work. Because there is a one-to-one correspondance between G_p^M and 2^{pM}-qubit computational base, we label the computational basis by $\boldsymbol{x} = (x_1, ..., x_M) \in G_p^M$. The quantity $\tilde{u}_j^{(q)} \in [-1, 1]$ are temporal estimated values for $\langle O_j \rangle$ at the qth iteration.

As rigorously shown in Ref. [12], the gradient estimation algorithm [22] can simultaneously extract the values $2^q \pi^{-1} \langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle$ from the quantum state (1) with an additive error specified by p and a certain success probability. Thus, using the successful results from the gradient estimation, we can update $\tilde{u}_j^{(q)}$ to $\tilde{u}_j^{(q+1)}$ such that $\tilde{u}_j^{(q+1)}$ is more close to the target value $\langle O_j \rangle$. More precisely, this update yields a $q+1$ binary-bit accurate estimate $\tilde{u}_j^{(q+1)}$ for $\langle O_j \rangle$ because of the enhanced resolution $2^q \langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle$ in the probing state $|\Upsilon(q)\rangle$. Consequently, we can obtain ε-close estimates at the end of the iteration step, if the gradient estimation at every step is successfully performed.

3 Performance guarantee of algorithm

HL multiple observables estimation. We prove the rigorous performance guarantee for estimation efficiency of the proposed protocol as follows.

Theorem 1 (Theorem 2 in the technical manuscript). *Let $\varepsilon \in (0, 1)$ be a target precision. For given M observables $\{O_j\}_{j=1}^M$ and a state preparation U_ψ, there exists a quantum algorithm that samples estimators $\{\hat{u}_j\}_j$ for $\{\langle \psi | O_j | \psi \rangle\}_{j=1}^M$ satisfying*

$$\max_{j=1,2,...,M} \mathbb{E}\left[(\hat{u}_j - \langle \psi | O_j | \psi \rangle)^2 \right] \leq \varepsilon^2$$

using $\mathcal{O}(\varepsilon^{-1}\sqrt{M} \log M)$ queries to the state preparation U_ψ and $U_\psi^\dagger$ in total.

The scaling $1/\varepsilon$ of queries to U_ψ with respect to root MSE ε achieves the same scaling to the Heisenberg limit in the gradient estimation; see the technical manuscript. The squared root dependence regarding M originates from the uniform amplification of block-encoded (sum of) observables [27], which is consistent with the idea used in the previous method [35]. As for the $\log M$ term, its origin is the repetition of the measurement to (1) in each iteration step, in order to boost the success probability by taking median of estimates.

Constant space overhead. In addition to the HL scaling in query complexity, our scheme has a significant improvement in space complexity compared to the previous non-iterative counterparts [35, 21]. While the previous methods determine all of the $\mathcal{O}(\log(1/\varepsilon))$ binary bits of $\langle O_j \rangle$ by a quantum circuit with $\mathcal{O}(M \log(1/\varepsilon))$ readout qubits, our scheme determines only 1 binary bit of $\langle O_j \rangle$ at each iteration step. Therefore, by the help of the adaptive procedure, our scheme requires quantum circuits with $\mathcal{O}(M)$-qubits overhead, to prepare $|\Upsilon(q)\rangle$ with the fixed precision parameter $p = 3$. This can be summarized as follows:

Theorem 2 (Theorem 7 in the technical manuscript). *Suppose that we have access to block-encoded d-dimensional observables $\{O_j\}_{j=1}^M$, a $\log_2 d$-qubit state preparation U_ψ, and its inverse $U_\psi^\dagger$, such that $M > \mathcal{O}(\log d)$. Then, we can approximately prepare the probing state $|\Upsilon(q)\rangle$ for any integer $q \geq 0$ and $\tilde{u}_j^{(q)} \in [-1, 1]$, using an*

$$\mathcal{O}(M + \log_2 d)\text{-}qubit$$

circuit. Furthermore, each quantum circuit with q requires $\mathcal{O}(\mathrm{poly}(2^q\sqrt{M \log d}) + \mathrm{poly}(\sqrt{M}(q + \log M)))$ classical computation for finding circuit parameters, and it consists of $\mathcal{O}(2^q\sqrt{M \log d})$ uses of U_ψ and $U_\psi^\dagger$, $\mathcal{O}(2^q M(q + \log M))$ uses of unitary gates for block-encoded observables.

Robustness in high-precision regime. The quantum circuit employed in Theorem 2 requires classical tuning of $\tilde{\mathcal{O}}(\sqrt{M}/\varepsilon)$ circuit parameters (more precisely, $\tilde{\mathcal{O}}(2^q\sqrt{M})$ parameters in step q) for QSP. The classical computation for finding $\tilde{\mathcal{O}}(\sqrt{M}/\varepsilon)$ parameters is also required in the existing work by Ref. [35]. However, it is challenging to find such a large number of circuit parameters in a stable way as pointed out in previous works [30].

To avoid the numerical instability, we here provide an alternative way to prepare the probing state (1) using the *Grover-like repetition*, which is a special case of QSP such that the corresponding quantum circuit parameters are analytically derived.

Theorem 3 (Theorem 8 in the technical manuscript). *Suppose the same conditions on $\{O_j\}_{j=1}^M$ and U_ψ as in Theorem 2. If the iteration step $q \geq 0$ satisfies the following condition ($\delta' := 2^{-14}$)*

$$q \geq \log_4 \left[\frac{2^3 \cdot 33^3}{625 \ln(2d/\delta')} \frac{\left\lceil \sqrt{2(M+1)\ln(2d/\delta')} \right\rceil}{\sqrt{\ln(2d/\delta')}} \right], \quad (2)$$

and for given $\tilde{u}_j^{(q)} \in [-1, 1]$, $|\langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle| \leq 2^{-q}$ holds for all j, then we can approximately prepare the probing state $|\Upsilon(q)\rangle$, with the success probability at least 0.462 with ancilla qubits measurement result indicating success, using an $\mathcal{O}(M + \log_2 d)$-qubit circuit. Furthermore, each quantum circuit with q requires

$$\mathcal{O}(\mathrm{poly}(\sqrt{M}(q + \log M)))$$

classical computation, and it has the same gate complexity as that of Theorem 2.

Although this method cannot deterministically prepare the probing state, the success probability can be increased with a constant number of circuit repetitions, thus maintaining the same total query complexity when using Grover-like repetition instead of Theorem 2. We remark that the condition $|\langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle| \leq 2^{-q}$ is trivially satisfied in Algorithm 1; see the technical manuscript. In particular, if the number of target observables satisfies $M = \mathcal{O}((\log_2 d)^2)$, then the right hand side in Eq. (2) becomes constant, and therefore, the alternative scheme is valid in a wide range of ε.

References

[1] Alán Aspuru-Guzik, Anthony D Dutoi, Peter J Love, and Martin Head-Gordon. Simulated quantum computation of molecular energies. *Science*, 309(5741):1704–1707, 2005.

[2] D. W. Berry, H. M. Wiseman, and J. K. Breslin. Optimal input states and feedback for interferometric phase estimation. *Phys. Rev. A*, 63:053804, Apr 2001.

[3] Michael E Beverland, Prakash Murali, Matthias Troyer, Krysta M Svore, Torsten Hoeffler, Vadym Kliuchnikov, Guang Hao Low, Mathias Soeken, Aarthi Sundaram, and Alexander Vaschillo. Assessing requirements to scale to practical quantum advantage. *arXiv preprint arXiv:2211.07629*, 2022.

[4] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.

[5] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002.

[6] Shouvanik Chakrabarti, Rajiv Krishnakumar, Guglielmo Mazzola, Nikitas Stamatopoulos, Stefan Woerner, and William J Zeng. A threshold for quantum advantage in derivative pricing. *Quantum*, 5:463, 2021.

[7] Rui Chao, Dawei Ding, Andras Gilyen, Cupjin Huang, and Mario Szegedy. Finding angles for quantum signal processing with machine precision. *arXiv preprint arXiv:2003.02831*, 2020.

[8] Andrew M Childs, Dmitri Maslov, Yunseong Nam, Neil J Ross, and Yuan Su. Toward the first quantum simulation with quantum speedup. *Proceedings of the National Academy of Sciences*, 115(38):9456–9461, 2018.

[9] Yulong Dong, Xiang Meng, K Birgitta Whaley, and Lin Lin. Efficient phase-factor evaluation in quantum signal processing. *Physical Review A*, 103(4):042419, 2021.

[10] Alicja Dutkiewicz, Thomas E O'Brien, and Thomas Schuster. The advantage of quantum control in many-body hamiltonian learning. *arXiv preprint arXiv:2304.07172*, 2023.

[11] Alicja Dutkiewicz, Barbara M Terhal, and Thomas E O'Brien. Heisenberg-limited quantum phase estimation of multiple eigenvalues with few control qubits. *Quantum*, 6:830, 2022.

[12] András Gilyén, Srinivasan Arunachalam, and Nathan Wiebe. Optimizing quantum optimization algorithms via faster quantum gradient computation. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1425–1444. SIAM, 2019.

[13] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, 2019.

[14] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[15] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222–229, 2011.

[16] Jeongwan Haah. Product Decomposition of Periodic Functions in Quantum Signal Processing. *Quantum*, 3:190, October 2019.

[17] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. Query-optimal estimation of unitary channels in diamond distance. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 363–390, 2023.

[18] BL Higgins, DW Berry, SD Bartlett, MW Mitchell, HM Wiseman, and GJ Pryde. Demonstrating heisenberg-limited unambiguous phase estimation without adaptive measurements. *New Journal of Physics*, 11(7):073023, 2009.

[19] Brendon L Higgins, Dominic W Berry, Stephen D Bartlett, Howard M Wiseman, and Geoff J Pryde. Entanglement-free heisenberg-limited phase estimation. *Nature*, 450(7168):393–396, 2007.

[20] Hsin-Yuan Huang, Richard Kueng, Giacomo Torlai, Victor V Albert, and John Preskill. Provably efficient machine learning for quantum many-body problems. *Science*, 377(6613):eabk3333, 2022.

[21] William J. Huggins, Kianna Wan, Jarrod McClean, Thomas E. O'Brien, Nathan Wiebe, and Ryan Babbush. Nearly optimal quantum algorithm for estimating multiple expectation values. *Phys. Rev. Lett.*, 129:240501, Dec 2022.

[22] Stephen P. Jordan. Fast quantum algorithm for numerical gradient estimation. *Phys. Rev. Lett.*, 95:050501, Jul 2005.

[23] Shelby Kimmel, Guang Hao Low, and Theodore J Yoder. Robust calibration of a universal single-qubit gate set via robust phase estimation. *Physical Review A*, 92(6):062315, 2015.

[24] Emanuel Knill, Gerardo Ortiz, and Rolando D Somma. Optimal quantum measurements of expectation values of observables. *Physical Review A*, 75(1):012328, 2007.

[25] Yunchao Liu, Srinivasan Arunachalam, and Kristan Temme. A rigorous and robust quantum speed-up in supervised machine learning. *Nature Physics*, 17(9):1013–1017, 2021.

[26] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996.

[27] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by uniform spectral amplification. *arXiv preprint arXiv:1707.05391*, 2017.

[28] Guang Hao Low and Isaac L. Chuang. Hamiltonian Simulation by Qubitization. *Quantum*, 3:163, July 2019.

[29] Guang Hao Low, Theodore J. Yoder, and Isaac L. Chuang. Methodology of resonant equiangular composite quantum gates. *Phys. Rev. X*, 6:041067, Dec 2016.

[30] Kaoru Mizuta and Keisuke Fujii. Recursive quantum eigenvalue and singular-value transformation: Analytic construction of matrix sign function by newton iteration. *Phys. Rev. Res.*, 6:L012007, Jan 2024.

[31] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[32] Patrick Rall. Quantum algorithms for estimating physical quantities using block encodings. *Physical Review A*, 102(2):022408, 2020.

[33] Nikitas Stamatopoulos, Daniel J. Egger, Yue Sun, Christa Zoufal, Raban Iten, Ning Shen, and Stefan Woerner. Option Pricing using Quantum Computers. *Quantum*, 4:291, July 2020.

[34] Yohichi Suzuki, Shumpei Uno, Rudy Raymond, Tomoki Tanaka, Tamiya Onodera, and Naoki Yamamoto. Amplitude estimation without phase estimation. *Quantum Information Processing*, 19(2):75, January 2020.

[35] Joran van Apeldoorn, Arjan Cornelissen, András Gilyén, and Giacomo Nannicini. Quantum tomography using state-preparation unitaries. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1265–1318. SIAM, 2023.

[36] Kaito Wada, Kazuma Fukuchi, and Naoki Yamamoto. Quantum-enhanced mean value estimation via adaptive measurement. *arXiv preprint arXiv:2210.15624*, 2022.

[37] Guoming Wang, Dax Enshan Koh, Peter D. Johnson, and Yudong Cao. Minimizing estimation runtime on noisy quantum computers. *PRX Quantum*, 2:010346, Mar 2021.

[38] Lexing Ying. Stable factorization for phase factors of quantum signal processing. *Quantum*, 6:842, October 2022.

[39] Nobuyuki Yoshioka, Tsuyoshi Okubo, Yasunari Suzuki, Yuki Koizumi, and Wataru Mizukami. Hunting for quantum-classical crossover in condensed matter problems. *arXiv preprint arXiv:2210.14109*, 2022.

Heisenberg-limited adaptive gradient estimation for multiple observables

Kaito Wada,[1, *] Naoki Yamamoto,[1, 2, †] and Nobuyuki Yoshioka[3, 4, 5, ‡]

[1] *Department of Applied Physics and Physico-Informatics, Keio University,*
3-14-1 Hiyoshi, Kohoku-ku, Yokohama, Kanagawa, 223-8522, Japan
[2] *Quantum Computing Center, Keio University, Hiyoshi 3-14-1, Kohoku, Yokohama 223-8522, Japan*
[3] *Department of Applied Physics, University of Tokyo,*
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
[4] *Theoretical Quantum Physics Laboratory, RIKEN Cluster for Pioneering Research (CPR), Wako-shi, Saitama 351-0198, Japan*
[5] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

In quantum mechanics, measuring a general observable has an inherent statistical uncertainty such as variance or mean squared error. While the uncertainty can be reduced by averaging several samples, the number of samples should be minimized when each sample is very costly; this is precisely the case in future quantum computing. Meanwhile, one of the goals of quantum computing is to explore numerous observables in large quantum systems that are beyond the capabilities of classical computers. In this work, we provide an adaptive quantum algorithm for estimating the expectation values of M general observables within root mean squared error ε simultaneously, using $\mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M)$ queries to state preparation oracle; the total queries achieves the scaling of Heisenberg limit $1/\varepsilon$, a fundamental bound on the estimation precision, and the sublinear scaling of the number of observables M. The proposed method is an adaptive version of the quantum gradient estimation algorithm and has a resource-efficient implementation due to its adaptiveness. Specifically, the space overhead in the proposed method is $\mathcal{O}(M)$ which does not depend on the estimation precision ε. In addition, our method can avoid the numerical instability problem of constructing quantum circuits in a large-scale task (e.g., $\varepsilon \ll 1$ in our case), which appears in the actual application of many quantum algorithms relying on quantum signal processing techniques.

I. INTRODUCTION

A. Background

Attaining a quantum enhancement in unknown parameter estimation lies as one of the most fundamental tasks in quantum technology. It has been noticed in the quantum metrological community from the late 20th century that there exists a gap between the standard quantum limit (SQL), the statistical scaling of the measurement count $\mathcal{O}(1/\varepsilon^2)$ for target accuracy of ε that is based on the central limit theorem, and the Heisenberg limit (HL), the scaling $\mathcal{O}(1/\varepsilon)$ due to quantum uncertainty relations that are quantified by a natural metric called the mean squared error (MSE). The HL can theoretically be achieved using entanglement or coherence (i.e., sequential applications of a sensing channel) in quantum probes under the absence of noise [1, 2], while its experimental verification has not been realized for a long time until the quantum phase estimation procedure by Higgins *et al.* that uses a novel adaptive measurement [3]. Aside from Ref. [3], intensive quest for experimental realization of the scaling beyond the SQL has provoked numerous interesting ideas such as the use of quantum error correction [4–7], exploiting the non-Markovianity of the environment [8, 9].

The preceding pursuit for the fundamental limitation by quantum mechanics naturally pertains to the quantum-enhanced measurement of multiple observables. This long-standing question has been posed mainly in the community of quantum computing, since an overwhelming numbers of quantum algorithms estimate the expectation values of local and/or global observables; not to mention scientific application of quantum computers for quantum simulation of many-body systems in natural science [10–15], such a task is also ubiquitous in industrial use such as quantum machine learning [16–18] and quantum finance [19, 20]. Note that, while one may employ the modified amplitude estimation algorithm [21–23] individually for M observables to simply obtain the HL scaling of $\mathcal{O}(M/\varepsilon)$ in terms of root MSE ε, here we seek for simultaneous improvement on the target accuracy ε and observable count M. Simply put, our goal is to construct a protocol that achieves both the HL scaling and the sublinear scaling with respect to M in estimating all of M observables.

Indeed, some previous works based on the gradient estimation algorithm [24, 25] have reported nearly Heisenberg-limited scaling, although with multiplicative logarithmic correction $\log(1/\varepsilon)$ [26, 27]; there is no work that achieves the ultimate precision scaling following the HL in light of its definition. Furthermore, existing works argue the estimation accuracy in terms of confidence intervals, which crucially fails to bound the worst-case behavior of a single run, unlike the MSE. As is well known in the field of quantum metrology [2, 28–30], the MSE successfully bounds other measures of uncertainty, while the converse does not hold in general. Considering that any

[*] wkai1013keio840@keio.jp
[†] yamamoto@appi.keio.ac.jp
[‡] nyoshioka@ap.t.u-tokyo.ac.jp

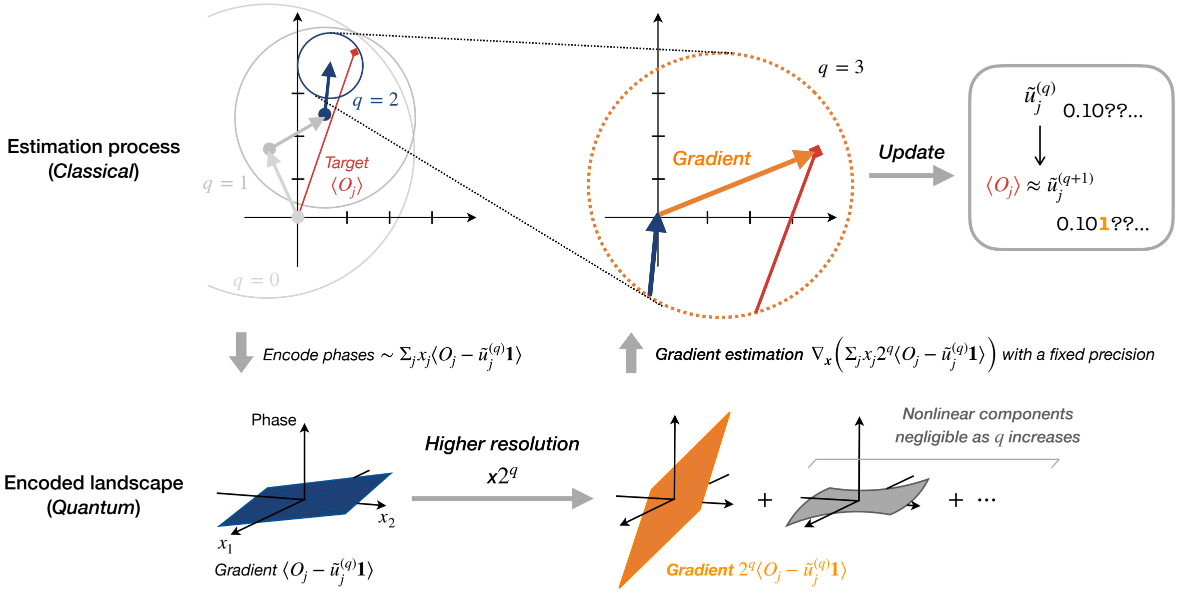

Estimation process
(Classical)
$q = 2$
$q = 1$
$q = 0$
Target
$\langle O_j \rangle$
$q = 3$
Gradient
Update
$\tilde{u}_j^{(q)}$ 0.10??...
$\langle O_j \rangle \approx \tilde{u}_j^{(q+1)}$
0.101??...
Encode phases $\sim \Sigma_j x_j \langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle$
Gradient estimation $\nabla_x \left(\Sigma_j x_j 2^q \langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle\right)$ with a fixed precision
Encoded landscape
(Quantum)
Phase
x_1
x_2
Gradient $\langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle$
Higher resolution
x2^q
Nonlinear components
negligible as q increases
+
+ ⋯
Gradient $2^q\langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle$

FIG. 1. Graphical summary of the proposed method. Our algorithm estimates the expectation values of quantum observables $\{\langle O_j \rangle\}_{j=1}^{M}$ regarding a quantum state $|\psi\rangle$ prepared by a unitary U_ψ, with an adaptive procedure. In each iteration step q, we first encode the values of estimation errors $\{\langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle\}$ for a unitary gate, where $\tilde{u}_j^{(q)} \in [-1, 1]$ denotes a temporal estimated value from the previous step, for the target value $\langle O_j \rangle$. Then, we coherently amplify the estimation errors by the factor of 2^q via Grover-like repetition (or Hamiltonian simulation) on the encoding unitary and read out *zoomed-in* values $\{2^q \langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle\}$ simultaneously by gradient estimation protocol with a fixed measurement precision. From the measurement results, we update the temporal estimates $\tilde{u}_j^{(q)}$ to $\tilde{u}_j^{(q+1)}$. By repeating this procedure for $q = 0, 1, ..., \lceil \log_2(1/\varepsilon) \rceil$, this algorithm estimates the M observables simultaneously within at most root MSE ε. The algorithm uses $\mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M)$ queries to the state preparation unitary U_ψ that indicates the scaling of Heisenberg limit, that is, the inverse of root MSE ε, together with the nearly squared root dependence on the number of observables M, which comes from the spectral amplification process in the encoding of $\{\langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle\}$.

quantum algorithm to estimate observables queries the state preparation oracle of target quantum state whose complexity usually scales with the system size, it is crucial to design an estimation algorithm that achieves the HL scaling in terms of the MSE.

A key insight for enhancement can be borrowed from the history of phase estimation algorithm [31]. It has been well-recognized that the textbook style of the phase estimation algorithm [32] encounters two major bottlenecks that prevents the algorithm from practical benefit; the large ancilla consumption of $\mathcal{O}(\log(1/\varepsilon))$ and the poor query complexity scaling with the target root MSE ε, i.e., only obeying the SQL $\mathcal{O}(1/\varepsilon^2)$ [3, 33, 34]. While the former can be addressed by the iterative phase estimation [31], it was not until the work by Higgins *et al.* that proposed to overcome both issues by utilizing adaptive measurement scheme to achieve the HL with a constant number of ancilla [3]. Although a followup work has shown that HL scaling can be achieved even without relying on the adaptive scheme, there is in practice an increase in the estimation variance by a constant factor [29]. On the other hand, if the large ancilla consumption is acceptable, it is known that the quantum phase estimation algorithm with an entangled ancillary state, instead of a uniform superposition state, can achieve the HL [33–36]. From the above observations, we argue that adaptive strategy is crucial for resource-efficient implementation of quantum estimation that saturates the ultimate scaling limited by purely fundamental principles of quantum physics.

B. Summary of results

Driven by such a situation, we make a significant contribution to multiple observables estimation of number M with root MSE of ε. Concretely, we explicitly construct an adaptive estimation scheme as summarized as Algorithm 1, which satisfies the following features (each correspond to Theorem 2, 7, and 8, respectively):

- *Heisenberg-limited scaling with sublinear scaling on M.* The proposed observable estimation achieves the pure HL scaling with root MSE ε as

$$\mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M)$$

in query to the state preparation. Also, this scaling indicates a nearly quadratic improvement regarding M, compared to the parallel use of the (modified) quantum amplitude estimation [21–23, 37–39].

- *Constant space overhead.* The quantum circuits in the proposed scheme require at most additional $\mathcal{O}(M)$ qubits, which is independent of the target root MSE ε.

- *Robustness in high-precision regime.* When the high precision $\varepsilon \ll 1$ is required, the quantum circuits in our method have at most $\mathcal{O}(\log(1/\varepsilon))$ parameterized gates for QSVT [13], which can be tuned by $\mathcal{O}(\mathrm{polylog}(1/\varepsilon))$ classical computation, while the previous method [26] requires to tune $\mathcal{O}(1/\varepsilon)$ gates with $\mathcal{O}(\mathrm{poly}(1/\varepsilon))$ classical computation. This significant reduction in classical computation allows us to avoid the numerical instability problem [40–44] that spoils the quantum enhancement.

The first feature is a mathematical guarantee of estimation performance, and the other features highlight ease of practical implementation of our method.

In our algorithm, we sample from an $\mathcal{O}(M + \log_2 d)$-qubit circuit with an alternating sequence of a global interaction to encode the expectation values of target observables and a controlled rotation over the target $\log_2 d$-qubit system (and some ancillary system). The global interaction for observables and the total circuit length are adaptively adjusted to read out the expectation values in high resolution, keeping the space overhead small. Then, we classically process the samples similarly to the adaptive (iterative) phase estimation algorithms [29, 30, 45, 46] and use the processing results to construct the quantum circuit at the next step. The sublinear scaling in the number M of observables comes from the spectral amplification process [13, 47] embedded in the global interaction. This reason for the speedup on M is the same as the previous method [26]. Importantly, the proposed algorithm is the first adaptive extension of quantum gradient estimation [24, 25], which allows us to evaluate the M-dimensional gradient of a real scalar function $f(\boldsymbol{x})$ on $\mathbb{R}^M$ with sublinear scaling on M.

We remark that the classical computation in the third point is required for the circuit construction, especially for quantum signal processing (QSP) [48, 49]. QSP provides a systematic way to operate a 1-qubit system under a wide range of polynomial functions of degree n, using $\mathcal{O}(n)$ parameterized quantum gates, and it is also a key component of a more general technique for quantum matrix polynomials, called quantum singular value transformation (QSVT) [13]. In the framework of QSP (also QSVT), we need to tune the parameterized gates classically for a desired polynomial. Although finding this parameter for a degree-n polynomial can be achieved in $\mathcal{O}(\mathrm{poly}(n))$ classical computation time, it exhibits numerical instability for large n; this instability leads to undesired algorithmic errors in the resulting quantum circuit, posing a central challenge in the practical application of QSVT [40]. To resolve this, various optimization techniques have been investigated [40–44], and currently, they require 10^2–10^4 seconds to tune $n \sim 10^4$ parameters. In the previous method for multiple observables estimation [26], the number of circuit parameters is given by $n = \tilde{\mathcal{O}}(\sqrt{M}/\varepsilon)$, leading to a quite large runtime in classical computation e.g., $\sim M/\varepsilon^2$ [sec] when we use the method in Ref. [42] (assuming it works in such a large n). In contrast, our method requires to tune only $\mathcal{O}(\sqrt{M}\log(M/\varepsilon))$ parameters under a certain condition, by partially using a special polynomial whose parameters can be analytically determined. This exponential improvement in classical computation time, regarding estimation accuracy $1/\varepsilon$, significantly lowers the barrier of the practical implementation of our method.

II. PROBLEM SETUP

We consider estimating quantum expectation values of given d-dimensional M Hermitian operators $\{O_j\}_{j=1}^M$ with the spectral norm $\|O_j\| \leq 1$, regarding a quantum state $|\psi\rangle$. Here, d is a power of 2. The target state $|\psi\rangle$ is assumed to be prepared by a state preparation oracle $U_\psi : |\mathbf{0}\rangle \mapsto |\psi\rangle$ and an initial state $|\mathbf{0}\rangle := |0\rangle^{\otimes \log_2 d}$, and we assume oracular access to U_ψ and $U_\psi^\dagger$. The observables are assumed to be accessed by some block-encoded unitaries over the d-dimensional system and some ancilla system; that is, for each observable O_j, we assume access to a unitary gate B_j whose top-left block matrix is O_j. (Precise definition of this encoding is provided in Sec. IV.) In this setup, our goal is to *efficiently* obtain samples from estimators for the target values $\langle O_j\rangle := \langle\psi| O_j |\psi\rangle$ within the root mean squared error (MSE) ε. In particular, we aim to simultaneously achieve the HL scaling regarding ε and the sublinear scaling regarding M, for estimating all $\langle O_j\rangle$.

The performance of quantum algorithms for this task is usually quantified by the total number of queries to the state preparation U_ψ and $U_\psi^\dagger$. This is because U_ψ has complexity that usually scales with the system size, and as a result, the state preparation U_ψ is the most dominant factor in the total execution time for various settings. Under the natural assumption that $U_\psi^\dagger$ has the same cost as U_ψ, it is crucial to design an estimation algorithm that minimizes the statistical uncertainty using a limited number of queries to U_ψ and $U_\psi^\dagger$.

III. ADAPTIVE GRADIENT ESTIMATION FOR MULTIPLE QUANTUM OBSERVABLES

Our adaptive estimation algorithm is given in Algorithm 1. This algorithm can be seen as an extension of the adaptive (iterative) phase estimation [3, 29, 31, 45,

Algorithm 1 Adaptive observables estimation

```
Input: $\log_2 d$-qubit state preparation unitary $U_\psi$; observables $\{O_j\}_{j=1}^M$ with the spectral norm $\|O_j\| \leq 1$ such
    that $M > \mathcal{O}(\log d)$ holds; confidence parameter $c \in (0, 3/8(1+\pi)^2]$; target root mean squared error (MSE)
    $\varepsilon \in (0,1)$.
Output: A sample $(\tilde{u}_1, ..., \tilde{u}_M)$ from an estimator $\hat{\boldsymbol{u}} = (\hat{u}_1, ..., \hat{u}_M)$ whose $j$-th element estimates $\langle\psi|O_j|\psi\rangle$ within
    the MSE $\varepsilon^2$ as
        $\max_{j=1,2,...,M} \mathbb{E}\left[(\hat{u}_j - \langle\psi|O_j|\psi\rangle)^2\right] \leq \varepsilon^2$
Set a fixed precision parameter $p := 3$ and temporal estimates $\tilde{u}_j^{(0)} := 0$ for all $j$.
for $q = 0, 1, ..., q_{\max} := \lceil\log_2(1/\varepsilon)\rceil$ do
    Measure $\mathcal{O}(\log M/\delta^{(q)})$ approximate copies of the probing state
        $|\Upsilon(q)\rangle := \frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x} \in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^q \pi^{-1} \langle O_j - \tilde{u}_j^{(q)} \mathbf{1}\rangle} |\boldsymbol{x}\rangle$
    after $p$-qubit inverse quantum Fourier transformations.
    Here, $\delta^{(q)} := c/8^{q_{\max}-q}$ is a failure probability.
    Set the coordinate-wise median of the measurement outputs as $g_j^{(q)}$.
    Update $\tilde{u}_j^{(q+1)} := \tilde{u}_j^{(q)} + \pi 2^{-q} g_j^{(q)}$
    Truncate $\tilde{u}_j^{(q+1)}$ in $[-1,1]$
end for
return final estimates $\tilde{u}_j := \tilde{u}_j^{(q_{\max}+1)}$
```

46] to the quantum gradient estimation [24, 25], which efficiently estimates the gradient ∇f of a smooth real scalar function $f(\boldsymbol{x})$ that is assumed to be encoded in an oracle; see Appendix A for the review of the gradient estimation. In the following, we focus on the estimation performance and the total query complexity regarding the use of U_ψ and $U_\psi^\dagger$ in Algorithm 1. Also, we provide its high-level overview in Fig. 1. Appendix B gives complete proof of theorems together with showing concrete implementation method for the algorithm.

The key idea of the proposed adaptive algorithm is to prepare the following *probing* state $|\Upsilon(q)\rangle$ at each iteration step q, from which the approximated expectation values can be extracted via the gradient estimation algorithm [24, 25]:

$$|\Upsilon(q)\rangle := \frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x} \in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^q \pi^{-1} \langle O_j - \tilde{u}_j^{(q)} \mathbf{1}\rangle} |\boldsymbol{x}\rangle\,, \tag{1}$$

where $\mathbf{1}$ denotes the identity operator. Also, p denotes a fixed precision parameter and G_p^M is defined as a set of grid points:

$$G_p := \left\{\frac{\mu}{2^p} - \frac{1}{2} + \frac{1}{2^{p+1}} : \mu \in \{0, 1, \cdots, 2^p - 1\}\right\}.$$

Note that we label the pM-qubit computational basis $|\mu_1\rangle|\mu_2\rangle ... |\mu_M\rangle$ ($\mu_j \in \{0, 1, ..., 2^p - 1\}$) by each grid point $\boldsymbol{x} = (x_1, x_2, ..., x_M)$ in G_p^M via one-to-one correspondence between G_p and the computational basis set. The quantities $\tilde{u}_j^{(q)} \in [-1, 1]$ in the probing state Eq. (1) are temporal estimated values for $\langle O_j\rangle$ at the iteration step q. Later we will show that $p = 3$ is sufficient for our algorithm to successfully work.

The probing state $|\Upsilon(q)\rangle$ can be prepared by first intializing the pM-qubit probe system, the $\log_2 d$-qubit target system, and some ancilla systems to encode the observables. Then, applying a q-dependent interaction unitary on the whole system and then performing a postselection on the target-ancilla systems, we approximately obtain the probing state. The query complexity regarding U_ψ and $U_\psi^\dagger$ of this state preparation process is given as follows.

Corollary 1 (Probing state preparation)**.** *Suppose that we have access to block-encoded $d \times d$ observables $\{O_j\}_{j=1}^M$ via some unitaries, a $\log_2 d$-qubit state preparation U_ψ, and its inverse $U_\psi^\dagger$, such that $M > \mathcal{O}(\log d)$ holds. Then, we can prepare the probing state $|\Upsilon(q)\rangle$, up to 1/12 Euclidean distance error, for (any) integer $q \geq 0$ and $\tilde{u}_j^{(q)} \in [-1, 1]$, using $\mathcal{O}(2^q\sqrt{M \log d})$ queries to U_ψ and $U_\psi^\dagger$ in total.*

This corollary directly follows from Theorem 7 and 8 shown in the next section, both of which give methods to prepare the probing state $|\Upsilon(q)\rangle$: one is based on the Hamiltonian simulation protocol (Theorem 7), and the other is based on the Grover-like repetition (Theorem 8).

Suppose we have the probing state $|\Upsilon(q)\rangle$ at the qth iteration, with a temporal estimate $\tilde{u}_j^{(q)}$ for $\langle O_j\rangle$. Then, on the phase of $|\boldsymbol{x}\rangle$ in $|\Upsilon(q)\rangle$, the estimation error $\langle O_j - \tilde{u}_j^{(q)} \mathbf{1}\rangle$ is amplified by the factor of 2^q; this means that when $\tilde{u}_j^{(q)}$ matches $\langle O_j\rangle$ in the first q binary (fraction) digits as

$$\left|\langle O_j\rangle - \tilde{u}_j^{(q)}\right| \leq \frac{1}{2^q}, \tag{2}$$

the 2^q-fold amplification *zooms in* on the significant digits of $\langle O_j\rangle - \tilde{u}_j^{(q)}$ to shift the values toward upper digits. As proved in Ref. [25], the gradient estimation for $|\Upsilon(q)\rangle$ can simultaneously extract these zoomed-in values $2^q \langle O_j - \tilde{u}_j^{(q)} \mathbf{1}\rangle$ (with $1/\pi$) or equivalently the gradient of the linear function on the phase:

$$f(\boldsymbol{x}) := \frac{1}{\pi} \sum_j x_j 2^q \langle O_j - \tilde{u}_j^{(q)} \mathbf{1}\rangle\,,$$

with an additive error specified by the precision parameter p and a certain success probability (see Lemma 9).

Note that, in our case, the gradient estimation algorithm is simply to perform the computational basis measurement (with rewriting $|\mu\rangle$ as $|x\rangle$) on the probing state after applying a slightly modified version of p-qubit inverse quantum Fourier transformation, which is defined in Eq. (A6).

In step 4 of Algorithm 1, we use the measurement outputs $\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}, ..., \boldsymbol{k}^{(\mathcal{O}(\log M/\delta^{(q)}))}$ obtained in Step 3 to construct the coordinate-wise median $g_j^{(q)}$; that is, $g_j^{(q)}$ is defined as the middle value separating the greater and lesser halves of $\{k_j^{(1)}, k_j^{(2)}, ...\}$. Then, under the condition of Eq. (2), we can prove that the median $g_j^{(q)}$ satisfies

$$\left| g_j^{(q)} - \frac{2^q \langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle}{\pi} \right| \le \frac{1}{2\pi}, \tag{3}$$

for all $j = 1, 2, ..., M$ with success probability bigger than $1 - \delta^{(q)}$; later we will carefully choose the probability $\delta^{(q)}$ in order that a final estimator has the minimal statistical uncertainty. Using the successfully obtained $g_j^{(q)}$ satisfying Eq. (3), we update the temporal estimate as

$$\tilde{u}_j^{(q+1)} := \tilde{u}_j^{(q)} + \pi 2^{-q} g_j^{(q)}.$$

Then, it is straightforward to prove

$$\left| \langle O_j \rangle - \tilde{u}_j^{(q+1)} \right| \le \frac{1}{2^{q+1}},$$

for all j. Thus, using the outcomes from the gradient estimation algorithm at each step, we can iteratively determine one binary fraction digit of the target value $\langle O_j \rangle$ by updating $\tilde{u}_j^{(q)}$ to $\tilde{u}_j^{(q+1)}$. Repeating this iteration step $q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$ times, we obtain estimates for $\{\langle O_j \rangle\}_j$ within the root MSE ε.

Now, we describe the above result in a precise way. A more detailed proof is given in Appendix B 2.

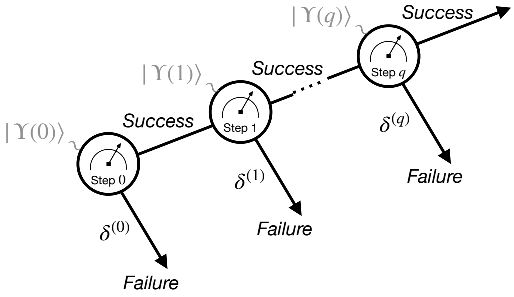
Theorem 2 (Heisenberg-limited multiple observables estimation). ***Let*** *$\varepsilon \in (0, 1)$ be a target precision. For given M observables $\{O_j\}_{j=1}^M$ and a state preparation U_ψ, there exists a quantum algorithm that outputs a sample from estimators $\{\hat{u}_j\}_{j=1}^M$ for $\{\langle O_j \rangle\}$ satisfying*

$$\max_{j=1,2,...,M} \text{MSE}[\hat{u}_j] \le \varepsilon^2, \tag{4}$$

using $\mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M)$ queries to the state preparation U_ψ and $U_\psi^\dagger$ in total. Here, the mean squared error of an estimator $\hat{u}_j$ is defined as

$$\text{MSE}[\hat{u}_j] := \mathbb{E}\left[(\hat{u}_j - \langle O_j \rangle)^2 \right].$$

Sketch of the proof. The outline of the proof is similar as that of the previous methods for Heisenberg-limited phase estimation or its application [29, 45, 46, 50], but it is required to carefully check the condition for gradient estimation at each iteration step. Specifically, this condition is given by Eq. (2) for all j. If this condition holds and the precision parameter p is taken as $p = 3$, then a single shot measurement result $\boldsymbol{k} := (k_1, ..., k_M) \in G_p^M$ in Step 3 of Algorithm 1 follows



: Gradient estimation at step q

FIG. 2. Probability tree diagram in Algorithm 1.

$$\Pr\left[\left| k_j - \frac{2^q(\langle O_j \rangle - \tilde{u}_j^{(q)})}{\pi} \right| > \frac{1}{2\pi} \right] < \frac{1}{3}, \tag{5}$$

for every $j = 1, 2, \cdots, M$. The derivation of this inequality is based on our numerical finding; see Appendix B 2. We remark that the failure probability represented by the left hand side of Eq. (5) can be exponentially suppressed to $\delta^{(q)}/M$ by using the coordinate-wise median $g_j^{(q)}$ of the measurement results over $\mathcal{O}(\log M/\delta^{(q)})$ copies of the (approximate) probing state, instead of the single shot result k_j. This repetition is the origin of the $\log M$ term in the total query complexity.

In the first iteration step $q = 0$, the condition Eq. (2) is trivially satisfied, and the gradient estimation can yield $1/2\pi$-close estimates of the target quantities for all j. This probability is at least $1 - \delta^{(0)}$ due to the union bound. As for the iteration step $q \ge 1$, if all of the previous steps succeed in the gradient estimation, we can show that Eq. (2) holds for all j at the iteration step q. On the other hand, if the gradient estimation fails at the iteration step q (while all processes have been successfully executed up to the $(q-1)$th step), the condition Eq. (2) is not satisfied; as a result, outputs of the gradient estimation may not improve the temporal estimate in the subsequent processes. However, in this case, it can be shown that the additive error $|\tilde{u}_j - \langle O_j \rangle|$ of the final estimate $\tilde{u}_j := \tilde{u}_j^{(q_{\max}+1)}$ is at most $(1+\pi)/2^q$ because the outputs of gradient estimation are always in $[-1/2, 1/2]$ from the definition of G_p^M. From the above analysis, we can bound the additive error of the final estimate for all branches in Fig. 2.

The failure probability $\delta^{(q)}$ should be very small at the beginning of iteration steps q because the error of top fraction bits have a significant impact on the MSE of the final estimator. From the analysis in Ref. [50], the choice of $\delta^{(q)} := c/8^{q_{\max}-q}$ $(c \in (0, 3/8(1+\pi)^2))$ is sufficient, and then the MSE of the final estimator $\hat{u}_j$ (its realization is $\tilde{u}_j$) is calculated as at most ε^2 for all $j = 1, 2, ..., M$, from the tree diagram Fig. 2 and the above error evaluation in each branch.

To derive the query complexity for the state preparation U_ψ, we use the result in Corollary 1. In the iteration step q, preparing $\mathcal{O}(\log M/\delta^{(q)})$ copies of the probing state Eq. (1) uses $\mathcal{O}(2^q \sqrt{M \log d} \log(M/\delta^{(q)}))$ queries to the state preparation unitary U_ψ and its inverse. Thus, the summation of the queries over $q = 0, 1, ..., q_{\max}$ ($q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$) is directly calculated as $\mathcal{O}(\varepsilon^{-1} \sqrt{M \log d} \log M)$, which completes the proof of Theorem 2. □

In Theorem 2, the scaling $1/\varepsilon$ of queries to U_ψ with respect to the root MSE ε achieves the same scaling to the Heisenberg limit (HL) in the gradient estimation, which is derived in Appendix A. We remark that, to the best of our knowledge, this is the first derivation of the HL in gradient estimation in terms of MSE, while the previous work [25] shows a similar lower bound (additionally, including $\sqrt{M}$ dependency) on queries to an oracle for a target function $f(\boldsymbol{x})$ on $\boldsymbol{x} \in G_p^M$, in another metric of statistical uncertainty (i.e., a confidence interval). Also, in the stringent measure of statistical uncertainty, the root MSE ε [28], all the existing works [26, 27] in multiple observables estimation only proves the nearly HL scaling that includes logarithmic terms on ε such as $\log(M/\varepsilon)$.

In addition to the Heisenberg-limited scaling regarding ε, our protocol has the nearly squared root dependence regarding the total number of observables M. This is a nearly quadratic improvement regarding M compared to the standard method (i.e., quantum amplitude estimation) of estimating the expectation values of observables. Furthermore, when we focus on another metric of statistical uncertainty — a confidence interval comprised of estimators with an additive error $\pm\epsilon_{\rm add}$ for some confidence level, which is considered in Refs. [26, 27], the query complexity of our method is essentially optimal in terms of M and $\epsilon_{\rm add}$ as well as these previous methods. Here, the query lower bound in multiple observables estimation in terms of a confidence interval is proved in Ref. [27] as follows.

Lemma 3 (Corollary 3 in Ref. [27])**.** *Let M be a positive integer power of 2 and let $\epsilon_{\rm add} \in (0, 1/3\sqrt{M})$. Let $\mathcal{A}$ be any algorithm that takes as an input an arbitrary set of M observables $\{O_j\}_{j=1}^M$. Suppose that, for every quantum state $|\psi\rangle$, accessed via a state preparation oracle U_ψ, $\mathcal{A}$ outputs estimates of each $\langle\psi| O_j |\psi\rangle$ to within additive error $\epsilon_{\rm add}$ with high probability at least $2/3$. Then, there exists a set of observables $\{O_j\}_{j=1}^M$ such that $\mathcal{A}$ applied to $\{O_j\}_{j=1}^M$ must use $\Omega(\epsilon_{\rm add}^{-1}\sqrt{M})$ queries to U_ψ.*

The proposed algorithm can be easily extended to an estimation protocol that outputs an $\epsilon_{\rm add}$-close estimate of $\{\langle O_j \rangle\}_j$ with high probability ($\geq 2/3$) at the cost of a slight increase of the total query complexity (i.e., $\mathcal{O}(\epsilon_{\rm add}^{-1}\sqrt{M}\log^2 M)$) [51]. Consequently, we establish from the Lemma 3 that this extended protocol achieves the worst-case query optimality (up to the $\log^2 M$ correction) in the high-precision regime $\epsilon_{\rm add} \in (0, 1/3\sqrt{M})$.

Finally, we remark that the preparation and measurement for multiple copies of the probing state in step 3 of Algorithm 1 can be performed in parallel if we are allowed to use multiple quantum computers, which may practically important to reduce the total execution time.

IV. STATE PREPARATION FOR ADAPTIVE GRADIENT ESTIMATION

In this section, we provide two quantum algorithms to prepare the probing state Eq. (1), using the state preparation U_ψ, $U_\psi^\dagger$, and the unitary gates $\{B_j\}_{j=1}^M$ that encode the target observables $\{O_j\}_{j=1}^M$ with the help of some ancilla system. The two methods are summarized in Theorems 7 and 8; Theorem 7 provides a method based on Hamiltonian simulation protocol, and Theorem 8 provides a method based on Grover-like repetition. Both Theorems 7 and 8 prove that the total space complexity to prepare the probing state $|\Upsilon(q)\rangle$ is $\mathcal{O}(M + \log_2 d)$. In addition, Theorem 8 shows an exponential improvement in the classical computation time for constructing explicit quantum circuits under a certain condition, compared to Theorem 7.

In the following, we first review an efficient quantum computation method of block-encoded matrices. Then, we describe the two methods for the probing state preparation.

A. Preliminary

Here, we review some important results in efficiently calculating block-encoded matrices on a quantum computer. The basic tool to represent matrices by unitary operators of dilated quantum systems is *block encoding*:

Definition 1 (Block encoding)**.** For positive values α, ε and a non-negative integer a, we say that an $(n + a)$-qubit unitary U is an (α, a, ε)-block-encoding of an n-qubit operator A, if

$$\|A - \alpha(\langle 0|^{\otimes a} \otimes \mathbf{1})U(|0\rangle^{\otimes a} \otimes \mathbf{1})\| \leq \varepsilon.$$

For simplicity, we shorten the perfect (i.e., $\alpha = 1$ and $\varepsilon = 0$) block encoding of A as a-block-encoding of A.

For instance, any unitary operator (e.g., a Pauli operator $X \otimes Z \otimes \cdots$) is trivially a 0-block-encoding of itself. There are various ways to construct block encodings; see Ref. [13]. Specifically, we here focus on the method called the linear combination of unitaries (LCU) [52, 53]. Let $A := \sum_{i=1}^m c_i U_i$ be a linear combination of unitary operators $\{U_i\}_{i=1}^m$ with real coefficients $c_i \in \mathbb{R}$. Without loss of generality, we assume $c_i > 0$ because -1 can be absorbed into U_i. In order to implement A, we use the

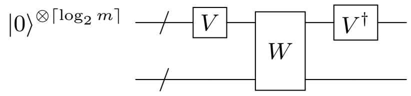


FIG. 3. Linear combination of unitaries (LCU) method. The circuit is a $\lceil\log_2 m\rceil$-block-encoding of $\|c\|_1^{-1}\sum_{i=1}^m c_iU_i$ ($c_i > 0$). PREPARE $V : |0\rangle^{\otimes\lceil\log_2 m\rceil} \mapsto \sum_{i=1}^m \sqrt{\frac{c_i}{\|c\|_1}}|i\rangle$ and SELECT $W = \sum_{i=1}^m |i\rangle\langle i| \otimes U_i$.

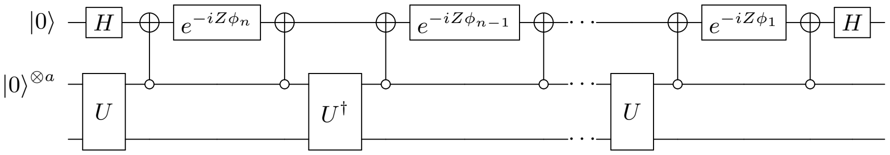


FIG. 4. Quantum circuit for quantum singular value (eigenvalue) transformation for real polynomials P of odd degree n. U denotes an a-block-encoding of a Hermitian operator A. The NOT gate is controlled by $|0\rangle^{\otimes a}$ of the a qubits, which is represented by the white circle $\circ$. For a given real polynomial P of degree n, the n circuit parameters $\{\phi_i\}_{i=1}^n$ are calculated in $\mathcal{O}(\text{poly}(n))$ classical computation time.

following two unitary operations. The first one, called PREPARE, encodes the positive coefficients $\{c_i\}_{i=1}^m$ as

$$V : |\mathbf{0}\rangle \mapsto \sum_{i=1}^m \sqrt{\frac{c_i}{\|c\|_1}}|i\rangle,$$

where $\|\bullet\|_1$ denotes L^1-norm, and $|\mathbf{0}\rangle$ and $|i\rangle$ denote an initial state and the computational basis in a $\lceil\log_2 m\rceil$-qubit ancilla system, respectively. The other, called SELECT, encodes the unitary operartors U_i conditioned by the $\lceil\log_2 m\rceil$-qubit ancilla system:

$$W = \sum_{i=1}^m |i\rangle\langle i| \otimes U_i.$$

Using the two operations V and W, it can be shown that the unitary operator $(V^\dagger \otimes \mathbf{1})W(V \otimes \mathbf{1})$ is a $(\|c\|_1, \lceil\log_2 m\rceil, 0)$-block-encoding of A, as in Fig. 3. Note that if the coefficients in LCU are controlled by other qubit registers, it may be useful to modify the PREPARE operator instead of including the phase of c_i to the SELECT operator, in order to save the number of controlled operations.

Once we have a block encoding of a target operator, we can systematically transform the block encoding to perform various tasks. Here, we show examples of such transformations that will be used in the following subsection.

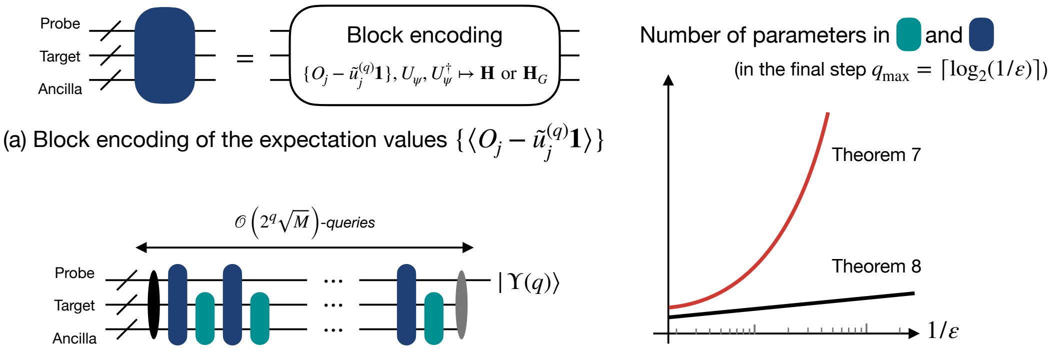
Lemma 4 (Uniform singular value amplification [13, 47])**.** *Let $\gamma > 1$ and let $\delta, \varepsilon \in (0, 1/2)$. Suppose we have an a-block-encoding U of A, $(\|A\| \le (1-\delta)/\gamma)$. Then, we can implement a $(1, a{+}1, \varepsilon)$-block-encoding of γA with $m = \mathcal{O}(\gamma\delta^{-1}\log(\gamma/\varepsilon))$ queries to U or $U^\dagger$, $2m$ uses of NOT gates controlled by a-qubit, $\mathcal{O}(m)$ single-qubit gates, and $\mathcal{O}(\text{poly}(m))$ classical computation to find quantum circuit parameters.*

Lemma 5 (Quantum eigenvalue transformation by Chebyshev polynomials [13])**.** *Let m be a positive integer, and let U be an a-block-encoding of a Hamiltonian H. Then, for the m-th Chebyshev polynomial of the first kind $T_m(x)$, we can implement a $(1, a, 0)$-block-encoding of $T_m(H)$, with m uses of U or $U^\dagger$ and m uses of reflection on $|0\rangle^{\otimes a}$.*

Lemma 6 (Optimal block-Hamiltonian simulation [49])**.** *Let $t \in \mathbb{R}\backslash\{0\}$, $\varepsilon'' \in (0, 1)$, and let U be a $(1, a, 0)$-block-encoding of a Hamiltonian H. Then, we can implement a $(1, a+2, \varepsilon'')$-block-encoding of e^{itH}, with $4Q$ queries to controlled U or its inverse, $2Q$ uses of NOT gates controlled by $(a+1)$-qubit, $\mathcal{O}(Q)$ uses of single-qubit or two-qubit gates, and $\mathcal{O}(\text{poly}(Q))$ classical computation to find quantum circuit parameters, where $Q = \mathcal{O}(t+\log(1/\varepsilon''))$.*

Lemma 4 and Lemma 5 can be implemented with a quantum circuit in Fig. 4. Also, we can implement the optimal Hamiltonian simulation Lemma 6 with a similar circuit as Fig. 4; the explicit circuit constructions are provided in Refs. [13, 49, 54].

Importantly, the quantum circuit in Fig. 4 reflects the underlying structure that are common in the above lemmas; this quantum circuit implements a general method, called the quantum singular value transformation (QSVT), to transform singular values (eigenvalues) of a block-encoded matrix based on a large class of polynomials [13]. The QSVT uses the idea of quantum signal processing (QSP) [48, 49] that characterizes achievable 1-qubit unitary transformations comprised of an alternating 1-qubit gate sequence of the *signal* rotation with


Probe
Target
Ancilla
=
Block encoding
$\{O_j - \tilde{u}_j^{(q)}\mathbf{1}\}, U_\psi, U_\psi^\dagger \mapsto \mathbf{H}$ or $\mathbf{H}_G$
Number of parameters in 🟩 and 🟦
(in the final step $q_{\max} = \lceil \log_2(1/\varepsilon) \rceil$)
Theorem 7
Theorem 8
$1/\varepsilon$
$\mathcal{O}\left(2^q\sqrt{M}\right)$-queries
Probe
Target
Ancilla
$|\Upsilon(q)\rangle$

(a) Block encoding of the expectation values $\{\langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle\}$

(b) Quantum circuit for probing state preparation

(c) Circuit parameters for QSP

FIG. 5. Preparation of the probing state $|\Upsilon(q)\rangle$ at the qth iteration. The blue unitary gate in (a) and (b) denotes a block-encoding of the Hamiltonian $\mathbf{H}$ or $\mathbf{H}_{\mathrm{G}}$ in Eq. (6) or (17), respectively, and the green unitary gate in (b) is a controlled rotation (or reflection) gate. The blue and green unitary gates contain parameterized gates for QSP, and the total number of circuit parameters scales as in (c) with respect to the target root MSE ε. As the graph in (c) indicates, the method in Theorem 8 has a much smaller number of circuit parameters for QSP compared to that of Theorem 7.

a unknown angle and the *processing* rotation with a controllable angle. To bridge the gap between QSP and QSVT, *Qubitization* [49] is a crucial technique that splits (a part of) ancilla-target systems into some qubits labeled by the eigenvalue (singular values [13]) and constructs parallel signal rotations over the qubits (e.g., U and $U^\dagger$ in Fig. 4). Here, the rotation angle depends on the corresponding singular value. Then, using additional processing rotations with controllable parameters $\{\phi_i\}$ (likewise the controlled rotation between U and $U^\dagger$ in Fig. 4), we can transform the singular values in parallel by a polynomial that depends on the controllable parameters $\{\phi_i\}$; the achievable polynomials in QSVT are characterized by QSP. See the review [55] for details of the theoretical perspective of QSVT.

In practice, a typical flow of QSVT consists of two steps: (i) finding the circuit parameter $\{\phi_i\}_{i=1}^n$ (called the phase sequence) for a given degree-n real polynomial P on classical computers, (ii) running the $\mathcal{O}(n)$-depth quantum circuit in Fig. 4 on a quantum computer, using the classically tuned parameters. Note that in the process (ii), we may need a post-selection on ancilla qubits. For a given degree-n polynomial P that has definite parity and $P(x) \in [-1, 1]$ for $x \in [-1, 1]$, the n circuit parameters $\{\phi_i\}_{i=1}^n$ in Fig. 4 can be found by $\mathcal{O}(\mathrm{poly}(n, \log(1/\delta)))$ classical computation for some error δ. Then, using the parameters this circuit results in an $(a + 1)$-block-encoding of $P(A)$. In Lemma 4, we can take an odd real polynomial $P(x)$ with degree $m = \mathcal{O}(\gamma\delta^{-1} \log(\gamma/\varepsilon))$ such that $P(x) \approx \gamma x$ holds [13, 47]. In particular, the phase sequence $\{\phi_i\}$ for the Chebyshev polynomial of the first kind T_n is analytically calculated and has a unique structure (Lemma 9 in Ref. [13]); as a result, we can eliminate the additional ancilla qubit and replace the $2n$ controlled NOT gates with n reflections on $|0\rangle^{\otimes a}$ in the circuit of Fig. 4.

B. Probing state preparation

Before proceeding to the proof of Theorems 7 and 8, we first provide an overview of our method to prepare $|\Upsilon(q)\rangle$ in Fig. 5. As seen in the figure, the proposed two methods to prepare $|\Upsilon(q)\rangle$ have a similar structure: Fig. 5(a) shows the block encoding of a Hamiltonian that encodes the expectation values of observables $\langle O_j - \tilde{u}_j^{(q)}\mathbf{1}\rangle$ and Fig. 5(b) shows alternating applications of the block encoding and a processing operation with a tuned parameter, which is based on Lemma 5 or Lemma 6. In the proof of Theorems 7 and 8, we depict the circuit for (a) and (b), respectively; then we evaluate the approximation error between the final state of the circuit and the probing state $|\Upsilon(q)\rangle$.

More detailed proofs and explicit quantum circuit diagrams for these Theorems are provided in Appendix B.

1. *Hamiltonian simulation*

Theorem 7 (Informal. Lemma 13)**.** *Suppose that we have access to block-encoded $d \times d$ observables $\{O_j\}_{j=1}^M$, a $\log_2 d$-qubit state preparation U_ψ, and its inverse $U_\psi^\dagger$, such that $M > \mathcal{O}(\log d)$. Then, we can prepare the probing state $|\Upsilon(q)\rangle$ for any integer $q \geq 0$ and $\tilde{u}_j^{(q)} \in [-1, 1]$ up to $1/12$ Euclidean distance error, using an*

$$\mathcal{O}(M + \log_2 d)\text{-}qubit$$

circuit regardless of q. Furthermore, each quantum circuit with q requires

$$\mathcal{O}(\mathrm{poly}(2^q\sqrt{M \log d}) + \mathrm{poly}(\sqrt{M}(q + \log M)))$$

classical computation for finding circuit parameters, and it consists of

$$\mathcal{O}(2^q\sqrt{M\log d}) \ \ \textit{uses of} \ \ U_\psi \ \textit{and} \ U_\psi^\dagger,$$

$\mathcal{O}(2^qM(q+\log M))$ uses of unitary gates for block-encoded observables, and $\mathcal{O}(2^qM(q+\log M)\log dM)$ uses of single-qubit and two-qubit gates.

Sketch of the proof. In this Theorem, we take the Hamiltonian $\mathbf{H}$ to encode the observables $\{O_j\}$ as

$$\mathbf{H} := \sum_{\boldsymbol{x}\in G_p^M} \tilde{f}(\boldsymbol{x})\,|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\,, \tag{6}$$

where the target observables are approximately encoded in the eigenvalues $\tilde{f}(\boldsymbol{x})$ as

$$\tilde{f}(\boldsymbol{x}) \approx \frac{1}{\sigma}\sum_{j=1}^{M} x_j\,\langle\tilde{O}_j^{(q)}\rangle\,, \quad \sigma = \mathcal{O}(\sqrt{M\log d}), \tag{7}$$

Here, σ denotes the rescaling factor of the Hamiltonian $\mathbf{H}$ such that $\mathbf{H}$ can be encoded in a unitary operator. Also, we defined $\tilde{O}_j^{(q)} := (O_j - \tilde{u}_j^{(q)}\mathbf{1})/2$ for the identity $\mathbf{1}$. The approximation error in Eq. (7) is specified below.

Setting aside the details for now, we suppose that we have a (perfect) block encoding of the Hamiltonian $\mathbf{H}$ that acts on the pM-qubit probe system, $\log_2 d$-qubit target system, and ancilla systems (specified below), as illustrated in Fig. 5. Then, the optimal Hamiltonian simulation protocol Lemma 6 yields a quantum circuit W for an ϵ'-precise block encoding of time evolution operator

$$e^{i\mathbf{H}t} = \sum_{\boldsymbol{x}\in G_p^M} e^{i\tilde{f}(\boldsymbol{x})t}\,|\boldsymbol{x}\rangle\langle\boldsymbol{x}| \tag{8}$$

with time $t > 0$, using $\mathcal{O}(t + \log(1/\epsilon'))$ queries to the block encoding of $\mathbf{H}$. Note that in the case $t = 2\sigma t'$ for some positive integer t', the resulting time evolution operator approximates t' times applications of the *phase oracle* for an affine linear function $f(\boldsymbol{x}) = \sum_j x_j\,\langle O_j\rangle$ in the theory of gradient estimation. Then, applying W for

$$t := 2^{p+q+2}\sigma$$

to the uniform superposition state $|+\rangle^{\otimes pM}$ in the probe system and the initial state $|\mathbf{0}\rangle$ in the ancilla-target systems, we can approximately prepare the target state:

$$\begin{aligned} &W\,|+\rangle^{\otimes pM}\,|\mathbf{0}\rangle \\ &\quad\approx \frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^q \pi^{-1}\langle O_j - \tilde{u}_j^{(q)}\rangle}\,|\boldsymbol{x}\rangle\,|\mathbf{0}\rangle\,. \end{aligned} \tag{9}$$

From the triangle inequality, this approximation error is given by the sum of ϵ' (more precisely, $\epsilon' + \sqrt{2\epsilon'}$ in Euclidean distance) from the transformation $\mathbf{H} \mapsto e^{i\mathbf{H}t}$ and the error from the observable encoding in Eq. (7), that is,

$$\epsilon' + \sqrt{2\epsilon'} + \left\|\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x}\in G_p^M} e^{i\tilde{f}(\boldsymbol{x})t}\,|\boldsymbol{x}\rangle - |\Upsilon(q)\rangle\right\|. \tag{10}$$

To quantify the error of the third term in Eq. (10) (or the error of Eq. (7)), we here construct the block encoding of the Hamiltonian $\mathbf{H}$ from the state preparation U_ψ ($U_\psi^\dagger$) and unitary gates $\{B_j\}$ that are a-block-encodings of observables $\{O_j\}$ for some $a \in \mathbb{N}$. First, we can construct a quantum circuit $U^{(\boldsymbol{x})}$ for a block encoding $M^{-1}\sum_{j=1}^M x_j\tilde{O}_j^{(q)}$ (with the rescaling factor M, instead of σ) for a given $\boldsymbol{x} \in G_p^M$, via the LCU method with the controlled version of each B_j. The LCU requires additional $\mathcal{O}(\log M)$ qubits to encode the coefficients $\{x_j/M\}$. Using controlled versions of $U^{(\boldsymbol{x})}$, we can obtain a quantum circuit for

$$U'_{\mathrm{SEL}} := \sum_{\boldsymbol{x}\in G_p^M} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes U^{(\boldsymbol{x})}. \tag{11}$$

Here, we remark that the resulting quantum circuit for Eq. (11) has at most $\mathcal{O}(pM\log(1/\delta))$-depth for some implementation error δ that comes from the encoding of the coefficients $\{x_j/M\}$; see Remark 11.

Then, the circuit

$$\left(\mathbf{1}\otimes U_\psi^\dagger\right)\cdot U'_{\mathrm{SEL}}\cdot(\mathbf{1}\otimes U_\psi) \tag{12}$$

is a block encoding of the following Hamiltonian:

$$\mathbf{H}' := \sum_{\boldsymbol{x}}\left(\sum_j x_j\cdot\frac{\langle\tilde{O}_j^{(q)}\rangle}{M}\right)|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\,.$$

This Hamiltonian $\mathbf{H}'$ has the normalization factor M that is quadratically larger than σ in $\mathbf{H}$. In estimating the expectation value $\langle\tilde{O}_j^{(q)}\rangle$ via gradient estimation, we need to amplify $\mathbf{H}'$ by the factor M to prepare Eq. (1). This means that we need the time evolution operator $e^{i\mathbf{H}'t}$ of $t = 2^{p+q+2}M$, which results in no speedup for the total queries to U_ψ regarding the number M of observables. To obtain the quadratic speedup regarding M, the method in Ref. [26] uses the singular value amplification Lemma 4. Importantly, this amplification can be performed with no use of U_ψ. From the random matrix series inequality, we can show that for a large part of G_p^M (more precisely, for a subset $F \subset G_p^M$ such that $|F| \geq (1-\delta')|G_p^M|$ for any $\delta' > 0$), the condition of the amplification is satisfied for $\gamma = M/\sigma = \mathcal{O}(\sqrt{M})$, as well as the analysis in Ref. [26]. Therefore, we can amplify the block encoding $U^{(\boldsymbol{x})}$ by γ for such $\boldsymbol{x} \in F$; as a result, we have a quantum circuit for

$$U_{\mathrm{obs}} := \sum_{\boldsymbol{x}\in G_p^M} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes U_{\mathrm{obs}}^{(\boldsymbol{x})}, \tag{13}$$

where $U_{\text{obs}}^{(\boldsymbol{x})}$ is an ϵ''-precise block encoding of the Hamiltonian $\sigma^{-1}\sum_j x_j \tilde{O}_j^{(q)}$ if $\boldsymbol{x} \in F$. By multiplying U_ψ and $U_\psi^\dagger$ into U_{obs} as well as Eq. (12), we finally arrive at the block encoding of the Hamiltonian $\mathbf{H}$. We note that the amplification is valid when $\sigma = \mathcal{O}(\sqrt{M \log_2 d})$ is smaller than M, and this is satisfied by the condition $M > \mathcal{O}(\log d)$.

Since the block encoding $\mathbf{H}$ consists of (i) the LCU method, (ii) adding the pM-qubit control to $U^{(\boldsymbol{x})}$, (iii) the singular value amplification, and (iv) multiplying the conjugation of U_ψ, the main contribution to the space complexity comes from the steps (i) and (ii). The other processes (iii), (iv), and the Hamiltonian simulation protocol $\mathbf{H} \mapsto e^{i\mathbf{H}t}$ introduce constant or no ancilla qubits. The LCU method (i) introduces $\mathcal{O}(\log M)$-qubit registers, and thus the number of qubits of U'_{SEL} scales as $pM + \log M + \log d$. Recalling that the precision parameter p is fixed to a constant (i.e, $p = 3$) in the probing state $|\Upsilon(q)\rangle$, we conclude that the total space complexity is $\mathcal{O}(M + \log_2 d)$, which is independent of the root MSE ε.

As for the gate complexity, we here focus on the number of queries to U_ψ (or $U_\psi^\dagger$) and U'_{SEL}. A comprehensive analysis on the total gate complexity is provided in Lemma 13. Here, we need to carefully choose the parameters $\varepsilon', \varepsilon''$, and δ' so that the entire approximation error Eq. (10) is smaller than $1/12$; in particular, this is achieved by taking ε' and δ' as some constants, and $\varepsilon'' = \mathcal{O}(1/(2^q\sigma))$. Since the block encoding of $\mathbf{H}$ consists of two uses of U_ψ and $U_\psi^\dagger$ and $m := \mathcal{O}(M\sigma^{-1}\log(M/(\sigma\varepsilon'')))$ uses of control-U'_{SEL}, then the total queries can be evaluated by multiplying $\mathcal{O}(t)$ for the Hamiltonian simulation protocol, which proves the gate complexity in Theorem 7. In addition, the number of circuit parameters for the singular value amplification (iii) and the Hamiltonian simulation protocol are given by m and t, respectively. Thus, we need to tune the parameters in classical $\mathcal{O}(\text{poly}(m))$ and $\mathcal{O}(\text{poly}(t))$ time, as discussed in Sec. IV A. □

Our scheme has a significant improvement in space complexity compared to the previous non-iterative counterparts [26, 27]. While the non-iterative methods determine all of the $\mathcal{O}(\log 1/\varepsilon)$ binary fraction bits of $\langle O_j \rangle$ by a single quantum circuit with additional $\mathcal{O}(M\log(1/\varepsilon))$ (or $\mathcal{O}(M\log(M/\varepsilon))$) qubits to read out the observables, our scheme determines only 1 binary fraction bit of $\langle O_j \rangle$ at each iteration step. Specifically, the previous non-iterative method [26] uses the Hamiltonian simulation with $t = 2^p$ in Eq. (8), where the number of read-out qubits is $p = \mathcal{O}(\log(\sqrt{M\log d}/\varepsilon))$ (i.e., $q = 0$). In contrast, by the adaptive nature of our scheme, space overhead of quantum circuits for the probing states $|\Upsilon(q)\rangle$ is $\mathcal{O}(M)$ ($\mathcal{O}(M + \log_2 d)$ in total), and this is independent of the estimation precision ε. Here, a similar improvement of space overhead can be found in the previous works on the adaptive (iterative) versions of quantum phase estimation [3, 29, 31, 45, 46]. Also, we remark that the significant reduction of space overhead directly leads to the reduction of the number of controlled operations, which is also crucial in practical implementation.

2. *Grover-like repetition*

The quantum circuit employed in Theorem 7 requires classical tuning of $\tilde{\mathcal{O}}(\sqrt{M}/\varepsilon)$ circuit parameters (more precisely, $\tilde{\mathcal{O}}(2^q\sqrt{M})$ parameters in step q) for QSP. The classical computation for finding $\tilde{\mathcal{O}}(\sqrt{M}/\varepsilon)$ parameters is also required in the existing work by van Apeldoorn *et al.* [26]. However, it is challenging to find such a large number of circuit parameters in a stable way as pointed out in previous works [40–44], while the n-parameter finding can be performed by $\mathcal{O}(\text{poly}(n, \log(1/\delta)))$ classical computation for some error δ in theory [13].

To avoid the numerical instability, we here provide an alternative way to prepare the probing state (1) using the *Grover-like repetition*, which is a special case of QSP such that the corresponding quantum circuit parameters are analytically derived.

Theorem 8 (Informal. Lemma 14)**.** *Suppose we have access to block-encoded $d \times d$ observables $\{O_j\}_{j=1}^M$, a $\log_2 d$-qubit state preparation U_ψ, and its inverse $U_\psi^\dagger$, such that $M > \mathcal{O}(\log d)$. If the iteration step $q \geq 0$ satisfies the following condition ($\delta' := 2^{-14}$)*

$$q \geq \log_4 \left[\frac{2^3 \cdot 33^3}{625 \ln(2d/\delta')} \frac{\left\lceil \sqrt{2(M+1)\ln(2d/\delta')} \right\rceil}{\sqrt{\ln(2d/\delta')}} \right], \quad (14)$$

and for given $\tilde{u}_j^{(q)} \in [-1, 1]$,

$$\left| \langle\psi| \left(O_j - \tilde{u}_j^{(q)} \mathbf{1} \right) |\psi\rangle \right| \leq 2^{-q} \quad \textit{for all} \quad j = 1, 2, ..., M, \quad (15)$$

holds, then we can successfully prepare the probing state $|\Upsilon(q)\rangle$ up to $1/12$ Euclidean distance error, with probability at least 0.462 with ancilla qubits measurement result indicating success, using an

$$\mathcal{O}(M + \log_2 d)\textit{-qubit}$$

circuit regardless of q. Furthermore, each quantum circuit with q requires

$$\mathcal{O}(\text{poly}(\sqrt{M}(q + \log M)))$$

classical computation, and it has the same gate complexity as that of Theorem 7.

Here, we remark that the condition Eq. (15) is trivially satisfied at the iteration step q in Algorithm 1 when all the previous gradient estimations are successfully performed, as discussed in Sec. III.

Sketch of the proof. This method uses eigenvalue transformation of (a slightly modified version of) the Hamiltonian $\mathbf{H}$ in Eq. (6) based on the Chebyshev polynomial of the first kind $T_t(x)$, that is, Lemma 5. Here, the degree t is given by $t = 2^{p+q+2}\sigma$. We note that since the resulting operator $T_t[\mathbf{H}]$ is non-unitary, post-selection of ancilla qubits in the block encoding is required to implement $T_t[\mathbf{H}]$, meaning that the state preparation by this method is stochastic. As mentioned in Sec. IV A, the eigenvalue transformation based on the Chebyshev polynomials $T_t(x)$ can be considered as a special case in QSVT; that is, it has an analytical solution of circuit parameters (or phase sequence). Therefore, in this alternative method, the circuit parameter finding is required only for the construction of the Hamiltonian $\mathbf{H}$; the total runtime for the classical computation is at most $\mathcal{O}(\mathrm{polylog}(1/\varepsilon))$ (more precisely, $\mathcal{O}(\mathrm{poly}(\sqrt{M}(q + \log M)))$ at step $q \leq \lceil \log_2(1/\varepsilon) \rceil$).

Now, we consider the action of the resulting operator $T_t[\mathbf{H}]$. Applying $T_t[\mathbf{H}]$ to the uniform superposition state $|+\rangle^{\otimes pM}$, we obtain an unnormalized state proportional to

$$\sum_{s=\pm1} \sum_{\boldsymbol{x} \in G_p^M} e^{ist \arccos\left[\tilde{f}(\boldsymbol{x})\right]} |\boldsymbol{x}\rangle \,. \tag{16}$$

Therefore, we need to correct the phase of $|\boldsymbol{x}\rangle$ from $e^{\pm it \arccos[\tilde{f}(\boldsymbol{x})]}$ to $e^{it\tilde{f}(\boldsymbol{x})}$ in order to match the probing state $|\Upsilon(q)\rangle$.

As for the sign $s = \pm 1$ of the phase, we can correct it by slightly modifying the Hamiltonian $\mathbf{H}$ with the help of an additional 1-qubit ancilla system. Let $\mathbf{H}_{\mathrm{G}}$ be a Hamiltonian defined as

$$\mathbf{H}_{\mathrm{G}} := \sum_{(\boldsymbol{x},y) \in G_p^M \times G_1} \tilde{f}'(\boldsymbol{x}, y) \, |\boldsymbol{x}, y\rangle \langle \boldsymbol{x}, y| \,, \tag{17}$$

where $|y\rangle$ denotes a computational basis on the additional ancilla system and

$$\tilde{f}'(\boldsymbol{x}, y) \approx \frac{1}{\sigma'} \left(y \, \langle O_{M+1} \rangle + \sum_{j=1}^{M} x_j \, \langle \tilde{O}_j^{(q)} \rangle \right) . \tag{18}$$

Here, O_{M+1} denotes a 1-qubit observable proportional to the identity that acts on the additional ancilla system, and $\sigma' = \mathcal{O}(\sqrt{M \log d})$ is the rescaling factor for block encoding. The block encoding of $\mathbf{H}_{\mathrm{G}}$ can be constructed in a similar way to that of the Hamiltonian $\mathbf{H}$; the corresponding circuit has the same complexity as that of $\mathbf{H}$. Then, applying $T_t[\mathbf{H}_{\mathrm{G}}]$ to the uniform superposition state $|+\rangle^{\otimes pM+1}$, we can show that the following holds: (for simplicity, we write O_{M+1} as $\tilde{O}_{M+1}^{(q)}$)

$$\begin{aligned} \frac{1}{\mathcal{N}_t \sqrt{2^{pM}}} \sum_{\boldsymbol{x},y} T_t \left(\tilde{f}'(\boldsymbol{x}, y) \right) |\boldsymbol{x}, y\rangle &\approx \frac{1}{2\sqrt{2^{pM}}} \sum_{s=\pm1} \sum_{(\boldsymbol{x}, x_{M+1}) \in G_p^M \times G_1} e^{ist\left(\pi/2 - (\sigma')^{-1} \sum_{j=1}^{M+1} x_j \langle \tilde{O}_j^{(q)} \rangle\right)} |\boldsymbol{x}\rangle \, |x_{M+1}\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{s=\pm1} \left(\frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x} \in G_p^M} e^{2\pi i 2^p \sum_{j=1}^{M} (s x_j) \pi^{-1} 2^{q+1} \langle \tilde{O}_j^{(q)} \rangle} |\boldsymbol{x}\rangle \otimes \frac{1}{\sqrt{2}} \sum_{k \in G_1} e^{2\pi i 2k(s/4)} |k\rangle \right) , \end{aligned} \tag{19}$$

where $\mathcal{N}_t$ is the normalization factor. In the second equality, we chose the constant factor of O_{M+1} as

$$O_{M+1} := \frac{\pi(1/4 + 4l)}{2^{p+q}} I,$$

where l is an arbitrary integer satisfying $\|2^{q+1} O_{M+1}\| \leq 1$ and I denotes the 1-qubit identity. In the next paragraph, we explain the approximation of the first line in Eq. (19) in detail. The sign $s = \pm 1$ in Eq. (19) can be corrected as follows. By applying the inverse quantum Fourier transformation to the 1-qubit additional ancila system in the state Eq. (19), followed by controlled $X^{\otimes pM}$ gate (which flips the sign as $X^{\otimes pM} |\boldsymbol{x}\rangle = |-\boldsymbol{x}\rangle$), we obtain the probing state Eq. (1) in the pM-qubit registers.

The approximation in the first line of Eq. (19) comes from the non-linearity of the phase function $\arccos x$ in Eq. (16). Here, we recall that $\tilde{f}'(\boldsymbol{x}, y)$ is approximately given by the linear combination of $\langle O_j - \tilde{u}_j^{(q)} \mathbf{1} \rangle$. Using this fact, we can show that $|\tilde{f}'(\boldsymbol{x}, y)|$ scales as $\mathcal{O}(2^{-q})$ for a large part of $G_p^M \times G_1$ from the assumption of $|\langle \tilde{O}_j^{(q)} \rangle| \leq 1/2^{q+1}$ and the Hoeffding's inequality. Moreover, the error between the function $\arccos(x)$ and a linear function $\pi/2 - x$ can be upper bounded by $\mathcal{O}(|x|^3)$. As a result, the non-linearity of $\arccos x$ in Eq. (16) can be ignored for a large part of $G_p^M \times G_1$:

$$\left| \arccos\left[\tilde{f}'(\boldsymbol{x}, y)\right] - \left(\frac{\pi}{2} - \tilde{f}'(\boldsymbol{x}, y) \right) \right| = \mathcal{O}(2^{-3q}),$$

and it decreases much faster than the amplification $t = \mathcal{O}(2^q \sigma)$, as the iteration step q proceeds. Then, we prove the approximation error in Eq. (19) is at most $1/12$ in Euclieadn distance error under the assumption of this theorem. At the same time, we can evaluate the normalization factor as $|\mathcal{N}_t - 1| \leq 2\sqrt{6\delta'}$, thereby proving the post-selection probability $\mathcal{N}_t^2/2 > 0.462$.

Finally, we mention the space and gate complexity of this Theorem. As well as in the proof of Theorem 7, we can count the number of qubits in the block encoding of $\mathbf{H}_{\mathrm{G}}$, and it scales as $pM + \log M + \log d$ in total. Thus, the method has the space complexity $\mathcal{O}(M+\log_2 d)$ that is also independent of the target precision ε. As for the gate complexity, the main contribution comes from the eigenvalue transformation $\mathbf{H}_{\mathrm{G}} \mapsto T_t[\mathbf{H}_{\mathrm{G}}]$, which uses $t = \mathcal{O}(2^q\sigma')$ queries of the block encoding of $\mathbf{H}_{\mathrm{G}}$. This indicates that the gate complexity of the method is the same as that of the method in Theorem 7. □

In the alternative method, we require finding $\tilde{\mathcal{O}}(q\sqrt{M})$ circuit parameters, which comes from the singular value amplification to construct the Hamiltonian Eq. (17) than the Grover-like repetition. Thus, the alternative method shows an exponential improvement of runtime in classical computation with respect to the iteration q (or ε), compared to the method in Theorem 7 and the previous method [26], if certain conditions on the iteration step q are satisfied. Recalling that the iteration step is upper bounded by $q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$ for the target root MSE ε, the alternative method can be used if there exists the iteration steps q satisfying $q \leq q_{\max}$ and the inequality Eq. (14). In Sec. IV B 3, we numerically investigate the range of iteration steps q for the use of Theorem 8, especially for the case of $M = \mathcal{O}((\log_2 d)^k)$ for some k.

Finally, we mention the success probability of Theorem 8. While we cannot prepare the probing state $|\Upsilon(q)\rangle$ deterministically in the alternative method, the success probability can be easily boosted by a constant number of repetitions of the circuit runs. Therefore, the total query complexity remains unchanged when we use Theorem 8 instead of Theorem 7 to prepare the probing state of Eq. (1).

3. *Applicability condition for the probing state preparation by Grover-like repetition*

Here, we investigate the threshold of iteration step q in Theorem 8. We rewrite the threshold Eq. (14) as $q^* := \log_2(1/\varepsilon^*)$ by defining ε^* as

$$1/\varepsilon^* := \sqrt{C \ln^{-3/2}(2d/\delta') \left\lceil \sqrt{2(M+1)\ln(2d/\delta')} \right\rceil}, \quad (20)$$

where $C := 2^3 \cdot 33^3/625$. Since the iteration step q runs from 0 to $q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$, we need that the threshold $1/\varepsilon^*$ is smaller than the inverse of the target root MSE $1/\varepsilon$ in order to use the state preparation by the Grover-like repetition.

To clarify this point, we here plot the threshold $1/\varepsilon^*$ for several cases $M = N^1, N^2, N^3, N^4$, and 2^N under target system with the number of qubits $N \equiv \log_2 d$. In Fig. 6, we confirm that the threshold $\log_2(1/\varepsilon^*)$ converges to some constant (~ 5) in the case of $M = N^2$, which is consistent with Eq. (20) because $(1/\varepsilon^*)^2 = \mathcal{O}(\sqrt{M}/N)$ holds. Thus, particularly in this case $M = \mathcal{O}(N^2)$, the method in Theorem 8 is available in a wide range of target precision ε regardless of N. On the other hand, if the number of observables scales as 2^N, the threshold $\log_2(1/\varepsilon^*)$ increases linearly regarding N (note that the horizontal axis in Fig. 6 is logarithmic). This means that in the case of $M = \mathcal{O}(2^N)$, the Grover-based method is applicable only for small-size systems, otherwise the target precision ε is exponentially small with respect to N (the base of the exponential is $2^{-1/4} \approx 0.841$).

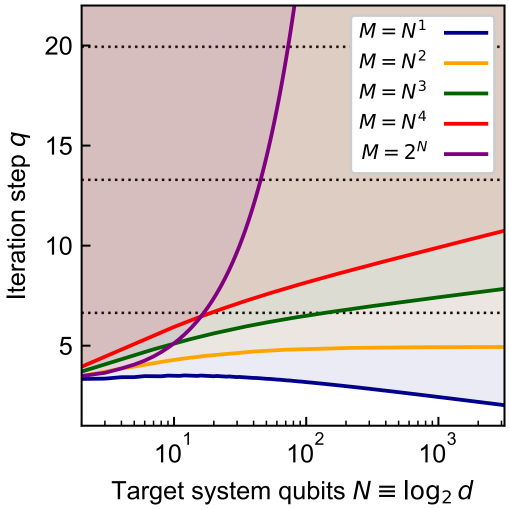


FIG. 6. The condition for the Grover-based state preparation (Theorem 8). The solid lines represent the threshold $q^* := \log_2(1/\varepsilon^*)$ of iteration steps in Eq. (20) (or Eq. (14)). When the iteration step q exceeds the solid lines, we can use the Grover-like repetition to prepare the probing state Eq. (1), instead of using Hamiltonian simulation. The horizontal dotted lines represent $q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$ for $\varepsilon = 10^{-2}$ (bottom), 10^{-4} (middle), and 10^{-6} (top), respectively.

Now, we focus on the case that we require more precise estimates as the number of observables M increases. From the definition of ε^*, if the desired precision ε satisfy $\varepsilon^2 \ll N/(C\sqrt{M})$, then there exists iteration steps q for the Grover-based method. Specifically, considering the desired precision is given by $\varepsilon = c_{\mathrm{mse}}/\sqrt{M} \in (0, 1/\sqrt{M})$ for some $c_{\mathrm{mse}} \in (0,1)$, we can evaluate the difference between the upper bound $q_{\max}$ of iteration steps and the threshold q^* as follows:

$$q_{\max} - q^* \geq \Omega\left(\log\left(N\sqrt{M}\right)\right). \quad (21)$$

Thus, the range of iteration step q such that the Grover-based method is available enlarges in this case, as N or M increases.

V. CONCLUSION

In this work, we proved that multiple quantum observables can be simultaneously estimated with quantum resources at the scaling of Heisenberg limit $1/\varepsilon$ for a root MSE ε. At the same time, the total resource shows a nearly quadratic improvement with respect to the number of observables M, compared to the standard method for this task i.e., the (modified) quantum amplitude estimation [21–23, 37–39]. The resources are quantified by the total number of queries to a state preparation unitary U_ψ whose complexity usually scales as the size of quantum system. We prove these results by explicitly constructing an adaptive quantum algorithm. The key idea of the proposed method is to prepare a quantum state with phases that encode the expectation values of observables, followed by the measurement for quantum gradient estimation [24, 25]. Then, our method determines a single binary digit of the target observables from the measurement outcomes and update the quantum state so that the next measurement has sufficient resolution to determine the next fraction bit. Importantly, our method can be considered as an extension of the iterative or adaptive phase estimation algorithms [3, 29, 31, 45, 46] to the gradient estimation algorithm.

In addition to the Heisenebrg-limited scaling in MSE, the proposed method significantly reduces the requirement of actual implementation, compared to the state-of-the-art algorithms for multiple observables estimation [26, 27]. First, the adaptive nature of the proposed method allows us to reduce an additional space overhead to $\mathcal{O}(M)$ qubits from $\mathcal{O}(M\log(1/\varepsilon))$ qubits in the previous methods. This results in a significant improvement on the space overhead when precise estimates of observables are required. Also, the proposed method can be executed in a parallel way during each iteration step, leading to reduction of the total execution time if we can use several quantum computers.

Next, in constructing quantum circuits of the proposed method, we provide two methods along with their quantum circuit diagrams; one is based on the optimal Hamiltonian simulation protocol and the other is based on Grover-like repetition. While the former can be used in any iteration steps q, in the final step, it requires classical finding of $\mathcal{O}(1/\varepsilon)$ circuit parameters, as well as the previous method, for quantum signal processing (QSP) [48, 49]. As shown in the previous works [42], such a circuit parameter finding requires $\sim 1/\varepsilon^2$ [sec] in classical computation time; the resulting numerical instability is one of the central problems in practical application of QSP or its extension, quantum singular value transformation (QSVT) [13]. The alternative method based on Grover-like repetition can avoid this problem by partially using the QSP for Chebyshev polynomials whose circuit parameters are analytically derived. As a result, the Grover-based method requires only $\mathcal{O}(\mathrm{polylog}(1/\varepsilon))$ classical computation in total, under a specific condition on q. This shows an exponential improvement in classical computation with respect to the target root MSE ε, thereby reducing the barrier of actual implementation significantly. As for the condition of the alternative method, we numerically investigate it in various setups such as $M = \mathcal{O}(N^k)$ for some k and size of target system N.

ACKNOWLEDGEMENTS

We thank fruitful discussions with Arjan Cornelissen and Yuki Koizumi. K.W. was supported by JSPS KAKENHI Grant Number JP 24KJ1963 and JST SPRING, Grant Number JPMJSP2123. N. Yamamoto was supported by MEXT Quantum Leap Flagship Program Grant Number JPMXS0118067285 and JPMXS0120319794, and JSPS KAKENHI Grant Number 20H05966. N. Y. wishes to thank by JST CREST Grant Number JPMJCR23I4, JST PRESTO No. JPMJPR2119, JST ERATO Grant Number JPMJER2302, JST Grant Number JPMJPF2221, and the support from IBM Quantum.

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum-enhanced measurements: beating the standard quantum limit, Science **306**, 1330 (2004).

[2] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nature photonics **5**, 222 (2011).

[3] B. L. Higgins, D. W. Berry, S. D. Bartlett, H. M. Wiseman, and G. J. Pryde, Entanglement-free heisenberg-limited phase estimation, Nature **450**, 393 (2007).

[4] E. M. Kessler, I. Lovchinsky, A. O. Sushkov, and M. D. Lukin, Quantum error correction for metrology, Phys. Rev. Lett. **112**, 150802 (2014).

[5] G. Arrad, Y. Vinkler, D. Aharonov, and A. Retzker, Increasing sensing resolution with error correction, Phys. Rev. Lett. **112**, 150801 (2014).

[6] W. Dür, M. Skotiniotis, F. Fröwis, and B. Kraus, Improved quantum metrology using quantum error correction, Phys. Rev. Lett. **112**, 080801 (2014).

[7] S. Zhou, M. Zhang, J. Preskill, and L. Jiang, Achieving the heisenberg limit in quantum metrology using quantum error correction, Nature communications **9**, 78 (2018).

[8] Y. Matsuzaki, S. C. Benjamin, and J. Fitzsimons, Magnetic field sensing beyond the standard quantum limit under the effect of decoherence, Phys. Rev. A **84**, 012103 (2011).

[9] A. W. Chin, S. F. Huelga, and M. B. Plenio, Quantum metrology in non-markovian environments, Phys. Rev. Lett. **109**, 233601 (2012).

[10] S. Lloyd, Universal quantum simulators, Science **273**, 1073 (1996), https://www.science.org/doi/pdf/10.1126/science.273.5278.1073.

[11] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon, Simulated quantum computation of molecular energies, Science **309**, 1704 (2005).

[12] A. M. Childs, D. Maslov, Y. Nam, N. J. Ross, and Y. Su, Toward the first quantum simulation with quantum speedup, Proceedings of the National Academy of Sciences **115**, 9456 (2018).

[13] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (2019) pp. 193–204.

[14] M. E. Beverland, P. Murali, M. Troyer, K. M. Svore, T. Hoeffler, V. Kliuchnikov, G. H. Low, M. Soeken, A. Sundaram, and A. Vaschillo, Assessing requirements to scale to practical quantum advantage, arXiv preprint arXiv:2211.07629 (2022).

[15] N. Yoshioka, T. Okubo, Y. Suzuki, Y. Koizumi, and W. Mizukami, Hunting for quantum-classical crossover in condensed matter problems, arXiv preprint arXiv:2210.14109 (2022).

[16] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, Quantum machine learning, Nature **549**, 195 (2017).

[17] Y. Liu, S. Arunachalam, and K. Temme, A rigorous and robust quantum speed-up in supervised machine learning, Nature Physics **17**, 1013 (2021).

[18] H.-Y. Huang, R. Kueng, G. Torlai, V. V. Albert, and J. Preskill, Provably efficient machine learning for quantum many-body problems, Science **377**, eabk3333 (2022).

[19] N. Stamatopoulos, D. J. Egger, Y. Sun, C. Zoufal, R. Iten, N. Shen, and S. Woerner, Option Pricing using Quantum Computers, Quantum **4**, 291 (2020).

[20] S. Chakrabarti, R. Krishnakumar, G. Mazzola, N. Stamatopoulos, S. Woerner, and W. J. Zeng, A threshold for quantum advantage in derivative pricing, Quantum **5**, 463 (2021).

[21] Y. Suzuki, S. Uno, R. Raymond, T. Tanaka, T. Onodera, and N. Yamamoto, Amplitude estimation without phase estimation, Quantum Information Processing **19**, 75 (2020).

[22] G. Wang, D. E. Koh, P. D. Johnson, and Y. Cao, Minimizing estimation runtime on noisy quantum computers, PRX Quantum **2**, 010346 (2021).

[23] K. Wada, K. Fukuchi, and N. Yamamoto, Quantum-enhanced mean value estimation via adaptive measurement, arXiv preprint arXiv:2210.15624 (2022).

[24] S. P. Jordan, Fast quantum algorithm for numerical gradient estimation, Phys. Rev. Lett. **95**, 050501 (2005).

[25] A. Gilyén, S. Arunachalam, and N. Wiebe, Optimizing quantum optimization algorithms via faster quantum gradient computation, in *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, 2019) pp. 1425–1444.

[26] J. van Apeldoorn, A. Cornelissen, A. Gilyén, and G. Nannicini, Quantum tomography using state-preparation unitaries, in *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)* (SIAM, 2023) pp. 1265–1318.

[27] W. J. Huggins, K. Wan, J. McClean, T. E. O'Brien, N. Wiebe, and R. Babbush, Nearly optimal quantum algorithm for estimating multiple expectation values, Phys. Rev. Lett. **129**, 240501 (2022).

[28] D. W. Berry, H. M. Wiseman, and J. K. Breslin, Optimal input states and feedback for interferometric phase estimation, Phys. Rev. A **63**, 053804 (2001).

[29] B. Higgins, D. Berry, S. Bartlett, M. Mitchell, H. Wiseman, and G. Pryde, Demonstrating heisenberg-limited unambiguous phase estimation without adaptive measurements, New Journal of Physics **11**, 073023 (2009).

[30] F. Belliardo and V. Giovannetti, Achieving heisenberg scaling with maximally entangled states: An analytic upper bound for the attainable root-mean-square error, Phys. Rev. A **102**, 042613 (2020).

[31] A. Y. Kitaev, Quantum measurements and the abelian stabilizer problem, arXiv preprint quant-ph/9511026 (1995).

[32] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge university press, 2010).

[33] W. van Dam, G. M. D'Ariano, A. Ekert, C. Macchiavello, and M. Mosca, Optimal quantum circuits for general phase estimation, Phys. Rev. Lett. **98**, 090501 (2007).

[34] T. Kaftal and R. Demkowicz-Dobrzański, Usefulness of an enhanced kitaev phase-estimation algorithm in quantum metrology and computation, Phys. Rev. A **90**, 062313 (2014).

[35] A. Luis and J. Peřina, Optimum phase-shift estimation and the quantum description of the phase difference, Phys. Rev. A **54**, 4564 (1996).

[36] R. Babbush, C. Gidney, D. W. Berry, N. Wiebe, J. McClean, A. Paler, A. Fowler, and H. Neven, Encoding electronic spectra in quantum circuits with linear t complexity, Phys. Rev. X **8**, 041015 (2018).

[37] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, Quantum amplitude amplification and estimation, Contemporary Mathematics **305**, 53 (2002).

[38] E. Knill, G. Ortiz, and R. D. Somma, Optimal quantum measurements of expectation values of observables, Physical Review A **75**, 012328 (2007).

[39] P. Rall, Quantum algorithms for estimating physical quantities using block encodings, Physical Review A **102**, 022408 (2020).

[40] J. Haah, Product Decomposition of Periodic Functions in Quantum Signal Processing, Quantum **3**, 190 (2019).

[41] R. Chao, D. Ding, A. Gilyen, C. Huang, and M. Szegedy, Finding angles for quantum signal processing with machine precision, arXiv preprint arXiv:2003.02831 (2020).

[42] Y. Dong, X. Meng, K. B. Whaley, and L. Lin, Efficient phase-factor evaluation in quantum signal processing, Physical Review A **103**, 042419 (2021).

[43] L. Ying, Stable factorization for phase factors of quantum signal processing, Quantum **6**, 842 (2022).

[44] K. Mizuta and K. Fujii, Recursive quantum eigenvalue and singular-value transformation: Analytic construction of matrix sign function by newton iteration, Phys. Rev. Res. **6**, L012007 (2024).

[45] S. Kimmel, G. H. Low, and T. J. Yoder, Robust calibration of a universal single-qubit gate set via robust phase estimation, Physical Review A **92**, 062315 (2015).

[46] A. Dutkiewicz, B. M. Terhal, and T. E. O'Brien, Heisenberg-limited quantum phase estimation of multiple eigenvalues with few control qubits, Quantum **6**, 830 (2022).

[47] G. H. Low and I. L. Chuang, Hamiltonian simulation by uniform spectral amplification, arXiv preprint arXiv:1707.05391 (2017).

[48] G. H. Low, T. J. Yoder, and I. L. Chuang, Methodology of resonant equiangular composite quantum gates, Phys. Rev. X **6**, 041067 (2016).

[49] G. H. Low and I. L. Chuang, Hamiltonian Simulation by Qubitization, Quantum **3**, 163 (2019).

[50] A. Dutkiewicz, T. E. O'Brien, and T. Schuster, The advantage of quantum control in many-body hamiltonian learning, arXiv preprint arXiv:2304.07172 (2023).

[51] This modified algorithm simply repeats Algorithm 1 $\mathcal{O}(\log(M))$ times and takes a coordinate-wise median of the outputs as a final estimate.

[52] A. M. Childs and N. Wiebe, Hamiltonian simulation using linear combinations of unitary operations, arXiv preprint arXiv:1202.5822 (2012).

[53] D. W. Berry, A. M. Childs, and R. Kothari, Hamiltonian simulation with nearly optimal dependence on all parameters, in *2015 IEEE 56th annual symposium on foundations of computer science* (IEEE, 2015) pp. 792–809.

[54] G. H. Low and I. L. Chuang, Optimal hamiltonian simulation by quantum signal processing, Phys. Rev. Lett. **118**, 010501 (2017).

[55] J. M. Martyn, Z. M. Rossi, A. K. Tan, and I. L. Chuang, Grand unification of quantum algorithms, PRX Quantum **2**, 040203 (2021).

[56] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum metrology, Phys. Rev. Lett. **96**, 010401 (2006).

[57] W. Górecki, R. Demkowicz-Dobrzański, H. M. Wiseman, and D. W. Berry, π-corrected heisenberg limit, Phys. Rev. Lett. **124**, 030501 (2020).

[58] W. Górecki, Heisenberg limit beyond quantum fisher information, arXiv preprint arXiv:2304.14370 (2023).

[59] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, Parameter estimation of quantum channels, IEEE Transactions on Information Theory **54**, 5172 (2008).

[60] D. W. Berry, B. L. Higgins, S. D. Bartlett, M. W. Mitchell, G. J. Pryde, and H. M. Wiseman, How to perform the most accurate possible phase measurements, Phys. Rev. A **80**, 052114 (2009).

[61] L. Laneve, Robust oracle quantum-state preparation via quantum signal processing, arXiv preprint arXiv:2305.04705 (2023).

[62] More precisely, in the setup of Lemma 9 without any Euclidean distance error, we numerically evaluate the probability of an event $|k_j - g_j| > 1/2\pi$ for $g_j \in [-1/\pi, 1/\pi]$ when $p = 3$.

Appendix A: Quantum gradient estimation

1. Review of Jordan's algorithm

For a given blackbox of a real scalar function $f(\boldsymbol{x})$ on $\boldsymbol{x} \in \mathbb{R}^M$, the quantum algorithm introduced by Stephen P. Jordan [24] can efficiently estimate the M-dimensional gradient of $\nabla f(\mathbf{0})$, with use of less queries to the blackbox compared to classical case. Here, the target point $\boldsymbol{x} = \mathbf{0}$ can be taken as $\boldsymbol{x} \neq \mathbf{0}$ by trivially redefining $f(\boldsymbol{x})$. The quantum algorithm consists of three steps: (i) prepare a superposition state of grid points $\boldsymbol{x}$ around the target point $\boldsymbol{x} = \mathbf{0}$, (ii) apply the blackbox of the target function f to the state and evaluate a phase $e^{if(\boldsymbol{x})}$ at each grid point, and (iii) measure the resulting state by the computational basis labeled by the grid points after the inverse quantum Fourier transformations.

To begin with, we define a set of grid points G_p^M around $\boldsymbol{x} = \mathbf{0}$ to evaluate f, as follows:

$$G_p^M := \left\{ \frac{\mu}{2^p} - \frac{1}{2} + \frac{1}{2^{p+1}} : \mu \in \{0, 1, \cdots, 2^p - 1\} \right\}^M , \tag{A1}$$

where p denotes a positive integer which specifies the estimation precision later. Note that because there is a bijection map

$$\varphi : \mu \mapsto \varphi(\mu) := \frac{\mu}{2^p} - \frac{1}{2} + \frac{1}{2^{p+1}} \in G_p, \tag{A2}$$

we always label the p-qubit computational basis $|\mu\rangle$ by the corresponding element $x \equiv \phi(\mu) \in G_p$. Then, applying the Hadamard gates to initialized pM-qubit registers, we have the superposition state of the grid points $\boldsymbol{x} := (x_1, ..., x_M) \in G_p^M$:

$$\frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x} \in G_p^M} |\boldsymbol{x}\rangle = \frac{1}{\sqrt{2^{pM}}} \sum_{(x_1, \ldots, x_M) \in G_p^M} |x_1\rangle |x_2\rangle \cdots |x_M\rangle . \tag{A3}$$

Here, each $|x_j\rangle$ contains p-qubit registers. Next, we assume access to the *phase oracle* O_f for $f(\boldsymbol{x})$ defined as [25]

$$O_f : |\boldsymbol{x}\rangle \to e^{if(\boldsymbol{x})} |\boldsymbol{x}\rangle \quad \text{for all} \quad \boldsymbol{x} \in G_p^M . \tag{A4}$$

Note that Ref. [25] provides a generic analysis of Jordan's algorithm based on the phase (and probability) oracle, while the original paper [24] assumes another powerful oracle (i.e., η-accurate Binary oracle for f that outputs $f(\boldsymbol{x})$ binarily with accuracy η from an input $\boldsymbol{x}$).

Now, to clarify the basic idea of Jordan's algorithm, we consider a special case where the target function f is an affine linear function, i.e., for a target gradient vector $\boldsymbol{g} \in [-1/3, 1/3]^M$ and some constant $f_0 \in \mathbb{R}$, $f(\boldsymbol{x}) = \boldsymbol{g} \cdot \boldsymbol{x} + f_0$. For such linear functions, the application of the (modified) phase oracle $O_f^{2\pi 2^p}$ to the input state Eq. (A3) yields

$$\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p f(\boldsymbol{x})}\left|\boldsymbol{x}\right\rangle$$
$$= e^{2\pi i 2^p f_0}\cdot \bigotimes_{j=1}^{M}\left[\frac{1}{\sqrt{2^p}}\sum_{x_j\in G_p} e^{2\pi i 2^p x_j g_j}\left|x_j\right\rangle\right]. \quad \text{(A5)}$$

Then, we apply a slightly modified version of the inverse quantum Fourier transformation $\mathrm{QFT}^\dagger_{G_p}$ over the p-qubit system: for all $x\in G_p$,

$$\mathrm{QFT}_{G_p}: \left|x\right\rangle \mapsto \frac{1}{\sqrt{2^p}}\sum_{k\in G_p} e^{2\pi i 2^p xk}\left|k\right\rangle. \quad \text{(A6)}$$

Note that QFT_{G_p} is the same as the usual p-qubit QFT up to conjugation with a tensor product of p single-qubit gates [25]. The statistics of the computational basis measurement to Eq. (A5) with $\mathrm{QFT}^\dagger_{G_p}$ are similar to that of the output of standard quantum phase estimation algorithm [32]. More precisely, let $(k_1,k_2,...,k_M)\in G_p^M$ be a result of the computational basis measurement, then the following holds [25]:

$$\Pr\left[\left|k_j - g_j\right| > \frac{3}{2^p}\right] \le \frac{1}{4} \quad \text{for every} \quad i = 1,2,\cdots,M. \quad \text{(A7)}$$

In the above description, we assumed that the target function is affine linear. However, if a target function is very close to some affine linear function and thereby the equality of Eq. (A5) approximately holds, we can prove similar results to Eq. (A7), as follows.

Lemma 9 ([25, 26]). *Let $\boldsymbol{g}\in\mathbb{R}^M$ such that $\|\boldsymbol{g}\|_\infty \le 1/3$. Suppose we can prepare the quantum state $\left|\Psi\right\rangle$ that is 1/12-close in the Euclidean distance to the following state*

$$\left(\mathrm{QFT}^\dagger_{G_p}\right)^{\otimes M}\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \boldsymbol{g}\cdot\boldsymbol{x}}\left|\boldsymbol{x}\right\rangle. \quad \text{(A8)}$$

Then, measuring the quantum state $\left|\Psi\right\rangle$ in the computational basis, we obtain a coordinate-wise estimate $(k_1,...,k_M)\in G_p^M$ satisfying

$$\Pr\left[\left|k_j - g_j\right| > \frac{3}{2^p}\right] \le \frac{1}{3} \quad \textit{for every} \quad j = 1,2,\cdots,M.$$

Proof. By the closeness assumption, the trace distance between $\left|\Psi\right\rangle$ and Eq. (A8) is upper bounded by 1/12. Since the trace distance provides the upper bound of the total variation distance of two probability measures defined by the two quantum states and an arbitrary common POVM (Theorem 9.1 [32]), the probability (A7) is modified at most 1/12 by measuring $\left|\Psi\right\rangle$ instead of Eq. (A8). □

For more regular functions, Ref. [25] provides an improved version of Jordan's algorithm, using the higher-order finite-difference formulas to enhance the linearity of the target functions in a certain domain.

2. Heisenberg limit

The phase oracle O_f for a smooth real function $f(\boldsymbol{x})$ on $\boldsymbol{x}\in\mathbb{R}^M$ with gradient $\boldsymbol{g} := \nabla f(\boldsymbol{0})$ corresponds to the time evolution operator (with unit time) generated by the following Hamiltonian

$$H(\boldsymbol{g}) + V, \quad H(\boldsymbol{g}) := \sum_{\boldsymbol{x}\in G_p^M} (\boldsymbol{g}\cdot\boldsymbol{x})\left|\boldsymbol{x}\right\rangle\left\langle\boldsymbol{x}\right|, \quad \text{(A9)}$$

where V is a $\boldsymbol{g}$-independent Hermitian operator that commutes with $H(\boldsymbol{g})$. Thus, the estimation of $\boldsymbol{g}$ from O_f with appropriate choice of an input state and a final measurement can be considered as one of the (multi-parameter) unitary estimation problems. Such unitary estimation problems are widely studied in the field of quantum metrology, and one of the major topics in this field is to devise quantum estimation protocols that can achieve the higher precision than any classical protocol [2, 56]. In particular, the Heisenberg limit provides a fundamental bound on the estimation precision (in terms of root mean squared error) under given resources, and it is typically given as $1/t$ where t denotes the total number of resources to be used [2, 57]. Here, we derive the Heisenberg limit in quantum gradient estimation.

To derive the fundamental bound, we here consider a general adaptive estimation protocol [56], which is illustrated in Fig. 7. In the general protocol, we first prepare an arbitrary input state ρ_{in} between the system on which O_f acts and an ancilla system with an arbitrary number of qubits. Then, we apply the following sequence of quantum operations to the input state:

$$U_t(O_f\otimes\mathbf{1})\cdots U_2(O_f\otimes\mathbf{1})U_1(O_f\otimes\mathbf{1}), \quad \text{(A10)}$$

where $\mathbf{1}$ denotes the identity and U_i $(i=1,2,...,t)$ are $\boldsymbol{g}$-independent arbitrary unitary operators acting on the whole system. This sequence contains t uses of the phase oracle in total. Finally, the output state is measured by an arbitrary POVM $\{M_{\boldsymbol{g}}\}$, and we write the corresponding single-shot estimator for g_j as $\hat{g}_j$. Because the interaction U_i to the ancilla systems can extract the information during the estimation process, this protocol also includes adaptive techniques. Obviously, the original method for gradient estimation is captured in this general protocol, by setting ρ_{in} to the uniform superposition state without ancilla qubits, $U_i = \mathbf{1}$ for all i, and $M_{\boldsymbol{g}}$ to the computational basis measurement with the inverse quantum Fourier transformation. Note that the $\boldsymbol{g}$-independent part of O_f can be included in each U_j, and therefore in the following, we consider $O_f = e^{iH(\boldsymbol{g})}$ without loss of generality.

We here remark that $e^{iH(\boldsymbol{g})}$ can be written as a tensor product of time evolutions

$$\bigotimes_{j=1}^{M}\left(\sum_{x_j\in G_p} e^{ig_jx_j}\left|x_j\right\rangle\left\langle x_j\right|\right) \quad \text{(A11)}$$

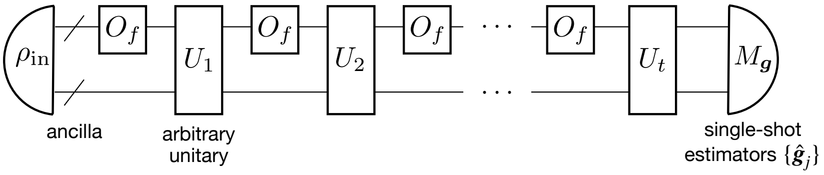


FIG. 7. A general adaptive protocol for estimating $\boldsymbol g$ in O_f.

by the generators $H_j := \sum_{x_j} x_j |x_j\rangle\langle x_j|$ with the bounded spectral norm $\|H_j\| \le 1/2$. Therefore, the estimation of $\boldsymbol g = (g_1, ..., g_M)$ is essentially equal to the estimation of evolving time g_j in each $e^{ig_jH_j}$. Now, we are ready to prove the Heisenberg limit in quantum gradient estimation.

Theorem 10 (Heisenberg limit in quantum gradient estimation)**.** *Suppose we have access to the phase oracle O_f for a smooth real function f on $\mathbb{R}^M$ with gradient $\boldsymbol g := \nabla f(\mathbf 0)$ and g_j belongs to some finite interval $\Theta \subset \mathbb{R}$ for all j. Then, the single-shot estimators $\hat g_j$, obtained from the general adaptive estimation protocol in Fig. 7 with t uses of the phase oracle O_f, satisfy the following inequality:*

$$\min_{j=1,2,\cdots,M} \widehat{\mathrm{MSE}}\left[\hat g_j\right] \ge \frac{\pi^2}{t^2} \quad as \quad t\to\infty, \tag{A12}$$

where $\widehat{\mathrm{MSE}}[\hat g_j]$ denotes the supremum of the mean squared error (MSE) for $\hat g_j$ over the known interval Θ, i.e., the maximum value of MSE over all possible target values $g_j \in \Theta$.

Proof. We prove this theorem by contradiction. Suppose there is a protocol such that for an index $j \in \{1, ..., M\}$, $\widehat{\mathrm{MSE}}\left[\hat g_j\right] < \pi^2/(t^2\Delta G_p^2)$ holds as t goes to ∞, where ΔG_p denotes the difference between extreme eigenvalues of $H_j = \sum_{x_j\in G_p} x_j|x_j\rangle\langle x_j|$ i.e., $\max G_p - \min G_p \le 1$. Now, we recall that the phase oracle O_f can be considered as the product of $e^{ig_jH_j}$ without loss of generality. Then, focusing on the estimation of g_j in the single-parameter unitary $e^{ig_jH_j}$, it can be shown that there is no protocol using the total t uses of $e^{ig_jH_j}$ such that $\widehat{\mathrm{MSE}}[\hat g_j]$ can be less than $\pi^2/t^2\Delta G_p^2$ as t increases [57, 58], which contradicts the above assumption. Therefore, we conclude that

$$\widehat{\mathrm{MSE}}[\hat g_j] \ge \frac{\pi^2}{t^2\Delta G_p^2} \ge \frac{\pi^2}{t^2} \quad \text{as} \quad t\to\infty$$

holds for all j, which completes the proof of Theorem 10. □

As for the achievability of the lower bound, the same methodology as the phase estimation with the minimum phase uncertainty [33–36] can be applied to design an optimal protocol, because the gradient estimation can be considered as separable applications of the phase estimation protocol. Hereafter, we describe an optimal protocol of gradient estimation that is applicable to an affine linear function $f(\boldsymbol x) = \boldsymbol x\cdot\boldsymbol g$ without any adaptive operations. Let us consider M tensor products of an ansatz state $\sum_{x\in G_p} a_x|x\rangle$, where a_x is a real amplitude, as an initial input state instead of the equal superposition state Eq. (A3). Then, applying the phase oracle O_f 2^{p+1} times to the input state and performing the computational basis measurement after $\mathrm{QFT}^\dagger_{G_p}$s, we obtain the measurement result k_j with the probability

$$\Pr\left[k_j\right] = \left|\sum_{x_j=0}^{2^p-1} \frac{a_{x_j}}{\sqrt{2^p}} e^{2\pi i 2^p x_j(g'_j - k_j)}\right|^2, \tag{A13}$$

where $g'_j := g_j/\pi$. For simplicity, we drop the subscript j in the following. Taking the measurement outcome k as an estimator of g', we can approximately evaluate the MSE of k as follows:

$$\mathbb{E}\left[(k-g')^2\right] \simeq \frac{1}{2\pi^2}\left(1 - \mathbb{E}\left[\cos\left(2\pi(k-g')\right)\right]\right), \tag{A14}$$

where we can check the right hand side is close to the MSE when $(k - g')$ is small by the Taylor expansion. As shown in Ref. [59], the expectation of cosine can be analytically calculated:

$$\begin{aligned}&\mathbb{E}\left[\cos\left(2\pi(k-g')\right)\right]\\ &= \sum_{k=1}^{2^p-1} a_{k-1}a_k + a_0a_{2^p-1}\cos\left[2\pi 2^p\left(g' + \frac12 - \frac{1}{2^{p+1}}\right)\right].\end{aligned} \tag{A15}$$

Here, a_k is equivalent to $a_{\varphi(k)}$ for the bijection map defined in Eq. (A2). Therefore, if we take $a_0 = 0$, then the right hand side of Eq. (A14) can be written as a quadratic form $(1/2\pi^2)\sum_{k,l=1}^{2^p-1} A_{kl}a_ka_l$ for the symmetric matrix A:

$$A = \begin{pmatrix} 1 & -1/2 & & \\ -1/2 & 1 & -1/2 & \\ & -1/2 & 1 & \ddots \\ & & \ddots & \ddots \end{pmatrix}. \tag{A16}$$

The minimum eigenvalue and the corresponding eigenvector of A is known as

$$2\sin^2\frac{\pi}{2^{p+1}} \tag{A17}$$

and

$$a_k = \sqrt{\frac{2}{2^p}} \sin \frac{k\pi}{2^p}, \tag{A18}$$

respectively. Consequently, combining Eqs. (A14) and (A17), we can confirm that this protocol achieves the lower bound of Theorem 10 when $t = 2^{p+1}$ is sufficiently large, as

$$\mathbb{E}\left[(\pi k - g)^2\right] \simeq \left(\frac{\pi}{2^{p+1}}\right)^2 . \tag{A19}$$

Finally, we remark that the original implementation of the gradient estimation cannot achieve the quadratic speedup regarding total queries t, i.e., $\varepsilon^2 = \mathcal{O}(1/t^2)$ for a MSE ε^2, even in the target function is an affine linear. This can be checked from Eq. (A14); the uniform superposition state $a_x = 1/\sqrt{2^p}$ for all x gives

$$\min_{g'} \mathbb{E}\left[\cos\left(2\pi(k - g')\right)\right] = 1 - \frac{2}{2^p}, \tag{A20}$$

and thus, $\max_g \mathbb{E}\left[(\pi k - g)^2\right] = \mathcal{O}(1/t)$, which is the same scaling as the shot noise or the standard quantum limit (SQL). Note that this result is consistent with that the quantum phase estimation algorithm fails to achieve the Heisenberg limit when the input ancilla qubits are initialized as the uniform superposition state, unlike the optimal entangled state as in Eq. (A18) [3, 29, 60]. We remark that the proposed adaptive method in this work performs gradient estimation at the same scaling as the Heisenberg limit $\mathcal{O}(1/\varepsilon)$ even when the target function is *approximately* affine linear.

Appendix B: Circuit implementation and theoretical guarantees of the proposed method

In Sec. B 1, we design two methods to prepare the quantum state $|\Upsilon(q)\rangle$ in Eq. (1): one is based on the Hamiltonian simulation protocol, and the other is based on Grover-like repetition. Finally, the performance of the proposed algorithm is analyzed in Sec. B 2. In the following, we often refer to the detailed version Algorithm 1*, instead of Algorithm 1 in Sec. III.

1. Probing state preparation

Here, we provide two quantum algorithms to prepare the probing state $|\Upsilon(q)\rangle$ in Eq. (1), using block encodings of observables $\{O_j\}$ and the state preparation oracle U_ψ. First, we describe a method to construct the block encoding of a linear combination of observables.

a. *Amplified block encoding for observables*

Algorithm 1* Adaptive observables estimation (A detailed version.)

Input: $\log_2 d$-qubit state preparation unitary U_ψ; observables $\{O_j\}_{j=1}^M$ with the spectral norm $\|O_j\| \le 1$ such that

$$M > 2\ln d + 24 = \mathcal{O}(\log d) \tag{B1}$$

holds; confidence parameter $c \in (0, 3/8(1+\pi)^2]$; target precision parameter $\varepsilon \in (0,1)$.

Output: A sample $(\tilde{u}_1, ..., \tilde{u}_M)$ from an estimator $\hat{\boldsymbol{u}} = (\hat{u}_1, ..., \hat{u}_M)$ whose j-th element estimates $\langle O_j \rangle := \langle\psi|O_j|\psi\rangle$ within MSE ε^2 as

$$\max_{j=1,2,...,M} \mathbb{E}\left[(\hat{u}_j - \langle O_j\rangle)^2\right] \le \varepsilon^2$$

```
Set $p := 3$ and $\tilde{u}_j^{(0)} := 0,\ (j = 1, 2, \cdots, M)$
for $q = 0, 1, ..., q_{\max} := \lceil \log_2(1/\varepsilon) \rceil$ do
    Set
        $\tilde{O}_j^{(q)} := \frac{O_j - \tilde{u}_j^{(q)}\mathbf{1}}{2}$ and $\delta^{(q)} := \frac{c}{8^{q_{\max}-q}}$
    Prepare $\mathcal{O}(\log(M/\delta^{(q)}))$ copies of a quantum state that is 1/12-close (in Euclidean distance) to
        $\left(\mathrm{QFT}_{G_p}^\dagger\right)^{\otimes M} |\Upsilon(q)\rangle$, where
        $|\Upsilon(q)\rangle := \frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^{q+1}\pi^{-1}\langle \tilde{O}_j^{(q)}\rangle} |\boldsymbol{x}\rangle$,
    using Lemma 13 or Lemma 14 and perform the computational basis measurement on each of them. Note that each measurement outputs a result in the form of $(x_1, ..., x_M) \in G_p^M$.
    Set coordinate-wise medians of the measurement results as $g_j^{(q)}$
    Set $\tilde{u}_j^{(q+1)} := \tilde{u}_j^{(q)} + \pi 2^{-q} g_j^{(q)}$
    if there are some $j$ such that $\tilde{u}_j^{(q+1)} \ge 1$ (or $\le -1$) then
        Set $\tilde{u}_j^{(q+1)} = 1$ (or $-1$) for such $j$
    end if
end for
return $\tilde{u}_j := \tilde{u}_j^{(q_{\max}+1)}$
```

Let B_j $(j = 1, ..., M)$ be an a-block-encoding of a $d \times d$ observable O_j, and let $\mathbf{p} := (p_1, ..., p_M)$ be a sequence of positive integers. Here, we define a set $G_{\mathbf{p}}$ of grid points as

$$G_{\mathbf{p}} := G_{p_1} \times \cdots \times G_{p_M},$$

where each G_p is defined as in Eq. (A1). For any element $\boldsymbol{x} = (x_1, ..., x_M) \in G_{\mathbf{p}}$, we can construct an $(a + \lceil \log_2 M \rceil + 1)$-block-encoding of $\tilde{H}^{(\boldsymbol{x})} := M^{-1} \sum_{j=1}^M x_j O_j$ by using the LCU method. The corresponding SELECT operation denoted by U_{SEL} is given by

$$U_{\mathrm{SEL}} := \sum_{j=1}^{M} |j\rangle\langle j| \otimes B_j .$$

As for the PREPARE operation, we consider implementation with and without reflecting the signs of coefficients as $P_{\mathrm{R}}^{(\boldsymbol{x})}$ and $P_{\mathrm{L}}^{(\boldsymbol{x})}$, defined as

$$P_{\mathrm{R}}^{(\boldsymbol{x})} : |0\rangle^{\otimes\lceil \log_2 M\rceil} \mapsto \sum_{j=1}^{M} \mathrm{sgn}(x_j)\sqrt{\frac{|x_j|}{\|\boldsymbol{x}\|_1}}\,|j\rangle . \tag{B2}$$

$$P_{\mathrm{L}}^{(\boldsymbol{x})} : |0\rangle^{\otimes\lceil \log_2 M\rceil} \mapsto \sum_{j=1}^{M} \sqrt{\frac{|x_j|}{\|\boldsymbol{x}\|_1}}\,|j\rangle \tag{B3}$$

Then, we can confirm that the unitary $(P_{\mathrm{L}}^{(\boldsymbol{x})} \otimes \mathbf{1})^\dagger U_{\mathrm{SEL}} (P_{\mathrm{R}}^{(\boldsymbol{x})} \otimes \mathbf{1})$ is a block encoding of $\propto \tilde{H}^{(\boldsymbol{x})}$ because for any $|\psi\rangle$,

$$\begin{aligned}
&(P_{\mathrm{L}}^{(\boldsymbol{x})} \otimes \mathbf{1})^\dagger U_{\mathrm{SEL}} (P_{\mathrm{R}}^{(\boldsymbol{x})} \otimes \mathbf{1})\, |0\rangle^{\otimes\lceil \log_2 M\rceil} |\psi\rangle \\
&\quad = \sum_{j=1}^{M} \mathrm{sgn}(x_j)\sqrt{\frac{|x_j|}{\|\boldsymbol{x}\|_1}}\,(P_{\mathrm{L}}^{(\boldsymbol{x})})^\dagger |j\rangle \otimes B_j |\psi\rangle \\
&\quad = |0\rangle^{\otimes\lceil \log_2 M\rceil} \otimes \sum_{j=1}^{M} \frac{x_j}{\|\boldsymbol{x}\|_1} B_j |\psi\rangle + |\tilde{\psi}^{\perp}\rangle ,
\end{aligned} \tag{B4}$$

where $\langle 0|^{\otimes\lceil \log_2 M\rceil} |\tilde{\psi}^{\perp}\rangle = 0$. While the block encoding has the normalization factor $\|\boldsymbol{x}\|_1$ which depends on $\boldsymbol{x}$, it can be modified to M by introducing an additional single ancilla qubit and a single rotation gate $R_y(\theta) = e^{i\theta Y}$. As a result, the following unitary is $(a + \lceil \log_2 M\rceil + 1)$-block-encoding of $\tilde{H}^{(\boldsymbol{x})}$:

$$(I \otimes P_{\mathrm{L}}^{(\boldsymbol{x})} \otimes \mathbf{1})^\dagger\, (I \otimes U_{\mathrm{SEL}})\, (R_y(\theta_{\boldsymbol{x}}) \otimes P_{\mathrm{R}}^{(\boldsymbol{x})} \otimes \mathbf{1}), \tag{B5}$$

where I denotes the 1-qubit identity, and $R_y(\theta_{\boldsymbol{x}}) : |0\rangle \mapsto \frac{\|\boldsymbol{x}\|_1}{M}|0\rangle + \sqrt{1 - \left(\frac{\|\boldsymbol{x}\|_1}{M}\right)^2}\,|1\rangle$.

In this block encoding of $\tilde{H}^{(\boldsymbol{x})}$, only PREPARE operation depends on the grid point $\boldsymbol{x} \in G_{\mathbf{p}}$. Thus, by adding a control to $P_{\mathrm{L}}^{(\boldsymbol{x})}$, $P_{\mathrm{R}}^{(\boldsymbol{x})}$, and R_y, and then sequentially applying them to each $\boldsymbol{x}$, we can implement the following unitary

$$U'_{\mathrm{SEL}} := \sum_{\boldsymbol{x}\in G_{\mathbf{p}}} |\boldsymbol{x}\rangle\langle \boldsymbol{x}| \otimes U^{(\boldsymbol{x})}, \tag{B6}$$

where $U^{(\boldsymbol{x})}$ denotes the block encoding of $\tilde{H}^{(\boldsymbol{x})}$. Because the detailed circuit description of U'_{SEL} is not required in the following, we deal with the unitary U'_{SEL} as an oracle for observables $\{O_j\}_{j=1}^{M}$, instead of U_{SEL}, for a simple expression of gate complexity.

Remark 11. The above straightforward construction of U'_{SEL} results in a very large circuit with $\mathcal{O}(2^{\|\mathbf{p}\|_1})$-depth. Fortunately, we can construct a more efficient circuit by further modifying the PREPARE operation, using a similar way to Ref. [61]. As shown in the Sec. 3 of Ref. [25], we can implement $\sum_{x\in G_p} |x\rangle\langle x| \otimes e^{-ixZ}$ with $\mathcal{O}(p)$-depth circuit using $p+1$ (controlled) single-qubit rotation gates. By sequentially applying the $|j\rangle$-controlled version of this gate (see Fig. 8) over x_j-register, the additional single ancilla qubit, and the $\lceil \log_2 M\rceil$ qubits, we obtain a $\boldsymbol{x}$-controlled block encoding of $e^{i\mathcal{H}^{(\boldsymbol{x})}}$, where $\mathcal{H}^{(\boldsymbol{x})} := \sum_{j=1}^{M} x_j |j\rangle\langle j|$. The corresponding circuit diagram is shown in Fig. 9. Then, we can obtain an ϵ-precise block encoding of $(2/\pi)\mathcal{H}^{(\boldsymbol{x})}$, via the eigenvalue transformation for the logarihm of unitaries: $e^{i\mathcal{H}^{(\boldsymbol{x})}} \mapsto \mathcal{H}^{(\boldsymbol{x})}$ (Corollary 71 in [13]). This implementation consists of $\mathcal{O}(\log(1/\epsilon))$ uses of block-encoding of $e^{i\mathcal{H}^{(\boldsymbol{x})}}$ or its inverse. Now, introducing the SELECT U_{SEL} and Hadamard gates, we have an ϵ-precise block-encoding of $(2M/(\pi 2^{\lceil \log_2 M\rceil}))\tilde{H}^{(\boldsymbol{x})}$ controlled by $\boldsymbol{x}$, using at most $\mathcal{O}(\|\mathbf{p}\|_1 \log(1/\varepsilon))$-depth circuit over $\mathcal{O}(\|\mathbf{p}\|_1 + a + \lceil \log_2 M\rceil + \log_2 d)$ qubits in total:

$$\begin{aligned}
&\langle \mathbf{0}| H^{\otimes\lceil \log_2 M\rceil} \otimes \mathbf{1} \cdot U_{\mathrm{SEL}} \cdot \frac{2}{\pi}\mathcal{H}^{(\boldsymbol{x})} H^{\otimes\lceil \log_2 M\rceil} |\mathbf{0}\rangle \otimes \mathbf{1} \\
&= \frac{2M}{\pi 2^{\lceil \log_2 M\rceil}} \frac{1}{M} \sum_{j=1}^{M} x_j B_j .
\end{aligned} \tag{B7}$$

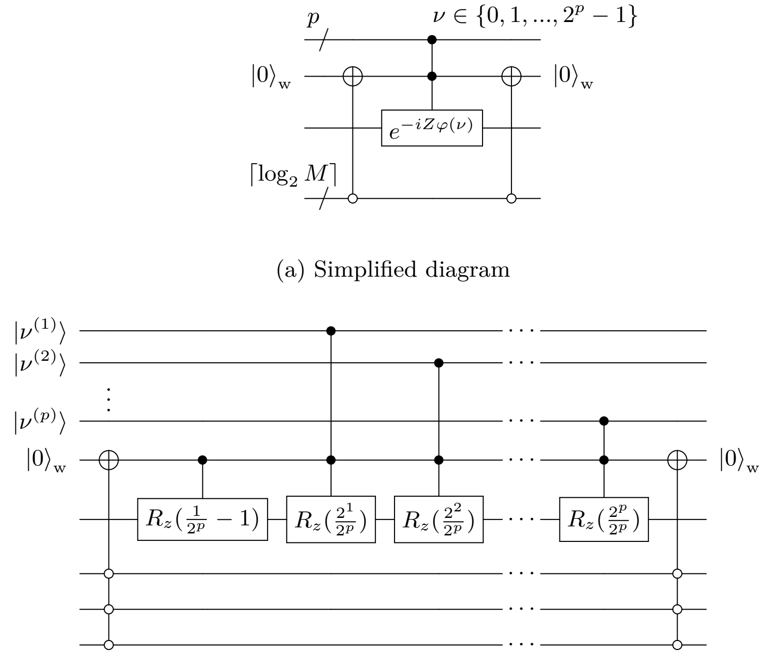
Note that this block encoding has a single use of $U_{\mathrm{SEL}} = \sum_j |j\rangle\langle j| \otimes B_j$ regardless of ϵ.

Using U'_{SEL}, U_ψ, and its conjugation $U_\psi^\dagger$, we obtain a block encoding of the following Hamiltonian:

$$\sum_{\boldsymbol{x}} \langle\psi|\tilde{H}^{(\boldsymbol{x})}|\psi\rangle\, |\boldsymbol{x}\rangle\langle\boldsymbol{x}| = \sum_{\boldsymbol{x}} \left(\sum_j x_j \cdot \frac{\langle O_j\rangle}{M}\right) |\boldsymbol{x}\rangle\langle\boldsymbol{x}| .$$

This allows us to simulate the phase oracle for the affine linear function $\sum_j x_j \langle O_j\rangle/M$ by using the block-Hamiltonian simulation (Lemma 6). However, in estimating the expectation value $\langle O_j\rangle$, we need to amplify the function by the factor M due to the normalization factor $1/M$ in $\tilde{H}^{(\boldsymbol{x})}$, which may result in no speedup for the total queries to U_ψ regarding the number M of observables. To obtain the quadratic speedup regarding M, Ref. [26] (Lemma 36) uses a linear amplification of $\tilde{H}^{(\boldsymbol{x})}$ by Lemma 4, and this amplification can be performed with no use of U_ψ. Here, we provide a slightly modified version of the Lemma 36 in Ref. [26] as follows.

Lemma 12. *Let $\delta' > 0$, $\varepsilon' \in (0, 1/2)$, and let $\mathbf{p} = (p_1, p_2, ..., p_M)$ be any sequence of positive integers. Suppose that for $d \times d$ observables $\{O_j\}_{j=1}^{M}$ with $\|O_j\| \leq 1$ (d is a power of 2), we have access to the oracle $U'_{\mathrm{SEL}} = \sum_{\boldsymbol{x}\in G_{\mathbf{p}}} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes U^{(\boldsymbol{x})}$, where $U^{(\boldsymbol{x})}$ is an $(a + \lceil \log_2 M\rceil)$-block encoding of observable $\tilde{H}^{(\boldsymbol{x})} := M^{-1}\sum_{j=1}^{M} x_j O_j$ for*



(a) Simplified diagram

(b) Detailed diagram in the case of $\lceil \log_2 M \rceil = 3$

FIG. 8. Quantum circuit for $|0\rangle^{\otimes \lceil \log_2 M \rceil}$-controlled unitary $\sum_\nu |\nu\rangle \langle \nu| \otimes e^{-iZ\varphi(\nu)}$. The qubit $|0\rangle_{\mathrm{w}}$ is an additional work qubit. Here, we recall $\varphi(\mu) := \frac{\mu}{2^p} - \frac{1}{2} + \frac{1}{2^{p+1}} \in G_p$ in Eq. (A2). $R_z(x) := e^{-ixZ/2}$.

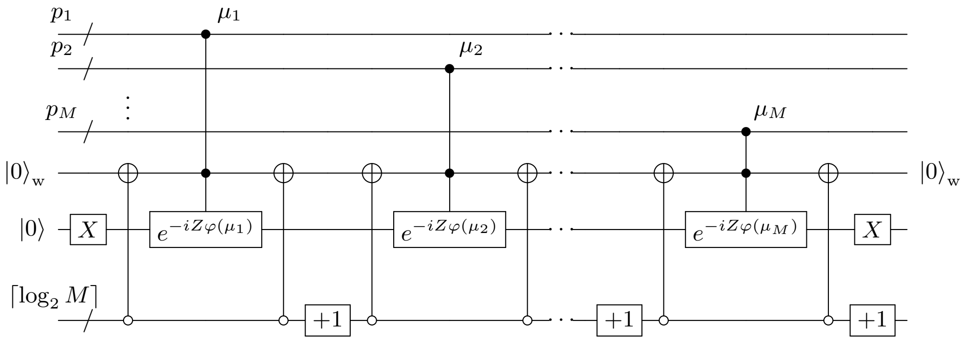


FIG. 9. Quantum circuit for a 2-block-encoding of $\sum_{\boldsymbol{x}} |\boldsymbol{x}\rangle \langle \boldsymbol{x}| \otimes e^{i\mathcal{H}^{(\boldsymbol{x})}}$, where $\mathcal{H}^{(\boldsymbol{x})} := \sum_{j=1}^{M} x_j |j\rangle \langle j|$. The gate $+1$ denotes a bit increment operation such as $|1\rangle \to |2\rangle \to \cdots \to |M\rangle \to |1\rangle$.

some $a \in \mathbb{N}$. If the following inequality holds

$$\sigma := \left\lceil \sqrt{2M \ln(2d/\delta')} \right\rceil < M, \qquad \text{(B8)}$$

then there exists a subset F of $G_{\mathbf{p}}$ with the cardinality $|F| \geq (1-\delta')|G_{\mathbf{p}}|$, and we can implement a unitary (with $\|\mathbf{p}\|_1 + \lceil \log_2 M \rceil + \log_2 d + a + 1$ qubits in total)

$$U_{\mathrm{obs}} := \sum_{\boldsymbol{x} \in G_{\mathbf{p}}} |\boldsymbol{x}\rangle \langle \boldsymbol{x}| \otimes U_{\mathrm{obs}}^{(\boldsymbol{x})} \qquad \text{(B9)}$$

such that $U_{\mathrm{obs}}^{(\boldsymbol{x})}$ is a $(1, a + \lceil \log_2 M \rceil + 1, \varepsilon')$-block-encoding of the Hamiltonian

$$H^{(\boldsymbol{x})} := \frac{1}{\sigma} \sum_{j=1}^{M} x_j O_j \quad \text{if} \quad \boldsymbol{x} \in F \subset G_{\mathbf{p}}. \qquad \text{(B10)}$$

For $m := \mathcal{O}(M\sigma^{-1} \log(M\sigma^{-1}/\varepsilon'))$, this implementation of U_{obs} uses m queries to U'_{SEL} or its inverse, $2m$ NOT gates controlled by $(a + \lceil \log_2 M \rceil)$-qubit, and $\mathcal{O}(m)$ single-qubit gates, with $\mathcal{O}(\mathrm{poly}(m))$ classical precomputation for *finding quantum circuit parameters. The circuit diagram for $U_{\rm obs}$ is shown in Fig. 10.*

Proof of Lemma 12. Let $\gamma := M/\sigma > 1$. To perform the amplification in Lemma 4, it is required that the spectral norm $\|\tilde{H}^{(\boldsymbol{x})}\|$ is upper bounded by $(1-\delta)/\gamma$ for some $\delta \in (0, 1/2)$. To this end, we define a subset $F \subset G_{\mathbf{p}}$ such that

$$F := \left\{ \boldsymbol{x} \in G_{\mathbf{p}} : \|\tilde{H}^{(\boldsymbol{x})}\| < \frac{1}{2\gamma} \right\}.$$

If $\boldsymbol{x} \in F$, we can perform the linear amplification by γ and obtain $(1, a + \lceil \log_2 M \rceil + 1, \varepsilon')$-block-encoding of $\gamma \tilde{H}^{(\boldsymbol{x})}$ from Lemma 4. Next, we show the cardinality of F is equal or more than $(1-\delta') \prod_{j=1}^M 2^{p_j}$. Let us consider independent random variables X_j $(j = 1, ..., M)$ that are uniformly distributed on each G_{p_j}. Because the random variables are also symmetrically distributed on each G_{p_j}, the following matrix series inequality holds (Theorem 35 in [26]):

$$\begin{aligned} &\mathrm{Pr}_{X_1,...,X_M} \left[\left\| \sum_{j=1}^M (2X_j) O_j \right\| \geq t \right] \\ &\leq 2d \cdot \exp\left[-\frac{t^2}{2 \left\| \sum_{j=1}^M O_j^2 \right\|} \right]. \end{aligned} \tag{B11}$$

Thus, inserting M/γ into t, we obtain

$$\mathrm{Pr}_{X_1,...,X_M} \left[\left\| \tilde{H}^{(\boldsymbol{X})} \right\| \geq 1/2\gamma \right] \leq \delta'. \tag{B12}$$

Since the probability of an event $X_j = x_j$ $(j = 1, ..., M)$ is equal to $1/\prod_{j=1}^M 2^{p_j}$ for all x_j, we obtain $|F| \geq (1 - \delta') \prod_{j=1}^M 2^{p_j}$. The gate complexity follows from that of Lemma 4.

□

Here, we make some remarks for Lemma 12. The condition Eq. (B8) for the amplification, $M > \mathcal{O}(\log(d/\delta'))$, is crucial in our algorithm, and for a constant δ', this condition is satisfied when the number of observables is bigger than the number of qubits such as Eq. (B1).

When we use the circuit construction of $U'_{\rm SEL}$ in Remark 11, $U^{(\boldsymbol{x})}$ in the assumption of Lemma 12 should be replaced as the ϵ-precise block encoding of $(2M/(\pi 2^{\lceil \log_2 M \rceil}))\tilde{H}^{(\boldsymbol{x})}$. In this case, the error ε' in the block encoding $U_{\rm obs}^{(\boldsymbol{x})}$ of $H^{(\boldsymbol{x})}$ becomes $\varepsilon' + \mathcal{O}(m\sqrt{\epsilon})$, by the error propagation associated with the uniform amplification Lemma 4 (see; Lemma 22 in Ref. [13]). Thus, replacing ε' and ϵ with $\varepsilon'/2$ and $\mathcal{O}((\varepsilon'/m)^2)$, respectively, we obtain the ε'-precise block encoding $U_{\rm obs}^{(\boldsymbol{x})}$.

b. Approximated state preparation

Now, we are ready to show two quantum algorithms to prepare the probing state $|\Upsilon(q)\rangle$. Note that in the following lemmas, we explicitly construct a quantum circuit in its proof.

Lemma 13 (State preparation by Hamiltonian simulation)**.** *Let O_j $(j = 1, 2, ..., M)$ be $d \times d$ observables O_j (d is a power of 2) with $\|O_j\| \leq 1$, and let p be a positive integer. Also, let U_ψ be a $\log_2 d$-qubit state preparation oracle, and $\langle O_j \rangle := \langle \psi | O_j | \psi \rangle$. Suppose we have access to $U'_{\rm SEL} := \sum_{\boldsymbol{x} \in G_p^M} |\boldsymbol{x}\rangle \langle \boldsymbol{x}| \otimes U^{(\boldsymbol{x})}$, where $U^{(\boldsymbol{x})}$ is an $(a + \lceil \log_2 M \rceil)$-block-encoding of $M^{-1} \sum_{j=1}^M x_j O_j$ for some $a \in \mathbb{N}$. We assume $\sigma := \left\lceil \sqrt{2M \ln(2d/\delta')} \right\rceil < M$ holds for $\delta' = 2^{-10}$. Then, for any non-negative integer q, we can prepare the pM-qubit quantum state*

$$\frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x} \in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^{q+1} \pi^{-1} \langle O_j \rangle} |\boldsymbol{x}\rangle$$

up to 1/12 Euclidean distance error, with $4Q$ uses of U_ψ or $U_\psi^\dagger$, $4mQ$ uses of controlled $U'_{\rm SEL}$ or its inverse, $\mathcal{O}(mQ)$ uses of NOT gates controlled by at most $\mathcal{O}(a + \lceil \log_2 M \rceil + \log_2 d)$ qubits, $\mathcal{O}(mQ + pM)$ uses of single-qubit or two-qubit gates, additional $(\lceil \log_2 M \rceil + \log_2 d + a + 3)$ ancilla qubits, and $\mathcal{O}(\mathrm{poly}(Q) + \mathrm{poly}(m))$ classical precomputation for finding quantum circuit parameters, where

$$Q = \mathcal{O}\left(2^{p+q+2}\sigma\right) \quad and \quad m = \mathcal{O}\left(\frac{M}{\sigma}(p + q + \log M)\right).$$

Note that if we have a block encoding B_j of O_j, then a block encoding of $(O_j - \tilde{u}_j^{(q)} \mathbf{1})/2$ for any $\tilde{u}_j^{(q)} \in [-1, 1]$ is easily constructed by the LCU method; see Fig. 11. Therefore, Lemma 13 provides a method to approximately prepare the probing state $|\Upsilon(q)\rangle$.

Proof of Lemma 13. Let $\varepsilon'' = 2^{-14} \in (0, 1)$ and $\varepsilon' = \sqrt{\delta'}/(2^{p+q+2}\sigma) \in (0, 1/2)$. From the assumption and Lemma 12, we have a unitary

$$U_{\rm obs} := \sum_{\boldsymbol{x} \in G_p^M} |\boldsymbol{x}\rangle \langle \boldsymbol{x}| \otimes U_{\rm obs}^{(\boldsymbol{x})}, \tag{B13}$$

where $U_{\rm obs}^{(\boldsymbol{x})}$ is a $(1, a'' = a + \lceil \log_2 M \rceil + 1, \varepsilon')$-block-encoding of the Hamiltonian $H^{(\boldsymbol{x})} := \sigma^{-1} \sum_{j=1}^M x_j O_j$ if $\boldsymbol{x} \in F$ with $|F| \geq (1 - \delta')|G_p^M|$. Thus, using $U_\psi, U_\psi^\dagger$, and $U_{\rm obs}$, we can implement a $(1, a'' + \log_2 d, 0)$-block-encoding of the following Hamiltonian

$$\sum_{\boldsymbol{x} \in G_p^M} \tilde{f}(\boldsymbol{x}) |\boldsymbol{x}\rangle \langle \boldsymbol{x}|, \tag{B14}$$

where

$$\tilde{f}(\boldsymbol{x}) := \langle 0|^{\otimes a'' + \log_2 d} U_\psi^\dagger \cdot U_{\rm obs}^{(\boldsymbol{x})} \cdot U_\psi |0\rangle^{\otimes a'' + \log_2 d}.$$

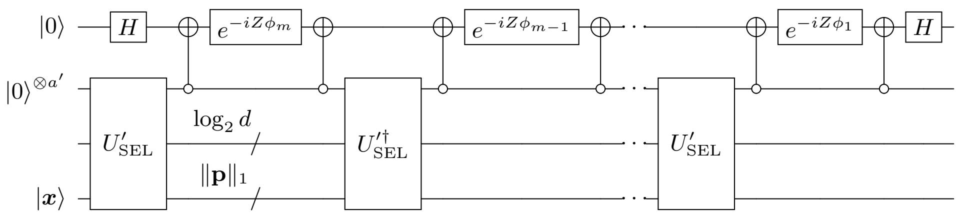


FIG. 10. Quantum circuit for $U_{\rm obs}$ in Eq. (B9). Here, $a' := \lceil \log_2 M \rceil + a$. The circuit parameters $\{\phi_j\}_{j=1}^m$ are adjusted for real QSP based on the degree-m odd polynomial $P(x) \approx \gamma x$, $\gamma = M/\sigma$. Note that $U'_{\rm SEL}$ contains a single use of $U_{\rm SEL} := \sum_{j=1}^M |j\rangle\langle j| \otimes B_j$.

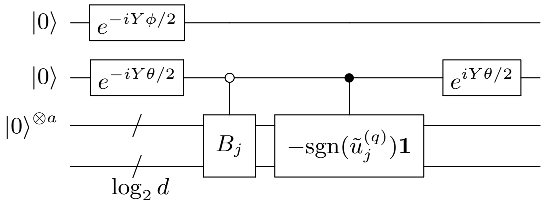


FIG. 11. Quantum circuit for an $(a+2)$-block-encoding of $\tilde{O}_j^{(q)} := (O_j - \tilde{u}_j^{(q)}\mathbf{1})/2$, where $\tilde{u}_j^{(q)} \in [-1,1]$. B_j is an a-block-encoding of O_j. The angles are defined as $\theta := 2\tan^{-1}\sqrt{|\tilde{u}_j^{(q)}|}$ and $\phi := 2\tan^{-1}\sqrt{4-(1+|\tilde{u}_j^{(q)}|)^2/(1+|\tilde{u}_j^{(q)}|)}$.

The corresponding quantum circuit is shown in Fig. 12. Thus, the block-Hamiltonian simulation (Lemma 6) yields the quantum circuit W for a $(1, a''+\log_2 d+2, \varepsilon'')$-block-encoding of time evolution operator

$$\sum_{\boldsymbol{x}\in G_p^M} e^{i\tilde{f}(\boldsymbol{x})t} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \quad \text{and} \quad t := 2^{p+2+q}\sigma. \tag{B15}$$

Note that a block encoding W' of ε''-precise time evolution operator e^{iHt} for some Hamiltonian H yields $\mathcal{O}(\sqrt{\varepsilon''})$-precise time evolved states, that is, for any state $|\psi\rangle$,

$$\left\| W' |\mathbf{0}\rangle |\psi\rangle - |\mathbf{0}\rangle e^{iHt} |\psi\rangle \right\| \le \varepsilon'' + \sqrt{2\varepsilon''},$$

where $|\mathbf{0}\rangle$ is the signal state for W'. Therefore, for $|\mathbf{0}\rangle = |0\rangle^{\otimes a''+\log_2 d+2}$ and the $+1$ eigenstate $|+\rangle$ of Pauli X , we obtain

$$\begin{aligned}
&\left\| W|\mathbf{0}\rangle|+\rangle^{\otimes pM} - \frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j \pi^{-1} 2^{q+1}\langle O_j\rangle} |\mathbf{0}\rangle|\boldsymbol{x}\rangle \right\| \\
&\le \varepsilon'' + \sqrt{2\varepsilon''} + \frac{1}{\sqrt{2^{pM}}} \left\| \sum_{\boldsymbol{x}\in G_p^M} e^{i\tilde{f}(\boldsymbol{x})t}|\boldsymbol{x}\rangle - \sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j \pi^{-1} 2^{q+1}\langle O_j\rangle} |\boldsymbol{x}\rangle \right\| \\
&\le \varepsilon'' + \sqrt{2\varepsilon''} + \sqrt{5\delta'} < \frac{1}{12}.
\end{aligned} \tag{B16}$$

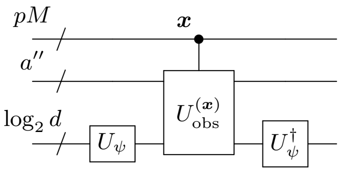


FIG. 12. Quantum circuit for a $(a'' + \log_2 d)$-block-encoding of $\sum_{\boldsymbol{x}\in G_p^M} \tilde{f}(\boldsymbol{x}) |\boldsymbol{x}\rangle \langle\boldsymbol{x}|$ in Eq. (B14).

Here, in the second inequality we used the following evaluation.

$$\begin{aligned}
&\left\| \sum_{\boldsymbol{x}\in G_p^M} e^{i\tilde{f}(\boldsymbol{x})t} |\boldsymbol{x}\rangle - \sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j \pi^{-1} 2^{q+1} \langle O_j\rangle} |\boldsymbol{x}\rangle \right\|^2 \\
&\le \sum_{\boldsymbol{x}\in G_p^M} \left| e^{i\tilde{f}(\boldsymbol{x})t} - e^{2\pi i 2^p \sum_{j=1}^M x_j \pi^{-1} 2^{q+1} \langle O_j\rangle} \right|^2 \\
&\le 4 \times 2^{pM}\delta' + \sum_{\boldsymbol{x}\in F} \left| e^{i\tilde{f}(\boldsymbol{x})t} - e^{2\pi i 2^p \sum_{j=1}^M x_j \pi^{-1} 2^{q+1} \langle O_j\rangle} \right|^2 \qquad (\because |F| \ge (1-\delta')|G_p^M|) \\
&\le 4 \times 2^{pM}\delta' + \sum_{\boldsymbol{x}\in F} \left| \tilde{f}(\boldsymbol{x})t - 2\pi 2^p \sum_{j=1}^M x_j \pi^{-1} 2^{q+1} \langle O_j\rangle \right|^2 \qquad (\because |e^{ia} - e^{ib}| \le |a-b|) \\
&\le 4 \times 2^{pM}\delta' + \sum_{\boldsymbol{x}\in F} (t\varepsilon')^2 \le 2^{pM} \times 5\delta' \quad (\because \varepsilon' := \sqrt{\delta'}/t).
\end{aligned} \tag{B17}$$

The gate complexity follows from that of Lemma 12 and Lemma 6.

□

Lemma 14 (State preparation by Grover-like repetition)**.** *Let O_j $(j = 1, 2, ..., M)$ be $d \times d$ observables O_j (d is a power of 2) with $\|O_j\| \le 1$, and let p be a positive integer. We assume the following two conditions holds for $\delta' := 2^{-14} \in (0,1)$:*

(i) $\sigma := \left\lceil \sqrt{2(M+1)\ln(2d/\delta')} \right\rceil < M+1.$

(ii) For a given $(\log_2 d)$-qubit quantum state $|\psi\rangle$ prepared by U_ψ, $|\langle O_j\rangle| \le 2^{-q-1}$ holds for all $j = 1, 2, ..., M$, where q denotes a non-negative integer satisfying

$$q \ge \log_4 \left[\frac{2^p \cdot 33^3}{625 \ln(2d/\delta')} \frac{\left\lceil \sqrt{2(M+1)\ln(2d/\delta')} \right\rceil}{\sqrt{\ln(2d/\delta')}} \right] \tag{B18}$$

Suppose we have access to $U'_{\mathrm{SEL}} := \sum_{\boldsymbol{x}\in G_p^M \times G_1} |\boldsymbol{x}\rangle \langle\boldsymbol{x}| \otimes U^{(\boldsymbol{x})}$, where $U^{(\boldsymbol{x})}$ is an $(a + \lceil \log_2(M+1) \rceil)$-block-encoding of

$$\frac{1}{M+1} \left(\sum_{j=1}^{M+1} x_j O_j \right)$$

for some $a \in \mathbb{N}$. Here, O_{M+1} denotes a 2×2 observable defined as

$$O_{M+1} := \frac{\pi(1/4 + 4l)}{2^{p+q}} I,$$

where l is an arbitrary integer satisfying $\|2^{q+1} O_{M+1}\| \le 1$ and I denotes the 1-qubit identity. Then, we can successfully prepare the following pM-qubit quantum state with a measurement result of ancilla qubits indicating the success:

$$\frac{1}{\sqrt{2^{pM}}} \sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p \sum_{j=1}^M x_j 2^{q+1} \pi^{-1} \langle O_j\rangle} |\boldsymbol{x}\rangle$$

up to 1/12 Euclidean distance error with the success probability ≥ 0.462. This implementation consists of $2t$ uses of U_ψ or $U_\psi^\dagger$, mt uses of U'_{SEL} or its inverse, $(2m+1)t$ uses of NOT gates controlled by at most $(a + \lceil \log_2(M +$

1)⌉ + $\log_2 d$) qubits, $\mathcal{O}(mt + pM)$ uses of single-qubit or two-qubit gates, additional $(\lceil \log_2(M+1)\rceil + \log_2 d + a + 2)$ ancilla qubits, and $\mathcal{O}(\mathrm{poly}(m))$ classical precomputation for finding quantum circuit parameters, where

$$t = 2^{p+q+2}\sigma \quad \text{and} \quad m = \mathcal{O}\left(\frac{M}{\sigma}\left(p + q + \log M\right)\right).$$

Proof of Lemma 14. Let $\varepsilon' = \sqrt{\delta'}/(2^{p+q+2}\sigma) \in (0, 1/2)$. From the assumption and Lemma 12, we have a unitary

$$U_{\text{obs}} := \sum_{(\boldsymbol{x},y)\in G_p^M \times G_1} |\boldsymbol{x}, y\rangle \langle \boldsymbol{x}, y| \otimes U_{\text{obs}}^{(\boldsymbol{x},y)}, \tag{B19}$$

where $U_{\text{obs}}^{(\boldsymbol{x},y)}$ is a $(1, a'' = a + \lceil \log_2 (M+1) \rceil + 1, \varepsilon')$-block-encoding of the Hamiltonian

$$H^{(\boldsymbol{x},y)} := \frac{1}{\sigma}\left(yO_{M+1} + \sum_{j=1}^{M} x_j O_j\right)$$

if $(\boldsymbol{x}, y) \in F$ with $|F| \geq (1-\delta')2|G_p^M|$. Thus, using $U_\psi, U_\psi^\dagger$, and U_{obs}, we can implement a $(1, a'' + \log_2 d, 0)$-block-encoding of the following Hamiltonian

$$\sum_{(\boldsymbol{x},y)\in G_p^M \times G_1} \tilde{f}(\boldsymbol{x}, y) |\boldsymbol{x}, y\rangle \langle \boldsymbol{x}, y|, \quad \text{where} \quad \tilde{f}(\boldsymbol{x}, y) := \langle 0|^{\otimes a'' + \log_2 d} U_\psi^\dagger \cdot U_{\text{obs}}^{(\boldsymbol{x},y)} \cdot U_\psi |0\rangle^{\otimes a'' + \log_2 d}. \tag{B20}$$

Since $U_{\text{obs}}^{(\boldsymbol{x},y)}$ is the ε'-precise block encoding of $H^{(\boldsymbol{x},y)}$, $\tilde{f}(\boldsymbol{x}, y)$ is close to an affine linear function as

$$\left| \tilde{f}(\boldsymbol{x}, y) - \frac{1}{\sigma}\left(y\langle O_{M+1}\rangle + \sum_{j=1}^{M} x_j \langle O_j \rangle\right)\right| \leq \varepsilon' \quad \text{for all} \quad (\boldsymbol{x}, y) \in F. \tag{B21}$$

Thus, Grover-like repetition on Eq. (B20), that is, Lemma 5 yields the quantum circuit W for an $(a'' + \log_2 d)$-block-encoding of the following operator

$$\sum_{(\boldsymbol{x},y)\in G_p^M \times G_1} T_t\left(\tilde{f}(\boldsymbol{x}, y)\right) |\boldsymbol{x}, y\rangle \langle \boldsymbol{x}, y| \quad \text{and} \quad t := 2^{p+q+2}\sigma.$$

Applying W to the state $|+\rangle^{\otimes pM+1} |\mathbf{0}\rangle$ with $|\mathbf{0}\rangle = |0\rangle^{\otimes a'' + \log_2 d}$, we obtain

$$W |+\rangle^{\otimes pM+1} |\mathbf{0}\rangle = \frac{\mathcal{N}_t}{\sqrt{2}}\left[\frac{1}{\mathcal{N}_t}\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x},y} T_t\left(\tilde{f}(\boldsymbol{x}, y)\right)|\boldsymbol{x}, y\rangle\right]|\mathbf{0}\rangle + \sqrt{1 - \left(\frac{\mathcal{N}_t}{\sqrt{2}}\right)^2}\,|\Phi^\perp\rangle, \tag{B22}$$

where $|\Phi^\perp\rangle$ denotes a normalized quantum state satifying $(\mathbf{1} \otimes |\mathbf{0}\rangle\langle\mathbf{0}|)\,|\Phi^\perp\rangle = \mathbf{0}$ and $\mathcal{N}_t$ is defined as:

$$\mathcal{N}_t := \left\| \frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x},y} T_t\left(\tilde{f}(\boldsymbol{x}, y)\right)|\boldsymbol{x}, y\rangle \right\|. \tag{B23}$$

Measuring the $(a'' + \log_2 d)$-qubit ancilla registers in (B22), we obtain the outcome $|\mathbf{0}\rangle$ and the following state with the probability $\mathcal{N}_t^2/2$:

$$\frac{1}{\mathcal{N}_t}\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x},y} T_t\left(\tilde{f}(\boldsymbol{x}, y)\right)|\boldsymbol{x}, y\rangle. \tag{B24}$$

In the following, we show this quantum state is close to the following state

$$\begin{aligned} &\frac{1}{\sqrt{2^{pM}}}\sum_{(\boldsymbol{x},x_{M+1})\in G_p^M \times G_1} \cos\left[t\left(\frac{\pi}{2} - \frac{1}{\sigma}\sum_{j=1}^{M+1} x_j \langle O_j\rangle\right)\right] |\boldsymbol{x}\rangle\,|x_{M+1}\rangle \\ &= \frac{1}{\sqrt{2}}\sum_{s=\pm 1}\sum_{\boldsymbol{x}\in G_p^M} \frac{1}{\sqrt{2^{pM}}} e^{2\pi i 2^p \sum_{j=1}^{M}(s x_j)\pi^{-1}2^{q+1}\langle O_j\rangle} |\boldsymbol{x}\rangle \otimes \mathrm{QFT}_{G_1}|s/4\rangle. \end{aligned} \tag{B25}$$

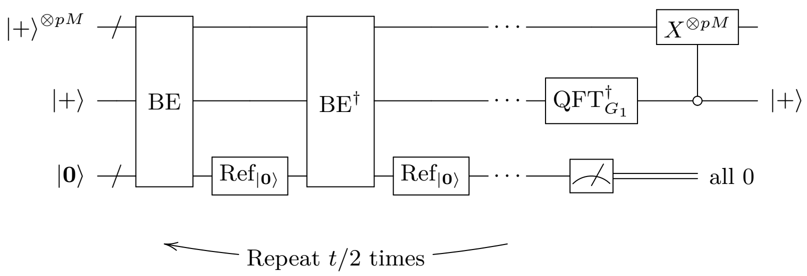


FIG. 13. Quantum circuit for the approximate probing state preparation $|\Upsilon(q)\rangle$ by Grover-like repetition. $|\mathbf{0}\rangle := |0\rangle^{\otimes a'' + \log_2 d}$ and BE denotes the block encoding of Eq. (B20). $\mathrm{Ref}_{|\mathbf{0}\rangle}$ is the reflection on $|\mathbf{0}\rangle$, i.e., $\mathrm{Ref}_{|\mathbf{0}\rangle} := 2\,|\mathbf{0}\rangle\,\langle\mathbf{0}| - \mathbf{1}$. The measurement outcome $|\mathbf{0}\rangle$ is obtained with the probability $\mathcal{N}_t^2/2 \geq 0.462$.

Note that the equality in Eq. (B25) can be shown as follows.

$$\begin{aligned}
&\sum_{(\boldsymbol{x}, x_{M+1}) \in G_p^M \times G_1} \cos\left[t\left(\frac{\pi}{2} - \frac{1}{\sigma}\sum_{j=1}^{M+1} x_j \langle O_j\rangle\right)\right] |\boldsymbol{x}\rangle\,|x_{M+1}\rangle \\
&= \frac{1}{2}\sum_{\boldsymbol{x},y}\sum_{s=\pm1} e^{-is\frac{t}{\sigma}\left(y\langle O_{M+1}\rangle + \sum_{j=1}^M x_j\langle O_j\rangle\right)}\,|\boldsymbol{x}\rangle\,|y\rangle \quad (\because e^{ist\pi/2} = e^{2\pi i s 2^{p+q}\sigma} = 1) \\
&= \frac{1}{\sqrt{2}}\sum_{s=\pm1}\sum_{\boldsymbol{x}\in G_p^M} e^{-ist\frac{1}{\sigma}\sum_{j=1}^M x_j\langle O_j\rangle}\,|\boldsymbol{x}\rangle \otimes \frac{1}{\sqrt{2}}\sum_{y\in G_1} e^{-ist\frac{1}{\sigma}y\langle O_{M+1}\rangle}\,|y\rangle \\
&= \frac{1}{\sqrt{2}}\sum_{s=\pm1}\sum_{\boldsymbol{x}\in G_p^M} e^{-ist\frac{1}{\sigma}\sum_{j=1}^M x_j\langle O_j\rangle}\,|\boldsymbol{x}\rangle \otimes \mathrm{QFT}_{G_1}\,|-s/4\rangle \quad (\because \langle O_{M+1}\rangle = \frac{\pi(1/4+4l)}{2^{p+q}}) \\
&= \frac{1}{\sqrt{2}}\sum_{s=\pm1}\sum_{\boldsymbol{x}\in G_p^M} e^{-is2\pi 2^p\sum_{j=1}^M x_j\pi^{-1}(2^{q+1})\langle O_j\rangle}\,|\boldsymbol{x}\rangle \otimes \mathrm{QFT}_{G_1}\,|-s/4\rangle\,.
\end{aligned} \tag{B26}$$

Thus, by applying $\mathrm{QFT}^\dagger_{G_1}$ and controlled $X^{\otimes pM}$ gate to the state (B22), we can prepare the target state:

$$\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x}\in G_p^M} e^{2\pi i 2^p\sum_{j=1}^M x_j 2^{q+1}\pi^{-1}\langle O_j\rangle}\,|\boldsymbol{x}\rangle \otimes |+\rangle \tag{B27}$$

up to some Euclidean distance error with the probability $\mathcal{N}_t^2/2$, because $X^{\otimes pM}\,|\boldsymbol{x}\rangle = |-\boldsymbol{x}\rangle$ holds. Note that $\mathrm{QFT}^\dagger_{G_1}$ and controlled $X^{\otimes pM}$ does not change the probability to obtain the success flag $|\mathbf{0}\rangle$. Here, we show the corresponding quantum circuit to prepare Eq. (B27) in Fig. 13.

For subsequent proof, we here show that for any $\delta' \in (0,1)$ and any real weight w_j $(j = 1, 2, ..., M+1)$, a subset F' of $G_p^M \times G_1$ defined as

$$F' := \left\{(\boldsymbol{x}, y) \in G_p^M \times G_1 : \left|\sum_{j=1}^{M+1} w_j x_j\right| < \sqrt{\frac{\ln(2/\delta')}{2}\sum_{j=1}^{M+1}|w_j|^2}\right\} \tag{B28}$$

has the cardinality $|F'| \geq (1-\delta')2^{pM+1}$. This fact can be proved from the Hoeffding's inequality as follows. Let us consider independent random variables X_j $(j = 1, 2, ..., M)$ and Y. Here, X_j are identically and uniformly distributed in G_p and Y is uniformly distributed in G_1. Note that the random variables are upper bounded by $1/2$ from the definition of G_p. Therefore, from the Hoeffding's inequality, we obtain

$$\mathrm{Pr}_{X_1,...,X_M,Y}\left[\left|\sum_{j=1}^{M+1} w_j X_j\right| \geq c\right] \leq 2\mathrm{exp}\left[-\frac{2c^2}{\sum_j |w_j|^2}\right]. \tag{B29}$$

Thus, taking c as $c = \sqrt{\frac{\ln(2/\delta')}{2}\sum_{j=1}^{M+1}|w_j|^2}$, we obtain

$$\mathrm{Pr}_{X_1,\dots,X_M,Y}\left[\left|\sum_{j=1}^{M+1} w_j X_j\right| \geq \sqrt{\frac{\ln(2/\delta')}{2}\sum_{j=1}^{M+1}|w_j|^2}\right] \leq \delta'. \tag{B30}$$

Since the independent random variables $X_1,\dots,X_M,Y$ has uniform distributions, F' has the cardinality $\geq 2^{pM+1}(1-\delta')$.

Now, we are ready to show the closeness between Eq. (B24) and Eq. (B25). Defining F' for $\delta' = 2^{-14}$ and $w_j = \langle O_j\rangle$ as

$$F' := \left\{(\boldsymbol{x},y)\in G_p^M \times G_1 : \left|\sum_{j=1}^{M+1} x_j\langle O_j\rangle\right| < \sqrt{\frac{\ln(2/\delta')}{2}\sum_{j=1}^{M+1}|\langle O_j\rangle|^2}\right\} \tag{B31}$$

and recalling that $|F'|,|F| \geq (1-\delta')2^{pM+1}$, we proceed as follows.

$$\begin{aligned}
&\left\|\sum_{(\boldsymbol{x},y)\in G_p^M\times G_1} T_t(\tilde{f}\,(\boldsymbol{x},y))\,|\boldsymbol{x}\rangle\,|y\rangle - \sum_{(\boldsymbol{x},y)\in G_p^M\times G_1} \cos\left[t\left(\frac{\pi}{2}-\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right)\right]|\boldsymbol{x}\rangle\,|y\rangle\right\|^2\\
&= \sum_{(\boldsymbol{x},x_{M+1})\in G_p^M\times G_1}\left|T_t(\tilde{f}(\boldsymbol{x},x_{M+1})) - \cos\left[t\left(\frac{\pi}{2}-\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right)\right]\right|^2\\
&\leq 4\times 2\times 2^{pM+1}\delta' + \sum_{(\boldsymbol{x},x_{M+1})\in F\cap F'}\left|t\cos^{-1}\left[\tilde{f}(\boldsymbol{x},x_{M+1})\right] - t\left(\frac{\pi}{2}-\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right)\right|^2,
\end{aligned} \tag{B32}$$

where we used $|\cos(a)-\cos(b)| \leq |a-b|$ and $G_p^M\times G_1 = (F\cap F')\cup(F^{\mathrm{c}}\cup(F')^{\mathrm{c}})$ in the third line. Now, we focus on the case $(\boldsymbol{x},x_{M+1})\in F\cap F'$.

$$\begin{aligned}
|\tilde{f}(\boldsymbol{x},x_{M+1})| &\leq \varepsilon' + \left|\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right| \qquad (\because \text{Eq. (B21)})\\
&\leq \varepsilon' + \sqrt{\frac{\sum_j|\langle O_j\rangle|^2}{4(M+1)}}\sqrt{\frac{\ln(2/\delta')}{\ln(2d/\delta')}} \qquad (\because \text{Eq. (B31)})\\
&\leq \frac{\sqrt{\delta'}}{2^{p+q+2}\sigma} + \frac{1}{2^{q+2}}\sqrt{\frac{\ln(2/\delta')}{\ln(2d/\delta')}} < \frac{33/10}{2^{q+2}\sqrt{\ln(2d/\delta')}} < 1/4.
\end{aligned} \tag{B33}$$

In the case of $|x|\leq 1/4$, $\left|\cos^{-1}(x)-\pi/2+x\right| \leq \frac{1}{5}|x|^3$ holds, and therefore we obtain

$$\begin{aligned}
&t\left|\cos^{-1}\left[\tilde{f}(\boldsymbol{x},x_{M+1})\right] - \left(\frac{\pi}{2}-\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right)\right|\\
&= t\left|\cos^{-1}\left[\tilde{f}(\boldsymbol{x},x_{M+1})\right] - \frac{\pi}{2} + \tilde{f}(\boldsymbol{x},x_{M+1}) + \left(\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle - \tilde{f}(\boldsymbol{x},x_{M+1})\right)\right|\\
&\leq t\varepsilon' + t\left|\cos^{-1}\left[\tilde{f}(\boldsymbol{x},x_{M+1})\right] - \frac{\pi}{2} + \tilde{f}(\boldsymbol{x},x_{M+1})\right|\\
&\leq t\varepsilon' + \frac{t}{5}\left|\frac{33/10}{2^{q+2}\sqrt{\ln(2d/\delta')}}\right|^3.
\end{aligned} \tag{B34}$$

From the assumption, the non-negative integer q satisfies $\frac{t}{5}\left|\frac{33/10}{2^{q+2}\sqrt{\ln(2d/\delta')}}\right|^3 \le \sqrt{\delta'}$, then we conclude that

$$\begin{aligned}&\left\|\sum_{(\boldsymbol{x},y)\in G_p^M\times G_1} T_t(\tilde{f}\,(\boldsymbol{x},y))\,|\boldsymbol{x}\rangle\,|y\rangle - \sum_{(\boldsymbol{x},y)\in G_p^M\times G_1}\cos\left[t\left(\frac{\pi}{2}-\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right)\right]|\boldsymbol{x}\rangle\,|y\rangle\right\|\\ &\le \sqrt{4\times 2\times 2^{pM+1}\delta' + \sum_{(\boldsymbol{x},x_{M+1})\in F\cap F'}(2\sqrt{\delta'})^2}\\ &\le 2\sqrt{6\delta'}\times\sqrt{2^{pM}}.\end{aligned} \tag{B35}$$

This leads to

$$1-2\sqrt{6\delta'} \le \mathcal{N}_t = \left\|\frac{1}{\sqrt{2^{pM}}}\sum_{\boldsymbol{x},y} T_t\left(\tilde{f}(\boldsymbol{x},y)\right)|\boldsymbol{x},y\rangle\right\| \le 1+2\sqrt{6\delta'} \tag{B36}$$

and

$$\begin{aligned}&\left\|\frac{1}{\mathcal{N}_t}\sum_{(\boldsymbol{x},y)\in G_p^M\times G_1} T_t(\tilde{f}\,(\boldsymbol{x},y))\,|\boldsymbol{x}\rangle\,|y\rangle - \sum_{(\boldsymbol{x},y)\in G_p^M\times G_1}\cos\left[t\left(\frac{\pi}{2}-\frac{1}{\sigma}\sum_{j=1}^{M+1}x_j\langle O_j\rangle\right)\right]|\boldsymbol{x}\rangle\,|y\rangle\right\|\\ &\le \sqrt{2^{pM}}\times\frac{4\sqrt{6\delta'}}{1-2\sqrt{6\delta'}} < \sqrt{2^{pM}}\times\frac{1}{12}.\end{aligned} \tag{B37}$$

Therefore, we can prepare the target state up to $1/12$ Euclidean distance error with the probability $\mathcal{N}_t^2/2 > 0.462$. Finally, the gate complexity follows from that of Lemma 12 and Lemma 5.

□

Note that we can coherently amplify the success probability in Lemma 14 by quantum amplitude amplification [37], while this requires a quantum circuit with 3-fold depth compared to the quantum circuit (before measurement) in Fig. 13.

2. Maximum mean squared error (MSE) and query complexity

Here, we evaluate the relation between the root mean squared error ε and the total queries to the state preparation in Algorithm 1*.

Proof of Theorem 2. The core idea of this proof is similar to the previous methods [45, 46, 50], but we need carefully to deal with the condition of gradient estimation. In the following, we prove this theorem based on the state preparation by Lemma 13; see remarks after this proof for the case of Lemma 14.

We start by clarifying the statistical property of $g_j^{(q)}$ in the step 5 of Algorithm 1*. The truncation in Step 7 guarantees $\tilde{u}_j^{(q)} \in [-1,1]$ for all q; we can construct a block-encoding U'_{SEL} for $\{\tilde{O}_j^{(q)}\}$, which is assumed to be accessible in Lemma 13, from the block encodings of $\{O_j\}$; see Fig. 11. Therefore, using the Lemma 13, we can prepare the quantum state in Step 4.

Now, we consider the case that the following condition for gradient estimation holds at the beginning of an iteration q: for all j,

$$\left|\langle\tilde{O}_j^{(q)}\rangle\right| = \left|\frac{\langle O_j\rangle - \tilde{u}_j^{(q)}}{2}\right| \le 2^{-q-1}. \tag{B38}$$

Then, a single shot measurement result $\boldsymbol{k} := (k_1,\ldots,k_M)\in G_p^M$ in Step 4 follows

$$\Pr\left[\left|k_j - \frac{2^q(\langle O_j\rangle - \tilde{u}_j^{(q)})}{\pi}\right| > \frac{3}{2^p}\right] \le \frac{1}{3},$$

for every $j = 1,2,\ldots,M$, from the analysis of gradient estimation in Lemma 9. If we take $p=5$, then the additive error $3/2^p$ is smaller than $1/2\pi$, and therefore, the temporal estimate $\tilde{u}_j^{(q)} + \frac{\pi}{2^q}k_j$ becomes a 1-bit more precise estimate of $\langle O_j\rangle$ at least $2/3$ probability. However, the choice of $p=5$ is sufficient but not tight. Here, we employ the following tighter bound that we numerically found [62]: if we take $p=3$,

$$\Pr\left[\left|k_j - \frac{2^q(\langle O_j\rangle - \tilde{u}_j^{(q)})}{\pi}\right| > \frac{1}{2\pi}\right] < 0.18 + \frac{1}{12}, \tag{B39}$$

holds for every j, where the term $1/12$ arises from the Euclidean distance error as well as Lemma 9. Since the

$g_j^{(q)}$ is defined as the coordinate-wise median of independent samples $\boldsymbol{k}^{(1)}, ..., \boldsymbol{k}^{(\#)}$, the Hoeffding's inequality for the independent and bounded random variables $\{\chi[|k_j^{(i)} - 2^q(\langle O_j\rangle - \tilde{u}_j^{(q)})/\pi| > 1/(2\pi)]\}_i$ yields

$$\Pr\left[\left|g_j^{(q)} - \frac{2^q(\langle O_j\rangle - \tilde{u}_j^{(q)})}{\pi}\right| > \frac{1}{2\pi}\right] \leq e^{-\frac{\#}{9}}, \tag{B40}$$

for every j. Here, $\chi[\bullet]$ denotes the indicator function. Therefore, taking $\# := 9\ln(M/\delta^{(q)})$ and using the union bound, we can bound the probability of the event

$$\mathbf{A}^{(q)} : \max_j \left|g_j^{(q)} - 2^q(\langle O_j\rangle - \tilde{u}_j^{(q)})/\pi\right| \leq \frac{1}{2\pi}$$

as $\Pr[\mathbf{A}^{(q)}] \geq 1 - \delta^{(q)}$. In the event $\mathbf{A}^{(q)}$, $|\langle\tilde{O}_j^{(q+1)}\rangle| \leq 2^{-q-2}$ holds even if we truncate $\tilde{u}_j^{(q+1)}$ in Step 7. On the other hand, if the condition Eq. (B38) is false, the gradient estimation does not work, and we only say that the measurement result $g_j^{(q)}$ is bounded as $g_j^{(q)} \in [-1/2, 1/2]$ because of the definition of G_p^M.

In the case of $q = 0$, the condition Eq. (B38) holds, and thus, the event $\mathbf{A}^{(0)}$ occurs with the probability $1 - \delta^{(0)}$. By repeating this, in branches such that all of $\{\mathbf{A}^{(q)}\}_{q=0}^{q'-1}$ occur, the temporal estimate $\tilde{u}_j^{(q')}$ satisfy $|\tilde{u}_j^{(q')} - \langle O_j\rangle| \leq 1/2^{q'}$ for all j. Moreover, considering branches such that all of $\{\mathbf{A}^{(q)}\}_{q=0}^{q'-1}$ occur but the complement of $\mathbf{A}^{(q')}$ occurs at the iteration q', we bound the additive error of the final estimate $\tilde{u}_j$ in such branches as follows:

$$\begin{aligned}|\tilde{u}_j - \langle O_j\rangle| &\leq |\tilde{u}_j - \tilde{u}_j^{(q')}| + |\tilde{u}_j^{(q')} - \langle O_j\rangle| \\ &\leq \pi\left|\sum_{q\geq q'} \frac{g_j^{(q)}}{2^q}\right| + \frac{1}{2^{q'}} \\ &\leq \frac{1+\pi}{2^{q'}}.\end{aligned} \tag{B41}$$

In the third line, we use the fact $|g_j^{(q)}| \leq 1/2$. Thus, we can calculate the mean squared error of $\hat{u}_j$ as

$$\begin{aligned}&\mathbb{E}\left[(\hat{u}_j - \langle O_j\rangle)^2\right] \\ &\leq \frac{1}{2^{2(q_{\max}+1)}} + (1+\pi)^2 \sum_{q=0}^{q_{\max}} \frac{\delta^{(q)}}{4^q} \\ &\leq \frac{1}{2^{2(q_{\max}+1)}} + (1+\pi)^2 c 2^{-2q_{\max}+1} \\ &\leq \varepsilon^2,\end{aligned} \tag{B42}$$

where we defined $q_{\max} := \lceil \log_2(1/\varepsilon)\rceil$. In the final line, we used the fact $c \in (0, 3/(8(1+\pi)^2)]$. The inequality holds for all j, which completes the proof of Eq. (4).

Next, we count the total queries to the state preparation U_ψ. At each iteration q, we prepare $\# := 9\ln(M/\delta^{(q)})$ copies of a quantum state that approximates the probing state $|\Upsilon(q)\rangle$. If we prepare a single copy of this state using the method in Lemma 13, then the $\mathcal{O}(2^{p+q+2}\sigma)$ queries to U_ψ and its inverse are required, and therefore the total queries are calculated as

$$\begin{aligned}&\sum_{q=0}^{q_{\max}} 2^{p+q+2}\sigma \times 9\ln(M/\delta^{(q)}) \\ &= 9\cdot 2^{p+2}\sigma \times \sum_{q=0}^{q_{\max}} 2^q \ln(M/\delta^{(q)}) \\ &= 9\cdot 2^{p+2}\sigma\left[2^{q_{\max}+1}\ln\frac{8M}{c} - (q_{\max}+2)\ln 8 - \ln\frac{M}{c}\right] \\ &= \mathcal{O}(\varepsilon^{-1}\sqrt{M}\log M).\end{aligned}$$

□

Here, we discuss the case that we employ Lemma 14 to the state preparation in Step 4 of Algorithm 1*. This alternative method can prepare the probing state $|\Upsilon(q)\rangle$ under the following conditions: (i) $|\langle\tilde{O}_j^{(q)}\rangle| \leq 2^{-q-1}$ and (ii) the iteration step q satisfies Eq. (B18). In the case that only the condition (i) (or equivalently, Eq. (B38)) is violated, the quantum circuit in Fig. 13 for Lemma 14 yields a pM-qubit quantum state that may be far from the target probing state. However, this does not affect the proof of Theorem 2 because it is only required that the measurement results at the end of Fig. 13 are in the range of $[-1/2, 1/2]$. On the other hand, the condition (ii) restricts the usage of the alternative method, as discussed in Sec. IV B 3.

Variational quantum simulation: a case study for understanding warm starts

Ricard Puig-I-Valls[1] [*] Marc Drudis[2 1] [†] Supanut Thanasilp[1 3] Zoë Holmes[1]

[1] *Institute of Physics, Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland*
[2] *IBM Quantum, IBM Research – Zurich, 8803 Rüschlikon, Switzerland*
[3] *Chula Intelligent and Complex Systems, Department of Physics, Faculty of Science, Chulalongkorn University, Bangkok, Thailand, 10330*

Abstract. The barren plateau phenomenon, characterized by loss gradients that vanish exponentially with system size, poses a challenge to scaling of variational quantum algorithms (VQAs). In our work, we explore the potential of warm starts, whereby initializing close to a solution, we hope to enjoy larger gradients. Focusing on an iterative variational method for quantum simulation, we analytically show that a small region around the initialization at each iteration exhibits substantial gradients with convexity guarantees. However, our study highlights scenarios where a good minimum shifts outside the region with guarantees. Our analysis leaves open the question whether such minima jumps necessitate optimization across barren plateau landscapes or whether there exist gradient flows, i.e., fertile valleys away from the plateau with substantial gradients, that allow for training.

Keywords: Variational Quantum Algorithms, Warm Start, Trainability guarantees, Barren Plateaus, Quantum Simulation

1 Summary

Barren plateaus, i.e., loss landscapes that concentrate exponentially in system size towards their mean value with high probability, [1–19] are widely thought to pose a significant barrier to the scaling up of variational quantum algorithms. However, barren plateaus are fundamentally a statement about the landscape on average. Indeed, regions of the landscape with significant gradients must exist around the minima. This has motivated the study of *warm starts* whereby the algorithm is cleverly initialized closer to one. Numerical studies indicate that these methods may be promising [20–23]. In parallel, analytic studies have proven that initializations around identity can exhibit non-exponentially vanishing gradients [24–28]. Nonetheless, a good solution may be far from this identity region.

Here we consider a family of variational quantum algorithms that inherently use warm starts and take this as a case study to better understand their potential and limitations. In particular, we study an approach for learning shorter depth circuits for simulating quantum systems by iteratively compressing real or imaginary time Trotter evolution circuits [29–35]. At each iteration, the previous solution is used to initialize the parameters to learn a new compressed circuit to implement a slightly longer evolution as shown in Fig. 1a).

This case study is an ideal playground for studying warm starts because its inbuilt structure allows one to analytically compute bounds on its trainability. **(I)** We start by proving that as long as the training in one time-step is successful then the algorithm will exhibit substantial gradients in a small region around the next initialization. **(II)** We then establish guarantees on the approximate convexity of the gradients in this region and further argue that for polynomially large time-steps the new optimum (called an adiabatic minimum) will typically remain in this convex region. These results are summarised in Fig. 1b.

However, these positive findings are partially tempered by the observation there is no guarantee that a good minimum remains in this region. **(III)** Namely, there exist cases where a good minimum jumps from the region with trainability guarantees. Our analysis leaves open the question of whether such minima jumps necessitate optimization across barren plateau landscapes or whether there exist gradient flows that allow for training. **(IV)** As numerically observed in our contrived example on a 10-qubit system, such fertile valleys, i.e. small regions away from the plateau with substantial gradients, that allow for successful training are theoretically possible. However, to what extent they arise in practise is an open question. We end by discussing the wider applications of our work to other iterative and/or perturbative variational quantum algorithms.

2 Framework

Iterative Variational Trotter Compression. One standard approach to simulate the time evolution of some initial state $|\psi_0\rangle$ under a Hamiltonian H is by a Trotter evolution where the total time t is broken down into a sequence of N short δt Trotter steps with $t = N\delta t$, such that $e^{-iHt}|\psi_0\rangle \approx \prod_{k=1}^{N} e^{-iH\delta t}|\psi_0\rangle$ where the approximation error is in $\mathcal{O}(N\delta t)$. However, these approaches are fundamentally limited by the linear growth of circuit depths with time simulated. Here we focus on the proposal to use a variational quantum algorithm to compress the depth of the Trotter circuit at each iteration of the algorithm [29–35] as shown in Fig. 1. More concretely, at any iteration of the algorithm, one variationally minimizes the following loss:

$$\mathcal{L}(\boldsymbol{\theta}) = 1 - |\langle\psi_0|U(\boldsymbol{\theta})^\dagger e^{-iH\delta t}U(\boldsymbol{\theta}^*)|\psi_0\rangle|^2 \qquad (1)$$

[*] The first two authors contributed equally to this work.

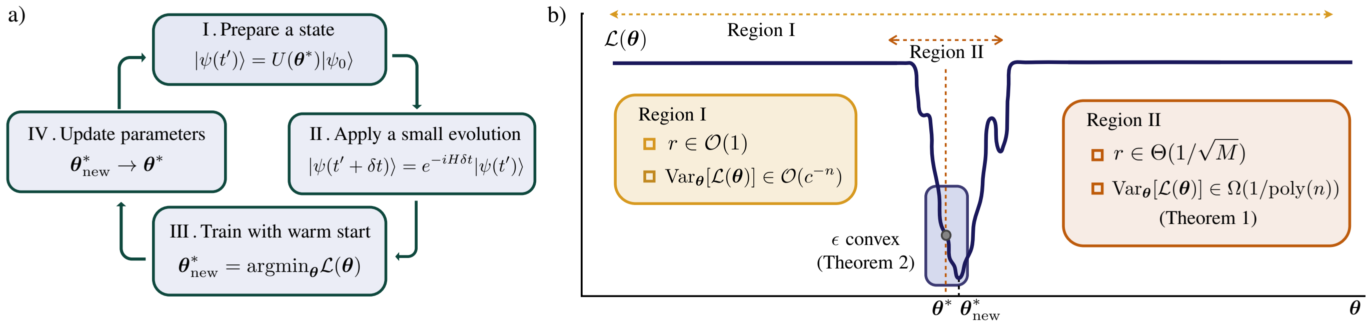

a)
I. Prepare a state
$|\psi(t')\rangle = U(\boldsymbol{\theta}^*)|\psi_0\rangle$
II. Apply a small evolution
$|\psi(t'+\delta t)\rangle = e^{-iH\delta t}|\psi(t')\rangle$
III. Train with warm start
$\boldsymbol{\theta}^*_{\rm new} = \text{argmin}_{\boldsymbol{\theta}}\mathcal{L}(\boldsymbol{\theta})$
IV. Update parameters
$\boldsymbol{\theta}^*_{\rm new} \rightarrow \boldsymbol{\theta}^*$
b)
$\mathcal{L}(\boldsymbol{\theta})$
Region I
Region II
Region I
$r \in \mathcal{O}(1)$
$\text{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \mathcal{O}(c^{-n})$
Region II
$r \in \Theta(1/\sqrt{M})$
$\text{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \Omega(1/\text{poly}(n))$
(Theorem 1)
ϵ convex
(Theorem 2)
$\boldsymbol{\theta}^*$ $\boldsymbol{\theta}^*_{\rm new}$
$\boldsymbol{\theta}$

Figure 1: a) Each iteration of the variational compression scheme consists of four steps. Starting from the top: (i) apply the circuit with the last set of parameters $\boldsymbol{\theta}^*$ to the initial state, (ii) apply $e^{-iH\delta t}$ for a small time-step δt, (iii) train the circuit initialising your parameters around the previous ones, (iv) update the parameters. b) We sketch a typical representation of a loss function $\mathcal{L}(\boldsymbol{\theta})$ with a barren plateau across the full landscape (Region I). In Theorem 1 we prove that in a hypercube of width $2r$ with $r \in \Theta\left(1/\sqrt{M}\right)$ (sketched as Region II) the variance of the loss is only polynomially vanishing in system size n. In Theorem 2 we prove that in a smaller hypercube (highlighted as the blue region) the landscape is approximately convex.

where $U(\boldsymbol{\theta})$ is a parameterized quantum circuit and $\boldsymbol{\theta}^*$ denotes the optimized parameters found at the previous iteration step [29, 31, 33]. At iteration k the loss $\mathcal{L}(\boldsymbol{\theta})$ is optimized using a hybrid quantum classical optimization loop to find the next set of optimal parameters $\boldsymbol{\theta}^*_{\rm new}$. We consider a general ansatz of the form $U(\boldsymbol{\theta}) = \prod_{i=1}^{M} V_i e^{-i\theta_i\sigma_i}$ where $\{\theta_i\}$ is a set of M uncorrelated trainable parameters, $\{V_i\}_{i=1}^{M}$ is a set of fixed unitary matrices and $\{\sigma_i\}_{i=1}^{M}$ is a set of generators on n qubits such that $\sigma_i = \sigma_i^\dagger$ and $\sigma_i^2 = \mathbb{1}$. In the manuscript we also consider the case of imaginary time evolution.

Gradient magnitudes and barren plateaus. For a wide class of problems (including the loss in Eq. (1) with random initialization) [1–19], one can show that the loss variance vanishes exponentially with problem sizes, i.e. $\text{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \mathcal{O}(c^{-n})$ with $c > 1$. On such *barren plateau* landscapes exponentially precise loss evaluations are required to navigate the towards the global minimum and hence the resources (shots) required for training also scales exponentially. This has prompted the search for strategies where loss variances vanish at worst polynomially with system size, $\text{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \Omega\left(1/\text{poly}(n)\right)$, such that resource requirements may scale polynomially.

3 Main results

Lower-bound on the loss variance. We analytically and rigorously provide guarantees for all iterations of the algorithm that the region around the starting point has substantial gradients for a sufficiently small time-step as sketched in Fig. 1b). Our guarantees are based on the observation that assuming the previous step was sufficiently well optimised, and the time-step δt is small enough, then one can initialize close enough to the new global minimum (or, more modestly, a good new minimum). We use this observation to derive Theorem 1 in our manuscript which analytically provides a loss variance lower bound. More concretely, consider a hypercube region $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r) := \{\boldsymbol{\theta}\}$ such that $\theta_i \in [\theta_i^* - r, \theta_i^* + r]\ \forall\ i$. Theorem 1 indicates that for a small $\delta t \in \mathcal{O}\left(1/\lambda_{\max}\right)$ with $\lambda_{\max}$ being the largest eigenvalue of H and $r \in \Theta\left(1/\sqrt{M}\right)$, the variance over $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$, where each parameter is uniformly sampled, scales at least polynomial in the system's size.

In Fig. 2(a - c), we numerically study the scaling of the variance and further empirically observe that for large r the loss variance vanishes exponentially, hence recovering a common barren plateau result. However, the width of the region of attraction, as indicated by non-exponentially vanishing loss variances, scales as $r \in \Theta\left(1/\sqrt{M}\right)$ (inline with our analytic bounds).

Convexity region and adiabatic minimum. Non-vanishing gradients in the region around the initialisation are a necessary condition to have any hope of successfully training a variational quantum algorithm but they are not sufficient. Of particular importance is the potential to become trapped in spurious local minima. One way to provide guarantees against this concern is to prove that this region is (approximately) convex. Theorem 2 in our manuscript analytically indicates that for each iteration it is possible to choose a polynomially small time-step δt such that the loss region around initialization (within the substantial gradient region) is *approximately* convex.

We then introduce the notion of the adiabatic minima (see Definition 2) as the minima that would be reached by increasing δt infinitely slowly and minimizing $\mathcal{L}(\boldsymbol{\theta})$ by gradient descent with a very small learning rate. Crucially, in Theorem 3, we argue that as long as the time-step is δt is not too large (i.e. decreases polynomially with the number of parameters M) we can ensure that an adiabatic minima is within the convex region with non-vanishing gradients, and thus it should be possible to train to the adiabatic minimum.

Minimum jump and fertile valleys. We explore the limitations of our analytic bounds. Firstly, we highlight that our analysis can not provide convergence guarantees to a good minimum because *minima jumps* are possible. Namely, from one time-step to the other, the adiabatic minimum can become a relatively poor local minimum and a superior minimum can emerge elsewhere in the

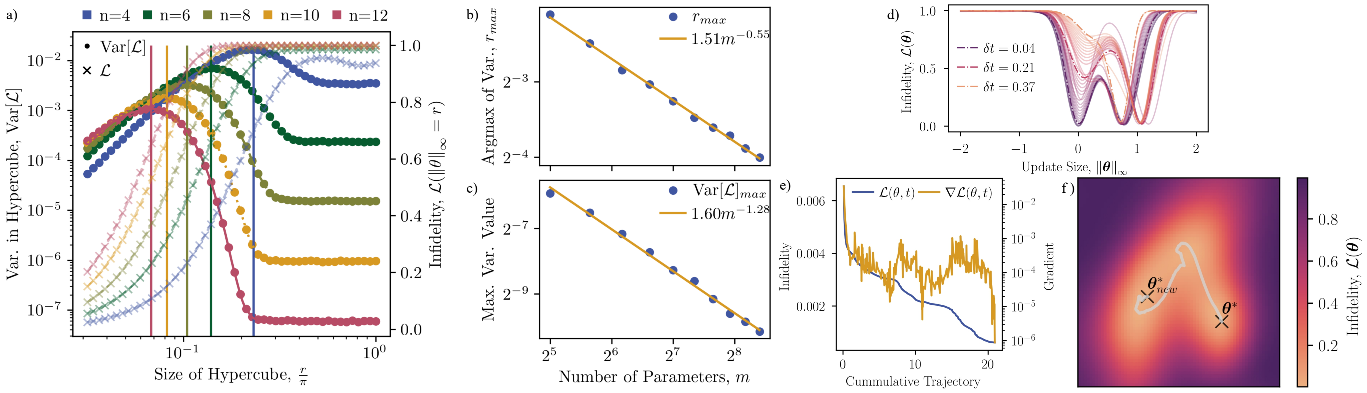


Figure 2: **(a - c) Variance of landscape and width of narrow gorge.** Here we study the landscape of $\mathcal{L}(\boldsymbol{\theta})$, for the first time-step of the variational Trotter compression algorithm, for different system sizes n as a function of the width of the hypercube r. We consider a hardware efficient ansatz with n layers and random initial parameters within the hypercube. a) We plot $\mathcal{L}(\boldsymbol{\theta})$ and its variance $\text{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}[\mathcal{L}(\boldsymbol{\theta})]$ as function of r/π. Since the shape of the landscape depends on the direction of the parameter update, to plot $\mathcal{L}(\boldsymbol{\theta})$ we have taken the average over 500 different directions. For $\text{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}[\mathcal{L}(\boldsymbol{\theta})]$, we keep track of its maximum value (marked with a vertical line) for each system size. b) The value $r_{\max}$ for which the variance peaks as function of the number of parameters in the ansatz. c) Maximum value of the variance for different system sizes. While the results shown here are for the first iteration of the variational compression scheme very similar results are observed at later iterations (in line with Theorem 1). **d) Minimum jump.** Here we show a 1D-cut of the landscape $\mathcal{L}(\boldsymbol{\theta})$ as we increase the time-step δt. The cut includes the initial parameters-with update $\delta t = 0$ and $||\boldsymbol{\theta}||_\infty = 0$. We choose a 10 qubit Ising Hamiltonian $H = \sum X_i X_{i+1} - 0.95 \sum Y_i$ on a 1D-lattice. We use a 2-layered Hamiltonian Variational Ansatz. **(e - f) Fertile valley.** Here we show a 2D plot of the loss landscape at $\delta t = 0.04$ for a 10 qubit Ising Hamiltonian $H = \sum X_i X_{i+1} - 0.95 \sum Y_i$ on a 1D-lattice and use a 2-layered Hamiltonian Variational Ansatz. e) We plot the loss and directional loss gradient along the trajectory from the old to new minimum. f) $\boldsymbol{\theta_0}$ is the initial starting point and $\boldsymbol{\theta^*}$ is the true global minimum. The axes are chosen using principle component analysis to project the multi-dimensional space into a 2D-plane using ORQVIZ [36] and the white line is the projection of the optimization trajectory onto this 2D-plane.

landscape. This has been illustrated in Fig 2d).

We are then faced with the question of whether such minima jumps necessitate optimisation across barren plateau landscapes or whether there exist gradient flows between these minima. We provide numerical evidence in Fig. 2(e - f) for a 10-qubit contrived example of a gradient flow from an initialization to a seemingly jumped minima which suggests such gradient flows can exist. Investigating whether such fertile valleys can exist for larger more complex problems is an important direction for future research on the scalability of VQAs.

4 Wider impact of our results

Our results illustrate the potential of warm starts to train VQA landscapes with barren plateaus. While we have framed our results here in the context of an iterative variational scheme for quantum simulation, most of our results here would carry over to other iterative variational approaches. In the manuscript we show how our results carry over to ground state preparation via imaginary time evolution. More generally, one could imagine starting with a circuit for preparing the ground state of an easier Hamiltonian and then iteratively perturbing the Hamiltonian and applying the variational quantum eigensolver between each perturbation. If the perturbations do not pass through a phase transition then such an iterative scheme is plausible and could potentially be characterised in a similar manner to as we have done here. Thus the impact of our results are by no means confined to variational quantum simulation methods but rather offer hope for the field more widely.

References

[1] Carlos Ortiz Marrero, Mária Kieferová, and Nathan Wiebe. "Entanglement-induced barren plateaus". In: *PRX Quantum* 2.4 (2021), p. 040316. DOI: 10.1103/PRXQuantum.2.040316. URL: https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.2.040316.

[2] Kunal Sharma et al. "Trainability of dissipative perceptron-based quantum neural networks". In: *Physical Review Letters* 128.18 (2022), p. 180505. DOI: 10.1103/PhysRevLett.128.180505.

[3] Taylor L Patti et al. "Entanglement devised barren plateau mitigation". In: *Physical Review Research* 3.3 (2021), p. 033090. DOI: 10.1103/PhysRevResearch.3.033090. URL: https://par.nsf.gov/servlets/purl/10328786.

[4] Samson Wang et al. "Noise-induced barren plateaus in variational quantum algorithms". In: *Nature Communications* 12.1 (2021), pp. 1–11. DOI: 10.1038/s41467-021-27045-6. URL: https://doi.org/10.1038/s41467-021-27045-6.

[5] Andrew Arrasmith et al. "Equivalence of quantum barren plateaus to cost concentration and narrow gorges". In: *Quantum Science and Technology* 7.4 (2022), p. 045015. DOI: 10.1088/2058-9565/ac7d06. URL: https://doi.org/10.1088/2058-9565/ac7d06.

[6] Martin Larocca et al. "Diagnosing Barren Plateaus with Tools from Quantum Optimal Control". In: *Quantum* 6 (Sept. 2022), p. 824. ISSN: 2521-327X. DOI: 10.22331/q-2022-09-29-824. URL: https://doi.org/10.22331/q-2022-09-29-824.

[7] Zoë Holmes et al. "Connecting ansatz expressibility to gradient magnitudes and barren plateaus". In: *PRX Quantum* 3 (1 Jan. 2022), p. 010313. DOI: 10.1103/PRXQuantum.3.010313. URL: https://doi.org/10.1103/PRXQuantum.3.010313.

[8] M. Cerezo et al. "Cost function dependent barren plateaus in shallow parametrized quantum circuits". In: *Nature Communications* 12.1 (2021), pp. 1–12. DOI: 10.1038/s41467-021-21728-w. URL: https://doi.org/10.1038/s41467-021-21728-w.

[9] Manuel S Rudolph et al. "Trainability barriers and opportunities in quantum generative modeling". In: *arXiv preprint arXiv:2305.02881* (2023). URL: https://arxiv.org/abs/2305.02881.

[10] Maria Kieferova, Ortiz Marrero Carlos, and Nathan Wiebe. "Quantum Generative Training Using Rényi Divergences". In: *arXiv preprint arXiv:2106.09567* (2021). URL: https://arxiv.org/abs/2106.09567.

[11] Jirawat Tangpanitanon et al. "Expressibility and trainability of parametrized analog quantum systems for machine learning applications". In: *Physical Review Research* 2.4 (2020), p. 043364. DOI: 10.1103/PhysRevResearch.2.043364. URL: https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.2.043364.

[12] Supanut Thanaslip et al. "Subtleties in the trainability of quantum machine learning models". In: *Quantum Machine Intelligence* 5.1 (2023), p. 21. DOI: 10.1007/s42484-023-00103-6. URL: https://link.springer.com/article/10.1007/s42484-023-00103-6.

[13] Zoë Holmes et al. "Barren plateaus preclude learning scramblers". In: *Physical Review Letters* 126.19 (2021), p. 190501. DOI: 10.1103/PhysRevLett.126.190501. URL: https://doi.org/10.1103/PhysRevLett.126.190501.

[14] Enrique Cervero Martín, Kirill Plekhanov, and Michael Lubasch. "Barren plateaus in quantum tensor network optimization". In: *Quantum* 7 (2023), p. 974. DOI: 10.22331/q-2023-04-13-974. URL: https://quantum-journal.org/papers/q-2023-04-13-974/.

[15] Enrico Fontana et al. "The Adjoint Is All You Need: Characterizing Barren Plateaus in Quantum Ansätze". In: *arXiv preprint arXiv:2309.07902* (2023). URL: https://arxiv.org/abs/2309.07902.

[16] Michael Ragone et al. "A Unified Theory of Barren Plateaus for Deep Parametrized Quantum Circuits". In: *arXiv preprint arXiv:2309.09342* (2023). URL: https://arxiv.org/abs/2309.09342.

[17] Supanut Thanasilp et al. "Exponential concentration and untrainability in quantum kernel methods". In: *arXiv preprint arXiv:2208.11060* (2022). URL: https://arxiv.org/abs/2208.11060.

[18] Alistair Letcher, Stefan Woerner, and Christa Zoufal. "From Tight Gradient Bounds for Parameterized Quantum Circuits to the Absence of Barren Plateaus in QGANs". In: *arXiv preprint arXiv:2309.12681* (2023). URL: https://arxiv.org/abs/2309.12681.

[19] Weijie Xiong et al. "On fundamental aspects of quantum extreme learning machines". In: *arXiv preprint arXiv:2312.15124* (2023). DOI: https://doi.org/10.48550/arXiv.2312.15124. URL: https://arxiv.org/abs/2312.15124.

[20] Harper R Grimsley et al. "Adaptive, problem-tailored variational quantum eigensolver mitigates rough parameter landscapes and barren plateaus". In: *npj Quantum Information* 9.1 (2023), p. 19. DOI: 10.1038/s41534-023-00681-0. URL: https://www.nature.com/articles/s41534-023-00681-0.

[21] James Dborin et al. "Matrix product state pre-training for quantum machine learning". In: *Quantum Science and Technology* 7.3 (2022), p. 035014. DOI: 10.1088/2058-9565/ac7073. URL: https://iopscience.iop.org/article/10.1088/2058-9565/ac7073/meta.

[22] Manuel S Rudolph et al. "Synergistic pretraining of parametrized quantum circuits via tensor networks". In: *Nature Communications* 14.1 (2023), p. 8367. URL: https://doi.org/10.1038/s41467-023-43908-6.

[23] Antonio Anna Mele et al. "Avoiding barren plateaus via transferability of smooth solutions in Hamiltonian Variational Ansatz". In: *arXiv preprint arXiv:2206.01982* (2022). URL: https://arxiv.org/abs/2206.01982.

[24] Kaining Zhang et al. "Escaping from the Barren Plateau via Gaussian Initializations in Deep Variational Quantum Circuits". In: *Advances in Neural Information Processing Systems.* 2022. URL: https://openreview.net/forum?id=jXgbJdQ2YIy.

[25] Chae-Yeun Park and Nathan Killoran. "Hamiltonian variational ansatz without barren plateaus". In: *arXiv preprint arXiv:2302.08529* (2023). URL: https://arxiv.org/abs/2302.08529.

[26] Yabo Wang et al. "Trainability Enhancement of Parameterized Quantum Circuits via Reduced-Domain Parameter Initialization". In: *arXiv preprint arXiv:2302.06858* (2023). URL: https://arxiv.org/abs/2302.06858v1.

[27] Chae-Yeun Park, Minhyeok Kang, and Joonsuk Huh. "Hardware-efficient ansatz without barren plateaus in any depth". In: *arXiv preprint arXiv:2403.04844* (2024). URL: https://arxiv.org/abs/2403.04844.

[28] Xiao Shi and Yun Shang. "Avoiding barren plateaus via Gaussian Mixture Model". In: *arXiv preprint arXiv:2402.13501* (2024). URL: https://arxiv.org/abs/2402.13501.

[29] Matthew Otten, Cristian L Cortes, and Stephen K Gray. "Noise-resilient quantum dynamics using symmetry-preserving ansatzes". In: *arXiv preprint arXiv:1910.06284* (2019). URL: https://arxiv.org/abs/1910.06284.

[30] Marcello Benedetti, Mattia Fiorentini, and Michael Lubasch. "Hardware-efficient variational quantum algorithms for time evolution". In: *Physical Review Research* 3.3 (2021), p. 033083. DOI: 10.1103/PhysRevResearch.3.033083. URL: https://doi.org/10.1103/PhysRevResearch.3.033083.

[31] Stefano Barison, Filippo Vicentini, and Giuseppe Carleo. "An efficient quantum algorithm for the time evolution of parameterized circuits". In: *Quantum* 5 (2021), p. 512. DOI: 10.22331/q-2021-07-28-512. URL: https://doi.org/10.22331/q-2021-07-28-512.

[32] Sheng-Hsuan Lin et al. "Real-and imaginary-time evolution with compressed quantum circuits". In: *PRX Quantum* 2.1 (2021), p. 010342. DOI: 10.1103/PRXQuantum.2.010342. URL: https://doi.org/10.1103/PRXQuantum.2.010342.

[33] Noah F. Berthusen et al. "Quantum dynamics simulations beyond the coherence time on noisy intermediate-scale quantum hardware by variational Trotter compression". In: *Phys. Rev. Res.* 4 (2 May 2022), p. 023097. DOI: 10.1103/PhysRevResearch.4.023097. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.4.023097.

[34] Tobias Haug and MS Kim. "Optimal training of variational quantum algorithms without barren plateaus". In: *arXiv preprint arXiv:2104.14543* (2021). URL: https://arxiv.org/abs/2104.14543.

[35] Gian Gentinetta, Friederike Metz, and Giuseppe Carleo. "Overhead-constrained circuit knitting for variational quantum dynamics". In: *arXiv preprint arXiv:2309.07857* (2023). DOI: https://doi.org/10.48550/arXiv.2309.07857. URL: https://arxiv.org/abs/2309.07857.

[36] Manuel S Rudolph et al. "ORQVIZ: visualizing high-dimensional landscapes in variational quantum algorithms". In: *arXiv preprint arXiv:2111.04695* (2021). DOI: https://doi.org/10.48550/arXiv.2111.04695. URL: https://arxiv.org/abs/2111.04695.

Variational quantum simulation: a case study for understanding warm starts

Ricard Puig-i-Valls,[1,*] Marc Drudis,[2,*] Supanut Thanasilp,[1,3] and Zoë Holmes[1]

[1] *Institute of Physics, Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland*
[2] *IBM Quantum, IBM Research – Zurich, 8803 Rüschlikon, Switzerland*
[3] *Chula Intelligent and Complex Systems, Department of Physics,*
Faculty of Science, Chulalongkorn University, Bangkok, Thailand, 10330

(Dated: April 23, 2024)

The barren plateau phenomenon, characterized by loss gradients that vanish exponentially with system size, poses a challenge to scaling variational quantum algorithms. Here we explore the potential of warm starts, whereby one initializes closer to a solution in the hope of enjoying larger loss variances. Focusing on an iterative variational method for learning shorter-depth circuits for quantum real and imaginary time evolution we conduct a case study to elucidate the potential and limitations of warm starts. We start by proving that the iterative variational algorithm will exhibit substantial (at worst vanishing polynomially in system size) gradients in a small region around the initializations at each time-step. Convexity guarantees for these regions are then established, suggesting trainability for polynomial size time-steps. However, our study highlights scenarios where a good minimum shifts outside the region with trainability guarantees. Our analysis leaves open the question whether such minima jumps necessitate optimization across barren plateau landscapes or whether there exist gradient flows, i.e., fertile valleys away from the plateau with substantial gradients, that allow for training.

I. INTRODUCTION

Variational quantum algorithms are a flexible family of quantum algorithms, whereby a problem-specific cost function is efficiently evaluated on a quantum computer, and a classical optimizer aims to minimize this cost by training a parametrized quantum circuit [1–3]. While a popular paradigm the potential of scaling these algorithms to interesting system sizes attracts much debate [4, 5], in part due to the barren plateau phenomenon [6–24]. Barren plateaus are loss landscapes that concentrate exponentially in system size towards their mean value and thus, with high probability, exhibit exponentially small gradients [10, 25]. As quantum losses are computed via measurement shots, on a barren plateau landscape the resources required for training typically scale exponentially, quickly becoming prohibitive.

However, barren plateaus are fundamentally a statement about the landscape on average. They do not preclude the existence of regions of the landscape with significant gradients and indeed, the region immediately around a good minimum, must have such gradients. This has motivated the study of *warm starts* whereby the algorithm is cleverly initialized closer to a minimum. Numerical studies indicate that these methods may be promising [26–29]. In parallel, analytic studies have proven that small angle initializations, whereby the parameterized quantum circuit is initialized in a small region typically around identity, can exhibit non-exponentially vanishing gradients [30–34]. However, a good solution may be far from this region.

Here we will consider a family of variational quantum algorithms that inherently use warm starts and take this as a case study to better understand their potential and limitations. In particular, we study an approach for learning shorter depth circuits for simulating quantum systems by iteratively compressing real or imaginary time Trotter evolution circuits [35–41]. While not necessarily always framed explicitly from this perspective, these approaches effectively use warm starts in virtue of their iterative constructions. At each iteration, the previous solution is used to initialize the parameters to learn a new compressed circuit to implement a slightly longer evolution.

This case study is an ideal playground for studying warm starts because its inbuilt structure allows one to analytically compute bounds on its trainability. We start by proving that as long as the training in one time-step is successful then the algorithm will exhibit substantial (at worst polynomially vanishing with problem size n) gradients in a small (a hypercube of radius $2r$ with $r \in \Omega(\frac{1}{\mathrm{poly}(n)})$) region around the next initialization. We then establish guarantees on the approximate convexity of the gradients in this region and further argue that for polynomially large time-steps the new optimum will typically remain in this convex region. These results are summarised in Fig. 1

However, these positive findings are partially tempered by the observation there is no guarantee that a good minimum remains in this region. Namely, there exist cases where a good minimum jumps from the region with trainability guarantees. Our analysis leaves open the question of whether such minima jumps necessitate optimization across barren plateau landscapes or whether there exist valleys away from the barren plateau that allow for training. Such fertile valleys, i.e. small regions away from the plateau with substantial gradients, that allow for successful training are theoretically possible but to what extent they arise in practise is an open question.

[*] The first two authors contributed equally to this work.

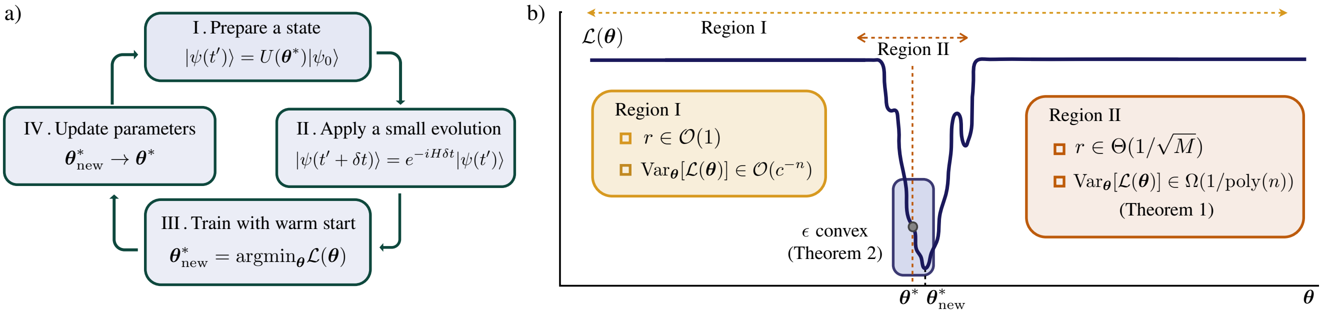

a)
I . Prepare a state
$|\psi(t')\rangle = U(\boldsymbol{\theta}^*)|\psi_0\rangle$
II . Apply a small evolution
$|\psi(t'+\delta t)\rangle = e^{-iH\delta t}|\psi(t')\rangle$
III . Train with warm start
$\boldsymbol{\theta}^*_{\rm new} = \mathrm{argmin}_{\boldsymbol{\theta}}\mathcal{L}(\boldsymbol{\theta})$
IV . Update parameters
$\boldsymbol{\theta}^*_{\rm new} \to \boldsymbol{\theta}^*$
b)
$\mathcal{L}(\boldsymbol{\theta})$
Region I
Region II
Region I
$r \in \mathcal{O}(1)$
$\mathrm{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \mathcal{O}(c^{-n})$
Region II
$r \in \Theta(1/\sqrt{M})$
$\mathrm{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \Omega(1/\mathrm{poly}(n))$
(Theorem 1)
ϵ convex
(Theorem 2)
$\boldsymbol{\theta}^*$ $\boldsymbol{\theta}^*_{\rm new}$
$\boldsymbol{\theta}$

FIG. 1. a) Each iteration of the variational compression scheme consists of four steps. Starting from the top: (i) apply the circuit with the last set of parameters $\boldsymbol{\theta}^*$ to the initial state, (ii) apply $e^{-iH\delta t}$ for a small time-step δt, (iii) train the circuit initialising your parameters around the previous ones, (iv) update the parameters. b) We sketch a typical representation of a loss function $\mathcal{L}(\boldsymbol{\theta})$ with a barren plateau across the full landscape (Region I). In Theorem 1 we prove that in a hypercube of width $2r$ with $r \in \Theta\left(\frac{1}{\sqrt{M}}\right)$ (sketched as Region II) the variance of the loss is only polynomially vanishing in system size n. In Theorem 2 we prove that in a smaller hypercube (highlighted as the blue region) the landscape is approximately convex.

II. PRELIMINARIES

A. Iterative Variational Trotter Compression

We consider simulating the evolution of some initial state $|\psi_0\rangle$ under a Hamiltonian H up to time t. That is, our aim is to implement a quantum circuit that approximates $e^{-iHt}|\psi_0\rangle$. One standard approach [42] to do so is to use the well known Trotter approximation to break the total evolution t into a sequence of N short δt evolutions, with $t = N\delta t$, such that

$$e^{-iHt}|\psi_0\rangle \approx \prod_{k=1}^{N} e^{-iH\delta t}|\psi_0\rangle \;, \tag{1}$$

where the approximation error is in $\mathcal{O}(N\delta t)$. Similarly, one can simulate imaginary time evolution (for ground or thermal state preparation) by setting $\tau = it$:

$$e^{-H\tau}|\psi_0\rangle \approx \prod_{k=1}^{N} e^{-H\delta\tau}|\psi_0\rangle \;, \tag{2}$$

with the error in $\mathcal{O}(N\delta\tau)$. However, these approaches are fundamentally limited by the linear growth of circuit depths with time simulated. This has prompted ongoing efforts to find alternative approaches that avoid this linear growth [35–38, 43–56].

Here we focus on the proposal to use a variational quantum algorithm to compress the depth of the Trotter circuit at each iteration of the algorithm [35–41] as shown in Fig. 1. More concretely, at any iteration of the algorithm, one variationally minimizes the following loss:

$$\mathcal{L}(\boldsymbol{\theta}) = 1 - |\langle\psi_0|U(\boldsymbol{\theta})^\dagger e^{-iH\delta t}U(\boldsymbol{\theta}^*)|\psi_0\rangle|^2 \tag{3}$$

where $U(\boldsymbol{\theta})$ is a parameterized quantum circuit and $\boldsymbol{\theta}^*$ denotes the optimized parameters found at the previous iteration step [35, 37, 39]. At iteration k the loss $\mathcal{L}(\boldsymbol{\theta})$ is optimized using a hybrid quantum classical optimization loop to find the next set of optimal parameters $\boldsymbol{\theta}^*_{\rm new}$. We note that while we focus on a fidelity loss here other cost functions are possible, e.g. in Ref. [36] they considered the real part of the state overlap and in Ref. [37] a local fidelity measure, and a similar analysis could be performed in those cases. It is also possible to use this approach to learn circuits to prepare approximate ground states and thermal states by replacing it with τ in Eq. (3) and with an appropriate choice in initial state $|\psi_0\rangle$ [36].

The success of this protocol depends on a variety of factors including the choice of *ansatz* for the parameterised circuit. Here we focus on a general ansatz of the form

$$U(\boldsymbol{\theta}) = \prod_{i=1}^{M} V_i U_i(\theta_i) \tag{4}$$

where $\{V_i\}_{i=1}^M$ are a set of fixed unitary matrices, $\{U_i(\theta_i) = e^{-i\theta_i\sigma_i}\}_{i=1}^M$ are parameter-dependent rotations, M is the number of parameters in the circuit, and $\{\sigma_i\}_{i=1}^M$ is a set of generators on n qubits such that $\sigma_i = \sigma_i^\dagger$ and $\sigma_i^2 = \mathbb{1}$. In this work, we assume that all parameters θ_j are uncorrelated.

B. Gradient magnitudes and barren plateaus

In recent years there has been concerted effort to understand when quantum losses are trainable or untrainable. Several factors can lead to untrainable losses including the presence of sub-optimal local minima [4, 57, 58], expressivity limitations [59] and abrupt transitions in layerwise learning [60]. However, much of this research has focused on loss gradients.

To train a variational quantum algorithm successfully, the loss landscape must exhibit sufficiently large loss gradients (or more generally, loss differences). Chebyshev's inequality bounds the probability that the cost value deviates from its average as

$$\mathrm{Pr}_{\boldsymbol{\theta}}(|\mathcal{L}(\boldsymbol{\theta}) - \mathbb{E}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})]| \geqslant \delta) \leqslant \frac{\mathrm{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})]}{\delta^2}\,, \tag{5}$$

for some $\delta > 0$ and the variance of the loss defined as

$$\mathrm{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] = \mathbb{E}_{\boldsymbol{\theta}}\left[\mathcal{L}^2(\boldsymbol{\theta})\right] - \left(\mathbb{E}_{\boldsymbol{\theta}}\left[\mathcal{L}(\boldsymbol{\theta})\right]\right)^2\,, \tag{6}$$

where the expectation value is taken over the parameters. Hence if the variance is small then the probability of observing non-negligible loss differences for any randomly chosen parameter setting is negligible.

For a wide class of problems [6–24], one can show that the loss variance vanishes exponentially with problem sizes, i.e. $\mathrm{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \mathcal{O}(c^{-n})$ with $c > 1$. On such *barren plateau* landscapes exponentially precise loss evaluations are required to navigate the towards the global minimum and hence the resources (shots) required for training also scales exponentially. This has prompted the search for architectures where loss variances vanish at worst polynomially with system size, $\mathrm{Var}_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \in \Omega\left(\frac{1}{\mathrm{poly}(n)}\right)$, such that resource requirements may scale polynomially.

III. MAIN RESULTS

In this paper we analyse the trainability of the variational Trotter compression scheme and use this to illustrate the complex interplay between the barren plateau phenomena, local minima and expressivity limitations. We start by presenting an overview of the factors we will consider, and the context provided by prior work, before proceeding to present our main analytic and numerical findings.

A. Overview of analysis

The variance of the loss, Eq. (6), necessarily depends on the parameter region it is computed over. The majority of analyses of quantum loss landscapes have assumed the angles are initialized according to some distribution in the region $[0, 2\pi]$ and hence considered the variance over the entire loss landscape [6–15, 17–23]. However, in practise one is interested in the loss landscape in the region explored during the optimisation process (i.e., in the region around the initialization, the region around the sufficiently 'good' minima and ideally the landscape that connects these regions). An analytic study of these different regions in the general case seems daunting. However, the structure provided by the variational Trotter compression scheme allows us to take steps in this direction.

Prior work has established that small angle initializations, whereby the parameterized quantum circuit is initialized in a small region around identity, provide a means of provably avoiding barren plateaus [30–34]. More concretely, let us define

$$\boldsymbol{\mathcal{V}}(\boldsymbol{\phi}, r) := \{\boldsymbol{\theta}\} \;\text{ such that }\; \theta_i \in [\phi_i - r, \phi_i + r] \;\forall\; i, \tag{7}$$

as the hypercube of parameter space centered around the point $\boldsymbol{\phi}$, and define $\boldsymbol{\mathcal{D}}(\boldsymbol{\phi}, r)$ as a uniform distribution over the hypercube $\boldsymbol{\mathcal{V}}(\boldsymbol{\phi}, r)$. It was shown in Ref. [32], that if the parameters are uniformly sampled in a small hypercube with $r \in \mathcal{O}\left(\frac{1}{\sqrt{L}}\right)$ around $\boldsymbol{\phi} = \mathbf{0}$ for some hardware efficient architecture with L being the number of layers, then the variance $\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}[\mathcal{L}(\boldsymbol{\theta})] \in \Omega\left(\frac{1}{\mathrm{poly}(L)}\right)$ decays only polynomially with the depth of the circuit. Similar conclusions were reached for the Hamiltonian Variational Ansatz in Refs. [31, 33] and for Gaussian initializations in Ref. [30, 34]. Typically in these cases the small angle initialization corresponds to initializing close to identity.

These guarantees can broadly be used to argue that the first iteration of variational Trotter compression scheme will exhibit non-vanishing variances for certain circuits. Moreover, assuming δt is small such that $e^{-iH\delta t}$ is close to identity, and assuming that the ansatz is sufficient expressive to be able to capture a good approximation of $e^{-iH\delta t}$, it is reasonable to expect that the good approximate solution circuit is contained within the region $\boldsymbol{\mathcal{V}}\left(\mathbf{0}, \frac{1}{\sqrt{M}}\right)$ that enjoys polynomial loss variances. However, at later time-steps, when $U(\boldsymbol{\theta})$ is far from identity, the guarantees provided for these small angle initializations are of debatable relevance.

Here we address the task of providing guarantees for all iterations of the algorithm for a very general family of parameterized quantum circuits. Our guarantees are based on the observation that assuming the previous step was sufficiently well optimised, and the time-step δt is small enough, then one can initialize close enough to the new global minimum (or, more modestly, a good new minimum) such that the landscape exhibits substantial gradients as sketched in Fig. 1b). In Section III B we use this observation to derive such analytical variance lower bounds. We note that Ref. [40] provides an approximate lower bound on the variance in the loss for an iterative compression scheme; however, to do so it makes a number of approximations and in effect assumes the convexity of the problem from the outset. We go beyond this by providing exact bounds without prior assumptions.

Non-vanishing gradients in the region around the initialisation are a necessary condition to have any hope of successfully training a variational quantum algorithm but they are far from sufficient. Of particular importance is the potential to become trapped in spurious local minima. One way to provide guarantees against this concern is to prove that this region is convex. We tackle this issue in Section III C by proving convexity guarantees in the region around the initialization provided by the previous iteration.

We then introduce the notion of the adiabatic minima as the minima that would be reached by increasing δt

infinitely slowly and minimizing $\mathcal{L}(\boldsymbol{\theta})$ by gradient descent with a very small learning rate in Section III D. We argue that as long as the time-step is δt is not too large (i.e. decreases polynomially with the number of parameters M) we can ensure that an adiabatic minima is within the convex region with non-vanishing gradients, and thus it should be possible to train to the adiabatic minimum.

Finally, in Section III E we explore the limitations of our analytic bounds. Firstly, we highlight that our analysis can not provide convergence guarantees to a good minimum because *minima jumps* are possible. Namely, from one time-step to the other, the adiabatic minimum can become a relatively poor local minimum and a superior minimum can emerge elsewhere in the landscape. We are then faced with the question of whether such minima jumps necessitate optimisation across barren plateau landscapes or whether there exist gradient flows between these minima. We provide numerical evidence for a 10-qubit contrived example of a gradient flow from an initialization to a seemingly jumped minima which suggests such gradient flows can exist.

B. Lower-bound on the variance

The variance of the loss function at any iteration around the parameters $\boldsymbol{\theta}^*$ obtained for the previous iteration will depend on the length of the time-step δt as well as the volume of the region of the parameter space explored. Here we study the variance of the loss in a uniformly sampled hypercube of sides $2r$ around $\boldsymbol{\theta}^*$ as defined in Eq. (7). As proven in Appendix B, we obtain the following bound.

Theorem 1 (Lower-bound on the loss variance, Informal)**.** *Consider the general ansatz in Eq. (4) and assume that in the first iteration the system is prepared in a product initial state $\rho_0 = \bigotimes_{j=1}^n \rho_j$ with ρ_j and let us choose σ_1 such that $\mathrm{Tr}[\rho_0\sigma_1\rho_0\sigma_1] = 0$. Given that the Trotter time-step is bounded as*

$$\delta t \in \mathcal{O}\left(\frac{1}{\lambda_{\max}}\right) \tag{8}$$

where $\lambda_{\max}$ is the largest eigenvalue of H and we consider uniformly sampling parameters in a hypercube of width $2r$ around the solution from the previous iteration $\boldsymbol{\theta}^*$, i.e. $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$, such that

$$r \in \Theta\left(\frac{1}{\sqrt{M}}\right) . \tag{9}$$

Then the variance at any iteration of the algorithm is lower bounded as

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] \in \Omega\left(\frac{1}{M}\right) . \tag{10}$$

Thus, for $M \in \mathcal{O}(\mathrm{poly}(n))$ we have

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] \in \Omega\left(\frac{1}{\mathrm{poly}(n)}\right) . \tag{11}$$

In Appendix E we present a version of Theorem 1 for the imaginary time evolution.

Theorem 1 establishes that within a small, but non-exponentially vanishing ($r \propto 1/\sqrt{M}$), region around the previous optimal solution, the loss landscape will exhibit non-exponentially vanishing gradients so long as $\delta t \in \mathcal{O}(1/\lambda_{\max})$. The constraint on the Trotter time-step is to ensure that a state corresponding to a previous solution has a large overlap with a new target state. If the Trotter step is too large, then the initialization no longer contains enough information about the target state and it is equivalent to initializing on the barren plateau region. The $\delta t \in \mathcal{O}(1/\lambda_{\max})$ scaling comes from a loose bound on the overlap between the old optimised state and the new target state and thus a larger δt is likely viable in practise.

On another related topic, our bound is presented here for simulating the evolution of an initially product state. This assumption is made for ease of presentation. However, as highlighted in the appendices, this assumption is not strictly necessary. Rather one just needs to ensure that a gate in the first layer has a non-trivial effect on the loss.

It is important to stress that Theorem 1 provides a sufficient, not a necessary, condition for observing polynomially vanishing gradients. For a necessary condition one would need to derive an upper bound as a function of r and δt. In general, this seems challenging and is likely to be highly ansatz dependent [61]. Instead we address this question numerically.

In Fig. 2 we study the landscape of $\mathcal{L}(\boldsymbol{\theta})$ for an initial time-step as a function of the width of the hypercube, $2r$. For concreteness, we consider a hardware efficient ansatz with n layers and uniformly sampled parameters within the hypercube. The variance over the full landscape ($r = \pi$) vanishes exponentially in n. However, as r is decreased the variance increases with r and ceases to decay exponentially in n. When r is very small the variance again begins to decrease. This is because for sufficiently small r we are computing the variance over a small region of the loss landscape at the base of the narrow gorge. This account is confirmed by the average behaviour of $\mathcal{L}(\boldsymbol{\theta})$ also shown in Fig. 2a). In particular, when the variance peaks, we have an infidelity of approximately 0.7 for each system size, which indicates that the peak of the variance is a good measure of the width of our gorge.

In Fig. 2 b) and c) we plot the r value for which the variance peaks and the maximum value of the variance as function of the number of parameters in the ansatz M. Both quantities decay polynomially in M. In particular, we find that $r_{\max}$ scales as $\frac{1}{\sqrt{M}}$ implying that the width of the gorge decreases with a $\frac{1}{\sqrt{M}}$ scaling. This is consistent with our theoretical lower bound, Theorem 1, which also suggests that to ensure at worst poly vanishing gradients its necessary to consider a region of width $\frac{1}{\sqrt{M}}$ around the minimum.

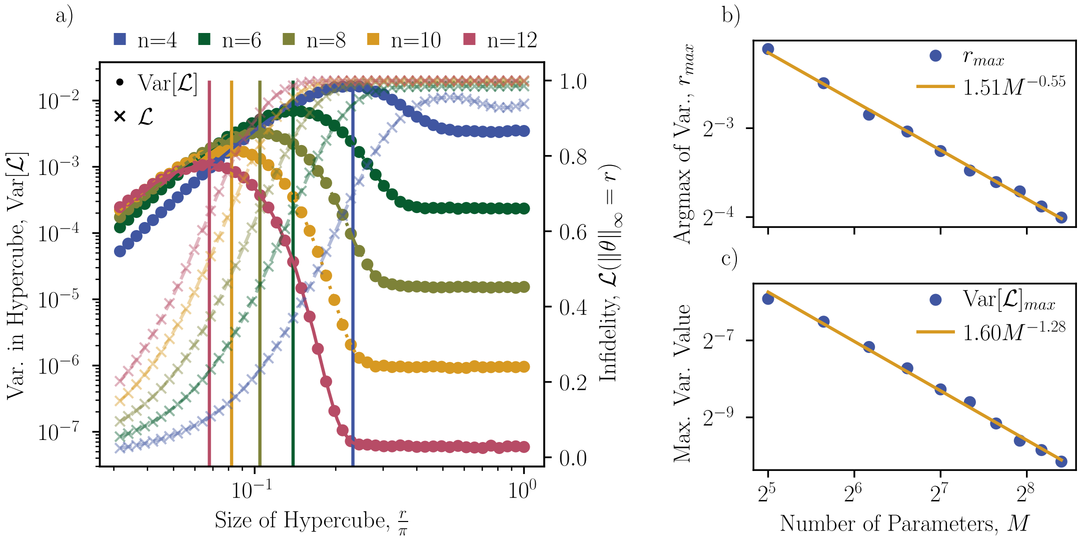


FIG. 2. **Variance of landscape and width of narrow gorge.** Here we study the landscape of $\mathcal{L}(\boldsymbol{\theta})$, for the first time-step of the variational Trotter compression algorithm, for different system sizes n as a function of the width of the hypercube r. We consider a hardware efficient ansatz with n layers and random initial parameters within the hypercube. a) We plot $\mathcal{L}(\boldsymbol{\theta})$ and its variance $\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}[\mathcal{L}(\boldsymbol{\theta})]$ as function of r/π. Since the shape of the landscape depends on the direction of the parameter update, to plot $\mathcal{L}(\boldsymbol{\theta})$ we have taken the average over 500 different directions. For $\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}[\mathcal{L}(\boldsymbol{\theta})]$, we keep track of its maximum value (marked with a vertical line) for each system size. b) The value $r_{\max}$ for which the variance peaks as function of the number of parameters in the ansatz. c) Maximum value of the variance for different system sizes. While the results shown here are for the first iteration of the variational compression scheme very similar results are observed at later iterations (in line with Theorem 1).

C. Convexity region around the starting point

Substantial gradients are a necessary condition but not sufficient condition for trainability. If the substantial gradients are attributable to poor local minima then finding a good solution is likely to be highly challenging. However, if as well as having substantial gradients, we can prove that the landscape is convex, or approximately convex, then training to a minimum looks promising. In this section, we present a theorem which shows that the region around the starting parameters is approximately convex. As expected, our condition depends both on the width of the hypercube region considered and the time-step δt taken.

A function is convex over a parameter range if its second order partial derivatives are all non-negative in that parameter range. In practise, a more convenient means of diagnosing convexity is to study the Hessian, $\nabla^2_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})]$, of a function. If the Hessian is positive semi definite, i.e. $\nabla^2_{\boldsymbol{\theta}}[\mathcal{L}(\boldsymbol{\theta})] \geqslant 0$, in a given parameter region then the function is convex in that region. We will introduce a notion of approximate convexity by relaxing this constraint and saying that a landscape is ϵ convex if the following condition holds:

Definition 1 (ϵ-convexity)**.** *A loss is ϵ-convex in the region $\boldsymbol{\theta} \in \boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$ if*

$$\left[\nabla^2_{\boldsymbol{\theta}}\mathcal{L}(\boldsymbol{\theta})\right]_{\min} \geqslant -|\epsilon| \tag{12}$$

for all $\boldsymbol{\theta} \in \boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$. Here $\nabla^2_{\boldsymbol{\theta}}\mathcal{L}(\boldsymbol{\theta})$ denotes the Hessian of $\mathcal{L}(\boldsymbol{\theta})$ and we denote $[A]_{\min}$ as the smallest eigenvalue of the matrix A.

If a loss is ϵ-convex the loss is convex up to ϵ small deviations, as sketched in Fig. 1b), and argued more formally in Appendix A 3. This notion is particularly important in a quantum context where the loss is only ever measured with a finite number of shots making it hard to tell apart ϵ negative curvatures from ϵ positive ones. Thus in practise the relevant ϵ will be determined by the shot noise floor.

Equipped with this definition we now show that a polynomially sized region around the starting point of the previous iteration is approximately convex.

Theorem 2 (Approximate convexity of the landscape, Informal)**.** *For a time-step of size*

$$\delta t \in \mathcal{O}\left(\frac{\mu_{\min} + 2|\epsilon|}{M\lambda_{\max}}\right) , \tag{13}$$

the loss landscape is ϵ-convex in a hypercube of width $2r_c$ around a previous optimum $\boldsymbol{\theta}^*$ i.e., $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$ such that

$$r_c \in \Omega\left(\frac{\mu_{\min} + 2|\epsilon|}{16M^2} - \frac{\lambda_{\max}\delta t}{M}\right) , \tag{14}$$

where $\mu_{\min}$ is the minimal eigenvalue of the Fisher information matrix associated with the loss at $\boldsymbol{\theta}^*$.

In Appendix E we show that an analogous convexity guarantee can be proven for imaginary time evolution.

Theorem 2 tells us that it is always possible to pick a polynomially scaling $\delta t, r_c$ such that the landscape of $\mathcal{L}(\boldsymbol{\theta})$ with respect to the parameters is approximately convex. The constraints on δt and r_c for convexity are pretty stringent in practice. However, convexity is also a lot to demand of a loss landscape. Nonetheless, it is nice to see that approximate convexity can be ensured at 'only' a polynomially scaling cost.

D. Adiabatic minimum

So far we have identified two constraints on our parameters that push in the direction of trainability guarantees. Specifically, we have established a region in our landscape with substantial gradients and approximate convexity. The final condition required for convergence guarantees is to ensure our target circuit, i.e., a good minimum, lies within this region.

To address this point, let us start by introducing the notion of the *adiabatic minima*. Intuitively, these are the minima that would be reached by increasing δt infinitely slowly and minimizing $\mathcal{L}(\boldsymbol{\theta})$ by gradient descent with a very small learning rate. By analogy, one can imagine dropping a marble in the initial minima and then slowly modifying the landscape by infinitesimally increasing δt. The position of the marble would correspond to our adiabatic minima and, in practice, it is where we expect our algorithm to converge for sufficiently small δt. In Fig. 3 a) we plot a cut through the cost landscape around the old minimum $\boldsymbol{\theta}^*$ as a function of δt. We can see that the minimum smoothly moves rightwards and increases with increasing δt. More formally, we define the adiabatic minima as follows.

Definition 2 (Adiabatic Minimum)**.** *For any time δt in the range $[0, T]$, a function*[1] *corresponding to the evolution of the adiabatic minima for some initial minimum $\boldsymbol{\theta}^*$, is a continuous function $\boldsymbol{\theta}_A(\delta t) \in C^\infty(\mathbb{R}, \mathbb{R}^m)$ such that $\boldsymbol{\theta}_A(0) = \boldsymbol{\theta}^*$ and $\nabla_{\boldsymbol{\theta}} \mathcal{L}(\boldsymbol{\theta}_A(\delta t), \delta t) = \mathbf{0}$. The adiabatic minimum at time δt is $\boldsymbol{\theta}_A(\delta t)$.*

One can ensure that the iterative variational compression scheme will converge to some minimum if the time-step is small enough that an adiabatic minimum is inside of the convex region with non-vanishing gradients. One can question how good this minimum will be but we will set aside this question for the moment. Thus our next step will be to assess how small the time-step needs to be picked in order to guarantee this. In the following theorem we formalize this concept by bounding the δt required to ensure an adiabatic minimum is in the substantial gradient region and in the convex region.

Theorem 3 (Adiabatic minimum is within provably 'nice' training region, Informal)**.** *If the time-step δt is chosen such that*

$$\delta t \in \mathcal{O}\left(\frac{\beta_A}{M\lambda_{\max}}\right) , \tag{15}$$

then the adiabatic minimum $\boldsymbol{\theta}_A(\delta t)$ is guaranteed to be within the non-exponentially-vanishing gradient region (as per Theorem 1), and additionally, if δt is chosen such that

$$\delta t \in \mathcal{O}\left(\frac{\beta_A(\mu_{\min} + 2|\epsilon|)}{M^{5/2}\lambda_{\max}}\right) , \tag{16}$$

then the adiabatic minimum $\boldsymbol{\theta}_A(\delta t)$ is guaranteed to be within the ϵ-convex region (as per Theorem 2) where

$$\beta_A := \frac{\dot{\boldsymbol{\theta}}_A^T(\delta t)\left(\nabla^2_{\boldsymbol{\theta}}\mathcal{L}(\boldsymbol{\theta})\big|_{\boldsymbol{\theta}=\boldsymbol{\theta}_A(\delta t)}\right)\dot{\boldsymbol{\theta}}_A(\delta t)}{\|\dot{\boldsymbol{\theta}}_A(\delta t)\|_2^2} \tag{17}$$

corresponds to the second derivative of the loss in the direction in which the adiabatic minimum moves.

Theorem 3 tells us that it suffices to consider a time-step that scales as $\delta t \in \Omega\left(\frac{1}{M}\right)$ to ensure that the adiabatic minimum falls in the region with substantial gradients, or more stringently to take $\delta t \in \Omega\left(\frac{1}{\text{poly}(M)}\right)$ to ensure that the adiabatic minimum falls within the $|\epsilon|$-convex region. As in general $M \sim \text{poly}(n)$ it follows that if δt is decreased polynomially with problem size, and the learning rate is chosen appropriately, it should be possible to train to the new adiabatic minimum.

We stress that this interpretation of Theorem 3 is only possible assuming that β_A is not exponentially vanishing. This is a reasonable assumption as $\beta_A \to 0$ corresponds to the curvature of the loss at the minimum being flat in the direction in which the adiabatic minimum moves. While this is conceivably possible it is unlikely in practise (as is supported by our numerics in Fig. 3 and Fig. 4). Moreover, the β_A dependence of Theorem 3 is a genuine feature that affects trainability, rather than a relic of our proof techniques. Namely, if the landscape is very flat in the direction of the new minimum then indeed the adiabatic minimum can move significant distances at short times. More poetically, one might visualise this case as a *barren gorge*. That is, a sub-region of the landscape within the substantial gradient region that nonetheless has vanishing gradients. Such features are possible but perhaps unlikely unless the ansatz is highly degenerate.

Another caveat is that Theorem 3 only holds in the case that there exists a well-defined adiabatic minimum function $\boldsymbol{\theta}_A(\delta t)$ in the time interval of interest. This is not always guaranteed to be the case because a minimum can vanish by evolving into a slope as δt increases. If this

[1] We note that it is in fact possible for a single initial minima to have multiple corresponding adiabatic minima functions if there are multiple directions with zero gradients.

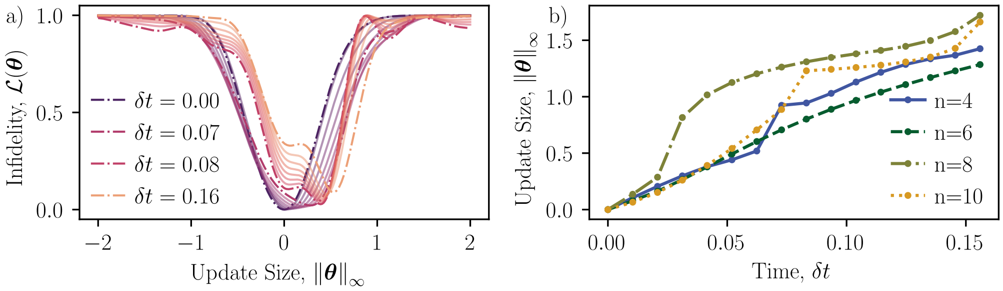


FIG. 3. **Routine evolution of the adiabatic minimum**. Here we study the landscape of $\mathcal{L}(\boldsymbol{\theta})$ as we increase the time-step δt. We study a 10 qubit Hamiltonian with nearest-neighbour interactions on a 1D lattice with $H = \sum X_i Z_{i+1} - 0.95 \sum Y_i$ where X_i, Y_i and Z_i are X-Pauli, Y-Pauli and Z-Pauli operators on the qubit i. a) We plot our landscape for different δt. The cuts in our high dimensional $\mathcal{L}(\boldsymbol{\theta})$ space contain both the initial parameters $\boldsymbol{\theta} = \mathbf{0}$ and the adiabatic minimum $\boldsymbol{\theta}_A(\delta t)$ at δt. b) We plot the size of our parameter update $\|\boldsymbol{\theta}\|_\infty$, i.e. the distance along the cuts between the old minimum and the new minimum, as a function of the time-step for different system sizes.

occurs then the continuity condition in our definition of the adiabatic minima function fails. Nonetheless, this is not a situation that necessarily causes trainability problems (if the minimum turns into a slope then training is possible down that slope), rather it is a situation that makes finding analytic trainability guarantees more challenging. For a more detailed discussion of this caveat and a proof of Theorem 3 see Appendix D.

Relatedly, it is worth mentioning that while Theorem 3 allows for polynomially shrinking step sizes in practise these step sizes are rather small. In particular, for the small problem sizes studied already in the literature practitioners have typically used larger step sizes than those that we have managed to derive guarantees for here. In parallel, we can see from our numerical implementations in Fig. 3 that training would seem viable for larger δt than allowed by our bounds. It is arguably an open question to what extent this can be attributed to looseness of our bounds or the small problem sizes that can be simulated classically. One thing to note in this regard is that optimisation is often much more successful in practise than can be analytically guaranteed or even explained. As such, in practise, larger δt may well be viable. This is specially relevant if one considers using adaptive approaches where δt is modified at each step until a given precision threshold is reached. While heuristic, this method in the worst case enjoys the mathematical guarantees proven here, while in the best case allows for larger time-steps (and so reduces the average number of time-steps required in total).

E. Minima jumps and fertile valleys

A final limitation of our analysis is that the adiabatic minimum (or indeed any minimum within the region with gradient guarantees) need not be a good minimum. The adiabatic minimum is the minimum that evolves away from the old minimum after the application of a time-step δt. However, it is possible that a different better minimum emerges in a different region of the landscape [60]. That is, it is possible for the best minimum (or, more modestly, simply a significantly better minimum) to *jump* from the initialization region to another region of the parameter landscape. As we only have lower bounds on the variance of the loss and convexity guarantees in the region around the initialization if the minimum jumps then we have no trainability guarantees to these superior minima. Moreover, if the full landscape has a barren plateau, which will be the case for most deep ansätze [20, 21], it may be very hard to train to this new minimum.

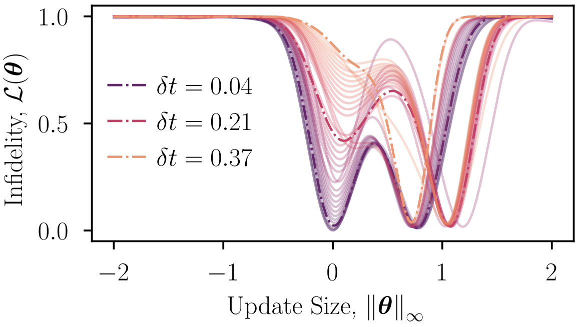


FIG. 4. **Minimum jump.** Here we show a 1D-cut of the landscape $\mathcal{L}(\boldsymbol{\theta})$ as we increase the time-step δt. The cut includes the initial parameters-with update $\delta t = 0$ and $||\boldsymbol{\theta}||_\infty = 0$. We choose a 10 qubit Ising Hamiltonian $H = \sum X_i X_{i+1} - 0.95 \sum Y_i$ on a 1D-lattice. We use a 2-layered Hamiltonian Variational Ansatz.

In Fig. 4 we suggest that such apparent *minimum jumps* can indeed occur. In particular we show a 1D cut of the landscape $\mathcal{L}(\boldsymbol{\theta})$ for different time-steps δt. The 1D cut includes both the ‘old minimum’ at time $\delta t = 0$ and a new minimum that emerges for larger δt. Even after a short time-step $\delta t = 0.04$ the best minimum has jumped

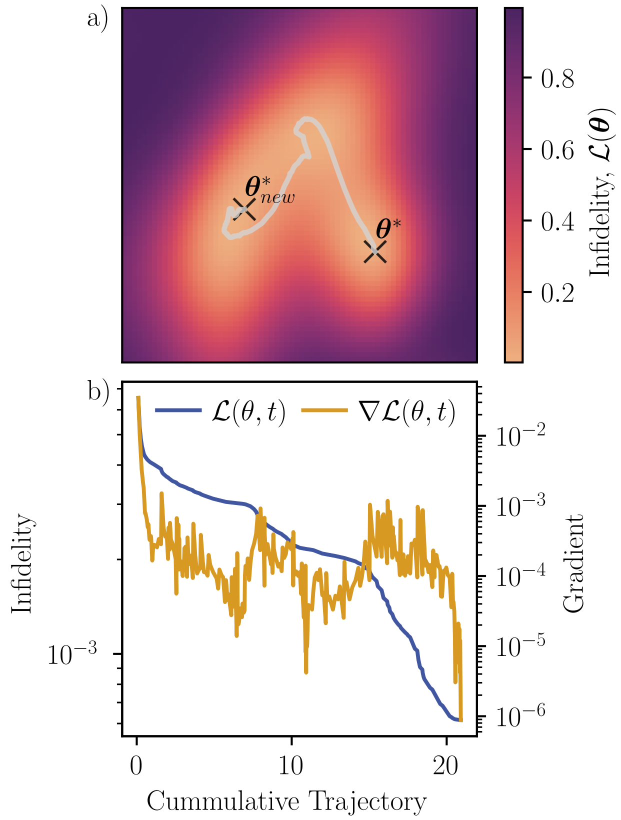


FIG. 5. **Fertile valley.** a) Here we show a 2D plot of the loss landscape at $\delta t = 0.04$ for a 10 qubit Ising Hamiltonian $H = \sum X_i X_{i+1} - 0.95 \sum Y_i$ on a 1D-lattice and use a 2-layered Hamiltonian Variational Ansatz. $\boldsymbol{\theta_0}$ is the initial starting point and $\boldsymbol{\theta^*}$ is the true global minimum. The axes are chosen using principle component analysis to project the multi-dimensional space into a 2D-plane using ORQVIZ [62] and the white line is the projection of the optimization trajectory onto this 2D-plane. b) We plot the loss and directional loss gradient along the trajectory from the old to new minimum.

by a distance $||\boldsymbol{\theta}||_\infty \approx 0.8$. At this short time, the new minimum is only very slightly superior to the adiabatic minimum. However, at longer times the new minimum becomes substantially better.

When a minimum jumps our theoretic guarantees developed in this manuscript lose most of their value. However, this does not mean that it is not possible to train (even in the case where the overall landscape exhibits a barren plateau). For training the 'only thing' we need is a gradient flow, i.e., a path with substantial gradients, from the initialization to the new minimum. Such fertile valleys with nice gradients can theoretically exist on a barren plateau landscape but to what extent they occur in practise is currently unknown.

In Fig. 5 we provide numerical evidence for a toy example of such a case. Specifically, we show a 2D cross-section of the landscape containing both an initialisation minimum and an apparently jumped minimum (marked by black crosses). We managed to successfully train from this initial minimum to the new minimum using the BFGS algorithm. This algorithm is a non-stochastic algorithm and so this indicates that there is indeed a trajectory between the two minima. As shown here in b) the gradients along this trajectory are of the order 10^{-3}, in contrast to of the order of 10^{-6} on average over the landscape for a 10 qubit problem as shown in Fig. 2. Thus, while a significant shot budget ($\sim 10^6$ shots) is likely needed for training it would seem that it is possible to train between these two minima without crossing into the most barren parts of the landscape.

The discussion in this section is necessarily heuristic. In our numerical investigations we found some minima jumps that we could train between (indicating a fertile valley) and other minima jumps where we could not. In the latter case there may or may not be fertile valleys. In both cases this is evidence for toy problems and at a small problem sizes (10 qubits). To what extent these phenomena occur at larger problem sizes, for more interesting problems and for relevant time-step sizes, remains entirely open.

IV. DISCUSSION

Thanks to significant progress in recent years, the barren plateau phenomenon, defined as an average statement for an entire loss landscape, is by now technically well understood [20, 21]. However, prior analyses are consistent with different accounts of the behaviour of the loss landscape in the subregions most important for optimization. In this work we have taken steps to address these open questions by investigating a popular iterative variational circuit compression scheme [35–41]. The iterative nature of this algorithm ensures that variational problem is repeatedly warm started at each iteration of the variational scheme.

Theorem 1 establishes that for short enough time-steps the loss variance is guaranteed to decrease at worst polynomially in the number of parameters M in a hypercube with a width that scales as $1/\sqrt{M}$ around the new initialization. Theorem 2 strengthens this result by arguing that in a region $\sim 1/M^2$ around the initialization the landscape will be approximately convex. Finally, we sew together these results with a bound on the distance the adiabatic minimum (Definition 2) can move after applying a Trotter step of length δt. Thus in Theorem 3 we establish that as long as the time-step is decreased polynomially with the number of trainable parameters in the ansatz the adiabatic minimum remains in the approximately convex region with substantial gradients. Hence we show that by decreasing the time-step appropriately one should be able to train to a new minimum.

Our analysis leaves room for further research opportunities. For one, the analytic bounds provided here are lower bounds. We do not here provide upper bounds.

Thus our analysis leaves open the question of whether the region exhibiting polynomial gradients strictly decreases as $1/\sqrt{M}$ or whether potentially a larger region exhibits substantial gradients. Our numerical implementations (Fig. 2) suggest that for the problems we have looked at this $1/\sqrt{M}$ is reasonable. However, analytic upper bounds to verify this would be more satisfying.

Moreover, whether these bounds are to be viewed positively or negatively remains open. While in 'complexity-theory-land' polynomial guarantees are typically satisfactory, in practise polynomially vanishing gradients, in polynomially shrinking regions, with polynomially shrinking step sizes may not be that appealing. In particular, the δt values that enjoy guarantees via Theorem 3 are typically smaller than those used currently by practitioners for the small problem sizes accessible currently. To what extent these bounds can be tightened versus to what extent they indicate a fundamental limitation remains to be seen. Indeed, there is always the possibility that heuristically the optimization turns out to be more effective than analytic guarantees would suggest (as is typically the case for optimizing classical machine learning models).

Here we have pushed our analysis beyond a conventional average case analyses for the full loss landscape. However, our analysis is still fundamentally an average case analysis within a hypercube around an initialization. The limitations of this are highlighted by our inability to analytically describe the minimum jumps and fertile valleys that we numerically observe in Fig. 4 and Fig. 5. To analytically study such phenomena new theoretical tools will need to be developed to analyse quantum landscapes.

We remark that recent work has highlighted a strong link between provable absence of barren plateaus and the classical simulability and surrogatability of the hybrid optimisation loop of a variational quantum algorithm [5]. The lower bounds obtained here are consistent with these claims. In particular, for classically simulable initial states one could perform early iterations fully classically and then later iterations by collecting data from quantum computer and then training a classical surrogate of the landscape. We leave a discussion of the relative merits of this approach to future work.

Finally, we have framed our results here in the context of an iterative variational scheme for quantum simulation; however, most of our results here would carry over to other iterative variational approaches. For example, one could imagine starting with a circuit for preparing the ground state of an easier Hamiltonian and then iteratively perturbing the Hamiltonian and applying the variational quantum eigensolver between each perturbation. If the perturbations do not pass through a phase transition then such an iterative scheme is plausible and could potentially be characterised in a similar manner to as we have done here.

V. ACKNOWLEDGMENTS

We thank Stefan Woerner, Christa Zoufal and Matthis Lehmkuehler for insightful conversations. We further thank Manuel Rudolph for helpful comments on a draft and his ORQVIZ wizardry. R.P. and M.D. acknowledge the support of the SNF Quantum Flagship Replacement Scheme (grant No. 215933). S.T. and Z.H. acknowledge support from the Sandoz Family Foundation-Monique de Meuron program for Academic Promotion.

[1] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles, Variational quantum algorithms, Nature Reviews Physics **3**, 625–644 (2021).

[2] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke, *et al.*, Noisy intermediate-scale quantum algorithms, Reviews of Modern Physics **94**, 015004 (2022).

[3] S. Endo, Z. Cai, S. C. Benjamin, and X. Yuan, Hybrid quantum-classical algorithms and quantum error mitigation, Journal of the Physical Society of Japan **90**, 032001 (2021).

[4] E. R. Anschuetz and B. T. Kiani, Beyond barren plateaus: Quantum variational algorithms are swamped with traps, Nature Communications **13**, 7760 (2022).

[5] M. Cerezo, M. Larocca, D. García-Martín, N. L. Diaz, P. Braccia, E. Fontana, M. S. Rudolph, P. Bermejo, A. Ijaz, S. Thanasilp, *et al.*, Does provable absence of barren plateaus imply classical simulability? or, why we need to rethink variational quantum computing, arXiv preprint arXiv:2312.09121 (2023).

[6] C. O. Marrero, M. Kieferová, and N. Wiebe, Entanglement-induced barren plateaus, PRX Quantum **2**, 040316 (2021).

[7] K. Sharma, M. Cerezo, L. Cincio, and P. J. Coles, Trainability of dissipative perceptron-based quantum neural networks, Physical Review Letters **128**, 180505 (2022).

[8] T. L. Patti, K. Najafi, X. Gao, and S. F. Yelin, Entanglement devised barren plateau mitigation, Physical Review Research **3**, 033090 (2021).

[9] S. Wang, E. Fontana, M. Cerezo, K. Sharma, A. Sone, L. Cincio, and P. J. Coles, Noise-induced barren plateaus in variational quantum algorithms, Nature Communications **12**, 1 (2021).

[10] A. Arrasmith, Z. Holmes, M. Cerezo, and P. J. Coles, Equivalence of quantum barren plateaus to cost concentration and narrow gorges, Quantum Science and Technology **7**, 045015 (2022).

[11] M. Larocca, P. Czarnik, K. Sharma, G. Muraleedharan, P. J. Coles, and M. Cerezo, Diagnosing Barren Plateaus with Tools from Quantum Optimal Control, Quantum **6**, 824 (2022).

[12] Z. Holmes, K. Sharma, M. Cerezo, and P. J. Coles, Connecting ansatz expressibility to gradient magnitudes and

barren plateaus, PRX Quantum **3**, 010313 (2022).

[13] M. Cerezo, A. Sone, T. Volkoff, L. Cincio, and P. J. Coles, Cost function dependent barren plateaus in shallow parametrized quantum circuits, Nature Communications **12**, 1 (2021).

[14] M. S. Rudolph, S. Lerch, S. Thanasilp, O. Kiss, S. Vallecorsa, M. Grossi, and Z. Holmes, Trainability barriers and opportunities in quantum generative modeling, arXiv preprint arXiv:2305.02881 (2023).

[15] M. Kieferova, O. M. Carlos, and N. Wiebe, Quantum generative training using rényi divergences, arXiv preprint arXiv:2106.09567 (2021).

[16] J. Tangpanitanon, S. Thanasilp, N. Dangniam, M.-A. Lemonde, and D. G. Angelakis, Expressibility and trainability of parametrized analog quantum systems for machine learning applications, Physical Review Research **2**, 043364 (2020).

[17] S. Thanaslip, S. Wang, N. A. Nghiem, P. J. Coles, and M. Cerezo, Subtleties in the trainability of quantum machine learning models, Quantum Machine Intelligence **5**, 21 (2023).

[18] Z. Holmes, A. Arrasmith, B. Yan, P. J. Coles, A. Albrecht, and A. T. Sornborger, Barren plateaus preclude learning scramblers, Physical Review Letters **126**, 190501 (2021).

[19] E. C. Martín, K. Plekhanov, and M. Lubasch, Barren plateaus in quantum tensor network optimization, Quantum **7**, 974 (2023).

[20] E. Fontana, D. Herman, S. Chakrabarti, N. Kumar, R. Yalovetzky, J. Heredge, S. Hari Sureshbabu, and M. Pistoia, The adjoint is all you need: Characterizing barren plateaus in quantum ansätze, arXiv preprint arXiv:2309.07902 (2023).

[21] M. Ragone, B. N. Bakalov, F. Sauvage, A. F. Kemper, C. O. Marrero, M. Larocca, and M. Cerezo, A unified theory of barren plateaus for deep parametrized quantum circuits, arXiv preprint arXiv:2309.09342 (2023).

[22] S. Thanasilp, S. Wang, M. Cerezo, and Z. Holmes, Exponential concentration and untrainability in quantum kernel methods, arXiv preprint arXiv:2208.11060 (2022).

[23] A. Letcher, S. Woerner, and C. Zoufal, From tight gradient bounds for parameterized quantum circuits to the absence of barren plateaus in qgans, arXiv preprint arXiv:2309.12681 (2023).

[24] W. Xiong, G. Facelli, M. Sahebi, O. Agnel, T. Chotibut, S. Thanasilp, and Z. Holmes, On fundamental aspects of quantum extreme learning machines, arXiv preprint arXiv:2312.15124 https://doi.org/10.48550/arXiv.2312.15124 (2023).

[25] J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven, Barren plateaus in quantum neural network training landscapes, Nature Communications **9**, 1 (2018).

[26] H. R. Grimsley, N. J. Mayhall, G. S. Barron, E. Barnes, and S. E. Economou, Adaptive, problem-tailored variational quantum eigensolver mitigates rough parameter landscapes and barren plateaus, npj Quantum Information **9**, 19 (2023).

[27] J. Dborin, F. Barratt, V. Wimalaweera, L. Wright, and A. G. Green, Matrix product state pre-training for quantum machine learning, Quantum Science and Technology **7**, 035014 (2022).

[28] M. S. Rudolph, J. Miller, D. Motlagh, J. Chen, A. Acharya, and A. Perdomo-Ortiz, Synergistic pretraining of parametrized quantum circuits via tensor networks, Nature Communications **14**, 8367 (2023).

[29] A. A. Mele, G. B. Mbeng, G. E. Santoro, M. Collura, and P. Torta, Avoiding barren plateaus via transferability of smooth solutions in Hamiltonian variational ansatz, arXiv preprint arXiv:2206.01982 (2022).

[30] K. Zhang, L. Liu, M.-H. Hsieh, and D. Tao, Escaping from the barren plateau via gaussian initializations in deep variational quantum circuits, in *Advances in Neural Information Processing Systems* (2022).

[31] C.-Y. Park and N. Killoran, Hamiltonian variational ansatz without barren plateaus, arXiv preprint arXiv:2302.08529 (2023).

[32] Y. Wang, B. Qi, C. Ferrie, and D. Dong, Trainability enhancement of parameterized quantum circuits via reduced-domain parameter initialization, arXiv preprint arXiv:2302.06858 (2023).

[33] C.-Y. Park, M. Kang, and J. Huh, Hardware-efficient ansatz without barren plateaus in any depth, arXiv preprint arXiv:2403.04844 (2024).

[34] X. Shi and Y. Shang, Avoiding barren plateaus via gaussian mixture model, arXiv preprint arXiv:2402.13501 (2024).

[35] M. Otten, C. L. Cortes, and S. K. Gray, Noise-resilient quantum dynamics using symmetry-preserving ansatzes, arXiv preprint arXiv:1910.06284 (2019).

[36] M. Benedetti, M. Fiorentini, and M. Lubasch, Hardware-efficient variational quantum algorithms for time evolution, Physical Review Research **3**, 033083 (2021).

[37] S. Barison, F. Vicentini, and G. Carleo, An efficient quantum algorithm for the time evolution of parameterized circuits, Quantum **5**, 512 (2021).

[38] S.-H. Lin, R. Dilip, A. G. Green, A. Smith, and F. Pollmann, Real-and imaginary-time evolution with compressed quantum circuits, PRX Quantum **2**, 010342 (2021).

[39] N. F. Berthusen, T. V. Trevisan, T. Iadecola, and P. P. Orth, Quantum dynamics simulations beyond the coherence time on noisy intermediate-scale quantum hardware by variational trotter compression, Phys. Rev. Res. **4**, 023097 (2022).

[40] T. Haug and M. Kim, Optimal training of variational quantum algorithms without barren plateaus, arXiv preprint arXiv:2104.14543 (2021).

[41] G. Gentinetta, F. Metz, and G. Carleo, Overhead-constrained circuit knitting for variational quantum dynamics, arXiv preprint arXiv:2309.07857 https://doi.org/10.48550/arXiv.2309.07857 (2023).

[42] S. Lloyd, Universal quantum simulators, Science , 1073 (1996).

[43] C. J. Trout, M. Li, M. Gutiérrez, Y. Wu, S.-T. Wang, L. Duan, and K. R. Brown, Simulating the performance of a distance-3 surface code in a linear ion trap, New Journal of Physics **20**, 043038 (2018).

[44] S. Endo, J. Sun, Y. Li, S. C. Benjamin, and X. Yuan, Variational quantum simulation of general processes, Physical Review Letters **125**, 010501 (2020).

[45] Y.-X. Yao, N. Gomes, F. Zhang, C.-Z. Wang, K.-M. Ho, T. Iadecola, and P. P. Orth, Adaptive variational quantum dynamics simulations, PRX Quantum **2**, 030307 (2021).

[46] K. Heya, K. M. Nakanishi, K. Mitarai, and K. Fujii, Subspace variational quantum simulator, arXiv preprint arXiv:1904.08566 (2019).

[47] C. Cirstoiu, Z. Holmes, J. Iosue, L. Cincio, P. J. Coles, and A. Sornborger, Variational fast forwarding for quantum simulation beyond the coherence time, npj Quantum Information **6**, 1 (2020).

[48] J. Gibbs, K. Gili, Z. Holmes, B. Commeau, A. Arrasmith, L. Cincio, P. J. Coles, and A. Sornborger, Long-time simulations for fixed input states on quantum hardware, npj Quantum Information **8**, 135 (2022).

[49] J. Gibbs, Z. Holmes, M. C. Caro, N. Ezzell, H.-Y. Huang, L. Cincio, A. T. Sornborger, and P. J. Coles, Dynamical simulation via quantum machine learning with provable generalization, Physical Review Research **6**, 013241 (2024).

[50] N. M. Eassa, J. Gibbs, Z. Holmes, A. Sornborger, L. Cincio, G. Hester, P. Kairys, M. Motta, J. Cohn, and A. Banerjee, High-fidelity dimer excitations using quantum hardware, arXiv preprint arXiv:2304.06146 https://doi.org/10.48550/arXiv.2304.06146 (2023).

[51] K. Bharti and T. Haug, Quantum-assisted simulator, Physical Review A **104**, 042418 (2021).

[52] J. W. Z. Lau, K. Bharti, T. Haug, and L. C. Kwek, Quantum assisted simulation of time dependent Hamiltonians, arXiv preprint arXiv:2101.07677 (2021).

[53] T. Haug and K. Bharti, Generalized quantum assisted simulator, arXiv preprint arXiv:2011.14737 (2020).

[54] E. Kökcü, T. Steckmann, Y. Wang, J. Freericks, E. F. Dumitrescu, and A. F. Kemper, Fixed depth hamiltonian simulation via cartan decomposition, Physical Review Letters **129**, 070501 (2022).

[55] T. Steckmann, T. Keen, A. F. Kemper, E. F. Dumitrescu, and Y. Wang, Simulating the mott transition on a noisy digital quantum computer via cartan-based fast-forwarding circuits, arXiv preprint arXiv:2112.05688 (2021).

[56] F. Jamet, A. Agarwal, C. Lupo, D. E. Browne, C. Weber, and I. Rungger, Krylov variational quantum algorithm for first principles materials simulations, arXiv preprint arXiv:2105.13298 https://doi.org/10.48550/arXiv.2105.13298 (2021).

[57] L. Bittel and M. Kliesch, Training variational quantum algorithms is NP-hard, Phys. Rev. Lett. **127**, 120502 (2021).

[58] E. R. Anschuetz, Critical points in quantum generative models, International Conference on Learning Representations (2022).

[59] A. Tikku and I. H. Kim, Circuit depth versus energy in topologically ordered systems, arXiv preprint arXiv:2210.06796 (2022).

[60] E. Campos, A. Nasrallah, and J. Biamonte, Abrupt transitions in variational quantum circuit training, Physical Review A **103**, 032607 (2021).

[61] P. Braccia, P. Bermejo, L. Cincio, and M. Cerezo, Computing exact moments of local random quantum circuits via tensor networks, arXiv preprint arXiv:2403.01706 (2024).

[62] M. S. Rudolph, S. Sim, A. Raza, M. Stechly, J. R. McClean, E. R. Anschuetz, L. Serrano, and A. Perdomo-Ortiz, Orqviz: visualizing high-dimensional landscapes in variational quantum algorithms, arXiv preprint arXiv:2111.04695 https://doi.org/10.48550/arXiv.2111.04695 (2021).

[63] J. Liu, H. Yuan, X.-M. Lu, and X. Wang, Quantum fisher information matrix and multiparameter estimation, Journal of Physics A: Mathematical and Theoretical **53**, 023001 (2019).

[64] M. Larocca, N. Ju, D. García-Martín, P. J. Coles, and M. Cerezo, Theory of overparametrization in quantum neural networks, Nature Computational Science **3**, 542 (2023).

[65] G. Tóth and I. Apellaniz, Quantum metrology from a quantum information science perspective, Journal of Physics A: Mathematical and Theoretical **47**, 424006 (2014).

[66] J. J. Duistermaat and J. A. C. Kolk, Taylor expansion in several variables, in *Distributions: Theory and Applications* (Birkhäuser Boston, Boston, 2010) pp. 59–63.

[67] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).

[68] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. (Cambridge University Press, 2012).

[69] X. Yuan, S. Endo, Q. Zhao, Y. Li, and S. C. Benjamin, Theory of variational quantum simulation, Quantum **3**, 191 (2019).

[70] S. McArdle, T. Jones, S. Endo, Y. Li, S. C. Benjamin, and X. Yuan, Variational ansatz-based quantum simulation of imaginary time evolution, npj Quantum Information **5**, 10.1038/s41534-019-0187-2 (2019).

[71] F. Verstraete, J. J. García-Ripoll, and J. I. Cirac, Matrix product density operators: Simulation of finite-temperature and dissipative systems, Phys. Rev. Lett. **93**, 207204 (2004).

[72] F. A. Wolf, A. Go, I. P. McCulloch, A. J. Millis, and U. Schollwöck, Imaginary-time matrix product state impurity solver for dynamical mean-field theory, Phys. Rev. X **5**, 041032 (2015).

Appendix A: Preliminaries

In this section, we briefly review some analytical tools and concepts that will be used through out the other sections.

1. Relation between Hessian of the loss function and quantum Fisher information

Given the optimal parameters obtained from the previous iteration $\boldsymbol{\theta}^*$ and a time-step δt of the Hamiltonian H, the loss function at the current iteration is of the form

$$\mathcal{L}(\boldsymbol{\theta}) = 1 - \left|\langle\psi_0|U^\dagger(\boldsymbol{\theta})e^{-iH\delta t}U(\boldsymbol{\theta}^*)|\psi_0\rangle\right|^2 \tag{A1}$$

$$= 1 - F\left(U(\boldsymbol{\theta})|\psi_0\rangle, e^{-iH\delta t}U(\boldsymbol{\theta}^*)|\psi_0\rangle\right) \tag{A2}$$

where $F\left(|\psi\rangle, |\phi\rangle\right)$ is a fidelity between two pure states $|\psi\rangle$ and $|\phi\rangle$. We remark that although δt is often taken as fixed and not optimised during the training process, the loss function also implicitly depends on δt.

The warm-start strategy is to initialise the training of the current iteration around $\boldsymbol{\theta}^*$. To analyse the trainability of this strategy, we often consider the expansion of the loss around $\boldsymbol{\theta}^*$ and $\delta t = 0$. In this context, it is convenient to write $\boldsymbol{x} = (\boldsymbol{\theta} - \boldsymbol{\theta}^*, \delta t)$ and $F(\boldsymbol{x}) := F\left(U(\boldsymbol{\theta})|\psi_0\rangle, e^{-iH\delta t}U(\boldsymbol{\theta}^*)|\psi_0\rangle\right)$. Upon expanding the loss around $\boldsymbol{x} = \boldsymbol{0}$, the connection between the Hessian of the loss function and the quantum fisher information is

$$\nabla^2_{\boldsymbol{x}}\mathcal{L}(\boldsymbol{x})\Big|_{\boldsymbol{x}=\boldsymbol{0}} = -\nabla^2 F(\boldsymbol{x})\Big|_{\boldsymbol{x}=\boldsymbol{0}} = \frac{1}{2}\mathcal{F}(\boldsymbol{0}) , \tag{A3}$$

where $\mathcal{F}(\boldsymbol{0})$ is the quantum fisher information evaluated at $\boldsymbol{x} = \boldsymbol{0}$ and measures how the quantum state $U(\boldsymbol{\theta}^*)|\psi_0\rangle$ is sensitive to local perturbations around $\boldsymbol{\theta}^*$ and $\delta t = 0$ [63–65].

2. Taylor remainder theorem

We present the Taylor remainder theorem which expresses a multivariate differentiable function as a series expansion. We refer the reader to Ref. [66] for further details.

Theorem 4 (Taylor reminder theorem). *Consider a multivariate differentiable function $f(\boldsymbol{x})$ such that $f : \mathbb{R}^N \to \mathbb{R}$ and some positive integer K. The function $f(\boldsymbol{x})$ can be expanded around some fixed point $\boldsymbol{a}$ as*

$$f(\boldsymbol{x}) = \sum_{k=0}^{K}\sum_{i_1,i_2,\ldots,i_k}^{N} \frac{1}{k!}\left(\frac{\partial^k f(\boldsymbol{x})}{\partial x_{i_1}\partial x_{i_2}\ldots\partial x_{i_k}}\right)\Bigg|_{\boldsymbol{x}=\boldsymbol{a}} (x_{i_1} - a_{i_1})(x_{i_2} - a_{i_2})\ldots(x_{i_k} - a_{i_k}) + R_{K,\boldsymbol{a}}(\boldsymbol{x}) , \tag{A4}$$

where the remainder is of the form

$$R_{K,\boldsymbol{a}}(\boldsymbol{x}) = \sum_{i_1,i_2,\ldots,i_{K+1}}^{N} \frac{1}{(K+1)!}\left(\frac{\partial^{K+1} f(\boldsymbol{x})}{\partial x_{i_1}\partial x_{i_2}\ldots\partial x_{i_{K+1}}}\right)\Bigg|_{\boldsymbol{x}=\boldsymbol{\nu}} (x_{i_1} - a_{i_1})(x_{i_2} - a_{i_2})\ldots(x_{i_{K+1}} - a_{i_{K+1}}) , \tag{A5}$$

with $\boldsymbol{\nu} = c\boldsymbol{x} + (1-c)\boldsymbol{a}$ for some $c \in [0,1]$.

As an example, we apply the Taylor remainder theorem to prove the following statement.

Lemma 5. *The fidelity between two pure states ρ and $e^{-iHt}\rho e^{iHt}$ (with the Hamiltonian H) can be upper bounded as*

$$F\left(\rho, e^{-itH}\rho e^{itH}\right) \geqslant 1 - 2\lambda^2_{\max}t^2 \tag{A6}$$

where $\lambda_{\max}$ is the largest eigenvalue of H.

Proof. First, we denote $F(t) := F\left(\rho, e^{-itH}\rho e^{itH}\right)$. By using Theorem 4 (expanding around $t = 0$ up to the second order), the fidelity is of the form

$$F(t) = 1 + \frac{t^2}{2}\left(\frac{d^2F(t)}{dt^2}\right)\Bigg|_{t=\tau} , \tag{A7}$$

where the zero order term is 1, the first order term is zero by a direct computation and the second order term is evaluated at some $\tau \in [0, t]$. We can then bound the second derivative as the following

$$\left(\frac{d^2F(t)}{dt^2}\right)\bigg|_{t=\tau} = \mathrm{Tr}\left(\rho e^{-iH\tau} i\left[i\left[\rho, H\right], H\right] e^{iH\tau}\right) \tag{A8}$$

$$\leqslant \|\rho\|_1 \|e^{-iH\tau} i\left[i\left[\rho, H\right], H\right] e^{iH\tau}\|_\infty \tag{A9}$$

$$\leqslant 4\lambda_{\text{max}}^2 \ , \tag{A10}$$

where the first inequality is due to Hölder's inequality. In the second inequality, we rely on the following identities: (i) $\|\rho\|_1 = 1$ for a pure state, (ii) the unitary invariance of the Schatten p-norm i.e., $\|UA\|_p = \|A\|_p$ for any unitary U, (iii) $\|i[A, B]\|_p \leqslant 2\|A\|_p\|B\|_p$ and lastly (iv) $\|AB\|_p \leqslant \|A\|_p\|B\|_p$. Thus, the fidelity can be lower bounded as

$$F(t) \geqslant 1 - 2\lambda_{\text{max}}^2 t^2 \ . \tag{A11}$$

This completes the proof. □

3. Approximate convexity

In this section, we provide a formal explanation of our definition of an ϵ-convex function. We start by defining what convexity is (see for example Ref. [67]) and we relate it to our notion of ϵ-convexity.

Definition 3 (Convexity)**.** *A differentiable function of several variables $f : \mathbb{R}^N \to \mathbb{R}$ is convex in a region $\mathcal{R}$, if and only if for all $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{R}$ the function fulfils*

$$f(\boldsymbol{x}) \geqslant f(\boldsymbol{y}) + \nabla f(\boldsymbol{y}) \cdot (\boldsymbol{x} - \boldsymbol{y}) \ . \tag{A12}$$

or equivalently, $\nabla^2 f(\boldsymbol{x})$ is positive semi-definite. Here $\nabla^2 f(\boldsymbol{x})$ denotes the Hessian of $f(\boldsymbol{x})$. Notice that we use $\nabla f(\boldsymbol{y}) = \nabla_{\tilde{\boldsymbol{y}}} f(\tilde{\boldsymbol{y}})|_{\tilde{\boldsymbol{y}}=\boldsymbol{y}}$, $\nabla^2 f(\boldsymbol{y}) = \nabla^2_{\tilde{\boldsymbol{y}}} f(\tilde{\boldsymbol{y}})|_{\tilde{\boldsymbol{y}}=\boldsymbol{y}}$

Informally this means that all the tangent planes to f are below f in the region $\mathcal{R}$. This is shown for one variable in Fig. 6 a).

Definition 1 (ϵ-approximate convexity.)**.** *A differentiable function of several variables $f : \mathbb{R}^N \to \mathbb{R}$ is ϵ-convex in a region $\mathcal{R}$ if*

$$\left[\nabla^2 f(\boldsymbol{x})\right]_{\text{min}} \geqslant -|\epsilon| \tag{A13}$$

for all $\boldsymbol{x} \in \mathcal{R}$. Here $\nabla^2 f(\boldsymbol{x})$ denotes the Hessian of $f(\boldsymbol{x})$ and we denote $[A]_{\text{min}}$ as the smallest eigenvalue of the matrix A.

If a function is ϵ-convex in a finite region $\mathcal{R}$, then we can show an equivalent intuition to the one for convexity. Indeed, if a function f is ϵ-convex in a finite region $\mathcal{R}$, then we can say that an "ϵ-displacement" in every tangent line is enough to make it below f in $\mathcal{R}$ as shown in Fig. 6 b).

Proposition 1. *If a differentiable function of several variables $f : \mathbb{R}^n \to \mathbb{R}$ is ϵ-convex in finite a region $\mathcal{R}$, then for all $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{R}$ the function fulfils*

$$f(\boldsymbol{x}) \geqslant f(\boldsymbol{y}) + \nabla f(\boldsymbol{y}) \cdot (\boldsymbol{x} - \boldsymbol{y}) - |\epsilon|\alpha \ , \tag{A14}$$

where $\alpha = \frac{1}{2}\max_{\boldsymbol{a},\boldsymbol{b}\in\mathcal{R}} ||\boldsymbol{a} - \boldsymbol{b}||_2^2$.

Proof. First we recall the Taylor reminder theorem in A 2. Then we can expand the function f around the point $\boldsymbol{y}$ as

$$f(\boldsymbol{x}) = f(\boldsymbol{y}) + \sum_i^n \frac{\partial f(\boldsymbol{q})}{\partial q_i}\bigg|_{\boldsymbol{q}=\boldsymbol{y}} (x_i - y_i) + \frac{1}{2}\sum_{i,j}^n \frac{\partial^2 f(\boldsymbol{q})}{\partial q_i \partial q_j}\bigg|_{\boldsymbol{q}=\boldsymbol{z}} (x_j - y_j)(x_i - y_i) \tag{A15}$$

$$= f(\boldsymbol{y}) + \nabla f(\boldsymbol{y}) \cdot (\boldsymbol{x} - \boldsymbol{y}) + \frac{1}{2}(\boldsymbol{x} - \boldsymbol{y})^T \nabla^2 f(\boldsymbol{z})(\boldsymbol{x} - \boldsymbol{y}) \ , \tag{A16}$$

for some $\boldsymbol{z} = c\boldsymbol{x} + (1 - c)\boldsymbol{y}$ with some $c \in [0, 1]$. In the last equality we wrote the expression in its vector form for simplicity.

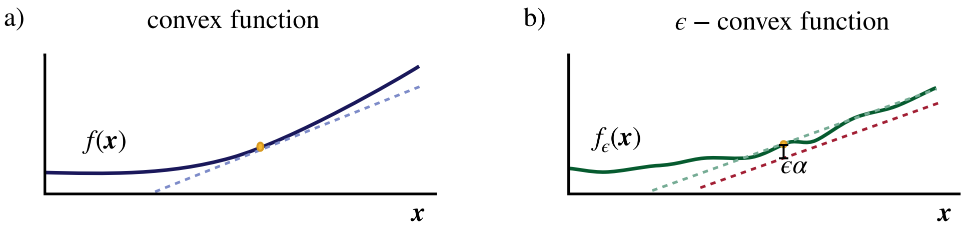


FIG. 6. **Convexity and ϵ-convexity.** Here we show two schematics for one variable functions. a) Represents a convex function and the tangent (dashed line). The tangent is always below f. b) Represents a ϵ-convex function and the tangent (dashed line). The light-green dashed line represents the tangent to the function. The red line represents the tangent displaced $\alpha\epsilon$ with respect to the green one. A "displacement of $\alpha\epsilon$" on the tangent makes it such that is always below the function.

Now if we apply the notion of ϵ-convexity we can lower-bound the right-hand side of the previous equality to find

$$f(\boldsymbol{x}) \geqslant f(\boldsymbol{y}) + \nabla f(\boldsymbol{y}) \cdot (\boldsymbol{x}-\boldsymbol{y}) - \frac{1}{2}|\epsilon|(\boldsymbol{x}-\boldsymbol{y})^T(\boldsymbol{x}-\boldsymbol{y}) \ , \tag{A17}$$

which can be further bounded by using that $(\boldsymbol{x}-\boldsymbol{y})^T(\boldsymbol{x}-\boldsymbol{y}) \leqslant \alpha$. Recall that $\alpha = \frac{1}{2}\max_{\boldsymbol{a},\boldsymbol{b}\in\mathcal{R}} ||\boldsymbol{a}-\boldsymbol{b}||_2^2$. With this we find

$$f(\boldsymbol{x}) \geqslant f(\boldsymbol{y}) + \nabla f(\boldsymbol{y}) \cdot (\boldsymbol{x}-\boldsymbol{y}) - |\epsilon|\alpha \ , \tag{A18}$$

□

Notice that in general α can increase with the dimension of the input $\boldsymbol{x}$ (for the loss function in Eq (3) this is equivalent to the number of parameters M) as well as with the size of the region that we demand ϵ-convexity over. That is, for a region of size r, α approximately scales as Mr^2. In the regime that is relevant to our work (particularly, Theorem 2), the region in which we require ϵ-convexity is of order $r \in \Omega\left(1/M^2\right)$ (for appropriately chosen δt). Hence, α decays with the number of parameters as $1/M^2$.

4. Upper bound on the eigenvalues

We present a simplified version of Gershgorin's circle theorem [68] which can be used to upper bound the eigenvalues of a real squared matrix.

Proposition 2. *Consider a real $M \times M$ matrix A and denote $\lambda_{\max}$ as the largest eigenvalue of A. Given that the sum of elements in any row is upper bounded by some value T_0, that is $\sum_j |A_{ij}| \leqslant T_0$ for any $i \in \{1, ..., M\}$, the largest eigenvalue of A can be bounded as*

$$\lambda_{\max} \leqslant T_0 \ \ . \tag{A19}$$

Proof. Let $\boldsymbol{v}$ be an eigenvector corresponding the largest eigenvalue of A. There exists the largest component in the eigenvector denoted as v_i. Then, we consider this eigenvector component in the eigenvalue equation

$$\sum_j A_{ij} v_j = \lambda_{\max} v_i \ . \tag{A20}$$

The bound of the largest eigenvalue follows as

$$\begin{aligned} \lambda_{\max} &\leqslant \sum_j \frac{|A_{i,j}| \cdot |v_j|}{|v_i|} && \text{(A21)}\\ &\leqslant \sum_j |A_{i,j}| && \text{(A22)}\\ &\leqslant T_0 \ , && \text{(A23)} \end{aligned}$$

where the first inequality is due to triangle inequality, the second inequality is from $\frac{|v_j|}{|v_i|} \leqslant 1$ and in the last inequality we use the assumption that $\sum_j |A_{i,j}| \leqslant T_0$. □

Appendix B: Lower bound of the variance of the loss function

In this section, we provide the exact formula for the lower bound of the loss function for the variational Trotter compression algorithm.

1. Exact formula for the lower bound

Proposition 3. *Consider the loss function $\mathcal{L}(\boldsymbol{\theta})$ as defined in Eq. (3) and with an ansatz of the general form defined in Eq. (4) with M parameters. The variance of $\mathcal{L}(\boldsymbol{\theta})$ over the hypercube parameter region $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$ around an optimal solution of the previous iteration $\boldsymbol{\theta}^*$ can be bounded as*

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}[\mathcal{L}(\boldsymbol{\theta})] \geqslant (c_+ - k_+^2) \min_{\tilde{\xi}\in[-1,1]} \left(k_+^{M-1}\Delta_{\boldsymbol{\theta}^*} + (1-k_+^{M-1})\tilde{\xi}\right)^2 , \tag{B1}$$

where we have

$$c_+ := \mathbb{E}_{\alpha\sim\boldsymbol{\mathcal{D}}(0,r)}[\cos^4 \alpha] , \tag{B2}$$

$$k_+ := \mathbb{E}_{\alpha\sim\boldsymbol{\mathcal{D}}(0,r)}[\cos^2 \alpha] , \tag{B3}$$

$$\Delta_{\boldsymbol{\theta}^*} := \mathrm{Tr}\left[(\rho_0 - \sigma_1\rho_0\sigma_1)U^\dagger\left(\boldsymbol{\theta^*}\right)\rho_{(\boldsymbol{\theta}^*,\delta t)}U\left(\boldsymbol{\theta^*}\right)\right] . \tag{B4}$$

Here σ_1 is the Pauli string associated with the first gate in the circuit $U(\boldsymbol{\theta})$ as defined in Eq. (4), $\rho_0 = |\psi_0\rangle\langle\psi_0|$ is an initial state before the time evolution and $\rho_{(\boldsymbol{\theta}^*,\delta t)} = e^{-iH\delta t}U(\boldsymbol{\theta^*})\rho_0 U^\dagger(\boldsymbol{\theta^*})e^{iH\delta t}$ with H being the underlying Hamiltonian of the quantum dynamics.

Proof. First, we recall that the loss function at each iteration (as defined in Eq. (3)) is of the form

$$\mathcal{L}(\boldsymbol{\theta}) = 1 - \left|\langle\psi_0|U^\dagger(\boldsymbol{\theta})|\psi(\boldsymbol{\theta}^*,\delta t)\rangle\right|^2 \tag{B5}$$

$$= 1 - \langle\psi_0|U^\dagger(\boldsymbol{\theta})\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta})|\psi_0\rangle \tag{B6}$$

for some initial state $|\psi_0\rangle$ and

$$\rho_{(\boldsymbol{\theta}^*,\delta t)} := |\psi(\boldsymbol{\theta}^*,\delta t)\rangle\langle\psi(\boldsymbol{\theta}^*,\delta t)| = e^{-iH\delta t}U(\boldsymbol{\theta}^*)|\psi_0\rangle\langle\psi_0|U^\dagger(\boldsymbol{\theta}^*)e^{iH\delta t} , \tag{B7}$$

where $\boldsymbol{\theta}^*$ is an optimal solution of the previous iteration. The parameterised quantum circuit $U(\boldsymbol{\theta})$ with M parameters takes the following general form

$$U\left(\boldsymbol{\theta}\right) = \prod_{i=1}^{M} V_i U_i(\theta_i) , \tag{B8}$$

where $\{V_i\}_{i=1}^M$ are some fixed unitaries and $\{U_i(\theta_i) = e^{-i\theta_i\sigma_i}\}_{i=1}^M$ are a set of parameterised rotation gates with σ_i being a Pauli string associated with the i^{th} gate. Crucially, the rotation gates can be re-expressed as perturbations $\boldsymbol{\alpha}$ around the previous optimal solution i.e., $\theta_i = \theta_i^* + \alpha_i$ for all i

$$U\left(\boldsymbol{\theta}\right) = \prod_{i=1}^{M} V_i U_i(\theta_i^*)U_i(\alpha_i) \tag{B9}$$

$$= \prod_{i=1}^{M} \widetilde{V}_i(\theta_i^*)U_i(\alpha_i) , \tag{B10}$$

where the first equality holds due to $e^{-i\theta_i\sigma_i} = e^{-i\theta_i^*\sigma_i}e^{-i\alpha_i\sigma_i}$ and in the second equality we denote $\widetilde{V}_i := \widetilde{V}_i(\theta_i^*) = V_i e^{-i\theta_i^*\sigma_i}$.

We consider the region of parameters around the previous optimum which can also be expressed in terms of $\boldsymbol{\alpha}$

$$\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r) = \{\boldsymbol{\theta} = \boldsymbol{\theta}^* + \boldsymbol{\alpha} \mid \ \alpha_i \in [-r, r]\} \ , \tag{B11}$$

where r is a characteristic length of the region. Now, we are interested in the variance of the loss function over $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$ such that each parameter is uniformly sampled

$$\begin{aligned}
\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] &= \mathrm{Var}_{\boldsymbol{\alpha}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}\left[\mathcal{L}(\boldsymbol{\theta} = \boldsymbol{\theta}^* + \boldsymbol{\alpha})\right] & \text{(B12)}\\
&= \mathrm{Var}_{\boldsymbol{\alpha}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}\left[1 - \mathcal{L}(\boldsymbol{\theta})\right] & \text{(B13)}\\
&= \mathbb{E}_{\boldsymbol{\alpha}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))^2\right] - \left(\mathbb{E}_{\boldsymbol{\alpha}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}[1 - \mathcal{L}(\boldsymbol{\theta})]\right)^2 \ , & \text{(B14)}
\end{aligned}$$

where the second equality is due to $\mathrm{Var}_{\boldsymbol{\alpha}}[b_1 X(\boldsymbol{\alpha}) + b_2] = (b_1)^2 \mathrm{Var}_{\boldsymbol{\alpha}} X(\boldsymbol{\alpha})$ for some constants b_1 and b_2.

Importantly, since all parameters are assumed to be uncorrelated, this allows us to compute the variance over each individual parameter one-by-one from the outermost parameter α_M towards the first parameter α_1. That is, each term in Eq. (B14) can be expressed as

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{\alpha}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))^2\right] &= \mathbb{E}_{\alpha_1,\alpha_2,\ldots,\alpha_M}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))^2\right] & \text{(B15)}\\
&= \mathbb{E}_{\alpha_1,\alpha_2,\ldots,\alpha_{M-1}}\mathbb{E}_{\alpha_M}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))^2\right] & \text{(B16)}\\
&:= \mathbb{E}_{\overline{\alpha_M}}\mathbb{E}_{\alpha_M}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))^2\right] \ , & \text{(B17)}
\end{aligned}$$

with $\overline{\alpha_M} := \alpha_1, \alpha_2, ..., \alpha_{M-1}$ and, similarly,

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{\alpha}\sim\boldsymbol{\mathcal{D}}(\mathbf{0},r)}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))\right] &= \mathbb{E}_{\alpha_1,\alpha_2,\ldots,\alpha_{M-1}}\mathbb{E}_{\alpha_M}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))\right] & \text{(B18)}\\
&:= \mathbb{E}_{\overline{\alpha_M}}\mathbb{E}_{\alpha_M}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))\right] \ . & \text{(B19)}
\end{aligned}$$

Before delving into computing these terms, we first stress the α_M dependence of the loss by writing

$$\begin{aligned}
1 - \mathcal{L}(\boldsymbol{\theta}) =& \ \left|\langle\psi_0|U^\dagger(\boldsymbol{\theta})|\psi(\boldsymbol{\theta}^*, \delta t)\rangle\right|^2 & \text{(B20)}\\
=& \ \langle\psi_{M-1}|U_M^\dagger(\alpha_M)\rho_M U_M(\alpha_M)|\psi_{M-1}\rangle \ , & \text{(B21)}
\end{aligned}$$

where we have defined

$$\begin{aligned}
|\psi_{M-1}\rangle &:= \prod_{i=1}^{M-1} \widetilde{V}_i(\theta_i^*) U_i(\alpha_i)|\psi_0\rangle \ , & \text{(B22)}\\
\rho_M &:= \widetilde{V}_M^\dagger(\theta_M^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}\widetilde{V}_M(\theta_M^*) \ . & \text{(B23)}
\end{aligned}$$

Remark that $|\psi_{M-1}\rangle$ depends on the other parameters $\{\alpha_i\}_{i=1}^{M-1}$ while ρ_M is independent of $\boldsymbol{\alpha}$. Next we use the identity

$$U_i(\alpha_i) = \cos(\alpha_i)\mathbb{1} - i\sin(\alpha_i)\sigma_i \ , \tag{B24}$$

to rewrite the loss as

$$\begin{aligned}
1 - \mathcal{L}(\boldsymbol{\theta}) =& \ \cos^2(\alpha_M)\langle\psi_{M-1}|\rho_M|\psi_{M-1}\rangle + \sin^2(\alpha_M)\langle\psi_{M-1}|\sigma_M\rho_M\sigma_M|\psi_{M-1}\rangle \\
& - \cos(\alpha_M)\sin(\alpha_M)\langle\psi_{M-1}|i[\rho_M, \sigma_M]|\psi_{M-1}\rangle & \text{(B25)}\\
=& \ \cos^2(\alpha_M)\langle\rho_M\rangle_{\psi_{M-1}} + \sin^2(\alpha_M)\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}} - \cos(\alpha_M)\sin(\alpha_M)\langle i[\rho_M, \sigma_M]\rangle_{\psi_{M-1}} \ , & \text{(B26)}
\end{aligned}$$

where in the final line we use the shorthand

$$\langle O\rangle_\psi := \langle\psi|O|\psi\rangle \ , \tag{B27}$$

for some observable O and some state $|\psi\rangle$.

We are now ready to proceed with the averaging over α_M in Eq. (B17) which results in

$$\begin{aligned}
\mathbb{E}_{\alpha_M}\left[(1 - \mathcal{L}(\boldsymbol{\theta}))^2\right] &= c_+\langle\rho_M\rangle_{\psi_{M-1}}^2 + c_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}^2 + c_0\langle i[\rho_M, \sigma_M]\rangle_{\psi_{M-1}}^2 & \text{(B28)}\\
&\quad + 2c_0\langle\rho_M\rangle_{\psi_{M-1}}\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}} \\
&\geqslant c_+\langle\rho_M\rangle_{\psi_{M-1}}^2 + c_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}^2 + 2c_0\langle\rho_M\rangle_{\psi_{M-1}}\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}} \ , & \text{(B29)}
\end{aligned}$$

where we have

$$c_+ = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \cos^4(\alpha_M)\ , \tag{B30}$$

$$c_- = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \sin^4(\alpha_M)\ , \tag{B31}$$

$$c_0 = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \cos^2(\alpha_M)\sin^2(\alpha_M)\ , \tag{B32}$$

$$0 = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \cos^3(\alpha_M)\sin(\alpha_M) = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \cos(\alpha_M)\sin^3(\alpha_M)\ . \tag{B33}$$

Similarly, by considering Eq. (B19), we have

$$\mathbb{E}_{\alpha_M}\left[1-\mathcal{L}(\boldsymbol{\theta})\right] = k_+\langle\rho_M\rangle_{\psi_{M-1}} + k_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\ , \tag{B34}$$

with

$$k_+ = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \cos^2(\alpha_M)\ , \tag{B35}$$

$$k_- = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \sin^2(\alpha_M)\ , \tag{B36}$$

$$0 = \frac{1}{2r}\int_{-r}^{r} d\alpha_M \cos(\alpha_M)\sin(\alpha_M)\ . \tag{B37}$$

From the above expressions, we can see that $\mathrm{Var}_\alpha[\cos^2(\alpha)] = c_+ - k_+^2$, $\mathrm{Var}_\alpha[\sin^2(\alpha)] = c_- - k_-^2$ and $\mathrm{Cov}_\alpha[\cos^2(\alpha), \sin^2(\alpha)] = c_0 - k_+k_-$. In addition, it can be verified by a direct computation that

$$c_+ - k_+^2 = c_- - k_-^2 = -(c_0 - k_+k_-) = \frac{-1+4r^2+\cos(4r)+r\sin(4r)}{32r^2}\ . \tag{B38}$$

Together, the variance in Eq. (B14) can be bounded as

$$\begin{aligned}
\mathrm{Var}_{\boldsymbol{\theta}}\left[\mathcal{L}(\boldsymbol{\theta})\right] &= \mathbb{E}_{\alpha_1,\dots,\alpha_{M-1}}\mathbb{E}_{\alpha_M}\left[(1-\mathcal{L}(\boldsymbol{\theta}))^2\right] - \left(\mathbb{E}_{\alpha_1,\dots,\alpha_{M-1}}\mathbb{E}_{\alpha_M}\left[1-\mathcal{L}(\boldsymbol{\theta})\right]\right)^2 && \text{(B39)}\\
&\geqslant \mathbb{E}_{\overline{\alpha_M}}\left[c_+\langle\rho_M\rangle^2_{\psi_{M-1}} + c_-\langle\sigma_M\rho_M\sigma_M\rangle^2_{\psi_{M-1}} + 2c_0\langle\rho_M\rangle_{\psi_{M-1}}\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right]\\
&\quad - \left(\mathbb{E}_{\overline{\alpha_M}}\left[k_+\langle\rho_M\rangle_{\psi_{M-1}} + k_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right]\right)^2 && \text{(B40)}\\
&= c_+\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle^2_{\psi_{M-1}}\right] - k_+^2\left(\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}\right]\right)^2\\
&\quad + c_-\mathbb{E}_{\overline{\alpha_M}}\left[\langle\sigma_M\rho_M\sigma_M\rangle^2_{\psi_{M-1}}\right] - k_-^2\left(\mathbb{E}_{\overline{\alpha_M}}\left[\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right]\right)^2\\
&\quad + 2c_0\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] - 2k_+k_-\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}\right]\mathbb{E}_{\overline{\alpha_M}}\left[\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] && \text{(B41)}\\
&= (c_+ - k_+^2)\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle^2_{\psi_{M-1}}\right] + k_+^2\mathrm{Var}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}\right]\\
&\quad + (c_- - k_-^2)\mathbb{E}_{\overline{\alpha_M}}\left[\langle\sigma_M\rho_M\sigma_M\rangle^2_{\psi_{M-1}}\right] + k_-^2\mathrm{Var}_{\overline{\alpha_M}}\left[\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right]\\
&\quad + 2(c_0 - k_+k_-)\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] + 2k_+k_-\mathrm{Cov}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}, \langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] && \text{(B42)}\\
&= (c_+ - k_+^2)\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle^2_{\psi_{M-1}} + \langle\sigma_M\rho_M\sigma_M\rangle^2_{\psi_{M-1}} - 2\langle\rho_M\rangle_{\psi_{M-1}}\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right]\\
&\quad + k_+^2\mathrm{Var}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}\right] + k_-^2\mathrm{Var}_{\overline{\alpha_M}}\left[\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] + 2k_+k_-\mathrm{Cov}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}}, \langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] && \text{(B43)}\\
&= (c_+ - k_+^2)\mathbb{E}_{\overline{\alpha_M}}\left[\langle\rho_M\rangle_{\psi_{M-1}} - \langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right]^2 + \mathrm{Var}_{\overline{\alpha_M}}\left[k_+\langle\rho_M\rangle_{\psi_{M-1}} + k_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] && \text{(B44)}\\
&\geqslant \mathrm{Var}_{\overline{\alpha_M}}\left[k_+\langle\rho_M\rangle_{\psi_{M-1}} + k_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] && \text{(B45)}
\end{aligned}$$

where the first inequality is due to Eq. (B29), we then reach Eq. (B42) by using the fact that $\mathrm{Var}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha})] = \mathbb{E}_{\boldsymbol{\alpha}}[X^2(\boldsymbol{\alpha})] - (\mathbb{E}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha})])^2$ and $\mathrm{Cov}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha}), Y(\boldsymbol{\alpha})] = \mathbb{E}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha})Y[\boldsymbol{\alpha}]] - \mathbb{E}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha})]\mathbb{E}_{\boldsymbol{\alpha}}[Y(\boldsymbol{\alpha})]$, Eq. (B43) is from the relation presented in Eq. (B38). Next, in Eq. (B44) we use the identity $\mathrm{Var}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha})+Y(\boldsymbol{\alpha})] = \mathrm{Var}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha})] + \mathrm{Var}_{\boldsymbol{\alpha}}[Y(\boldsymbol{\alpha})] + 2\mathrm{Cov}_{\boldsymbol{\alpha}}[X(\boldsymbol{\alpha}), Y(\boldsymbol{\alpha})]$ and to reach the next inequality we throw away the first positive term in the sum.

Notably, the variance of the term in Eq. (B45) is no longer taken over α_M (i.e., the contribution to the variance from α_M is already taken into account). In addition, by denoting $|\psi_{M-2}\rangle = \prod_{i=1}^{M-2} \widetilde{V}_i(\theta_i^*)U_i(\alpha_i)|\psi_0\rangle$ as well as

$$\widetilde{\rho}_{M-1} = k_+ \widetilde{V}^\dagger_{M-1}(\theta^*_{M-1})\rho_M \widetilde{V}_{M-1}(\theta_{M-1}) + k_- \widetilde{V}^\dagger_{M-1}(\theta^*_{M-1})\sigma_M \rho_M \sigma_M \widetilde{V}_{M-1}(\theta^*_{M-1}) \,, \tag{B46}$$

the lower bound in Eq. (B45) can be expressed as

$$\begin{aligned} \mathrm{Var}_{\boldsymbol{\theta}}\left[\mathcal{L}(\boldsymbol{\theta})\right] &\geqslant \mathrm{Var}_{\overline{\alpha_M}}\left[k_+\langle\rho_M\rangle_{\psi_{M-1}} + k_-\langle\sigma_M\rho_M\sigma_M\rangle_{\psi_{M-1}}\right] && \text{(B47)}\\ &= \mathrm{Var}_{\alpha_1,\alpha_2,\ldots,\alpha_{M-1}}\left[\langle\psi_{M-2}|U^\dagger_{M-1}(\alpha_{M-1})\widetilde{\rho}_{M-1}U_{M-1}(\alpha_{M-1})|\psi_{M-2}\rangle\right] && \text{(B48)} \end{aligned}$$

Crucially, the derivation steps from Eq. (B28) to Eq. (B48), which are used to get rid of α_M dependence, can be repeated to recursively integrate over other parameters. To be more precise, let us first define

$$|\psi_{M-l-1}\rangle = \prod_{i=1}^{M-l-1} \widetilde{V}_i(\theta_i^*)U_i(\alpha_i)|\psi_0\rangle \,, \tag{B49}$$

as well as a general recursive form of Eq. (B46)

$$\widetilde{\rho}_{M-l} = k_+ \widetilde{V}^\dagger_{M-l}(\theta^*_{M-l})\widetilde{\rho}_{M-l+1} \widetilde{V}_{M-l}(\theta^*_{M-l}) + k_- \widetilde{V}^\dagger_{M-l}(\theta^*_{M-l})\sigma_{M-l+1} \widetilde{\rho}_{M-l+1} \sigma_{M-l+1} \widetilde{V}_{M-l}(\theta^*_{M-l}) \,, \tag{B50}$$

where $l \in \{1, 2, ..., M-1\}$ and we have $\widetilde{\rho}_M = \rho_M$ which gives back Eq. (B46) for $l = 1$. We note that $\widetilde{\rho}_{M-l}$ can be seen as a mixed state between $\widetilde{V}^\dagger_{M-l}(\theta^*_{M-l})\widetilde{\rho}_{M-l+1}\widetilde{V}_{M-l}(\theta^*_{M-l})$ and $\widetilde{V}^\dagger_{M-l}(\theta^*_{M-l})\sigma_{M-l+1}\widetilde{\rho}_{M-l+1}\sigma_{M-l+1}\widetilde{V}_{M-l}(\theta^*_{M-l})$ for all l. This is since $k_+ + k_- = 1$ and ρ_M is a valid quantum state.

The variance then can be recursively lower bounded, leading to

$$\begin{aligned} \mathrm{Var}_{\boldsymbol{\theta}}\left[\mathcal{L}(\boldsymbol{\theta})\right] &\geqslant \mathrm{Var}_{\alpha_1,\alpha_2,\ldots,\alpha_{M-1}}\left[\langle\psi_{M-2}|U^\dagger_{M-1}(\alpha_{M-1})\widetilde{\rho}_{M-1}U_{M-1}(\alpha_{M-1})|\psi_{M-2}\rangle\right] && \text{(B51)}\\ &\geqslant \mathrm{Var}_{\alpha_1,\alpha_2,\ldots,\alpha_{M-l}}\left[\langle\psi_{M-l-1}|U^\dagger_{M-l}(\alpha_{M-l})\widetilde{\rho}_{M-l}U_{M-l}(\alpha_{M-l})|\psi_{M-l-1}\rangle\right] && \text{(B52)}\\ &\geqslant \mathrm{Var}_{\alpha_1}\left[\langle\psi_1|U^\dagger_1(\theta_1)\widetilde{\rho}_1U_1(\theta_1)|\psi_1\rangle\right] \,, && \text{(B53)} \end{aligned}$$

where in the second inequality we have recursively integrated out parameters $\alpha_{M-l+1}, ..., \alpha_M$ and in the last equality we have integrated out all the parameters except α_1.

All that remains is to explicitly bound the variance with respect to α_1

$$\begin{aligned} \mathrm{Var}_{\boldsymbol{\theta}}\left[\mathcal{L}(\boldsymbol{\theta})\right] &\geqslant \mathrm{Var}_{\alpha_1}\left[\langle\psi_1|U^\dagger_1(\theta_1)\widetilde{\rho}_1U_1(\theta_1)|\psi_1\rangle\right] && \text{(B54)}\\ &\geqslant \left(c_+\langle\widetilde{\rho}_1\rangle^2_{\psi_0} + c_-\langle\sigma_1\widetilde{\rho}_1\sigma_1\rangle^2_{\psi_0} + 2c_0\langle\widetilde{\rho}_1\rangle_{\psi_0}\langle\sigma_1\widetilde{\rho}_1\sigma_1\rangle_{\psi_0}\right) - \left(k_+\langle\widetilde{\rho}_1\rangle_{\psi_0} + k_-\langle\sigma_1\widetilde{\rho}_1\sigma_1\rangle_{\psi_0}\right)^2 && \text{(B55)}\\ &= (c_+ - k_+^2)\left(\langle\widetilde{\rho}_1\rangle_{\psi_0} - \langle\sigma_1\widetilde{\rho}_1\sigma_1\rangle_{\psi_0}\right)^2 && \text{(B56)}\\ &= (c_+ - k_+^2)\left(\mathrm{Tr}\left[\left(|\psi_0\rangle\langle\psi_0| - \sigma_1|\psi_0\rangle\langle\psi_0|\sigma_1\right)\widetilde{\rho}_1\right]\right)^2 && \text{(B57)} \end{aligned}$$

where Eq. (B55) to Eq. (B57) follows in the same manner as Eq. (B40) to Eq. (B45). From recursively expanding $\widetilde{\rho}_1$ (according to Eq. (B50)), we can write:

$$\begin{aligned} \widetilde{\rho}_1 &= k_+^{M-1}\left(\prod_{i=1}^{M}\widetilde{V}_i(\theta_i^*)\right)^\dagger \rho_{(\boldsymbol{\theta}^*,\delta t)} \left(\prod_{i=1}^{M}\widetilde{V}_i(\theta_i^*)\right) + (1-k_+^{M-1})\xi && \text{(B58)}\\ &= k_+^{M-1}U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*) + (1-k_+^{M-1})\xi && \text{(B59)}\\ & && \text{(B60)} \end{aligned}$$

where ξ is some complicated mixed state and, for clarification, we note that $k_+^{M-1} = (k_+)^{M-1}$ with k_+ defined in Eq B35 [2]. Thus we can write

$$\begin{aligned} \mathrm{Var}_{\boldsymbol{\theta}}\left[\mathcal{L}(\boldsymbol{\theta})\right] &\geqslant (c_+ - k_+^2)\left(\mathrm{Tr}\left[\left(|\psi_0\rangle\langle\psi_0| - \sigma_1|\psi_0\rangle\langle\psi_0|\sigma_1\right)\left(k_+^{M-1}U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*) + (1-k_+^{M-1})\xi\right)\right]\right)^2 && \text{(B61)}\\ &\geqslant (c_+ - k_+^2)\min_{\tilde{\xi}\in[-1,1]}\left(k_+^{M-1}\,\mathrm{Tr}\left[\left(|\psi_0\rangle\langle\psi_0| - \sigma_1|\psi_0\rangle\langle\psi_0|\sigma_1\right)U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\right] + (1-k_+^{M-1})\tilde{\xi}\right)^2 && \text{(B62)} \end{aligned}$$

[2] This clarification on k_+^M is included at the request of one of the authors.

where in the final line we minimize over the free parameter $\tilde{\xi} = \mathrm{Tr}\left[(|\psi_0\rangle\langle\psi_0| - \sigma_1|\psi_0\rangle\langle\psi_0|\sigma_1)\,\xi\right] \in [-1,1]$ by noting that $\mathrm{Tr}\left[(|\psi_0\rangle\langle\psi_0| - \sigma_1|\psi_0\rangle\langle\psi_0|\sigma_1)\,\xi\right]$ is bounded between -1 and 1. This completes the proof of the proposition. □

2. Proof of Theorem 1

In this subsection, we analytically show that the lower bound of the variance scales polynomially with the number of parameters M when the perturbation is within $1/\sqrt{M}$ region.

Theorem 1 (Lower-bound on the loss variance, Formal)**.** *Assume a product initial state $\rho_0 = \bigotimes_{j=1}^{n}\rho_j$ with ρ_j and let us choose σ_1 such that $\mathrm{Tr}[\rho_0\sigma_1\rho_0\sigma_1] = 0$. Given that the Trotter time-step δt respects*

$$\frac{1}{2\lambda_{\max}} \geqslant \delta t\ , \tag{B63}$$

where $\lambda_{\max}$ is the largest eigenvalue of H, and the perturbation r obeys

$$\frac{3r_0^2\left(1-4\lambda_{\max}^2\delta t^2\right)}{2(M-1)\left(1-2\lambda_{\max}^2\delta t^2\right)} \geqslant r^2\ , \tag{B64}$$

with some r_0 such that $0<r_0<1$, then the variance of the loss function within the region $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$ is lower bounded as

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] \geqslant \frac{4r^4}{45}\left(1-\frac{4r^2}{7}\right)\left[(1-r_0)(1-4\lambda_{\max}^2\delta t^2)\right]^2\ . \tag{B65}$$

In addition, by choosing r such that $r \in \Theta\left(\frac{1}{\sqrt{M}}\right)$, we have

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] \in \Omega\left(\frac{1}{M^2}\right)\ . \tag{B66}$$

Proof. From Proposition 3, we first recall the variance bound in Eq. (B1) is of the form

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}[\mathcal{L}(\boldsymbol{\theta})] \geqslant\ (c_+ - k_+^2)\min_{\tilde{\xi}\in[-1,1]}\left(k_+^{M-1}\Delta_{\boldsymbol{\theta}^*} + (1-k_+^{M-1})\tilde{\xi}\right)^2\ , \tag{B67}$$

where we have

$$c_+ := \mathbb{E}_{\alpha\sim\boldsymbol{\mathcal{D}}(0,r)}[\cos^4\alpha]\ , \tag{B68}$$

$$k_+ := \mathbb{E}_{\alpha\sim\boldsymbol{\mathcal{D}}(0,r)}[\cos^2\alpha]\ , \tag{B69}$$

$$\Delta_{\boldsymbol{\theta}^*} := \mathrm{Tr}\big[(\rho_0 - \sigma_1\rho_0\sigma_1)U^\dagger\left(\boldsymbol{\theta}^*\right)\rho_{(\boldsymbol{\theta}^*,\delta t)}U\left(\boldsymbol{\theta}^*\right)\big]\ . \tag{B70}$$

Here σ_1 is the Pauli string associated with the first gate in the circuit $U(\boldsymbol{\theta})$ as defined in Eq. (4), $\rho_0 = |\psi_0\rangle\langle\psi_0|$ is an initial state before the time evolution and $\rho_{(\boldsymbol{\theta}^*,\delta t)} = e^{-iH\delta t}U(\boldsymbol{\theta}^*)\rho_0 U^\dagger(\boldsymbol{\theta}^*)e^{iH\delta t}$ with H being the underlying Hamiltonian of the quantum dynamics.

We now notice that if the perturbation r is chosen such that the following condition is satisfied

$$k_+^{M-1}\Delta_{\boldsymbol{\theta}^*} \geqslant 1 - k_+^{M-1}\ , \tag{B71}$$

then $\tilde{\xi} = -1$ minimises the lower bound which leads to

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] \geqslant (c_+ - k_+^2)\left(k_+^{M-1}\Delta_{\boldsymbol{\theta}^*} - (1-k_+^{M-1})\right)^2 \tag{B72}$$

$$= (c_+ - k_+^2)\left(k_+^{M-1}\,\mathrm{Tr}\left[(\rho_0 - \sigma_1\rho_0\sigma_1)\,U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\right] - (1-k_+^{M-1})\right)^2 \tag{B73}$$

$$= (c_+ - k_+^2)\left(k_+^{M-1}\left(F\left(\rho_{(\boldsymbol{\theta}^*,0)},\rho_{(\boldsymbol{\theta}^*,\delta t)}\right) - \mathrm{Tr}\left[U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}\right]+1\right)-1\right)^2\ , \tag{B74}$$

where $F(\rho,\rho') = \mathrm{Tr}[\rho\rho']$ is the fidelity between two pure states ρ and ρ', and

$$\rho_{(\boldsymbol{\theta}^*,\delta t)} = |\psi(\boldsymbol{\theta}^*,\delta t)\rangle\langle\psi(\boldsymbol{\theta}^*,\delta t)| = e^{-iH\delta t}U(\boldsymbol{\theta}^*)\rho_0U^\dagger(\boldsymbol{\theta}^*)e^{iH\delta t}\ . \tag{B75}$$

We note that the condition in Eq. (B71) can be equivalently expressed as

$$k_+^{M-1} \geqslant \frac{1}{1+\Delta_{\boldsymbol{\theta}^*}} = \frac{1}{1+\mathrm{Tr}\left[\left(\rho_0 - \sigma_1\rho_0\sigma_1\right)U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\ \right]}\ , \tag{B76}$$

where we explicitly expand $\Delta_{\boldsymbol{\theta}^*}$.

Crucially, for the majority of the rest of the proof, we aim to show that the condition in Eq. (B76) is satisfied if the perturbation is chosen such that

$$\frac{3r_0^2\left(1-4\lambda_{\max}^2\delta t^2\right)}{2(M-1)\left(1-2\lambda_{\max}^2\delta t^2\right)} \geqslant r^2\ , \tag{B77}$$

where r_0 is some constant within the range $0 < r_0 < 1$. In order to prove this, we first note the following bound of k_+^{M-1} which follows as

$$k_+^{M-1} = \left(\frac{1}{2r}\int_{-r}^{r} d\alpha\cos^2(\alpha)\right)^{M-1} \tag{B78}$$

$$= \left(\frac{1}{2}+\frac{\sin(2r)}{4r}\right)^{M-1} \tag{B79}$$

$$\geqslant \left(1-\frac{r^2}{3}\right)^{M-1} \tag{B80}$$

$$\geqslant 1-\frac{(M-1)r^2}{3} \tag{B81}$$

$$> 1-\frac{(M-1)r^2}{3r_0^2}\ , \tag{B82}$$

where the first inequality is by directly expanding the base and keeping only the second order term, the second inequality is due to Bernoulli's inequality and finally the last inequality holds because $0 < r_0 < 1$. We will come back to this inequality soon.

Now, the term $\mathrm{Tr}\left[\left(\rho_0 - \sigma_1\rho_0\sigma_1\right)U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\ \right]$ can be bounded as follows. Since $\rho_0 = \bigotimes_{j=1}^n \rho_j$ is a product state, we can choose σ_1 to be a single rotation around the axis such that $\mathrm{Tr}[\rho_0\sigma_1\rho_0\sigma_1] = 0$ [3], which leads to

$$\mathrm{Tr}\left[\rho_{(\boldsymbol{\theta}^*,0)}U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)\right] = \mathrm{Tr}\left[\rho_0\sigma_1\rho_0\sigma_1\right] = 0\ . \tag{B83}$$

Then, we construct an orthonormal basis $\{|\phi_i\rangle\langle\phi_i|\}_{i=1}^{2^n}$ such that

$$|\phi_1\rangle\langle\phi_1| = \rho_{(\boldsymbol{\theta}^*,0)}\ , \tag{B84}$$

$$|\phi_2\rangle\langle\phi_2| = U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)\ , \tag{B85}$$

and the rest are some other orthornormal states necessary to complete the basis. With this basis, we have the following bound

$$\mathrm{Tr}\left[\left(\rho_0 - \sigma_1\rho_0\sigma_1\right)U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\ \right] = F\left(\rho_{(\boldsymbol{\theta}^*,0)},\rho_{(\boldsymbol{\theta}^*,\delta t)}\right) - \mathrm{Tr}\left[|\phi_2\rangle\langle\phi_2|\rho_{(\boldsymbol{\theta}^*,\delta t)}\right] \tag{B86}$$

$$\geqslant F\left(\rho_{(\boldsymbol{\theta}^*,0)},\rho_{(\boldsymbol{\theta}^*,\delta t)}\right) - \sum_{i=2}^{2^n}\mathrm{Tr}\left[|\phi_i\rangle\langle\phi_i|\rho(\boldsymbol{\theta}^*,\delta t)\right] \tag{B87}$$

$$= 2F\left(\rho_{(\boldsymbol{\theta}^*,0)},\rho_{(\boldsymbol{\theta}^*,\delta t)}\right) - 1 \tag{B88}$$

$$\geqslant 1-4\lambda_{\max}^2\delta t^2\ , \tag{B89}$$

where the first equality is by writing the first term in the fidelity form and writing the second term in $|\phi_2\rangle\langle\phi_2|$ in Eq. (B85), in the first inequality we include terms corresponding to other basis (which holds since $\mathrm{Tr}[\rho|\phi_i\rangle\langle\phi_i|] \geqslant 0$

[3] For example, consider the all-zero basis state as an initial state $\rho_0 = |00...0\rangle\langle 00...0|$. We can pick the first generator as $\sigma_1 = X_1$.

for any ρ and $|\phi_i\rangle\langle\phi_i|$). Next, the second equality is from the completeness of the basis $\sum_{i=1}^{2^n}|\phi_i\rangle\langle\phi_i| = \mathbb{1}$, the last inequality is due to Lemma 5 with $\lambda_{\max}$ being the largest eigenvalue of H.

We note that in order for the lower bound in Eq. (B89) to be informative it is required that $1 \geqslant 4\lambda_{\max}^2\delta t^2$. Up on rearranging, this leads to the constraint on the time-step as

$$\frac{1}{2\lambda_{\max}} \geqslant \delta t \ , \tag{B90}$$

which is the condition specified in Eq. (B63). By assuming that the time-step satisfying the aforementioned constrain, we now proceed from Eq. (B89) by adding 1 to both sides and rearranging the terms which leads to

$$\frac{1}{2-4\lambda_{\max}^2\delta t^2} \geqslant \frac{1}{1+\mathrm{Tr}\left[\left(\rho_0-\sigma_1\rho_0\sigma_1\right)U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\ \right]} \ . \tag{B91}$$

We remark that the right-hand side of Eq. (B91) appears in the condition in Eq. (B76).

We are now ready to put everything together. Importantly, the condition in Eq. (B76) is satisfied if we enforce the left-hand side of Eq. (B82) to be larger than the right-hand side of Eq. (B91). That is, we have $k_+^{M-1} \geqslant \frac{1}{1+\mathrm{Tr}\left[\left(\rho_0-\sigma_1\rho_0\sigma_1\right)U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}U(\boldsymbol{\theta}^*)\ \right]}$ to be true if the following holds

$$1-\frac{(M-1)r^2}{3r_0^2} \geqslant \frac{1}{2-4\lambda_{\max}^2\delta t^2} \ . \tag{B92}$$

By rearranging the inequality in Eq. (B92), we have the perturbation regime of r to be Eq. (B77) as previously stated.

The last step is to bound the variance when r satisfies Eq. (B77). the variance of the loss in Eq. (B74) can be bounded as

$$\begin{aligned}
\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}(\boldsymbol{\theta})\right] &\geqslant (c_+-k_+^2)\left[k_+^{M-1}\left(F\left(\rho_{(\boldsymbol{\theta}^*,0)},\rho_{(\boldsymbol{\theta}^*,\delta t)}\right)-\mathrm{Tr}\left[U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}\right]+1\right)-1\right]^2 && \text{(B93)}\\
&\geqslant (c_+-k_+^2)\left[k_+^{M-1}\left(2-4\lambda_{\max}^2\delta t^2\right)-1\right]^2 && \text{(B94)}\\
&\geqslant (c_+-k_+^2)\left[\left(1-\frac{(M-1)r^2}{3}\right)\left(2-4\lambda_{\max}^2\delta t^2\right)-1\right]^2 && \text{(B95)}\\
&\geqslant (c_+-k_+^2)\left[(1-r_0^2)(1-4\lambda_{\max}^2\delta t^2)\right]^2 && \text{(B96)}\\
&\geqslant \frac{4r^4}{45}\left(1-\frac{4r^2}{7}\right)\left[(1-r_0^2)(1-4\lambda_{\max}^2\delta t^2)\right]^2 \ , && \text{(B97)}
\end{aligned}$$

where the second inequality is due to Eq. (B89), the third inequality is by bounding k_+^{M-1} with Eq. (B81) and in the next inequality we explicitly use the perturbation regime of r in Eq. (B77). To reach the last inequality, we directly bound $c_+-k_+^2 = \frac{1}{2r}\int_{-r}^{r}d\alpha\cos^4(\alpha)-\left(\frac{1}{2r}\int_{-r}^{r}d\alpha\cos^2(\alpha)\right)^2 \geqslant \frac{4r^4}{45}-\frac{16r^6}{315}$ by expanding it in the series and keeping the terms which result in the lower bound.

□

We now comment on the assumption that an initial state ρ_0 is a product state and discuss a possible extension to an arbitrary initial state. In essence, the product state assumption is used in the proof above to ensure that the term $\Delta_{\boldsymbol{\theta}^*}$ in Eq. (B4) is non-vanishing (see Eq. (B83) to Eq. (B89)). However, we argue here that our results should hold more generally for arbitrary initial states as long as the first gate interacts non-trivially with the loss. In particular, this happens for a small enough Trotter time-step δt as long as the first gate does not rotate ρ_0 into a subspace that is fully parallel to itself.

To illustrate this, we can expand $e^{-iH\delta t}$ and keep only the leading order in δt with an arbitrary non-product initial state. Since ρ_0 is no longer limited to be a product state, the orthornormal basis construction where $U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)$ is chosen to be orthonormal to $\rho_{(\boldsymbol{\theta}^*,0)}$ (see Eq. (B83)) is no longer guaranteed. However, we can modify the steps slightly and decompose $U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)$ into a parellel and a perpendicular component i.e.,

$$U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*) = \left(a\left|\phi_1\right\rangle+b\left|\phi_2\right\rangle\right)\left(\left\langle\phi_1\right|a^*+\left\langle\phi_2\right|b^*\right) \ , \tag{B98}$$

where $|\phi_1\rangle\langle\phi_1| = \rho_{(\boldsymbol{\theta}^*,0)}$, $|\phi_2\rangle\langle\phi_2|$ is orthonormal to $\rho_{(\boldsymbol{\theta}^*,0)}$, a and b are coefficients in the parallel and orthogonal directions such that $|a|, |b| \leqslant 1$. Then we can use Taylor's series to expand

$$\begin{aligned}\mathrm{Tr}\left[U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1 U^\dagger(\boldsymbol{\theta}^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}\right] &= \mathrm{Tr}\left[(a|\phi_1\rangle + b|\phi_2\rangle)(\langle\phi_1| a^* + \langle\phi_2| b^*)\rho_{(\boldsymbol{\theta}^*,\delta t)}\right] && \text{(B99)}\\ &= \mathrm{Tr}\left[(a|\phi_1\rangle + b|\phi_2\rangle)(\langle\phi_1| a^* + \langle\phi_2| b^*) e^{-iH\delta t}|\phi_1\rangle\langle\phi_1| e^{iH\delta t}\right] && \text{(B100)}\\ &= |a|^2 + \delta t\left(iab^*\langle\phi_1| H|\phi_2\rangle - ia^*b\langle\phi_2| H|\phi_1\rangle\right) + \mathcal{O}\big(\delta t^2\big)\ , && \text{(B101)}\end{aligned}$$

where, for the purpose of demonstration, we are only interested in the leading order in δt. Therefore with this we have that the term $\Delta_{\boldsymbol{\theta}^*}$ is

$$\Delta_{\boldsymbol{\theta}^*} = (1-|a|^2) + \delta t\left(iab^*\langle\phi_1| H|\phi_2\rangle - ia^*b\langle\phi_2| H|\phi_1\rangle\right) + \mathcal{O}\big(\delta t^2\big)\ . \tag{B102}$$

Hence, for $|a| \in \Omega(1/\operatorname{poly}(n))$ (which is expected to hold when the first gate does not commute with ρ_0) and small Trotter time-step $\delta t \ll 1$, one can follow the same proof steps which then results in the polynomial scaling of the loss variance in the hypercube with r scaling polynomially.

Appendix C: Proof convexity

Theorem 2 (Approximate convexity of the landscape, Formal)**.** *For a time-step of size*

$$\delta t \leqslant \frac{\mu_{\min} + 2|\epsilon|}{16M\lambda_{\max}}\ , \tag{C1}$$

the loss landscape is ϵ-convex in a hypercube of width $2r_c$ around a previous optimum $\boldsymbol{\theta}^*$ i.e., $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$ such that

$$r_c \geqslant \frac{1}{M}\left(\frac{\mu_{\min} + 2|\epsilon|}{16M} - \lambda_{\max}\delta t\right)\ , \tag{C2}$$

where $\mu_{\min}$ is the minimal eigenvalue of the Fisher information matrix associated with the loss.

Proof. We first recall that the region of the loss function is ϵ-convex (i.e., Definition 1) if all eigenvalues of the Hessian matrix of the loss function i.e., $\mathcal{L}(\boldsymbol{\theta}) = 1 - F\left[U(\boldsymbol{\theta})\rho_0 U^\dagger(\boldsymbol{\theta}), \rho(\boldsymbol{\theta}^*, \delta t)\right]$ within the region are larger than $-|\epsilon|$, which can be re-expressed in terms of the fidelity as

$$\left[\nabla^2_{\boldsymbol{\theta}} F\left(U(\boldsymbol{\theta})\rho_0 U^\dagger(\boldsymbol{\theta}), \rho(\boldsymbol{\theta}^*, \delta t)\right)\right]_{\max} \leqslant |\epsilon|\ , \tag{C3}$$

for all $\boldsymbol{\theta} \in \boldsymbol{\mathcal{V}}(\theta^*, r)$ with $[A]_{\max}$ being the largest eigenvalue of the matrix A.

By using Taylor's expansion around $\boldsymbol{\theta}^*$ (see Theorem 4), the fidelity can be written in the form of

$$F(\boldsymbol{x}) = 1 - \sum_{i,j}\frac{x_i x_j}{4}\mathcal{F}_{ij}(\boldsymbol{0}) + \sum_{i,j,k}\frac{x_i x_j x_k}{6}\left(\frac{\partial^3 F(\boldsymbol{x})}{\partial x_i\partial x_j\partial x_k}\right)\bigg|_{\boldsymbol{x}=\boldsymbol{\nu}}\ , \tag{C4}$$

where we introduce the shorthand notation of the fidelity around this region as $F(\boldsymbol{x})$ with $\boldsymbol{x} = (\boldsymbol{\theta} - \boldsymbol{\theta}^*, \delta t)$, $\mathcal{F}_{ij}(\boldsymbol{0})$ are elements of the quantum fisher information at $\boldsymbol{x} = \boldsymbol{0}$, and the last term is the result of the Taylor's remainder theorem with $\boldsymbol{\nu} = c\boldsymbol{x}$ for some $c \in [0,1]$.

For convenience, we denote $\mathcal{A}_{ijk}(\boldsymbol{x}) = \frac{\partial^3 F(\boldsymbol{x})}{\partial x_i\partial x_j\partial x_k}$. This third derivative can be expressed as a nested commutator of the form (for $k > j > i$)

$$\mathcal{A}_{ijk}(\boldsymbol{x}) := \frac{\partial^3 F(\boldsymbol{x})}{\partial x_i\partial x_j\partial x_k} = \mathrm{Tr}\left[U^{(M+1,k)}i\left[U^{(k,j)}i\left[U^{(j,i)}i\left[U^{(i,0)}\rho_0 U^{(i,0)\dagger}, \sigma_i\right]U^{(j,i)\dagger}, \sigma_j\right]U^{(k,j)\dagger}, \sigma_k\right]U^{(M+1,k)\dagger}\rho_{(\boldsymbol{\theta}^*,0)}\right]\ , \tag{C5}$$

where $U(\boldsymbol{x}) = U^{(M+1,k)}U^{(k,j)}U^{(j,i)}U^{(i,0)}$ with $U^{(a,b)} = \prod_{l=a+1}^{b} e^{-ix_l\sigma_l}\widetilde{V}_l$ such that $\sigma_{M+1} := H$ and $\widetilde{V}_{M+1} = \mathbb{1}$. For clarification we emphasise that the notation $\sigma_{M+1} := H$ does *not* imply that $H^2 = \mathbb{1}$, H is still a general Hamiltonian, but rather this is just a way of simplifying the notation. That is, $U(\boldsymbol{x})$ is decomposed into 4 sections e.g., $U^{(i,0)}$ contains the part of $U(\boldsymbol{\theta})$ from the first gate to the i^{th} gate.

Now, we consider an element of $\nabla^2_{\boldsymbol{\theta}} F\left(\boldsymbol{x}\right)$ which can be obtained by explicitly differentiating $F(\boldsymbol{x})$ in Eq. (C4) with respect to the variational parameters (i.e., x_l and x_m cannot be δt)

$$\frac{\partial^2 F(\boldsymbol{x})}{\partial x_l \partial x_m} = -\frac{1}{2}\mathcal{F}_{lm}(\boldsymbol{0}) + \frac{1}{6}\widetilde{\mathcal{A}}_{lm}(\boldsymbol{\nu}) \ , \tag{C6}$$

with

$$\widetilde{\mathcal{A}}_{lm}(\boldsymbol{\nu}) = \sum_{i=1}^{M+1} x_i \left(\mathcal{A}_{lmi}(\boldsymbol{\nu}) + \mathcal{A}_{lim}(\boldsymbol{\nu}) + \mathcal{A}_{ilm}(\boldsymbol{\nu}) + \mathcal{A}_{mli}(\boldsymbol{\nu}) + \mathcal{A}_{mil}(\boldsymbol{\nu}) + \mathcal{A}_{iml}(\boldsymbol{\nu})\right) \ , \tag{C7}$$

where we remark that here the sum includes the time component δt.

Now, the largest eigenvalue of $\nabla^2_{\boldsymbol{\theta}} F\left(\boldsymbol{x}\right)$ can be bounded as

$$\left[\nabla^2_{\boldsymbol{\theta}} F\left(\boldsymbol{x}\right)\right]_{\max} \leqslant -\frac{1}{2}\left[\mathcal{F}(\boldsymbol{0})\right]_{\min} + \frac{1}{6}[\widetilde{\mathcal{A}}(\boldsymbol{\nu})]_{\max} \ , \tag{C8}$$

where we denote $[A]_{\min}$ as the smallest eigenvalue of the matrix A.

In order to bound $[\widetilde{\mathcal{A}}(\boldsymbol{\nu})]_{\max}$, we first consider the bound on $\mathcal{A}_{ilm}(\boldsymbol{\nu})$

$$\mathcal{A}_{ilm}(\boldsymbol{\nu}) \leqslant |\mathcal{A}_{ilm}(\boldsymbol{\nu})| \tag{C9}$$

$$\leqslant \left\| U^{(M+1,m)} i \left[U^{(m,l)} i \left[U^{(l,i)} i \left[U^{(i,0)} \rho_0 U^{(i,0)^\dagger}, \sigma_i \right] U^{(l,i)^\dagger}, \sigma_l \right] U^{(m,l)^\dagger}, \sigma_m \right] U^{(M+1,m)^\dagger} \right\|_\infty \left\| \rho_{(\boldsymbol{\theta}^*,0)} \right\|_1 \tag{C10}$$

$$\leqslant 2^3 \|\sigma_i\|_\infty \|\sigma_l\|_\infty \|\sigma_m\|_\infty \tag{C11}$$

$$= 8\|\sigma_i\|_\infty \ . \tag{C12}$$

Here the second inequality is due to Hölder's inequality. In the third inequality we use a few identities including (i) the one-norm of a pure state is 1, (ii) $\|UA\|_p = \|A\|_p$ for any unitary U, (iii) $\|i[A,B]\|_p = 2\|A\|_p\|B\|_p$ and lastly (iv) $\|AB\|_p \leqslant \|A\|_p\|B\|_p$. To reach the final equality, we recall that since x_l and x_m cannot be a time component δt, σ_l and σ_m are generators of the circuit which have $\|\sigma_l\|_\infty = \|\sigma_m\|_\infty = 1$.

We now bound the sum of the absolute of elements in a row of $\widetilde{\mathcal{A}}(\boldsymbol{\nu})$ as

$$\sum_{m=1}^{M} \left|\widetilde{\mathcal{A}}_{lm}(\boldsymbol{\nu})\right| \leqslant \sum_{m=1}^{M}\sum_{i=1}^{M+1} |x_i| \left(|\mathcal{A}_{lmi}(\boldsymbol{\nu})| + |\mathcal{A}_{lim}(\boldsymbol{\nu})| + |\mathcal{A}_{ilm}(\boldsymbol{\nu})| + |\mathcal{A}_{mli}(\boldsymbol{\nu})| + |\mathcal{A}_{mil}(\boldsymbol{\nu})| + |\mathcal{A}_{iml}(\boldsymbol{\nu})|\right) \tag{C13}$$

$$\leqslant 48 \sum_{m=1}^{M}\sum_{i=1}^{M+1} |x_i| \|\sigma_i\|_\infty \tag{C14}$$

$$\leqslant 48M\left(\lambda_{\max}\delta t + Mr\right) \tag{C15}$$

By invoking Proposition 2, the largest eigenvalue of the matrix can then be bounded as

$$[\widetilde{\mathcal{A}}(\boldsymbol{\nu})]_{\max} \leqslant 48M\left(\lambda_{\max}\delta t + Mr\right) \ . \tag{C16}$$

Finally, we can guarantee the region of ϵ-convexity (i.e., Eq. (C3)) by enforcing the following condition

$$-\frac{1}{2}\left[\mathcal{F}(\boldsymbol{0})\right]_{\min} + 8M\left(\lambda_{\max}\delta t + Mr\right) \leqslant |\epsilon| \ . \tag{C17}$$

Upon rearranging the terms, we have

$$r \leqslant \frac{1}{M}\left(\frac{\mu_{\min} + 2|\epsilon|}{16M} - \lambda_{\max}\delta t\right) \ . \tag{C18}$$

Indeed, this implies that *any* hypercube $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$ such that r satisfies Eq. (C18) is guaranteed to be approximately convex. Hence, we know that the total ϵ-convex region has to be at least of size $\frac{1}{M}\left(\frac{\mu_{\min}+2|\epsilon|}{16M} - \lambda_{\max}\delta t\right)$. More explicitly, by denoting r_c to be the length of the total ϵ-approximate convex region $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$, we have

$$r_c \geqslant \frac{1}{M}\left(\frac{\mu_{\min} + 2|\epsilon|}{16M} - \lambda_{\max}\delta t\right) \ . \tag{C19}$$

We note that the bound is only informative if the Trotter time-step respects

$$\delta t \leqslant \frac{\mu_{\min} + 2|\epsilon|}{16M\lambda_{\max}} \ . \tag{C20}$$

This completes the proof of the theorem. □

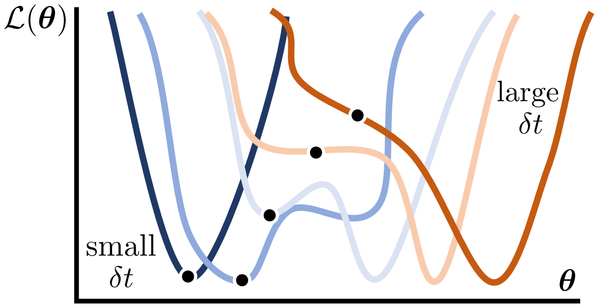


FIG. 7. **Adiabatic minima.** Here we show the adiabatic minima (highlighted in the black dots) as a function of the Trotter time-step δt. From dark blue to orange, we highlight how the loss function evolves with increasing δt. Indeed, when the time-step increases the adiabatic minima stops being the global minima. Then it turns into a saddle point and finally disappears to become a slope. As mentioned in the main text, when the adiabatic minima disappears it turns into a slope.

Appendix D: Adiabatic Moving Minima

In this section, we provide further analysis on the adiabatic moving minimum, including the proof of Theorem 3 and some some technical subtleties. We first recall the definition of the adiabatic minimum and also introduce a definition of the adiabatic shift.

Definition 2 (Adiabatic Minima)**.** *For any time δt in the range $[0, T]$, the function corresponding to the evolution of the adiabatic minima for some initial minimum $\boldsymbol{\theta}^*$, is a continuous function $\boldsymbol{\theta}_A(\delta t) \in C^\infty(\mathbb{R}, \mathbb{R}^m)$ such that $\boldsymbol{\theta}_A(0) = \boldsymbol{\theta}^*$ and*

$$\nabla_{\boldsymbol{\theta}} \mathcal{L}(\boldsymbol{\theta}_A(\delta t), \delta t) = \mathbf{0} \ . \tag{D1}$$

The adiabatic minimum at time δt is $\boldsymbol{\theta}_A(\delta t)$

Definition 4 (Adiabatic shift of the previous minima)**.** *The shift of the adiabatic minimum with respect to the previous optimal point is defined as*

$$\boldsymbol{\alpha}_A(\delta t) = \boldsymbol{\theta}_A(\delta t) - \boldsymbol{\theta}^* \ , \tag{D2}$$

and also respects

$$\nabla_{\boldsymbol{\alpha}} \mathcal{L}(\boldsymbol{\alpha}, \delta t)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(\delta t)} = \mathbf{0} \ , \tag{D3}$$

for any time δt.

Intuitively, the adiabatic function corresponds to the minima one would converge to by increasing δt infinitely slowly and minimizing $\mathcal{L}(\boldsymbol{\theta}, \delta t)$ by gradient descent with a very small learning rate. By analogy, one can imagine dropping a marble in the initial minima and then slowly modifying the landscape by increasing δt. The position of the marble would correspond to our adiabatic minima and in practice it is where we expect our algorithm to converge.

Up to this point, there are two caveats that we would like to highlight. First, this adiabatic minimum is not necessarily the global minimum (as discussed in Section III E - there could potentially be a jump in the global minimum). The other subtlety is that the existence of the adiabatic minimum is not always guaranteed for increasing δt. This is highlighted in Figure 7. While for a small Trotter time-step one intuitively expects to have the adiabatic minimum, it is not certain whether we have this for large Trotter time-steps. That is, the adiabatic function can cease to be continuous beyond T (and in practice we do not in general know what T is). Crucially, the discontinuity in the adiabatic minimum path implies that zero gradients now turn into some slopes. Hence, the lack of a continuous adiabatic minimum does not necessarily imply untrainability.

With these caveats in mind, we proceed under the assumption that the adiabatic minimum exists within the Trotter time-step of our interest. We first present Proposition 4 which shows that the shift in the adiabatic minimum can be bounded with the Trotter time-step.

Proposition 4. *Given a Trotter time-step of the current iteration δt and assuming that the adiabatic minimum exists within this time frame, the shift of the adiabatic minimum $\boldsymbol{\alpha}_A(\delta t)$ as defined in Definition 4 can be bounded as*

$$\|\boldsymbol{\alpha}_A(\delta t)\|_2 \leqslant \frac{2\sqrt{M}\lambda_{\max}\delta t}{\beta_A} \ , \tag{D4}$$

where M is the number of parameters, $\lambda_{\max}$ is the largest eigenvalue of the dynamic Hamiltonian H and $\beta_A = \frac{\dot{\boldsymbol{\alpha}}_A^T(\delta t)\left(\nabla^2_{\boldsymbol{\alpha}}\mathcal{L}(\boldsymbol{\alpha},\delta t)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(\delta t)}\right)\dot{\boldsymbol{\alpha}}_A(\delta t)}{\|\dot{\boldsymbol{\alpha}}_A(\delta t)\|_2^2}$.

Proof. We note that to improve readability of the proof it is more convenient here to use t to refer as a Trotter time-step (instead of δt as in other sections). We recall from Definition 4 that the adiabatic shift can be expressed as

$$\nabla_{\boldsymbol{\alpha}}\mathcal{L}(\boldsymbol{\alpha},t)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(t)} = \mathbf{0}\ , \tag{D5}$$

which holds for *any* t. For convenience, we denote $\nabla_{\boldsymbol{\alpha}_A}\mathcal{L} := \nabla_{\boldsymbol{\alpha}}\mathcal{L}(\boldsymbol{\alpha},t)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(t)}$. By a direct differentiation with respect to t, this leads to

$$\frac{d}{dt}\left(\nabla_{\boldsymbol{\alpha}_A}\mathcal{L}\right) = \partial_t\nabla_{\boldsymbol{\alpha}_A}\mathcal{L} + \left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A = \mathbf{0}\ , \tag{D6}$$

where we denote $\partial_t = \partial/\partial t$ and $\dot{\boldsymbol{\alpha}}_A = d\boldsymbol{\alpha}_A(t)/dt$. We remark that $\left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A$ is a matrix vector multiplication with $\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}$ a Hessian matrix evaluated at $\boldsymbol{\alpha}_A(t)$. By multiplying with $\frac{\dot{\boldsymbol{\alpha}}_A^T}{\|\dot{\boldsymbol{\alpha}}_A\|_2}$ from the left, we have

$$\frac{\dot{\boldsymbol{\alpha}}_A^T}{\|\dot{\boldsymbol{\alpha}}_A\|_2}\partial_t\nabla_{\boldsymbol{\alpha}_A}\mathcal{L} + \frac{\dot{\boldsymbol{\alpha}}_A^T\left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A}{\|\dot{\boldsymbol{\alpha}}_A\|_2^2}\|\dot{\boldsymbol{\alpha}}_A\|_2 = 0\ . \tag{D7}$$

For convenience, we denote $\beta_A := \dot{\boldsymbol{\alpha}}_A^T\left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A/\|\dot{\boldsymbol{\alpha}}_A\|_2^2$. By rearranging the terms, we can bound the norm of $\dot{\boldsymbol{\alpha}}_A(t)$ as

$$\begin{aligned}
\|\dot{\boldsymbol{\alpha}}_A(t)\|_2 &= \left\|-\frac{\dot{\boldsymbol{\alpha}}_A^T\partial_t\nabla_{\boldsymbol{\alpha}_A}\mathcal{L}}{\|\dot{\boldsymbol{\alpha}}_A\|_2\beta_A}\right\|_2 && \text{(D8)}\\
&\leqslant \frac{\|\partial_t\nabla_{\boldsymbol{\alpha}_A}\mathcal{L}\|_2}{\beta_A} && \text{(D9)}\\
&\leqslant \frac{\sqrt{M}\left|\partial_t\partial_{\alpha_A^{(i)}}\mathcal{L}\right|_{\max}}{\beta_A} && \text{(D10)}\\
&\leqslant \frac{2\sqrt{M}\lambda_{\max}}{\beta_A}\ , && \text{(D11)}
\end{aligned}$$

where the first inequality is due to Cauchy-Schwarz inequality, in the second inequality we expand the 2-norm out explicitly and take the largest value in the sum i.e., $\|\boldsymbol{a}\|_2 = \sqrt{\sum_{i=1}^M a_i^2} \leqslant \sqrt{M}|a_i|_{\max}$ with $\alpha_A^{(i)}$ being the i^{th} component of $\boldsymbol{\alpha}_A$. To reach the last inequality, we recall that the loss function is of the form $\mathcal{L}(\boldsymbol{\alpha},t) = 1 - \text{Tr}\left(e^{-iHt}\rho_{\boldsymbol{\theta}^*}e^{iHt}\rho_{\boldsymbol{\theta}}\right)$ where H is the dynamic Hamiltonian, $\rho_{\boldsymbol{\theta}^*}$ is the state corresponding to the solution of the previous iteration and $\rho_{\boldsymbol{\theta}}$ is the parametrized state that depends on $\boldsymbol{\alpha}$ and respects a parameter shift's rule. We can then bound the quantity of interest as

$$\begin{aligned}
\partial_t\partial_{\alpha_A^{(i)}}\mathcal{L} &= \frac{\partial}{\partial t}\left(\frac{\partial}{\partial\alpha^{(i)}}\mathcal{L}(\boldsymbol{\alpha},t)\right)\Bigg|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(t)} && \text{(D12)}\\
&= \frac{1}{2}\left(\frac{\partial}{\partial t}\mathcal{L}\left(\boldsymbol{\alpha}_A + \frac{\pi}{2}\hat{\alpha}_i\right) - \frac{\partial}{\partial t}\mathcal{L}\left(\boldsymbol{\alpha}_A - \frac{\pi}{2}\hat{\alpha}_i\right)\right) && \text{(D13)}\\
&= \frac{1}{2}\left(\text{Tr}\left(i[H, e^{-iHt}\rho_{\boldsymbol{\theta}^*}e^{iHt}]\rho_{\boldsymbol{\alpha}_{A,+}}\right) - \text{Tr}\left(i[H, e^{-iHt}\rho_{\boldsymbol{\theta}^*}e^{iHt}]\rho_{\boldsymbol{\alpha}_{A,-}}\right)\right) && \text{(D14)}\\
&\leqslant \left\|[H, e^{-iHt}\rho_{\boldsymbol{\theta}^*}e^{iHt}]\right\|_\infty && \text{(D15)}\\
&\leqslant 2\lambda_{\max}\ , && \text{(D16)}
\end{aligned}$$

where the second equality is due to a parameter shift's rule, in the third equality we perform the direct differentiation with t and denote $\boldsymbol{\alpha}_{A,+} = \boldsymbol{\alpha}_A + \frac{\pi}{2}\hat{\alpha}_i$ as well as $\boldsymbol{\alpha}_{A,-} = \boldsymbol{\alpha}_A - \frac{\pi}{2}\hat{\alpha}_i$. The first inequality is due to the triangle inequality followed by the Hölder's inequality with the fact that $\|\rho\|_1 = 1$ for any pure quantum state ρ. In the last inequality, we use $\|i[A,B]\|_p = 2\|A\|_p\|B\|_p$ and the unitary invariance of the p-norm $\|UA\|_p = \|A\|_p$ as well as $\|\rho\|_\infty = 1$ for any pure quantum state ρ.

Lastly, we can bound the shift of the adiabatic minimum as

$$\|\boldsymbol{\alpha}_A(t)\|_2 = \left\| \int_0^t \dot{\boldsymbol{\alpha}}_A(\tau) d\tau \right\|_2 \tag{D17}$$

$$\leqslant \int_0^t \|\dot{\boldsymbol{\alpha}}_A(\tau)\|_2 d\tau \tag{D18}$$

$$\leqslant \frac{2\sqrt{M}\lambda_{\max} t}{\beta_A} \,, \tag{D19}$$

which completes the proof.

□

Note that for the bound in Eq. D4 to be informative about the asymptotic scaling we require β_A to be at least polynomially small.

In order for the training to have convergence guarantees to the adiabatic minimum, we need to ensure that our time-step is small enough so that our *adiabatic minima* is inside of the trainable and convex regions. This is formalized in Theorem 3 which is presented in the main text and proved here.

Theorem 3 (Adiabatic minimum is within provably 'nice' region, Formal)**.** *If the time-step δt is chosen such that*

$$\delta t \leqslant \frac{\eta_0 \beta_A}{2M\lambda_{\max}} \,, \tag{D20}$$

with some small constant η_0, then the adiabatic minimum $\boldsymbol{\theta}_A(\delta t)$ is guaranteed to be within the non-vanishing gradient region (as per Theorem 1), and additionally, if δt is chosen such that

$$\delta t \leqslant \frac{\beta_A(\mu_{\min} + 2|\epsilon|)}{32\lambda_{\max} M^{5/2}\left(1 + \frac{\beta_A}{2M^{3/2}}\right)} \,. \tag{D21}$$

then the adiabatic minimum $\boldsymbol{\theta}_A(\delta t)$ is guaranteed to be within the ϵ-convex region (as per Theorem 2) where

$$\beta_A := \frac{\dot{\boldsymbol{\theta}}_A^T(\delta t)\left(\nabla^2_{\boldsymbol{\theta}} \mathcal{L}(\boldsymbol{\theta})\big|_{\boldsymbol{\theta}=\boldsymbol{\theta}_A(\delta t)}\right)\dot{\boldsymbol{\theta}}_A(\delta t)}{\|\dot{\boldsymbol{\theta}}_A(\delta t)\|_2^2} \tag{D22}$$

corresponds to the second derivative of the loss in the direction in which the adiabatic minimum moves.

Proof. From Proposition 4 and the norm inequality, the adiabatic minimum follows

$$\|\boldsymbol{\alpha}_A(\delta t)\|_\infty \leqslant \|\boldsymbol{\alpha}_A(\delta t)\|_2 \leqslant \frac{2\sqrt{M}\lambda_{\max}\delta t}{\beta_A} \,. \tag{D23}$$

What we want now is to incorporate the conditions of the regions of interest. That is, by fine-tuning δt, we want a guarantee that the new minimum is within (i) the non-vanishing gradient region and (ii) the convex region.

For (i) the non-vanishing gradient region, we recall from the formal version of Theorem 1 that given the Trotter time-step bounded as $\delta t \leqslant 1/2\lambda_{\max}$, the hypercube of width $2r$ has the substantial non-vanishing gradients when r follows

$$r = \frac{\eta_0}{\sqrt{M}} \,, \tag{D24}$$

with some constant η_0. Then, it is sufficient to have the guarantee that the adiabatic minimum is inside this region by imposing

$$\|\boldsymbol{\alpha}_A(\delta t)\|_\infty \leqslant \frac{2\sqrt{M}\lambda_{\max}\delta t}{\beta_A} \leqslant \frac{\eta_0}{\sqrt{M}} \,, \tag{D25}$$

which leads to

$$\delta t \leqslant \frac{\eta_0 \beta_A}{2M\lambda_{\max}} \,. \tag{D26}$$

For (ii) the convex region, from Theorem 2, recall that given $\delta t \leqslant \frac{\mu_{\min}+2|\epsilon|}{16M\lambda_{\max}}$, we have an ϵ-convex hypercube region of width $2r_c$ such that

$$r_c \geqslant \frac{1}{M}\left(\frac{\mu_{\min}+2|\epsilon|}{16M} - \lambda_{\max}\delta t\right) \, . \tag{D27}$$

Therefore, it is sufficient to guarantee that the adiabatic minimum is inside this convex region by imposing

$$\|\boldsymbol{\alpha}_A(\delta t)\|_\infty \leqslant \frac{2\sqrt{M}\lambda_{\max}\delta t}{\beta_A} \leqslant \frac{1}{M}\left(\frac{\mu_{\min}+2|\epsilon|}{16M} - \lambda_{\max}\delta t\right) \leqslant r_c \, . \tag{D28}$$

Upon rearranging the terms, the time-step is bounded as

$$\delta t \leqslant \frac{\beta_A(\mu_{\min}+2|\epsilon|)}{32\lambda_{\max}M^{5/2}\left(1+\frac{\beta_A}{2M^{3/2}}\right)} \, . \tag{D29}$$

We remark that this bound in Eq. (D29) is much tighter than the bound in Theorem 2 (specified above). That is, to have such a guarantee, δt is relatively shorter.

□

Appendix E: Imaginary Time Evolution

1. Framework

The variational imaginary time evolution can be used to prepare ground states and thermal states [69–72]. In this section, we focus on a variational Trotter compression version of imaginary time evolution [36]. Most steps of the algorithm are identical to the real-time version described in the main text except we substitute $\delta t \to i\delta\tau$. This leads to $U = e^{i\delta t H} \to \mathcal{U} = e^{-\delta\tau H}$. One key technicality is to add a constraint such that the state after the evolution is forced to be normalised. That is, we have

$$|\psi_{\delta\tau}\rangle = \frac{1}{\sqrt{Z}} e^{-\delta\tau H}|\psi\rangle \tag{E1}$$

where $Z = \langle\psi| e^{-2\tau H}|\psi\rangle$. We remark that $|\psi_{\delta\tau}\rangle$ is now a valid *pure* quantum state and thus there is a unitary that prepares it. To have any chance of preparing the ground state via imaginary time evolution the initial state $|\psi\rangle$ must have a non-vanishing overlap with the ground state. If the initial state is instead a maximally entangled state, and imaginary time evolution is applied to only half the Bell state, then this approach can be used to prepare a thermal double field state (and thereby a thermal state). However, in what follows we will focus on ground state preparation.

In the variational Trotter compression approach for imaginary time evolution, one aims to iteratively learn $|\psi_{\delta\tau}\rangle$ with a parametrized quantum circuit $U(\boldsymbol{\theta})$ (with parameters initialized around the optimal parameter values obtained from the previous iteration). More explicitly, the loss function at each iteration is of the form

$$\mathcal{L}_{\text{ITE}}(\boldsymbol{\theta}) = \text{Tr}\left[U(\boldsymbol{\theta})\rho U^\dagger(\boldsymbol{\theta})\frac{1}{Z}e^{-\delta\tau}U(\boldsymbol{\theta}^*)\rho U^\dagger(\boldsymbol{\theta}^*)e^{-\delta\tau}\right] \, , \tag{E2}$$

where $\boldsymbol{\theta}^*$ are the optimal parameters from the previous iteration. For details on how to compute this loss in practise see Ref. [36]. We further suppose that the parametrised quantum circuit is of the same form used in the real-time case i.e.,

$$U(\boldsymbol{\theta}) = \prod_{i=1}^{M} V_i U_i(\theta_i) \tag{E3}$$

where $\{V_i\}_{i=1}^M$ are a set of fixed unitary matrices, $\left\{U_i(\theta_i) = e^{-i\theta_i\sigma_i}\right\}_{i=1}^M$, are the parameter-dependant rotations, and $\{\sigma_i\}_{i=1}^M$ is a set of gate generators such that $\sigma_i^2 = \mathbb{1}$ e.g., Pauli strings on n qubits. Crucially, it is natural to consider the parameter initialization around $\boldsymbol{\theta}^*$ i.e.,

$$\boldsymbol{\theta} \sim \boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*, r) \, , \tag{E4}$$

with r being some small perturbation.

2. Summary of analytical results for imaginary time evolution

Here we summarize analytical results similar to those obtained for the real time evolution scenario. These include the existence of the non-vanishing gradient region with the warm-start initialization, the guarantee of the approximate convex region as well as the analysis on the adiabatic minimum. We note that the derivations of these results follow the same steps as in the case of the real-time evolution and are provided in Appendix E 3 for the completeness.

First, we show that the region around the optimal solution of the previous iteration exhibits substantial gradients. More precisely, the following theorem demonstrates the polynomial large variance of the loss function within in a small hypercube around the starting point. This theorem is similar to Theorem 1 (as discussed in Section III B of the main text).

Theorem 4 (Lower-bound on the loss variance for imaginary time evolution, Informal)**.** *Assume a product initial state $\rho_0 = \bigotimes_{j=1}^{n} \rho_j$ with ρ_j and let us choose σ_1 such that $\mathrm{Tr}[\rho_0\sigma_1\rho_0\sigma_1] = 0$. Given that the imaginary Trotter time-step scales as $\delta\tau \leqslant \frac{1}{\sqrt{24}\lambda_{\max}}$ where $\lambda_{\max}$ is the largest eigenvalue of H and we consider a hypercube of width $2r$ such that*

$$r = \Theta\left(\frac{1}{\sqrt{M}}\right) , \tag{E5}$$

the variance at any iteration of the variational compression algorithm is lower bounded as

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})\right] \in \Omega\left(\frac{1}{M}\right) . \tag{E6}$$

Thus, for $M \in \mathcal{O}(\mathrm{poly}(n))$, then we have

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})\right] \in \Omega\left(\frac{1}{\mathrm{poly}(n)}\right) . \tag{E7}$$

Next, we can ensure that for a sufficiently small time-step the loss landscape around the optimal solution of the previous iteration is $|\epsilon|$-convex. We refer the readers to Appendix A 3 for the definition of the $|\epsilon|$-convexity. This result is an imaginary time evolution version of Theorem 2 discussed in Section III C.

Theorem 5 (Approximate convexity of the landscape for imaginary time evolution, Informal.)**.** *For a time-step of size*

$$\delta\tau \in \mathcal{O}\left(\frac{\mu_{\min} + 2|\epsilon|}{M\lambda_{\max}}\right) \tag{E8}$$

the loss landscape is ϵ-convex in a hypercube of width $2r_c$ around a previous optimum $\boldsymbol{\theta}^*$ i.e., $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$ such that

$$r_c \in \Omega\left(\frac{\mu_{\min} + 2|\epsilon|}{16M^2} - 3\lambda_{\max}\delta\tau\right) \tag{E9}$$

where $\mu_{\min}$ is the minimal eigenvalue of the Fisher information matrix associated with the loss at $\boldsymbol{\theta}^*$.

A similar result on the adiabatic minimum in Theorem 3 can also be analytically obtained. Assuming the adiabatic minimum exists within our time interval of interest, we present below the scaling of imaginary time-step such that the adiabatic minimum is in the region with substantial gradients and in the convex region. We refer the readers to Section III D and Appendix D for the refresher of the adiabatic minimum.

Theorem 6 (Adiabatic minimum is within provably 'nice' region for imaginary time evolution, Informal)**.** *If the imaginary time-step $\delta\tau$ is chosen such that*

$$\delta\tau \in \mathcal{O}\left(\frac{\beta_A}{M\lambda_{\max}}\right) , \tag{E10}$$

then the adiabatic minimum $\boldsymbol{\theta}_A(\delta\tau)$ is guaranteed to be within the non-vanishing gradient region (as per Theorem 4), and additionally, if $\delta\tau$ is chosen such that

$$\delta\tau \in \mathcal{O}\left(\frac{\beta_A(\mu_{\min} + 2|\epsilon|)}{M^{5/2}\lambda_{\max}}\right) \tag{E11}$$

then the adiabatic minimum $\boldsymbol{\theta}_A(\delta\tau)$ is guaranteed to be within the ϵ-convex region (as per Theorem 5) where

$$\beta_A := \frac{\dot{\boldsymbol{\theta}}_A^T(\delta\tau)\left(\nabla^2_{\boldsymbol{\theta}}\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})\big|_{\boldsymbol{\theta}=\boldsymbol{\theta}_A(\delta\tau)}\right)\dot{\boldsymbol{\theta}}_A(\delta\tau)}{\|\dot{\boldsymbol{\theta}}_A(\delta\tau)\|_2^2} \tag{E12}$$

corresponds to the second derivative of the loss in the direction in which the adiabatic minimum moves.

Finally, it is crucial to note that the discussion about the minimum jumps and the potential existence of the fertile valley in Section III E is also applicable to imaginary time evolution.

3. Proof of analytical results

In this section, we analytically derive the analytical results presented in the previous sub-section. Again, these derivations are identical to the ones presented in Appendix B, Appendix C and Appendix D. We present them again here for completeness and the readers are also encouraged to look at those relevant appendices.

a. Bound on the variance of the landscape: Proof of Theorem 4

First, we introduce the equivalent version of Lemma 5 for imaginary time evolution.

Lemma 7. *The fidelity between two pure states ρ and $\rho_\tau = \frac{1}{Z}e^{-H\tau}\rho e^{-H\tau}$ with $Z = \mathrm{Tr}\left(e^{-H\tau}\rho e^{-H\tau}\right)$ can be upper bounded as*

$$F\left[\rho, \rho_\tau\right] \geqslant 1 - 12\lambda_{\max}^2\tau^2 \tag{E13}$$

where $\lambda_{\max}$ is the largest eigenvalue of H.

Proof. First, the derivative of the loss function with respect to time can be written as

$$\frac{d\rho_\tau}{dt} = -\{\rho_\tau, H\} + 2\,\mathrm{Tr}(H\rho_\tau)\rho_\tau\ , \tag{E14}$$

where $\{\cdot,\cdot\}$ is an anti-commutator.

Now we can use a Taylor's expansion around $\tau = 0$, and then the fidelity is of the form

$$F\left[\rho, \rho_\tau\right] = 1 + \frac{\tau^2}{2}\left(\frac{d^2F\left[\rho,\rho_\tau\right]}{d\tau^2}\right)\Bigg|_{\tau=\tau'} \tag{E15}$$

where the zero order term is 1, the first order term is zero by a direct computation and the second order term is evaluated at $\tau' \in [0,\tau]$ by Taylor's remainder (see Theorem 4). Thus we can bound the second derivative as follows.

$$\begin{aligned}\left(\frac{d^2F\left[\rho,\rho_\tau\right]}{d\tau^2}\right)\Bigg|_{\tau=\tau'} &= 2\mathrm{Re}\left[\mathrm{Tr}\left(\rho\rho_\tau H^2\right)\right] + 2\,\mathrm{Tr}(\rho H\rho_\tau H) - 8\,\mathrm{Tr}(H\rho_\tau)\mathrm{Re}[\mathrm{Tr}(\rho\rho_\tau H)] - 4\,\mathrm{Tr}\left(H^2\rho_\tau\right)\mathrm{Tr}(\rho\rho_\tau) \quad \text{(E16)}\\ &\quad + 8\,\mathrm{Tr}(\rho_\tau H)^2\,\mathrm{Tr}(\rho_\tau\rho)\\ &\leqslant 24\lambda_{\max}^2 \quad \text{(E17)}\end{aligned}$$

where in the inequality is due to (i) Hölder's inequality, (ii) $\|\rho\|_1 = 1$ for any pure quantum state ρ, (iii) $\|AB\|_p \leqslant \|A\|_p\|B\|_p$. More precisely, we used the following bounds to reach Eq. (E17)

$$\mathrm{Tr}\left(\rho\rho_\tau H^2\right) \leqslant ||\rho||_1||\rho_\tau H^2||_\infty \leqslant \lambda_{\max}^2 \tag{E18}$$

$$\mathrm{Tr}(\rho H\rho_\tau H) \leqslant ||\rho||_1||\rho_\tau H^2||_\infty \leqslant \lambda_{\max}^2 \tag{E19}$$

$$\mathrm{Tr}(\rho\rho_\tau H) \leqslant ||\rho||_1||\rho_\tau H||_\infty \leqslant \lambda_{\max} \tag{E20}$$

$$\mathrm{Tr}(H\rho_\tau) \leqslant \lambda_{\max} \tag{E21}$$

$$\mathrm{Tr}\left(H^2\rho_\tau\right) \leqslant \lambda_{\max}^2 \tag{E22}$$

$$\mathrm{Tr}(\rho_\tau\rho) \leqslant 1 \tag{E23}$$

Lastly, we can just substitute Eq. (E17) back to Eq. (E15) and obtain

$$F\left[\rho, \rho_\tau\right] \geqslant 1 - 12\tau^2\lambda_{\max}^2 \, , \tag{E24}$$

which completes the proof. □

We now present the formal version of Theorem 4 and provide a detailed proof.

Theorem 4 (Lower-bound on the loss variance for imaginary time evolution, Formal)**.** *Assume a product initial state $\rho_0 = \bigotimes_{j=1}^n \rho_j$ with ρ_j and let us choose σ_1 such that $\mathrm{Tr}[\rho_0\sigma_1\rho_0\sigma_1] = 0$. Given that the Trotter time-step $\delta\tau$ respects*

$$\frac{1}{\sqrt{24}\lambda_{\max}} \geqslant \delta\tau \, , \tag{E25}$$

where $\lambda_{\max}$ is the largest eigenvalue of H as well as the perturbation r follows

$$r^2 \leqslant \frac{3r_0^2(1 - 24\lambda_{\max}^2\delta\tau^2)}{2(M-1)(1 - 12\lambda_{\max}^2\delta\tau^2)} \, , \tag{E26}$$

with some r_0 such that $0 < r_0 < 1$, then the variance of the loss function within the region $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$ is lower bounded as

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})\right] \geqslant \frac{4r^2}{45}\left[(1 - r_0)(1 - 24\lambda_{\max}^2\delta\tau^2)\right]^2 \, . \tag{E27}$$

In addition, by choosing r such that $r \in \Theta\left(\frac{1}{\sqrt{M}}\right)$, then we have

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}\left[\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})\right] \in \Omega\left(\frac{1}{M}\right) \, . \tag{E28}$$

Proof. First, we note that Proposition 1 in Appendix B also applies for the imaginary time evolution. This is since all the proof steps in Proposition 1 hold when replacing $i\delta t \to \delta\tau$ and $\mathcal{L}(\boldsymbol{\theta}) \to \mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})$. Hence, this proof starts by recalling Proposition 1

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}[\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})] \geqslant \; (c_+ - k_+^2) \min_{\tilde{\xi}\in[-1,1]} \left(k_+^{M-1}\Delta_{\boldsymbol{\theta}^*} + (1 - k_+^{M-1})\tilde{\xi}\right)^2 , \tag{E29}$$

where the quantities in the bound above are

$$c_+ := \mathbb{E}_{\alpha\sim\boldsymbol{\mathcal{D}}(0,r)}[\cos^4\alpha] \, , \tag{E30}$$

$$k_+ := \mathbb{E}_{\alpha\sim\boldsymbol{\mathcal{D}}(0,r)}[\cos^2\alpha] \, , \tag{E31}$$

$$\Delta_{\boldsymbol{\theta}^*} := \mathrm{Tr}\big[(\rho_0 - \sigma_1\rho_0\sigma_1)U^\dagger\left(\boldsymbol{\theta^*}\right)\rho_{(\boldsymbol{\theta}^*,\delta\tau)}U\left(\boldsymbol{\theta^*}\right)\big] \, , \tag{E32}$$

$$\rho_{(\boldsymbol{\theta}^*,\delta\tau)} = \frac{1}{Z}e^{-H\delta\tau}U\left(\boldsymbol{\theta}^*\right)\rho_0 U^\dagger\left(\boldsymbol{\theta}^*\right)e^{-H\delta\tau} \, , \tag{E33}$$

$$Z = \mathrm{Tr}\left[e^{-H\delta\tau}U\left(\boldsymbol{\theta}^*\right)\rho_0 U^\dagger\left(\boldsymbol{\theta}^*\right)e^{-H\delta\tau}\right] \, . \tag{E34}$$

with σ_1 being the first (non commuting) gate of the ansatz and ρ_0 is the initial state.

Importantly, we notice that if the perturbation r is chosen such that the following condition is satisfied

$$k_+^{M-1}\Delta_{\boldsymbol{\theta}^*} \geqslant (1 - k_+^{M-1}) \tag{E35}$$

then $\hat{\xi} = -1$ minimises the variance lower bound in Eq. (E29) which leads to

$$\mathrm{Var}_{\boldsymbol{\theta}\sim\boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*,r)}[\mathcal{L}(\boldsymbol{\theta})] \geqslant \; (c_+ - k_+^2)\left(k_+^{M-1}(\Delta_{\boldsymbol{\theta}^*} + 1) - 1\right)^2 , \tag{E36}$$

Now, we focus now on $\Delta_{\boldsymbol{\theta}^*}$ which can be expressed as

$$\begin{aligned}\Delta_{\boldsymbol{\theta}^*} :=& \,\mathrm{Tr}\big[(\rho_0 - \sigma_1\rho_0\sigma_1)U^\dagger\left(\boldsymbol{\theta^*}\right)\rho_{(\boldsymbol{\theta}^*,\delta\tau)}U\left(\boldsymbol{\theta^*}\right)\big] & \text{(E37)}\\ =& F(\rho_{(\boldsymbol{\theta}^*,0)}, \rho_{(\boldsymbol{\theta}^*,\delta\tau)}) - \mathrm{Tr}\left[\sigma_1\rho_0\sigma_1 U^\dagger\left(\boldsymbol{\theta^*}\right)\rho_{(\boldsymbol{\theta}^*,\delta\tau)}U\left(\boldsymbol{\theta^*}\right)\right] & \text{(E38)}\end{aligned}$$

where we have the fidelity $F(\rho_{(\boldsymbol{\theta}^*,0)}, \rho_{(\boldsymbol{\theta}^*,\delta\tau)}) = \mathrm{Tr}\big(\rho_{(\boldsymbol{\theta}^*,0)}\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\big)$. Since $\rho_0 = \bigotimes_{j=1}^n \rho_j$ is a product state, we can choose σ_1 to be a single rotation around the axis such that $\mathrm{Tr}[\rho_0\sigma_1\rho_0\sigma_1] = 0$ which also implies

$$\mathrm{Tr}\left[\rho_{(\boldsymbol{\theta}^*,0)}U(\boldsymbol{\theta}^*)\sigma_1\rho_0\sigma_1U^\dagger(\boldsymbol{\theta}^*)\right] = \mathrm{Tr}\left[\rho_0\sigma_1\rho_0\sigma_1\right] = 0\,. \tag{E39}$$

Then, we define an orthonormal $\{\phi_i := |\phi_i\rangle\langle\phi_i|\}_{i=1}^{2^n}$ basis as

$$\phi_1 = \rho_{(\boldsymbol{\theta}^*,0)}\ , \tag{E40}$$

$$\phi_2 = U\left(\boldsymbol{\theta}^*\right)\sigma_1\rho_0\sigma_1U^\dagger\left(\boldsymbol{\theta}^*\right)\ , \tag{E41}$$

and other $\{\phi_i\}$ are necessary orthornormal states to complete the basis. We can upper bound the second term on the right hand side of Eq. (E37) as

$$\mathrm{Tr}\left[\sigma_1\rho_0\sigma_1U^\dagger\left(\boldsymbol{\theta}^*\right)\rho_{(\boldsymbol{\theta}^*,\delta\tau)}U\left(\boldsymbol{\theta}^*\right)\right] = \mathrm{Tr}\left(\phi_2\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\right) \tag{E42}$$

$$\leqslant \sum_{i=2}^{2^n}\mathrm{Tr}\left(\phi_i\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\right) \tag{E43}$$

$$= \mathrm{Tr}\left[(\mathbb{1}-\phi_1)\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\right] \tag{E44}$$

$$= F(\rho_{(\boldsymbol{\theta}^*,0)}, \rho_{(\boldsymbol{\theta}^*,\delta\tau)}) - 1 \tag{E45}$$

where in the inequality we add terms corresponding to other basis which holds because the trace of positive matrices is positive and in Eq. (E44) we use the fact that $\sum_i \phi_i = \mathbb{1}$.

With this we can lower-bound $\Delta_{\boldsymbol{\theta}^*}$ as follows

$$\Delta_{\boldsymbol{\theta}^*} \geqslant 2F(\rho_{(\boldsymbol{\theta}^*,0)}, \rho_{(\boldsymbol{\theta}^*,\delta\tau)}) - 1 \tag{E46}$$

$$\geqslant 1 - 24\lambda_{\mathrm{max}}^2\delta\tau^2 \tag{E47}$$

where we have used Lemma 7 in the last inequality. We remark that the bound in Eq. (E47) can be equivalently expressed as

$$\frac{1}{2-24\lambda_{\mathrm{max}}^2\delta\tau^2} \geqslant \frac{1}{1+\Delta_{\boldsymbol{\theta}^*}}\,. \tag{E48}$$

Importantly, for this bound to be informative (i.e., non-negative), we require the constrain on $\delta\tau$ as

$$\frac{1}{\sqrt{24}\lambda_{\mathrm{max}}} \geqslant \delta\tau\,. \tag{E49}$$

In this next step, we show how the condition in Eq. (E35) can be fulfilled. We note that the condition can be equivalently expressed as

$$k_+^{M-1} \geqslant \frac{1}{1+\Delta_{\boldsymbol{\theta}^*}} \tag{E50}$$

We consider the bound of k_+^{M-1} which follows as

$$k_+^{M-1} = \left(\frac{1}{2r}\int_{-r}^{r} d\alpha\cos^2(\alpha)\right)^{M-1} \tag{E51}$$

$$= \left(\frac{1}{2}+\frac{\sin(2r)}{4r}\right)^{M-1} \tag{E52}$$

$$\geqslant \left(1-\frac{r^2}{3}\right)^{M-1} \tag{E53}$$

$$\geqslant 1-\frac{(M-1)r^2}{3} \tag{E54}$$

$$> 1-\frac{(M-1)r^2}{3r_0^2}\ , \tag{E55}$$

where the first inequality is by directly expanding the base and keeping only the second order term, the second inequality is due to Bernoulli's inequality and finally the last inequality holds because $0 < r_0 < 1$.

With this we can see that the condition in Eq. (E50) holds if the right hand side of Eq. (E55) is larger then the left hand side of Eq. (E48) i.e.,

$$1 - \frac{(M-1)r^2}{3r_0^2} > \frac{1}{2 - 24\lambda_{\max}^2 \delta\tau^2} \quad \Rightarrow \quad k_+^{M-1} \geqslant \frac{1}{1 + \Delta_{\boldsymbol{\theta}^*}} \ . \tag{E56}$$

By rearranging Eq. (E56), we find the bound on the perturbation r as

$$r^2 \leqslant \frac{3r_0^2(1 - 24\lambda_{\max}^2\delta\tau^2)}{2(M-1)(1 - 12\lambda_{\max}^2\delta\tau^2)} \tag{E57}$$

.

By enforcing the condition of the perturbation in Eq. (E57), the variance can be lower-bounded further from Eq. (E36) as

$$\begin{aligned}
\mathrm{Var}_{\boldsymbol{\theta} \sim \boldsymbol{\mathcal{D}}(\boldsymbol{\theta}^*, r)}[\mathcal{L}(\boldsymbol{\theta})] \geqslant & \, (c_+ - k_+^2)\left[k_+^{M-1}(\Delta_{\boldsymbol{\theta}^*} + 1) - 1\right]^2 & \text{(E58)} \\
\geqslant & (c_+ - k_+^2)\left[\left(1 - \frac{(M-1)r^2}{3}\right)(2 - 24\lambda_{\max}^2\delta\tau^2) - 1\right]^2 & \text{(E59)} \\
\geqslant & \, (c_+ - k_+^2)\left[(1 - r_0^2)(1 - 24\lambda_{\max}^2\delta\tau^2)\right]^2 & \text{(E60)} \\
\geqslant & \frac{4r^4}{45}\left[(1 - r_0^2)(1 - 24\lambda_{\max}^2\delta\tau^2)\right]^2 \ , & \text{(E61)}
\end{aligned}$$

where the second inequality is due to Eq. (E47) and Eq. (E54), the third inequality is by the condition on r in Eq. (E57). To reach the last inequality, we directly bound $c_+ - k_+^2 = \frac{1}{2r}\int_{-r}^{r} d\alpha \cos^4(\alpha) - \left(\frac{1}{2r}\int_{-r}^{r} d\alpha \cos^2(\alpha)\right)^2 \geqslant \frac{4r^4}{45} - \frac{16r^6}{315}$ by expanding it in the series and keeping the terms which result in the lower bound. This completes the proof.

□

b. Convexity guarantee: Proof of Theorem 5

We devote this subsection to prove Theorem 5 which shows the convexity of the loss landscape for imaginary time evolution.

Theorem 5 (Approximate convexity of the landscape for imaginary time evolution, Formal)**.** *Given that the dynamic imaginary time follows*

$$\delta\tau \leqslant \frac{\mu_{\min} + 2|\epsilon|}{48M\lambda_{\max}} \ , \tag{E62}$$

the loss landscape is ϵ-convex in a hypercube of width $2r_c$ around a previous optimum $\boldsymbol{\theta}^*$ i.e., $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$ such that

$$r_c \geqslant \frac{1}{M}\left(\frac{\mu_{\min} + 2|\epsilon|}{16M} - 3\lambda_{\max}\delta\tau\right) \tag{E63}$$

where $\mu_{\min}$ is the minimal eigenvalue of the Fisher information matrix associated with the loss.

Proof. We first recall that the region of the loss function is ϵ-convex (i.e., Definition 1) if all eigenvalues of the Hessian matrix within the region are larger than $-|\epsilon|$, which can be re-expressed in terms of the fidelity as

$$\left[\nabla_{\boldsymbol{\theta}}^2 F\left(U(\boldsymbol{\theta})\rho_0 U^\dagger(\boldsymbol{\theta}), \rho_{(\boldsymbol{\theta}^*, \delta\tau)}\right)\right]_{\max} \leqslant |\epsilon| \ , \tag{E64}$$

for all $\boldsymbol{\theta} \in \boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$.

By using Taylor's expansion around $\boldsymbol{\theta}^*$ and Taylor reminder theorem (explained in Appendix A 2), we can write the fidelity like

$$F(\boldsymbol{x}) = 1 - \sum_{i,j} \frac{x_i x_j}{4}\mathcal{F}_{ij}(\boldsymbol{0}) + \sum_{i,j,k} \frac{x_i x_j x_k}{6}\left(\frac{\partial^3 F(\boldsymbol{x})}{\partial x_i \partial x_j \partial x_k}\right)\Bigg|_{\boldsymbol{x} = \boldsymbol{\nu}} \ , \tag{E65}$$

where we introduce the shorthand notation of the fidelity around this region as $F(\boldsymbol{x})$ with $\boldsymbol{x} = (\boldsymbol{\theta} - \boldsymbol{\theta}^*, \delta\tau)$, $\mathcal{F}_{ij}(\mathbf{0})$ are elements of the Quantum Fisher Information matrix at $\boldsymbol{x} = \mathbf{0}$, and the last term is the result of the Taylor's remainder theorem with $\boldsymbol{\nu} = c\boldsymbol{x}$ such that $c \in [0, 1]$. We remark that by this notation of $\boldsymbol{x}$ the imaginary time component is the last component of $\boldsymbol{x}$ i.e., $x_{M+1} = \delta\tau$.

A third order derivative in the last term when taken only with respect to the parameters $\boldsymbol{\theta}$ (i.e., no $\delta\tau$ component) can be expressed as (which is the same fashion as in Eq. (E14) for the real time dynamic case)

$$\frac{\partial^3 F(\boldsymbol{x})}{\partial\theta_i\partial\theta_j\partial\theta_k} = \frac{1}{Z}\operatorname{Tr}\left\{e^{-\delta\tau H}U^{(M,k)}i\left[U^{(k,j)}i\left[U^{(j,i)}i\left[U^{(i,0)}\rho_0 U^{(i,0)\dagger}, \sigma_i\right]U^{(j,i)\dagger}, \sigma_j\right]U^{(k,j)\dagger}, \sigma_k\right]U^{(M,k)\dagger}e^{-\delta\tau H}\rho_{(\boldsymbol{\theta}^*,0)}\right\}, \tag{E66}$$

where $U(\boldsymbol{\theta}) = U^{(M,k)}U^{(k,j)}U^{(j,i)}U^{(i,0)}$ with $U^{(a,b)} = \prod_{l=a+1}^{b} e^{-ix_l\sigma_l}\widetilde{V}_l$ (for $b < M+1$).

When the third derivative is taken with respect to the imaginary time in of the components, by direct calculation we have

$$\frac{\partial^3 F(\boldsymbol{x})}{\partial\theta_i\partial\theta_j\partial\tau} = \operatorname{Tr}\left[-\rho_{(\boldsymbol{\theta}^*,0)}\{\mathcal{B}_{i,j}, H\} + 2\operatorname{Tr}[H\mathcal{B}_{i,j}]\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\rho_{(\boldsymbol{\theta}^*,0)} + 2\operatorname{Tr}\left[\rho_{(\boldsymbol{\theta}^*,\delta\tau)}H\right]\mathcal{B}_{i,j}\rho_{(\boldsymbol{\theta}^*,0)}\right] \tag{E67}$$

where we defined $\mathcal{B}_{i,j} = \frac{\partial^2\rho_{(\boldsymbol{\theta}^*,\delta\tau)}}{\partial\theta_i\partial\theta_j}$ which can be written as a nested commutator as

$$\mathcal{B}_{i,j} = \frac{1}{Z}\operatorname{Tr}\left\{e^{-\tau H}U^{(M,k)}i\left[U^{(k,i)}i\left[U^{(i,0)}\rho_0 U^{(i,0)\dagger}, \sigma_i\right]U^{(j,i)\dagger}, \sigma_j\right]U^{(M,j)\dagger}e^{-\tau H}\rho_{(\boldsymbol{\theta}^*,0)}\right\}. \tag{E68}$$

We note that the other third derivative terms with respect to the imaginary time in more than one components can be also be expressed in a similar way. However, since they are not important in our analysis, we do not write them explicitly. Indeed, if we now compute the Hessian matrix of $F(\boldsymbol{x})$ with respect to the variational parameters $\boldsymbol{\theta}$, all the terms with higher derivatives in time will be 0.

We now focus on one element of this hessian matrix $\nabla^2_{\boldsymbol{\theta}}F(\boldsymbol{x})$ (recall that $\boldsymbol{x} = (\boldsymbol{\theta} - \boldsymbol{\theta}^*, \tau)$). For convenience, we denote $\mathcal{A}_{i,j,k}(\boldsymbol{x}) = \frac{\partial^3 F(\boldsymbol{x})}{\partial x_i\partial x_j\partial x_k}$. By direct compuation, we see that

$$\frac{\partial^2 F(x)}{\partial\theta_i\partial\theta_j} = -\frac{1}{2}\mathcal{F}_{j,k}(\mathbf{0}) + \frac{1}{6}\widetilde{\mathcal{A}}_{j,k}(\nu) \tag{E69}$$

with

$$\widetilde{\mathcal{A}}_{j,k}(\boldsymbol{\nu}) = \sum_{i=1}^{M+1} x_i\left(\mathcal{A}_{j,k,i}(\boldsymbol{\nu}) + \mathcal{A}_{j,i,k}(\boldsymbol{\nu}) + \mathcal{A}_{i,j,k}(\boldsymbol{\nu}) + \mathcal{A}_{k,j,i}(\boldsymbol{\nu}) + \mathcal{A}_{k,i,j}(\boldsymbol{\nu}) + \mathcal{A}_{i,k,j}(\boldsymbol{\nu})\right), \tag{E70}$$

where we remark that the sum up to $M+1$ is because $\delta\tau$ is included in this sum.

Thus, the largest eigenvalue of $\nabla^2_{\boldsymbol{\theta}}F(\boldsymbol{x})$ can be bounded as follows

$$\left[\nabla^2_{\boldsymbol{\theta}}F(\boldsymbol{x})\right]_{\max} \leqslant -\frac{1}{2}\left[\mathcal{F}(\mathbf{0})\right]_{\min} + \frac{1}{6}[\widetilde{\mathcal{A}}(\boldsymbol{\nu})]_{\max}, \tag{E71}$$

where we define $[A]_{\max}$ as the largest eigenvalue of the matrix A and similarly $[A]_{\min}$ is used for the smallest eigenvalue.

Our strategy is to bound $[\widetilde{\mathcal{A}}(\boldsymbol{\nu})]_{\max}$ with Proposition 2. To do this, we first consider a bound on $\mathcal{A}_{i,j,k}(\boldsymbol{x})$. We consider two cases when (i) the index k represents the parameter component or (ii) the index k represents the time component. For the first case, we can do the same steps as in the real time dynamics presented in Eq. (C9) to Eq. (C12), which is repeated here for completeness.

$$\begin{aligned}
\mathcal{A}_{i,j,k}(\boldsymbol{\nu}) &\leqslant |\mathcal{A}_{i,j,k}(\boldsymbol{\nu})| && \text{(E72)}\\
&\leqslant \left\|e^{-\delta\tau H}U^{(M,k)}i\left[U^{(k,j)}i\left[U^{(j,i)}i\left[U^{(i,0)}\rho_0 U^{(i,0)\dagger}, \sigma_i\right]U^{(j,i)\dagger}, \sigma_j\right]U^{(k,l)\dagger}, \sigma_k\right]U^{(M,k)\dagger}e^{-\delta\tau H}\right\|_\infty \left\|\rho_{(\boldsymbol{\theta}^*,0)}\right\|_1 && \text{(E73)}\\
&\leqslant 2^3\|\sigma_i\|_\infty\|\sigma_j\|_\infty\|\sigma_k\|_\infty && \text{(E74)}\\
&= 8 && \text{(E75)}
\end{aligned}$$

Here the second inequality is due to Hölder's inequality. In the third inequality we use a few identities including (i) the one-norm of a pure state is 1, (ii) $\|UA\|_p = \|A\|_p$ for any unitary U, (iii) $\|i[A,B]\|_p = 2\|A\|_p\|B\|_p$, (iv)

$\|AB\|_p \leqslant \|A\|_p \|B\|_p$ and lastly (v) $\|e^{-\delta\tau H}\|_\infty < 1$. To reach the final equality, we recall that since x_l and x_m cannot be a time component δt, σ_l and σ_m are generators of the circuit which have $\|\sigma_i\|_\infty = \|\sigma_j\|_\infty = \|\sigma_k\|_\infty = 1$.

For the second case with the index k representing th time component, we have the following

$$\begin{aligned}
\mathcal{A}_{i,j,M+1}(\boldsymbol{x}) &= \operatorname{Tr}\left[-\rho_{(\boldsymbol{\theta}^*,0)}\left\{\mathcal{B}_{i,j}, H\right\} + 2\operatorname{Tr}[H\mathcal{B}_{i,j}]\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\rho_{(\boldsymbol{\theta}^*,0)} + 2\operatorname{Tr}\big[\rho_{(\boldsymbol{\theta}^*,\delta\tau)}H\big]\mathcal{B}_{i,j}\rho_{(\boldsymbol{\theta}^*,0)}\right] && \text{(E76)}\\
&\leqslant \left|\operatorname{Tr}\left[-\rho_{(\boldsymbol{\theta}^*,0)}\left\{\mathcal{B}_{i,j}, H\right\} + 2\operatorname{Tr}[H\mathcal{B}_{i,j}]\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\rho_{(\boldsymbol{\theta}^*,0)} + 2\operatorname{Tr}\big[\rho_{(\boldsymbol{\theta}^*,\delta\tau)}H\big]\mathcal{B}_{i,j}\rho_{(\boldsymbol{\theta}^*,0)}\right]\right| && \text{(E77)}\\
&\leqslant \left|\operatorname{Tr}\left[-\rho_{(\boldsymbol{\theta}^*,0)}\left\{\mathcal{B}_{i,j}, H\right\}\right]\right| + \left|\operatorname{Tr}\left[2\operatorname{Tr}[H\mathcal{B}_{i,j}]\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\rho_{(\boldsymbol{\theta}^*,0)}\right]\right| + \left|\operatorname{Tr}\left[2\operatorname{Tr}\big[\rho_{(\boldsymbol{\theta}^*,\delta\tau)}H\big]\mathcal{B}_{i,j}\rho_{(\boldsymbol{\theta}^*,0)}\right]\right| && \text{(E78)}
\end{aligned}$$

Now we can bound each individual term in Eq. (E78) with

$$\begin{aligned}
&\left|\operatorname{Tr}\left[-\rho_{(\boldsymbol{\theta}^*,0)}\left\{\mathcal{B}_{i,j}, H\right\}\right]\right| \leqslant 2\left|\operatorname{Tr}\left[\rho_{(\boldsymbol{\theta}^*,0)}\mathcal{B}_{i,j}H\right]\right| && \text{(E79)}\\
&\left|\operatorname{Tr}\left[2\operatorname{Tr}[H\mathcal{B}_{i,j}]\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\rho_{(\boldsymbol{\theta}^*,0)}\right]\right| \leqslant 2\left|\operatorname{Tr}[H\mathcal{B}_{i,j}]\right| && \text{(E80)}\\
&\left|\operatorname{Tr}\left[2\operatorname{Tr}\big[\rho_{(\boldsymbol{\theta}^*,\delta\tau)}H\big]\mathcal{B}_{i,j}\rho_{(\boldsymbol{\theta}^*,0)}\right]\right| = 2||H||_\infty\left|\operatorname{Tr}\left[\mathcal{B}_{i,j}\rho_{(\boldsymbol{\theta}^*,0)}\right]\right| && \text{(E81)}
\end{aligned}$$

where we are using $|\operatorname{Tr}\big[\rho_{(\boldsymbol{\theta}^*,\delta\tau)}\rho_{(\boldsymbol{\theta}^*,0)}\big]| \leqslant 1$ in Eq. (E80) and Hölder's inequality in Eq. (E81). Now, all of the remaining terms can be bounded using Eq. (C9). Thus we obtain

$$\mathcal{A}_{i,j,M+1} \leqslant 24||H||_\infty \,. \tag{E82}$$

Now, we can bound the sum of the absolute of elements in a row of $\widetilde{\mathcal{A}}(\boldsymbol{\nu})$ as

$$\begin{aligned}
\sum_{j=1}^{M}\left|\widetilde{\mathcal{A}}_{ij}(\boldsymbol{\nu})\right| &\leqslant \sum_{j=1}^{M}\sum_{k=1}^{M+1}|x_k|\left(|\mathcal{A}_{i,j,k}(\boldsymbol{\nu})| + |\mathcal{A}_{i,k,j}(\boldsymbol{\nu})| + |\mathcal{A}_{k,i,j}(\boldsymbol{\nu})| + |\mathcal{A}_{j,i,k}(\boldsymbol{\nu})| + |\mathcal{A}_{j,k,i}(\boldsymbol{\nu})| + |\mathcal{A}_{k,j,i}(\boldsymbol{\nu})|\right) && \text{(E83)}\\
&\leqslant 48M(3\lambda_{\max}\delta\tau + Mr)\,. && \text{(E84)}
\end{aligned}$$

Finally we invoke Proposition 2. Thus, the largest eigenvalue of the matrix $\widetilde{\mathcal{A}}$, $[\widetilde{\mathcal{A}}_{j,k}]_{\max}$ can be bounded by

$$[\widetilde{\mathcal{A}}_{j,k}]_{\max} \leqslant 48M(3\lambda_{\max}\delta\tau + Mr_c)\,. \tag{E85}$$

With this result we can guarantee the legion of ϵ-convexity (i.e. Eq. (E64)) by enforcing the following condition

$$-\frac{1}{2}\left[\mathcal{F}(\mathbf{0})\right]_{\min} + 8M\left(3\lambda_{\max}\delta\tau + Mr\right) \leqslant |\epsilon|\,. \tag{E86}$$

Upon rearranging the terms, we find

$$r \leqslant \frac{1}{M}\left(\frac{\mu_{\min} + 2|\epsilon|}{16M} - 3\lambda_{\max}\delta\tau\right)\,. \tag{E87}$$

Indeed, this implies that *any* hypercube $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r)$ such that r satisfies Eq. (E87) is guaranteed to be approximately convex. Hence, we know that the total ϵ-convex region has to be at least of size $\frac{1}{M}\left(\frac{\mu_{\min}+2|\epsilon|}{16M} - 3\lambda_{\max}\delta\tau\right)$. More explicitly, by denoting r_c to be the length of the total ϵ-approximate convex region $\boldsymbol{\mathcal{V}}(\boldsymbol{\theta}^*, r_c)$, we have

$$r_c \geqslant \frac{1}{M}\left(\frac{\mu_{\min} + 2|\epsilon|}{16M} - \lambda_{\max}\delta\tau\right)\,. \tag{E88}$$

Finally, we note that the bound is only informative if the Trotter time-step respects

$$\delta\tau \leqslant \frac{\mu_{\min} + 2|\epsilon|}{48M\lambda_{\max}}\,. \tag{E89}$$

This completes the proof of the theorem.

□

c. *Adiabatic moving minima: Proof of Theorem 6*

In this subsection, we analytically prove Theorem 6. We first show an equivalent result to Proposition 4 for imaginary time evolution. We refer the readers to Appendix D for definitions of adiabatic minimum (Definition 2) and adiabatic shift (Definition 4).

Proposition 5. *Given a Trotter time-step of the current iteration $\delta\tau$ and assuming that the adiabatic minimum exists within this time frame, the shift of the adiabatic minimum $\boldsymbol{\alpha}_A(\delta\tau)$ as defined in Definition 4 can be bounded as*

$$\|\boldsymbol{\alpha}_A(\delta\tau)\|_2 \leqslant \frac{4\sqrt{M}\lambda_{\max}\delta\tau}{\beta_A} \,, \tag{E90}$$

where M is the number of parameters, $\lambda_{\max}$ is the largest eigenvalue of the dynamic Hamiltonian H and $\beta_A = \frac{\dot{\boldsymbol{\alpha}}_A^T(\delta\tau)\left(\nabla^2_{\boldsymbol{\alpha}}\mathcal{L}(\boldsymbol{\alpha},\delta\tau)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(\delta\tau)}\right)\dot{\boldsymbol{\alpha}}_A(\delta\tau)}{\|\dot{\boldsymbol{\alpha}}_A(\delta\tau)\|_2^2}$

Proof. The proof here is very similar to the equivalent version for Real Time Evolution. Through out this proof, it is more convenient to use τ as an imaginary Trotter time-step (instead of $\delta\tau$). We start by recalling that by Definition 4, the adiabatic shift follows

$$\nabla_{\boldsymbol{\alpha}}\mathcal{L}(\boldsymbol{\alpha},\tau)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(\tau)} = \mathbf{0} \,, \tag{E91}$$

which holds for any τ. Similarly to the previous case, we use this notation $\nabla_{\boldsymbol{\alpha}_A}\mathcal{L} := \nabla_{\boldsymbol{\alpha}}\mathcal{L}(\boldsymbol{\alpha},\tau)\big|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(\tau)}$.

We can derivative with respect to τ to find

$$\frac{d}{d\tau}\left(\nabla_{\boldsymbol{\alpha}_A}\mathcal{L}\right) = \partial_\tau\nabla_{\boldsymbol{\alpha}_A}\mathcal{L} + \left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A = \mathbf{0} \,, \tag{E92}$$

where we denote $\partial_\tau = \partial/\partial\tau$ and $\dot{\boldsymbol{\alpha}}_A(\tau) = d\boldsymbol{\alpha}_A(\tau)/d\tau$.

Recall that $\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}$ is a matrix vector multiplication with the $\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}$ is the Hessian Matrix evaluated at the adiabatic minima $\boldsymbol{\alpha}_A(\tau)$. We multiply from the left with $\dot{\boldsymbol{\alpha}}_A^T(\tau)/\|\dot{\boldsymbol{\alpha}}_A(\tau)\|_2$ to find

$$\frac{\dot{\boldsymbol{\alpha}}_A^T}{\|\dot{\boldsymbol{\alpha}}_A\|_2}\partial_\tau\nabla_{\boldsymbol{\alpha}_A}\mathcal{L} + \frac{\dot{\boldsymbol{\alpha}}_A^T\left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A}{\|\dot{\boldsymbol{\alpha}}_A\|_2^2}\|\dot{\boldsymbol{\alpha}}_A\|_2 = 0 \,. \tag{E93}$$

For convenience, we denote $\beta_A := \dot{\boldsymbol{\alpha}}_A^T\left(\nabla^2_{\boldsymbol{\alpha}_A}\mathcal{L}\right)\dot{\boldsymbol{\alpha}}_A/\|\dot{\boldsymbol{\alpha}}_A\|_2^2$. We then rearrange the terms to find a bound on the norm of $\dot{\boldsymbol{\alpha}}_A(\tau)$:

$$\begin{aligned} \|\dot{\boldsymbol{\alpha}}_A(\tau)\|_2 &= \left\| -\frac{\dot{\boldsymbol{\alpha}}_A^T\partial_\tau\nabla_{\boldsymbol{\alpha}_A}\mathcal{L}}{\|\dot{\boldsymbol{\alpha}}_A\|_2\beta_A} \right\|_2 && \text{(E94)} \\ &\leqslant \frac{\|\partial_\tau\nabla_{\boldsymbol{\alpha}_A}\mathcal{L}\|_2}{\beta_A} && \text{(E95)} \\ &\leqslant \frac{\sqrt{M}\left|\partial_\tau\partial_{\alpha_A^{(i)}}\mathcal{L}\right|_{\max}}{\beta_A} && \text{(E96)} \\ &\leqslant \frac{4\sqrt{M}\lambda_{\max}}{\beta_A} \,, && \text{(E97)} \end{aligned}$$

where in the first inequality we use Cauchy-Schwartz. In the second we expand the 2-norm explicitly and take the largest value of the sum (i.e. $\|\boldsymbol{a}\|_2 = \sqrt{\sum_{i=1}^M a_i^2} \leqslant \sqrt{M}|a_i|_{\max}$ with $\alpha_A^{(i)}$ being the i^{th} component of $\boldsymbol{\alpha}_A$).

To reach the last inequality we use the explicit form of the loss function $\mathcal{L}(\boldsymbol{\alpha},\tau) = 1 - \operatorname{Tr}\left(e^{-H\tau}\rho_{\boldsymbol{\theta}^*}e^{H\tau}\rho_{\boldsymbol{\theta}}\right)$ where H is the dynamical Hamiltonian, $\rho_{\boldsymbol{\theta}^*}$ is the state corresponding to the solution of the previous iteration and $\rho_{\boldsymbol{\theta}}$ is the parameterised state that depends on $\boldsymbol{\alpha}$ and respect a parameter shift rule. With this, we can bound the term

$\left|\partial_\tau \partial_{\alpha_A^{(i)}} \mathcal{L}\right|_{\max}$ as follows

$$\begin{aligned}
\left|\partial_\tau \partial_{\alpha_A^{(i)}} \mathcal{L}\right|_{\max} &= \left|\frac{\partial}{\partial\tau}\left(\frac{\partial}{\partial\alpha^{(i)}}\mathcal{L}(\boldsymbol{\alpha},\tau)\right)\bigg|_{\boldsymbol{\alpha}=\boldsymbol{\alpha}_A(\tau)}\right|_{\max} && \text{(E98)}\\
&= \left|\frac{1}{2}\left(\frac{\partial}{\partial\tau}\mathcal{L}\left(\boldsymbol{\alpha}_A+\frac{\pi}{2}\hat{\alpha}_i\right)-\frac{\partial}{\partial\tau}\mathcal{L}\left(\boldsymbol{\alpha}_A-\frac{\pi}{2}\hat{\alpha}_i\right)\right)\right|_{\max} && \text{(E99)}\\
&\leqslant \max_i\left|\frac{\partial}{\partial\tau}\mathcal{L}\left(\boldsymbol{\alpha}_A\pm\frac{\pi}{2}\hat{\alpha}_i\right)\right| && \text{(E100)}\\
&= \left\|e^{-H\tau}\left(-\{\rho_{\boldsymbol{\theta}^*},H\}+2\,\mathrm{Tr}[\rho_{\boldsymbol{\theta}^*}H]\rho_{\boldsymbol{\theta}^*}\right)e^{-\tau H}\right\|_\infty && \text{(E101)}\\
&\leqslant 4\lambda_{\max}\ , && \text{(E102)}
\end{aligned}$$

where we use the parameter shift rule in the second equality. In the first inequality we we maximise on all the possible terms of this parameter shift rule, and in the third equality we apply the derivative of imaginary time shown in E14, apply Hölder's inequality and use that $\|\rho\|_1 = 1$ for any pure quantum state ρ. In the last inequality we simply use the triangle inequality to bound the $\|A+B\|_p \leqslant \|A\|_p + \|B\|_p$.

Lastly, we can bound shift in the adiabatic minima as follows

$$\begin{aligned}
\|\boldsymbol{\alpha}_A(\tau)\|_2 &= \left\|\int_0^\tau \dot{\boldsymbol{\alpha}}_A(\tau')d\tau'\right\|_2 && \text{(E103)}\\
&\leqslant \int_0^\tau \|\dot{\boldsymbol{\alpha}}_A(\tau')\|_2 d\tau' && \text{(E104)}\\
&\leqslant \frac{4\sqrt{M}\lambda_{\max}\tau}{\beta_A}\ , && \text{(E105)}
\end{aligned}$$

which completes the proof.

□

We are now ready to prove Theorem 6 which is detailed in the following.

Theorem 6 (Adiabatic minimum is within provably 'nice' region for imaginary time evolution, Formal)**.** *If the imaginary time-step $\delta\tau$ is chosen such that*

$$\delta\tau \leqslant \frac{\eta_0\beta_A}{4M\lambda_{\max}}\ , \tag{E106}$$

for some small constant $\eth_0$. then the adiabatic minimum $\boldsymbol{\theta}_A(\delta\tau)$ is guaranteed to be within the non-vanishing gradient region (as per Theorem 4), and additionally, if $\delta\tau$ is chosen such that

$$\delta\tau leq\frac{\beta_A(\mu_{\min}+2|\epsilon|)}{64M^{5/2}\lambda_{\max}\left(1+\frac{3\beta_A}{4M^{3/2}}\right)}\ , \tag{E107}$$

then the adiabatic minimum $\boldsymbol{\theta}_A(\delta\tau)$ is guaranteed to be within the $|\epsilon|$-convex region (as per Theorem 5) where

$$\beta_A := \frac{\dot{\boldsymbol{\theta}}_A^T(\delta\tau)\left(\nabla^2_{\boldsymbol{\theta}}\mathcal{L}_{\mathrm{ITE}}(\boldsymbol{\theta})\big|_{\boldsymbol{\theta}=\boldsymbol{\theta}_A(\delta\tau)}\right)\dot{\boldsymbol{\theta}}_A(\delta\tau)}{\|\dot{\boldsymbol{\theta}}_A(\delta\tau)\|_2^2} \tag{E108}$$

corresponds to the second derivative of the loss in the direction in which the adiabatic minimum moves.

Proof. From Proposition 5 and the norm inequality, the adiabatic minimum follows

$$\|\boldsymbol{\alpha}_A(\delta\tau)\|_\infty \leqslant \|\boldsymbol{\alpha}_A(\delta\tau)\|_2 \leqslant \frac{4\sqrt{M}\lambda_{\max}\delta\tau}{\beta_A}\ . \tag{E109}$$

Now we want to incorporate the conditions of the region that we are interested. Indeed, by tuning $\delta\tau$, we want a guarantee that the adiabatic minimum is within (i) the region with substantial gradients and/or (ii) the convex region.

For (i) the region with substantial gradients, we recall from Theorem 4 that for the imaginary time scaling as $\delta\tau \leqslant 1/12\lambda_{\max}$, the hypercube of width $2r$ has polynomial large variance within the region where r scales as

$$r = \frac{\eta_0}{\sqrt{M}} \,, \tag{E110}$$

for some constant η_0. Hence, the sufficient condition to have the adiabatic minimum to be within this substantial gradient region is that

$$\|\boldsymbol{\alpha}_A(\delta\tau)\|_\infty \leqslant \frac{4\sqrt{M}\lambda_{\max}\delta\tau}{\beta_A} \leqslant \frac{\eta_0}{\sqrt{M}} \,, \tag{E111}$$

which, upon rearranging leads to

$$\delta\tau \leqslant \frac{\eta_0\beta_A}{4M\lambda_{\max}} \,. \tag{E112}$$

For (ii) the convex region, from Theorem 5, if we have the dynamic time bounded as $\delta\tau \leqslant \frac{\mu_{\min}+2|\epsilon|}{48M\lambda_{\max}}$, we have ϵ-convexity in the hypercube of with $2r_c$ for

$$r_c \geqslant \frac{1}{M}\left(\frac{\mu_{\min}+2|\epsilon|}{16M} - 3\lambda_{\max}\delta\tau\right) \tag{E113}$$

Therefore it is sufficient to have the guarantee that the adiabatic minima is inside this convex region by imposing

$$\|\boldsymbol{\alpha}_A(t)\|_\infty \leqslant \frac{4\sqrt{M}\lambda_{\max}\delta\tau}{\beta_A} \leqslant \frac{1}{M}\left(\frac{\mu_{\min}+2|\epsilon|}{16M} - 3\lambda_{\max}\delta\tau\right) \leqslant r_c \tag{E114}$$

which after rearranging terms the imaginary time-step is bounded by

$$\delta\tau \leqslant \frac{\beta_A(\mu_{\min}+2|\epsilon|)}{64M^{5/2}\lambda_{\max}\left(1+\frac{3\beta_A}{4M^{3/2}}\right)} \,. \tag{E115}$$

This completes the proof. □

Extending Classically Simulatable Bounds of Clifford Circuits with Nonstabilizer States via Framed Wigner Functions

Guedong Park[1] * Hyukjoon Kwon[2] † Hyunseok Jeong[1] ‡

[1] *Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*
[2] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 02455, Korea*

Abstract. Application of Wigner function to classically simulate the quantum circuit out of Clifford circuit regime has a limitation in qubit system due to negativity occurence by Clifford gates. We present a novel classical simulation method for qubit Clifford circuits based on the framed Wigner function. Here, a wide class of non-stabilizer states can be positively represented. Also, we prevent the negativity occurence after the Clifford operation by switching the frame defining the structure of Wigner function. From this formalism, we set a systematic algorithm to find the efficiently simulatable marginal measurements, hence extending the classically simulatable region of circuits in qubit system.

Keywords: Classical simulation of quantum circuit, Clifford circuit and stabilizer states, Gottesmann-Knill theorem, Discrete Wigner function, Vertex cover problem.

1 Introduction

Quantum algorithms, which are algorithms based on quantum mechanical principles, have been shown to outperform the classical algorithms for many computational tasks [1, 2]. However, not all quantum algorithms show such computational speed up over its classical counterparts. One typical example is Clifford circuits [3]: circuits consist of an input state in the computational basis and Clifford gates, resulting in a stabilizer state as an ouput. By the Gottesmann-Knill theorem [3], we can classically simulate an n-qubit Clifford circuit in $\mathcal{O}(n^3)$-time. The theorem necessitates [4] the usage of non-stabilizer states to achieve effective speed up over classical computer. However, classifying simulatable circuits even out of Clifford circuit regime has been important task to demonstrate the classical hardness of near-term quantum computing [5, 6, 7, 8].

In odd-prime dimensional system, one of the representative methods to extend the classical simulability of non-Clifford circuits is to utilize the Wigner function [9, 10]. Here, we use the Wigner function of discretized structure of phase space operator, alternative to original version of inifinite dimensional system. It enables some non-stabilizer mixed states to be positively represented and positivity of Wigner function of given state is not harmed under Clifford operations and Pauli measurements. Then we can make a classical simulation scheme based on such a stochastic representation of dynamics in the circuit. Therefore, the Wigner formalism extends the region of simulatable circuits over the realm of Gottesmann-Knill theorem.

These interesting facts lead us to apply such formalism to qubit (even dimensional) system. Furthermore, there exist non-stabilizer pure states with positive Wigner function [12]. However, similar classical simulation scheme is no longer valid due to its another exotic features. That is, Clifford operations can induce negativity in the Wigner function which prohibits the classical simulation of most qubit Clifford circuits. Although there have been many efforts to circumvent such problems [13, 14, 15, 16], these approaches have their own limitations. For example, the positive representation of non-stabilizer is unknown [13, 14, 15] or phase point of given state cannot be sampled or updated efficiently under Clifford operations and Pauli measurements [16, 15, 17]. Therefore, finding suitable structure of qubit Wigner formalism which includes from the simulability of Clifford circuits to non-Clifford cases is still under open questions.

In this paper [18], we propose a new efficient classical simulation algorithm for unitary Clifford circuits with non-stabilizer inputs based on the qubit Wigner function. To do so, we introduce a generalized notion of the Wigner function, parametrized by a family of *frame functions*. Our strategy is that under the following Clifford operation, we properly switch the frame defining the Wigner function to make an enacted state with positive Wigner function still preserve the positivity. From this, given that we efficiently sample the phase point from the Wigner function of an initial state, we have a deterministic update rule of phase point under Clifford operation. Negativity which was circumvented during the intermediate Clifford operation will be transferred to the measurement parts. Even if so, efficiently measurable qubits can be found by the solving vertex cover problem to the graph representation of the final frame. For log-depth random Clifford circuits with nonstabilizer inputs, we find that the number of simulatable qubits scales linearly with n for a 1D architecture, while observing a phase transition in its scaling for a completely connected architecture.

2 Main results

We consider n-qubit system. First, we define the *framed Wigner function*,

$$W_\rho^F(\mathbf{u}) \equiv \frac{1}{2^n}\mathrm{Tr}\left[\rho A^F(\mathbf{u})\right]. \quad (1)$$

*rbeh7336@snu.ac.kr
†hjkwon@kias.re.kr
‡jeongh@snu.ac.kr

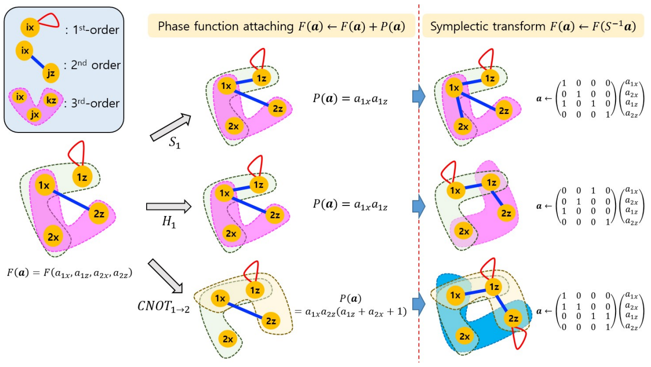

: 1st-order
: 2nd order
: 3rd-order
ix
jz
jx
kz
Phase function attaching $F(\boldsymbol{a}) \leftarrow F(\boldsymbol{a}) + P(\boldsymbol{a})$
Symplectic transform $F(\boldsymbol{a}) \leftarrow F(S^{-1}\boldsymbol{a})$
S_1
H_1
$CNOT_{1\to 2}$
1x
1z
2x
2z
$F(\boldsymbol{a}) = F(a_{1x}, a_{1z}, a_{2x}, a_{2z})$
$P(\boldsymbol{a}) = a_{1x}a_{1z}$
$P(\boldsymbol{a}) = a_{1x}a_{1z}$
$P(\boldsymbol{a}) = a_{1x}a_{2z}(a_{1z} + a_{2x} + 1)$
$\boldsymbol{a} \leftarrow \begin{pmatrix}1&0&0&0\\0&1&0&0\\1&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}a_{1x}\\a_{2x}\\a_{1z}\\a_{2z}\end{pmatrix}$
$\boldsymbol{a} \leftarrow \begin{pmatrix}0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}a_{1x}\\a_{2x}\\a_{1z}\\a_{2z}\end{pmatrix}$
$\boldsymbol{a} \leftarrow \begin{pmatrix}1&0&0&0\\1&1&0&0\\0&0&1&1\\0&0&0&1\end{pmatrix}\begin{pmatrix}a_{1x}\\a_{2x}\\a_{1z}\\a_{2z}\end{pmatrix}$

Figure 1: Hypergraph representation of frame changing. For example, the initial frame $F_{\text{in}}(\mathbf{a}) = a_{1z} + a_{1x}a_{2z} + a_{1x}a_{2x}a_{2z} + a_{1x}a_{1z}a_{2x}$ transforms to $F(\mathbf{a}) = a_{1z} + a_{1x}a_{1z} + a_{1x}a_{2x} + a_{1x}a_{2z} + a_{1x}a_{2x}a_{2z} + a_{1x}a_{1z}a_{2x}$ after the phase gate on the first qubit. Vertices connected by hyperedges comprise variables forming a single term in frame. $A \leftarrow B$ denotes that A is replaced by B.

Here $\mathbf{u} \in \mathbb{Z}_2^{2n}$, and the phase space operator $A^F(\mathbf{u})$ is defined as

$$A^F(\mathbf{u}) \equiv \frac{1}{2^n} \sum_{\mathbf{a}\in\mathbb{Z}_2^{2n}} (-1)^{[\mathbf{u},\mathbf{a}]+F(\mathbf{a})} T_{\mathbf{a}}, \tag{2}$$

where $\mathbf{a} = (\mathbf{a}_x, \mathbf{a}_z)$ and $T_{\mathbf{a}} \equiv \bigotimes_{j=1}^n i^{a_{jx}a_{jz}} X_j^{a_{jx}} Z_j^{a_{jz}}$ Also, $[\mathbf{u}, \mathbf{a}] = \mathbf{u}_x \cdot \mathbf{a}_z + \mathbf{u}_z \cdot \mathbf{a}_x$ is a $2n$-dimensional symplectic inner product. The structure of the Wigner function is parametrized as a *frame function* $F(\mathbf{a}) : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2$ satisfying $F(\mathbf{0}) = 0$. From the completeness relation $\text{Tr}\big[A^F(\mathbf{u})A^F(\mathbf{v})\big] = 2^n\delta_{\mathbf{u},\mathbf{v}}$, a quantum state can be expressed as

$$\rho = \sum_{\mathbf{u}\in\mathbb{Z}_2^{2n}} W_\rho^F(\mathbf{u})A^F(\mathbf{u}). \tag{3}$$

If $W_\rho^F(\mathbf{u}) \geq 0$ for $\forall \mathbf{u} \in \mathbb{Z}_2^{2n}$, we say ρ is *positively represented under the frame F*.

Given that ρ is positively represented under the frame F_{in}, let us enact the Clifford unitary $U \in \text{Cl}_n$. If we fix the frame after the operation, the Wigner function $W_{U\rho U^\dagger}^{F_{\text{in}}}(\mathbf{u})$ may have negativity. However, there exists a frame changing rule depending on U such that if we change the frame F_{in} to F, then we can preserve the positivity of evolved state. Then the update of Wigner function has a similar form with odd-prime dimensional case, i.e. there exists $\mathbf{k} \in \mathbb{Z}_2^{2n}$ and $2n$ by $2n$ binary symplectic matrix S corresponding to U such that

$$W_{U\rho U^\dagger}^F(S(\mathbf{u}+\mathbf{k})) = W_\rho^{F_{in}}(\mathbf{u}), \tag{4}$$

except that the frame is changed. Both S and $\mathbf{k}$ can be found efficiently. Furthermore, we can change the frame under the each of the Clifford bases $\{H, S, CNOT\}$ (see Fig. 1). From the fact that all Clifford operation can be decomposed with this basis, we can find up to 3rd-degree resulting frame, which positively represent $U\rho U^\dagger$, in poly(n)-time and $\mathcal{O}(n^3)$-memory. For example, it is well known that 2-qubit computational basis $|00\rangle\langle 00|$ is positively represented under the zero frame $F_{\text{in}} = 0$ and that if we enact Hadamard gate and CNOT gate to make a Bell state $|\Phi\rangle\langle\Phi|$ with $|\Phi\rangle = 1/\sqrt{2}\,|00\rangle + 1/\sqrt{2}\,|11\rangle$, then it has negativity with respect to zero frame. However, the Bell state can be positively represented under the non-local frame $F(\mathbf{a}) = a_{1x}a_{1z} + a_{1z}a_{2z}a_{1x} + a_{2z}a_{1x}a_{2x}$ (mod 2). From now on, we assume the final frame F has zero linear term since we can show that non-zero linear term can always be absorbed into $\mathbf{k}$.

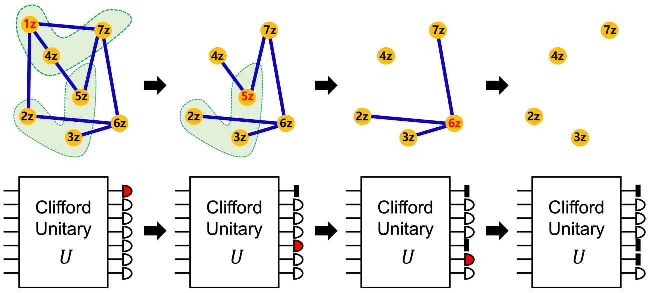


Figure 2: Identifying efficiently simulatable qubits by solving the vertex cover problem using a greedy algorithm. Lines and shaded regions represent the quadratic and cubic terms in the final frame function $F(\mathbf{0}, \mathbf{a}_z) = a_{1z}a_{4z}a_{7z} + a_{2z}a_{3z}a_{5z} + a_{1z}a_{4z} + a_{4z}a_{5z} + a_{5z}a_{7z} + a_{1z}a_{2z} + a_{2z}a_{6z} + a_{3z}a_{6z} + a_{6z}a_{7z}$. A qubit with the largest number of connected hyperedges is traced out at each step until all the edges vanishes. The outcomes of the remaining qubits are efficiently simulatable.

Another point is that there exists set of non-stabilizer states which can be positively represented under the specified frame functions. For example, n-copies of *F-state*, $|A\rangle \equiv \cos(\theta/2)\,|0\rangle + e^{i(\pi/4)}\sin(\theta/2)\,|1\rangle$ with $\theta = \cos^{-1}(1/\sqrt{3})$ is positively represented under the zero frame. Also, non-stabilizer state which can be formed by arbitrary Clifford operation to such F-copies can be positively represented under the another frame, which can be found by the frame chaning rule.

Moreover, from the final frame after the Clifford operation, we can select the marginal qubits whose Z-basis Pauli measurements can be exactly and efficiently simulated. We summarize aforementioned arguments as a following theorem.

Theorem 1. *Suppose an n-qubit quantum circuit composed of a product state input $\rho = \bigotimes_{i=1}^n \rho_i$ and a Clifford unitary U. If each ρ_i is positively represented in either zero or dual frame ($F = a_{ix}a_{iz}$), the final state $U\rho U^\dagger$ is positively represented within $\mathcal{O}(n^3)$-memory and $\mathcal{O}(\text{poly}(n))$-time costs. From this, one can sample the measurement outcomes of some marginal qubits in the computational basis within $\mathcal{O}(n^2)$-time cost, where these marginal qubits are determined by the frame F.*

The simulatable marginal qubits can be found from the graph representation of the final frame with $\mathbf{a}_x = \mathbf{0}$, i.e. $F(\mathbf{0}, \mathbf{a}_z)$. Since the final frame has at most 3rd-degree, we can represent $F(\mathbf{0}, \mathbf{a}_z)$ as 3rd-ordered hypergraph where vertices and lines indicate each variable and quadratic

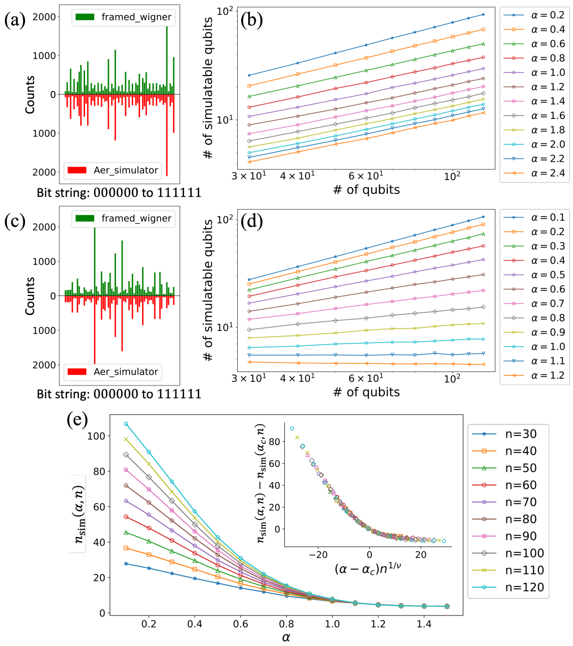


Figure 3: (a), (c): Comparison between sampling results using the framed Wigner function and Qiskit Aer simulator for a randomly chosen 10-qubit log-depth Clifford circuit with (a) 1D-neighboring and (c) completely connected architecture. For both cases, nonstabilizer input state $|A\rangle\langle A|^{\otimes 10}$ is taken, and 6 marginal qubits are selected after solving the vertex cover problem. The y-axis shows the number of counts of binary string that simulators sampled by taking a total of 20000 samples. (b), (d): The averaged number of simulatable qubits ($n_{\rm sim}$) by increasing the gate count $L = \alpha(n \ln n)$ of 1000 random Clifford circuits with (b) 1D-neighboring and (d) completely connected architectures. (e) Scaling behavior of $n_{\rm sim}$ by increasing α and data collapse after finite-size scaling.

term of frame function respectively, also 3rd-hyperedges describe cubic terms. If we trace the i-th ($i \in [n]$) qubit, then we eliminate all edges containing a_{iz} vertex. Repeating several times, when the resulting graph exhausts all hyperedges (including lines), then remaining qubits can be measured efficiently. *Vertex cover problem* is the problem to find the minimal vertices to trace out so that after above elimination routine, no edges are left. Such problem is directly related to finding the largest simulatable qubits, but is known to be NP-Hard [19]. However, we can approximately solve it by using the *greedy algorithm* [20] where for each repetition, we select the vertex which has the largest number of connecting edges. See the Fig. 2 for the schematic illustration of finding the simulatable marginals via the greedy algorithm.

3 Numerical simulations

We apply the proposed simulation algorithm to two different types of random n-qubit log-depth Clifford circuits, with 1D-neighboring and arbitrary long-range interactions (completely connected) between two qubits, where gate count is $L = \alpha n \ln(n)$. In both cases, we take the input state $\rho = |A\rangle\langle A|^{\otimes n}$, and adopt the greedy algorithm to find efficiently simulatable marginal qubits. Figure 3(a,c) shows that our simulation method successfully samples the measurement outcomes.

Figure 3(b) shows that for 1D architecture, the average number of classically simulatable qubits ($n_{\rm sim}$) increases linearly by n. This result can be compared to the tensor network simulation, where all the n-qubit outcomes of these circuits can be efficiently simulated with $e^{\mathcal{O}(\alpha \ln n)} \sim n^{\mathcal{O}(\alpha)}$ time cost [21, 22]. In contrast, our algorithm simulates a linear portion of qubits with $\mathcal{O}(\alpha \mathrm{poly}(n))$ time cost, including both finding the final frame F and solving its vertex cover problem. Therefore, our approach offers faster simulation when the α becomes large. We also observed remarkable improvement compared to the matrix product state simulator of the IBM Qiskit [23]. For the completely connected architecture, see Fig. 3 (d) and (e), we observed a sharp transition of $n_{\rm sim}$ depending on the gate count. From the finite sized scaling analysis, we checked such a transition occurred at the critical point $\alpha_c \simeq 0.81$. Even in this case, our simulator shows effective extension of simulatable region, given that efficient and exact classical simulability of even the constant-depth 2-D circuit is still not known [21].

References

[1] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review 41, 303, 1999.

[2] D. Deutsch, R. Jozsa. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences 439, 553, 1992.

[3] S. Aaronson, D. Gottesmann Improved Simulation of Stabilizer Circuits Physics Review A 70, 052328, 2004.

[4] S. Bravyi, A. Kitaev Universal quantum computation with ideal Clifford gates and noisy ancillas Physics Review A 70, 022316, 2005.

[5] M. J. Bremner, R. Jozsa, and D. J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy Proceedings of the royal society A 467, 459, 2010.

[6] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani. On the complexity and verification of quantum random circuit sampling Nature Physics 15, 159-163, 2019.

[7] K. Bu and D. E. Koh. Efficient Classical Simulation of Clifford Circuits with Nonstabilizer Input States Physical Review Letters 123, 170502, 2019.

[8] R. J. M. Yoganathan and S. Strelchuk. Quantum advantage of unitary Clifford circuits with magic

state inputs Proceedings of the royal society A 475, 20180427, 2010.

[9] A. Mari, J. Eisert. Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient Physical Review Letters 109, 230503, 2012.

[10] V. Veitch, C. Ferrie, D. Gross, and J. Emerson. Negative quasi-probability as a resource for quantum computation New Journal of Physics 14, 113011, 2012

[11] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega. Contextuality and Wigner-function negativity in qubit quantum computation Physics Review A 95, 052334

[12] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega. Contextuality and Wigner-function negativity in qubit quantum computation Physics Review A 95, 052334, 2017.

[13] L. Kocia and P. Love. Discrete Wigner formalism for qubits and noncontextuality of Clifford gates on qubit stabilizer states Physics Review A 96, 062134, 2017.

[14] N. Koukoulekidis, H. Kwon, H. H. Jee, D. Jennings, and M. S. Kim. Faster Born probability estimation via gate merging and frame optimisation Quantum 6, 838, 2022.

[15] R. Raussendorf, J. Bermejo-Vega, E. Tyhurst, C. Okay, and M. Zurel. Phase-space-simulation method for quantum computation with magic states on qubits Physics Review A 101, 012350, 2020.

[16] M. Zurel, C. Okay, and R. Raussendorf. Hidden Variable Model for Universal Quantum Computation with Magic States on Qubits Physical Review Letters 125, 260404, 2020.

[17] M. Zurel, C. Okay, and R. Raussendorf. Simulating quantum computation: how many "bits" for "it"? arXiv:2305.12787.

[18] (Technical Details)G. Park, H. Kwon, H. Jeong. Efficient Classical Simulation of Clifford Circuits from Framed Wigner Functions arXiv:2307.16688.

[19] I. Dinur and S. Safra. On the Hardness of Approximating Minimum Vertex Cover Annals of Mathematics, Second Series 162, 439, 2005.

[20] E. Halperin. Improved Approximation Algorithms for the Vertex Cover Problem in Graphs and Hypergraphs SIAM Journal on Computing 31, 1608, 2002.

[21] J. C. Napp, R. L. La Placa, A. M. Dalzell, F. G. S. L. Brandao, and A. W. Harrow. Efficient Classical Simulation of Random Shallow 2D Quantum Circuits Physical Review X 12, 021021, 2022.

[22] G. Vidal Efficient Classical Simulation of Slightly Entangled Quantum Computations Physical Review Letters 91, 147902, 2003.

[23] See the technical details for detailed discussions and referring the numerical speed measurement of the framed Wigner simulator.

Extending Classically Simulatable Bounds of Clifford Circuits with Nonstabilizer States via Framed Wigner Functions

Guedong Park,[1] Hyukjoon Kwon,[2, *] and Hyunseok Jeong[1, †]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*
[2] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 02455, Korea*

The Wigner function formalism has played a pivotal role in examining the non-classical aspects of quantum states and their classical simulatability. Nevertheless, its application in qubit systems faces limitations due to negativity induced by Clifford gates. In this work, we propose a novel classical simulation method for qubit Clifford circuits based on the framed Wigner function, an extended form of the Wigner function with an additional phase degree of freedom. In our framework, Clifford gates do not induce negativity by switching to a suitable frame; thereby, a wide class of nonstabilizer states can be represented positively. By leveraging this technique, we show that some marginal outcomes of Clifford circuits with nonstabilizer state inputs can be efficiently sampled at polynomial time and memory costs. We develop a graph-theoretical approach to identify classically simulatable marginal outcomes and apply it to log-depth random Clifford circuits. We also present the outcome probability estimation scheme using the framed Wigner function and discuss its precision. Our approach opens new avenues for utilizing quasi-probabilities to explore classically simulatable quantum circuits.

Applying quantum mechanical principles to computer science has led to the discovery of quantum algorithms [1, 2]. However, not every quantum algorithm manifests exponential speedup over classical algorithms as some quantum circuits can be efficiently simulated classically [3–5]. The best-known class of such quantum circuits is defined by the Gottesman-Knill theorem [3, 6]; circuits consist of an input state in the computational basis and Clifford gates, resulting in a stabilizer state as an output. While the theorem identifies necessary elements for universal quantum computation [7, 8], understanding the hardness of a more restrictive family of experimentally feasible quantum circuits, such as instantaneous quantum polynomial circuits [9], quantum random circuits [10], and unitary Clifford circuits with nonstabilizer inputs [5, 11, 12], also plays an important role in the near-term demonstration of quantum computational advantage.

Meanwhile, in a physics-oriented direction, the classical simulatability of quantum circuits has been studied based on the Wigner function [13], which describes quantum phase space. In quantum optics, Gaussian states are the only pure states with a positive Wigner function [14], and Gaussian operations preserve the positivity of the Wigner function. A remarkable similarity can be found in discrete variable quantum phase space with odd-prime dimensions [15], where stabilizer states and Clifford operations correspond to Gaussian states and Gaussian operations, respectively. This common feature enables the unified construction [16] of a classical simulation method for both discrete [17] and continuous [18, 19] variable quantum circuits with positive Wigner functions. Moreover, these approaches open up the possibility to simulate nonstabilizer mixed states with positive Wigner functions [17].

For a qubit system, however, classical simulation based on the Wigner function formalism is no longer applicable due to its exotic features [20–22]. A crucial problem arises as Clifford operations can induce negativity in the Wigner function [20, 23], which prohibits the classical simulation of most qubit Clifford circuits. Despite considerable efforts to address this problem [20, 22, 24, 25], these approaches have their own limitations. For example, the positive representation of the nonstabilizer state may not be fully identified [20, 24] or phase space points may not be efficiently sampled and tracked [22, 24, 25]. Thus, constructing a qubit Wigner function formalism that behaves well under Clifford operations and developing classical simulation algorithms based on it remain open problems.

In this Letter, we propose an efficient classical simulation algorithm for unitary Clifford circuits with nonstabilizer inputs based on the qubit Wigner function formalism. To this end, we adopt a generalized notion of the Wigner function parameterized by a family of frame functions [21–23], while actively utilizing its non-local form. Our key observation is that phase space points transform covariantly under qubit Clifford gates without inducing negativity when the frame is appropriately switched. This leads to the qubit Wigner function formalism consistent with the Gottesman-Knill theorem for simulating stabilizer states and significantly extends the classically simulatable regime of Clifford circuits with nonstabilizer inputs, allowing for efficient sampling of their marginal outcomes. We show that the efficiently simulatable marginal outcomes can be identified by solving the vertex cover problem [26] in graph theory. For log-depth random Clifford circuits, we find that the number of simulatable qubits scales linearly with n for a 1D architecture, while observing a phase transition in its scaling for a completely connected architecture. We also discuss the precision of probability estimation [23, 27] using our approach.

Simulating quantum circuits in phase space.—Suppose

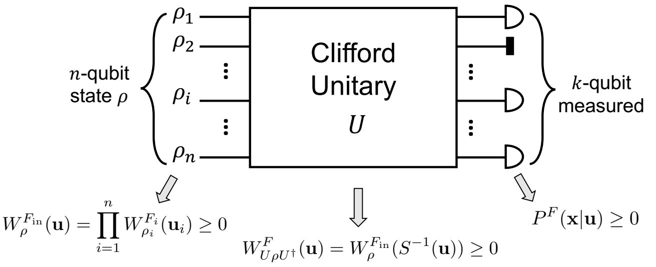

ρ_1
ρ_2
ρ_i
ρ_n
n-qubit state ρ
Clifford Unitary U
k-qubit measured
$W_\rho^{F_{\text{in}}}(\mathbf{u}) = \prod_{i=1}^{n} W_{\rho_i}^{F_i}(\mathbf{u}_i) \geq 0$
$W_{U\rho U^\dagger}^{F}(\mathbf{u}) = W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u})) \geq 0$
$P^F(\mathbf{x}|\mathbf{u}) \geq 0$

FIG. 1: Condition for efficient classical simulation of a Clifford circuit with a nonstabilizer input using the framed Wigner function.

a quantum circuit, consisting of initial state ρ, unitary evolution U, and measurement operators $\{\Pi_{\mathbf{x}}\}$ with outcomes $\mathbf{x}$. One way to classically simulate the outcomes $\mathbf{x}$ following the probabilities $p(\mathbf{x}) = \mathrm{Tr}[U\rho U^\dagger \Pi_{\mathbf{x}}]$ is by representing quantum states in phase space [16, 17, 27]. This can be done by mapping a quantum state to a distribution in phase space V as $\rho = \sum_{\mathbf{u}\in V} W_\rho(\mathbf{u}) A(\mathbf{u})$, where $A(\mathbf{u})$ are phase space operators composing an operator basis. The outcome probability is then represented as

$$p(\mathbf{x}) = \sum_{\mathbf{u}\in V} W_{U\rho U^\dagger}(\mathbf{u}) P(\mathbf{x}|\mathbf{u}), \tag{1}$$

where $P(\mathbf{x}|\mathbf{u}) \equiv \mathrm{Tr}[A(\mathbf{u})\Pi_{\mathbf{x}}]$. The phase space distribution $W_\rho(\mathbf{u})$ is well-normalized but can have negative values, in general, often referred to as *quasi-probability* [13]. Nevertheless, some quantum circuits may have both positive $W_{U\rho U^\dagger}(\mathbf{u})$ and $P(\mathbf{x}|\mathbf{u})$. In this case, the outcomes $\mathbf{x}$ can be classically simulated by sampling the phase space point $\mathbf{u}$ from $W_{U\rho U^\dagger}(\mathbf{u})$, followed by sampling $\mathbf{x}$ from the conditional probability distribution $P(\mathbf{x}|\mathbf{u})$ [16].

The canonical form of phase space for an n-qubit system is given by a $2^n \times 2^n$ lattice, $\mathbf{u} = (\mathbf{u}_x, \mathbf{u}_z) = (u_{1x}, u_{2x}, \cdots, u_{nx}, u_{1z}, u_{2z}, \cdots, u_{nz}) \in V_n = \mathbb{Z}_2^n \times \mathbb{Z}_2^n$, where the phase space operator $A(\mathbf{u}) \equiv \frac{1}{2^n}\sum_{\mathbf{a}\in V_n}(-1)^{[\mathbf{u},\mathbf{a}]} T_{\mathbf{a}}$ is constructed from the Weyl operator $T_{\mathbf{a}} \equiv \bigotimes_{i=1}^{n} i^{a_{ix}a_{iz}} X^{a_{ix}} Z^{a_{iz}}$. Here, $[\mathbf{u},\mathbf{a}] \equiv \mathbf{u}_x \cdot \mathbf{a}_z + \mathbf{u}_z \cdot \mathbf{a}_x$ is a symplectic inner product and X and Z are Pauli operators corresponding to shift and boost operations in phase space, respectively. This leads to the *discrete Wigner function* defined as $W_\rho(\mathbf{u}) \equiv \frac{1}{2^n}\mathrm{Tr}(\rho A(\mathbf{u}))$ [21, 23, 27], which shares common properties with the continuous-variable Wigner function [13, 21]: (i) it is real-valued and well-normalized, $\sum_{\mathbf{u}\in V_n} W_\rho(\mathbf{u}) = 1$; (ii) it is covariant under translation, $W_{T_{\mathbf{a}}\rho T_{\mathbf{a}}^\dagger}(\mathbf{u}) = W_\rho(\mathbf{u}+\mathbf{a})$; and (iii) its marginals indicate correct outcome probabilities.

On the other hand, the qubit Wigner function has exotic properties compared with the odd prime dimensional or continuous variable Wigner function [16, 17] that Clifford operations can induce negativity [21]. For example, a two-qubit state $|00\rangle$ in the computational basis state has a positive Wigner function, but after applying the Hadamard and CNOT gates, the resulting Bell state $|\Phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ has a negative Wigner function. This strongly limits the range of classically simulatable quantum circuits using qubit Wigner functions [28].

Efficient classical simulation via framed Wigner functions— To circumvent this problem, we introduce an additional degree of freedom to the qubit Wigner function [21–23]. We define a *framed Wigner function*

$$W_\rho^F(\mathbf{u}) \equiv \frac{1}{2^n}\mathrm{Tr}\left[\rho A^F(\mathbf{u})\right], \tag{2}$$

using a *frame function* F that characterizes an additional phase factor of phase space operators,

$$A^F(\mathbf{u}) \equiv \frac{1}{2^n}\sum_{\mathbf{a}\in V_n}(-1)^{[\mathbf{u},\mathbf{a}]+F(\mathbf{a})} T_{\mathbf{a}}. \tag{3}$$

The frame function maps a phase space point to a binary value, i.e., $F(\mathbf{a}) \in \{0,1\}$ for $\mathbf{a} \in V_n$, and satisfies the condition $F(\mathbf{0}) = 0$ to ensure that W_ρ^F is well-normalized. For example, a single qubit has two choices of frames, $F(a_x, a_z) = 0$ (zero frame) or $F(a_x, a_z) = a_x a_x$ (dual frame), up to translation symmetry under $T_{(a_x,a_z)}$ [21]. The framed Wigner function also respects some other properties of the conventional Wigner function, a special case with $F(\mathbf{a}) = 0$, such as covariance under translation and having a proper notion of marginals [15, 21, 29].

In terms of the framed Wigner function, the probability in Eq. (1) can be rewritten as

$$p(\mathbf{x}) = \sum_{\mathbf{u}\in V_n} W_{U\rho U^\dagger}^F(\mathbf{u}) P^F(\mathbf{x}|\mathbf{u}), \tag{4}$$

where $P^F(\mathbf{x}|\mathbf{u}) \equiv \mathrm{Tr}[A^F(\mathbf{u})\Pi_{\mathbf{x}}]$. Consequently, the circuit is classically simulatable when both $W_{U\rho U^\dagger}^F(\mathbf{u})$ and $P^F(\mathbf{x}|\mathbf{u})$ are positively represented. Our main result states that the additional degree of freedom given by the frame function (or simply frame) leads to a wider class of efficiently simulatable quantum circuits (see also Fig. 1):

Theorem 1. *Suppose an n-qubit quantum circuit composed of a product state input $\rho = \bigotimes_{i=1}^{n}\rho_i$ and a Clifford unitary U. If each ρ_i is positively represented in either zero or dual frame, the final state $U\rho U^\dagger$ is positively represented in a frame F, which can be evaluated from the initial frame with $\mathcal{O}(n^3)$-memory and $\mathcal{O}(\mathrm{poly}(n))$-time costs. From this, one can sample the measurement outcomes of some marginal qubits in the computational basis within $\mathcal{O}(n^2)$-time cost, where these marginal qubits are determined by the frame F.*

We highlight that pure nonstabilizer input states, such as $|A\rangle = \cos(\theta/2)|0\rangle + e^{i(\pi/4)}\sin(\theta/2)|1\rangle$ with $\theta = \cos^{-1}(1/\sqrt{3})$ [30], as well as their multiple copies

$|A\rangle^{\otimes m}$ can be positively represented by the framed Wigner function [21]. This can be compared to Ref. [22] utilizing a different phase space structure, wherein multi-copy nonstabilizer states are not always positively represented. While any quantum circuit can have a positive representation [24], it does not necessarily imply efficient classical simulation. In contrast, we explicitly construct a classical simulation algorithm that is efficient in both time and memory costs.

Compared to the classical simulation algorithm in Ref. [11], our algorithm covers some high Pauli-rank input states, such as $|A\rangle$. Moreover, our method provides an exact simulation, whereas Ref. [11] focuses on approximate simulation whose time cost depends on the accuracy. Hence, our results significantly extend a family of classically simulatable quantum circuits, despite their general hardness [5, 12].

The key idea of our algorithm is to defer the negativity induced by Clifford gates, enabling the phase point update until the measurement, summarized as follows:

Observation 1 (Clifford covariance under frame switching)**.** *For any Clifford gate U and input frame F_{in}, one can always find a frame F, a symplectic transform S, and $\mathbf{v} \in V_n$ such that $W^F_{U\rho U^\dagger}(S(\mathbf{u}) + \mathbf{v}) = W^{F_{\text{in}}}_\rho(\mathbf{u})$. Consequently, when an input state ρ is positively represented, i.e., $W^{F_{\text{in}}}_\rho(\mathbf{u}) \geq 0$, the output state can also be positively represented, i.e., $W^F_{U\rho U^\dagger}(\mathbf{u}) \geq 0$.*

While this stems from the fact that a Clifford gate transforms any Pauli operator to another Pauli operator up to the phase factor [6], a detailed form of F and S can be found in the Supplementary Material [31]. For example, the Bell state $|\Phi\rangle$, which exhibits negativity in the conventional Wigner function, can be positively represented under the frame $F(\mathbf{a}) = a_{1x}a_{1z} + a_{1z}a_{2z}a_{1x} + a_{2z}a_{1x}a_{2x} \pmod 2$. This observation can be applied to all stabilizer states and a wide class of nonstabilizer states generated from Clifford circuits. Compared to the case of a fixed framed function with adaptive Pauli measurements, where single-qubit operations are the only operations that preserve the positivity of the Wigner function [21], our result shows that positivity is preserved for any unitary, i.e., non-adaptive, Clifford operations by switching the frame.

We sketch the classical simulation algorithm described in Theorem 1, starting from the phase space point sampling. The framed Wigner function of a product input state $\rho = \bigotimes_{i=1}^n \rho_i$ is written as $W^{F_{\text{in}}}_\rho(\mathbf{u}) = \prod_{i=1}^n W^{F_i}_{\rho_i}(u_{ix}, u_{iz})$ with $F_{\text{in}}(\mathbf{a}) = \sum_{i=1}^n F_i(a_{ix}, a_{iz})$, where F_i can be either zero or dual frame. Hence, when $W^{F_i}_{\rho_i}$ is positive for every $i = 1, \cdots, n$, the phase space point of the final state following the distribution $W^F_{U\rho U^\dagger}(\mathbf{u}) = W^{F_{\text{in}}}_\rho(S^{-1}(\mathbf{u}))$ can be sampled by i) sampling (u_{ix}, u_{iz}) from each $W^{F_i}_{\rho_i}(u_{ix}, u_{iz})$, and then ii) applying the symplectic transform S to $(u_{1x}, \cdots, u_{nx}, u_{1z}, \cdots, u_{nz})$ followed by adding $\mathbf{v}$ from Observation 1, which overall takes $\mathcal{O}(n^2)$-time.

On the other hand, the positive Wigner function does not suffice for efficient classical simulation of the quantum circuit. One issue is that a frame function $F(\mathbf{a})$ may contain the high-degree monomials in $\mathbf{a}$, such as $\prod_{i=1}^n a_{ix}a_{iz}$. This gives rise to an exploding number of possible frame choices $(2^{(2^{2n}-2n-1)})$ [32], requiring exponential memory cost. For Clifford circuits with product state inputs, however, we show that the frame functions with polynomials of degree 3, i.e., cubic, are sufficient to run the proposed protocol. In other words, the frame can be written in the form, $F(\mathbf{a}) = \sum_{\mu,\nu} c_{\mu\nu} a_\mu a_\nu + \sum_{\mu,\nu,\omega} c_{\mu\nu\omega} a_\mu a_\nu a_\omega \pmod 2$, where $\mu, \nu, \omega \in \{1x, \ldots, nx, 1z, \ldots, nz\}$ and $c_{\mu\nu}, c_{\mu\nu\omega} \in \{0, 1\}$. This is because any frame function for each ith input qubit is either 0 or $a_{ix}a_{iz}$, and every frame transformation under a Clifford gate adds up to cubic terms [31]. We also note that linear terms can always be absorbed in the translation under $T_{\mathbf{a}}$ [21]. Thus, the possible number of frames is reduced into $2^{\mathcal{O}(n^3)}$, which can be efficiently manipulated with a $\mathcal{O}(n^3)$ bit memory.

For a given phase space point $\mathbf{u}$, the outcomes $\mathbf{x}$ can be classically sampled under the condition $P^F(\mathbf{x}|\mathbf{u}) \geq 0$. A sufficient condition for efficient sampling of the n-qubit computational basis measurement $\Pi_{\mathbf{x}} = |\mathbf{x}\rangle\langle\mathbf{x}|$ with $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}_2^n$ can be found as $F(\mathbf{0}_x, \mathbf{a}_z) = 0$, which leads to $P^F(\mathbf{x}|\mathbf{u}) = \langle\mathbf{x}| A^F(\mathbf{u}) |\mathbf{x}\rangle = (1/2^n) \sum_{\mathbf{a}_z \in \mathbb{Z}_2^n} (-1)^{(\mathbf{u}_x + \mathbf{x})\cdot\mathbf{a}_z + F(\mathbf{0}_x, \mathbf{a}_z)} = \delta_{\mathbf{x},\mathbf{u}_x}$ by noting that $\langle\mathbf{x}| T_{\mathbf{a}} |\mathbf{x}\rangle = \delta_{\mathbf{a}_x,\mathbf{0}_\mathbf{x}}(-1)^{\mathbf{x}\cdot\mathbf{a}_z}$. This directly leads to the outcome sampling of $\mathbf{x} = \mathbf{u}_x$ from the given phase space point $\mathbf{u}$. Remarkably, any Clifford circuit with a stabilizer input always has positive representation in a frame F obeying this condition so that *all the n-qubit outcomes can be efficiently simulated for stabilizer states*, reproducing the result of the Gottesman-Knill theorem [31].

For nonstabilizer inputs, however, it is uncommon to obtain a frame F with the condition $F(\mathbf{0}_x, \mathbf{a}_z) = 0$. Nevertheless, an efficient classical simulation of some marginal outcomes is still possible. We note that after tracing out the jth qubit, the phase space operator of the remaining qubits is given by $\text{Tr}_j[A^F(\mathbf{u})] = A^{F'}(\mathbf{u}')$ with $\mathbf{u}' = (\mathbf{u}'_x, \mathbf{u}'_z) \in V_{n-1}$ with $\mathbf{u}'_\lambda = (u_{1\lambda}, \cdots, u_{(j-1)\lambda}, u_{(j+1)\lambda}, \cdots, u_{n\lambda})$ for $\lambda = x, z$ and $F'(\mathbf{a}') = F(\mathbf{a})|_{a_{jx}=a_{jz}=0}$ with $\mathbf{a}' \in V_{n-1}$ similarly defined as $\mathbf{u}'$. Hence, all the monomials containing a_{jx} or a_{jz} are removed in the reduced frame F'. We repeat this step for $(n-k)$ times until the reduced frame of the remaining k-qubits satisfies $F'(\mathbf{0}'_x, \mathbf{a}'_z) = 0$. Therefore, the measurement outcomes $\mathbf{x}' = (x'_1, \cdots, x'_k) \in \mathbb{Z}_2^k$ on the remaining k-marginal qubits $\Pi_{\mathbf{x}'} = |\mathbf{x}'\rangle_M \langle\mathbf{x}'| \otimes \mathbb{1}_T$ can be efficiently sampled from $\mathbf{u}$ as $P^F(\mathbf{x}'|\mathbf{u}) = \text{Tr}[A^F(\mathbf{u})\Pi_{\mathbf{x}'}] = \langle\mathbf{x}'|A^{F'}(\mathbf{u}')|\mathbf{x}'\rangle = \delta_{\mathbf{x}',\mathbf{u}'_x}$, where M and T represent the Hilbert space of the measured and traced-

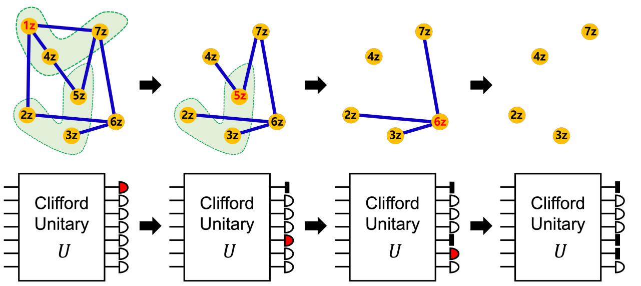


FIG. 2: Identifying efficiently simulatable qubits by solving the vertex cover problem using a greedy algorithm. Lines and shaded regions represent the hyperedges of $\mathcal{E}_2$, and $\mathcal{E}_3$, respectively. A qubit with the largest number of connected hyperedges is traced out at each step until all the hyperedges vanishes. The outcomes of the remaining qubits are efficiently simulatable.

out qubits, respectively.

Furthermore, finding efficiently simulatable marginal qubits can be translated into a graph problem by taking $\mathcal{V} = \{a_{1z}, \cdots, a_{nz}\}$ as vertices and by expressing $F(\mathbf{0}_x, \mathbf{a}_z) = \sum_{(i,j)\in\mathcal{E}_2} a_{iz}a_{jz} + \sum_{(i,j,k)\in\mathcal{E}_3} a_{iz}a_{jz}a_{kz}$ (mod 2) as hyperedges $\mathcal{E}_2$ and $\mathcal{E}_3$ connecting two and three vertices, respectively. We note that tracing out the jth qubit (taking $a_{jz} = 0$) corresponds to removing the vertex a_{jz} along with all hyperedges connected to it. Hence, removing vertices that fully cover the hyperedges leads to the remaining k-qubits satisfying $F'(\mathbf{0}'_x, \mathbf{a}'_z) = 0$. While finding the minimum number of such vertices, so-called the vertex cover problem, is an NP-hard problem [33], there exists a sub-optimal algorithm, for example, a *greedy algorithm* [26] running in poly-time (see Fig. 2).

Examples.—We apply the proposed simulation algorithm to two different types of random n-qubit log-depth Clifford circuits with 1D-neighboring and arbitrary long-range (completely connected) interactions between two qubits, where gate count is $L = \alpha n \ln(n)$ (see Refs. [31, 34] for more details). In both cases, we take the input state $\rho = |A\rangle\langle A|^{\otimes n}$ and adopt the greedy algorithm to find efficiently simulatable marginal qubits. As the circuit depth increases, the hypergraph of the final frame becomes more complicated, requiring a larger number of vertices (qubits) to be removed (traced out) [31]. Figure 3(a,c) shows that our simulation method successfully samples the measurement outcomes.

Figure 3(b) shows that for 1D architecture, the average number of classically simulatable qubits (n_{sim}) increases linearly by n. This result can be compared to the tensor network simulation, where all the n-qubit outcomes of these circuits can be efficiently simulated with $e^{\mathcal{O}(\alpha \ln n)} \sim n^{\mathcal{O}(\alpha)}$ time cost [35, 36]. In contrast, our algorithm simulates a linear portion of qubits with $\mathcal{O}(\alpha\text{poly}(n))$ time cost, including both evaluating the final frame F and solving its vertex cover problem [31].

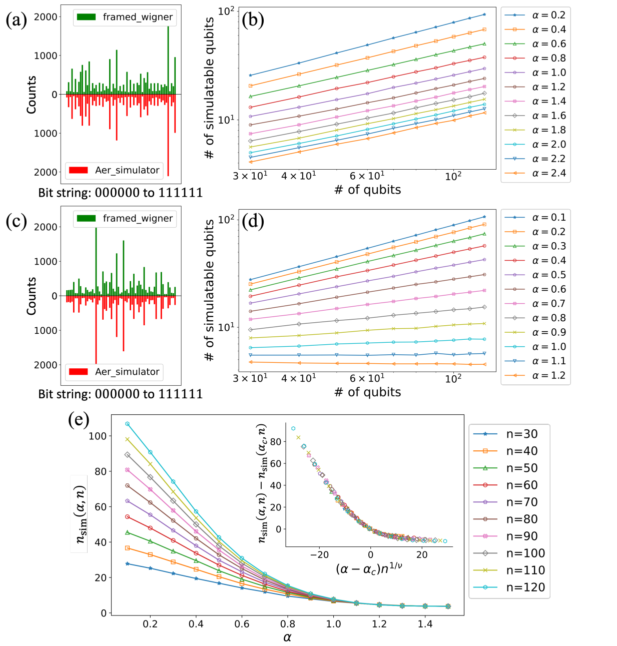


FIG. 3: (a), (c): Comparison between sampling results using the framed Wigner function and Qiskit Aer simulator for a randomly chosen 10-qubit log-depth Clifford circuit with (a) 1D-neighboring and (c) completely connected architecture. For both cases, nonstabilizer input state $|A\rangle\langle A|^{\otimes 10}$ is taken, and 6 marginal qubits are selected after solving the vertex cover problem. The y-axis shows the number of counts of binary string that simulators sampled by taking a total of 20000 samples. (b), (d): The averaged number of simulatable qubits (n_{sim}) by increasing the gate count $L = \alpha(n \ln n)$ of 1000 random Clifford circuits with (b) 1D-neighboring and (d) completely connected architectures. (e) Scaling behavior of n_{sim} by increasing α and data collapse after finite-size scaling.

Therefore, for the selected marginal outcomes, our approach offers a faster simulation than the tensor network method when the circuit depth α becomes large. From the numerical simulation, we observe remarkable improvement compared to the matrix product state simulator of the IBM Qiskit [31].

For the completely connected architecture, we observe a sharp transition of n_{sim} depending on the gate count. For $\alpha \leq \alpha_c$, n_{sim} scales linearly by increasing the number of qubits. In contrast, if the gate count exceeds a certain value $\alpha \geq \alpha_c$, we observe the sub-linear scaling of the n_{sim} (see Fig. 3(d)). From the finite-size scaling analysis by taking a general scaling form $n_{\text{sim}}(\alpha, n) - n_{\text{sim}}(\alpha_c, n) = f((\alpha - \alpha_c)n^{1/\nu})$ [37], we numerically estimate the critical value $\alpha_c \approx 0.81$ and $\nu \approx 1.28$ (see Fig. 3(e)). We conjecture that this critical phenomenon is closely related to the anti-concentration properties of the completely connected random circuit [34] as their critical points closely align, $\alpha = 5/6$.

Born probability estimation.— The framed Wigner function can also be utilized for estimating the Born probability in Eq. (4) under less restrictive conditions than outcome sampling. When the final phase space point $\mathbf{u}$ can be efficiently sampled from $W^F_{U\rho U^\dagger}(\mathbf{u}) \geq 0$, one can take an estimator $\hat{p}^F_{\mathbf{u}}(\mathbf{x}) = P^F(\mathbf{x}|\mathbf{u})$ for each $\mathbf{u}$. This leads to an unbiased estimation of the probability $p(\mathbf{x}) = \mathbb{E}_{\mathbf{u}}[\hat{p}^F_{\mathbf{u}}(\mathbf{x})]$, where $\mathbb{E}_{\mathbf{u}}[\cdot]$ denotes averaging over phase space points $\mathbf{u}$ from the distribution $W^F_{U\rho U^\dagger}(\mathbf{u})$ [27]. The estimator $\hat{p}^F_{\mathbf{u}}(\mathbf{x})$ is not necessarily positive and can be efficiently calculated for every $\mathbf{u}$ when $F(\mathbf{0}_x, \mathbf{a}_z)$ is quadratic [38–40]. One can also apply a procedure similar to the sampling scheme by tracing out $(n-k)$ qubits until $F'(\mathbf{0}'_x, \mathbf{u}'_z)$ becomes quadratic, resulting in an efficient estimation of the k-marginal outcome probability. The proposed protocol can be generalized for an arbitrary product state by mixing two different frames without affecting the degree of the reduced frame of the final state [31].

We analyze the precision of the proposed estimator using the mean squared error (MSE), $\mathrm{Var}_{\mathrm{Wig}}(\mathbf{x}') \equiv \mathbb{E}_{\mathbf{u}}[|\hat{p}^F_{\mathbf{u}}(\mathbf{x}') - p(\mathbf{x}')|^2]$ [41, 42]. The average MSE over all possible outcomes becomes $\overline{\mathrm{Var}}_{\mathrm{Wig}} \equiv 1/2^k \sum_{\mathbf{x}' \in \mathbb{Z}_2^k} \mathrm{Var}_{\mathrm{Wig}}(\mathbf{x}') = (1 - Z^{(k)}_{\mathrm{col}})/2^k$, where $Z^{(k)}_{\mathrm{col}} \equiv \sum_{\mathbf{x}' \in \mathbb{Z}_2^k} p(\mathbf{x}')^2 \geq 1/2^k$ is the collision probability of the k-marginal outcomes [10, 34]. This improves the previous result using the estimator in terms of the Pauli operator [43] with the average MSE of $\overline{\mathrm{Var}}_{\mathrm{Pauli}} = (1 - 1/2^k) Z^{(k)}_{\mathrm{col}} \geq \overline{\mathrm{Var}}_{\mathrm{Wig}}$ [31].

Remarks.— We have constructed a classical simulation algorithm for a Clifford circuit with nonstabilizer inputs based on the framed Wigner function. Our key observation is that the phase space point can be covariantly transformed under any Clifford gate by switching the frame of the Wigner function, which significantly extends the regime of positively represented states. Our protocol offers a classically efficient sampling of marginal outcomes with efficient time and memory cost, where these outcomes can be identified by solving the vertex cover problem. As examples, we have explored log-depth Clifford circuits and observed that the number of simulatable qubits behaves differently between locally and completely connected circuits.

While our approach of introducing a family of frame functions establishes a clear connection between Clifford operations and positive Wigner functions, even for a qubit system, it also leaves potential extensions and further exploration. A crucial question would be whether the proposed methods can be further extended to classically simulate non-Clifford circuits or adaptive Clifford circuits in the presence of noise.

The authors thank Kyunghyun Baek for helpful discussions. This work was supported by the National Research Foundation of Korea (NRF) grants funded by the Korean government (Grant Nos. NRF-2020R1A2C1008609, 2023R1A2C1006115 and NRF-2022M3E4A1076099) via the Institute of Applied Physics at Seoul National University, and by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (IITP-2021-0-01059 and IITP-2023-2020-0-01606). H.K. is supported by the KIAS Individual Grant No. CG085301 at Korea Institute for Advanced Study.

* Electronic address: hjkwon@kias.re.kr

† Electronic address: jeongh@snu.ac.kr

[1] P. W. Shor, SIAM Rev. **41**, 303 (1999).

[2] D. Deutsch and R. Jozsa, Proc. R. Soc. A **439**, 553 (1992).

[3] D. Gottesman, arXiv:quant-ph/9807006 (1998).

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[5] R. Jozsa and M. V. d. Nest, arXiv:1305.6190 (2013).

[6] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).

[7] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[8] M. Howard and E. Campbell, Phys. Rev. Lett. **118**, 090501 (2017).

[9] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A. **467**, 459 (2010).

[10] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Nat. Phys. **15**, 159 (2019).

[11] K. Bu and D. E. Koh, Phys. Rev. Lett. **123**, 170502 (2019).

[12] R. J. M. Yoganathan and S. Strelchuk, Proc. R. Soc. A **475**, 20180427 (2019).

[13] E. Wigner, Phys. Rev. **40**, 749 (1932).

[14] F. Soto and P. Claverie, J. Math. Phys. **24**, 97 (1983).

[15] D. Gross, J. Math. Phys. **47**, 122107 (2006).

[16] A. Mari and J. Eisert, Phys. Rev. Lett. **109**, 230503 (2012).

[17] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New J. Phys. **14**, 113011 (2012).

[18] V. Veitch, N. Wiebe, C. Ferrie, and J. Emerson, New J. Phys. **15**, 013037 (2013).

[19] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, Phys. Rev. X **6**, 021039 (2016).

[20] L. Kocia and P. Love, Phys. Rev. A **96**, 062134 (2017).

[21] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega, Phys. Rev. A **95**, 052334 (2017).

[22] R. Raussendorf, J. Bermejo-Vega, E. Tyhurst, C. Okay, and M. Zurel, Phys. Rev. A **101**, 012350 (2020).

[23] N. Koukoulekidis, H. Kwon, H. H. Jee, D. Jennings, and M. S. Kim, Quantum **6**, 838 (2022).

[24] M. Zurel, C. Okay, and R. Raussendorf, Phys. Rev. Lett. **125**, 260404 (2020).

[25] M. Zurel, C. Okay, and R. Raussendorf, arXiv:2305.17287 (2023).

[26] E. Halperin, SIAM J. Comput. **31**, 1608 (2002).

[27] H. Pashayan, J. J. Wallman, and S. D. Bartlett, Phys. Rev. Lett. **115**, 070501 (2015).

[28] L. Kocia, Y. Huang, and P. Love, Entropy **19**, 353 (2017).

[29] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters,

Phys. Rev. A **70**, 062101 (2004).

[30] H. Qassim, H. Pashayan, and D. Gosset, Quantum **5**, 606 (2021).

[31] Supplemental Material for detailed discussions and proofs.

[32] N. Nisan and M. Szegedy, Comput. Complex. **4**, 301 (1994).

[33] I. Dinur and S. Safra, Ann. Math. **162**, 439 (2005).

[34] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, PRX Quantum **3**, 010333 (2022).

[35] J. C. Napp, R. L. La Placa, A. M. Dalzell, F. G. S. L. Brandão, and A. W. Harrow, Phys. Rev. X **12**, 021021 (2022).

[36] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).

[37] B. Skinner, J. Ruhman, and A. Nahum, Phys. Rev. X **9**, 031009 (2019).

[38] A. Montanaro, J. Phys. A: Math. Theor. **50**, 084002 (2017).

[39] K. Bu and D. E. Koh, Commun. Math. Phys. **390**, 471 (2022).

[40] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Quantum **3**, 181 (2019).

[41] L. G. V. M. R. Jerrum and V. V. Vazirani, Theor. Comput. Sci. **43**, 169 (1986).

[42] B. Charles, SIAM Rev. **27**, 264 (1985).

[43] H. Pashayan, S. D. Bartlett, and D. Gross, Quantum **4**, 223 (2020).

Supplemental Materials: Extending Classically Simulatable Bounds of Clifford Circuits with Nonstabilizer States via Framed Wigner Functions

Guedong Park,[1] Hyukjoon Kwon,[2] and Hyunseok Jeong[3]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*
[2] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 02455, Korea*
[3] *Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*

CONTENTS

I. PROOF OF THEOREM 1

In this section, we prove Theorem 1 in the main text. Let us first restate Theorem 1 and clarify each step of the proof.

Theorem 1. *Suppose an n-qubit quantum circuit composed of a product state input $\rho = \bigotimes_{i=1}^{n} \rho_i$ and a Clifford unitary U. If each ρ_i is positively represented in either zero or dual frame, the final state $U\rho U^\dagger$ is positively represented within $\mathcal{O}(n^3)$-memory and $\mathcal{O}(\mathrm{poly}(n))$-time costs. From this, one can sample the measurement outcomes of some marginal qubits in the computational basis within $\mathcal{O}(n^2)$-time cost, where these marginal qubits are determined by the frame F.*

To complete the proof, we separately show the following four main parts of Theorem 1.

1. The Wigner representation of a product state input via zero or dual frame.
2. Changing the positively representing frame by the Clifford operation and how the Wigner function transforms as a result. This proves Observation 1.
3. Time and memory complexities of task 2.
4. The capability of classical simulation with a reduced frame after marginalization.

Additionally, we will prove that all stabilizer states can be positively represented under a specific frame so that single-qubit Pauli measurements on all qubits can be efficiently carried out via our method, hence reproducing the result of the Gottesmann-Knill theorem [1]. Finally, we will discuss the accessibility of information on sampled outcomes when the final frame has relaxed conditions of its degree.

A. Wigner representation of a product state

We discuss how a product state can be positively represented under a quadratic frame function. When we consider only a single qubit system, the frame function can have up to a second degree. Therefore, there are two frame $F = 0$ (*zero frame*) and $F = a_{1x}a_{1z}$ (*dual frame*). Now, suppose that for $i \in [n]$, each single qubit state ρ_i is positively represented under $F_i = b_i a_{ix} a_{iz}$ with $b_i = 0$ (zero frame) or $b_i = 1$ (dual frame). Also, we define the Pauli operator acting on the i-th qubit, $T_{\mathbf{a}_i} \equiv i^{a_{ix}a_{iz}} X^{a_{ix}} Z^{a_{iz}}$. Then, we can rewrite ρ_i as

$$\rho_i = \frac{1}{2} \sum_{\mathbf{u}_i, \mathbf{a}_i \in \mathbb{Z}_2^2} W_{\rho_i}(\mathbf{u}_i)(-1)^{[\mathbf{u}_i, \mathbf{a}_i] + b_i a_{ix} a_{iz}} T_{\mathbf{a}_i}. \tag{1}$$

Consequently, we obtain the Wigner representation of a product state input as follows:

$$\rho = \bigotimes_i^n \rho_i = \frac{1}{2^n} \sum_{\mathbf{u}, \mathbf{a} \in V_n} \left(\prod_{i=1}^n W_{\rho_i}(\mathbf{u}_i) \right) (-1)^{[\mathbf{u}, \mathbf{a}] + \sum_{i=1}^n b_i a_{ix} a_{iz}} T_{\mathbf{a}}, \tag{2}$$

where $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n)$, $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n)$, and $T_{\mathbf{a}} = \bigotimes_{i=1}^n T_{\mathbf{a}_i}$. Note that ρ is positively represented under the frame $\sum_{i=1}^n b_i a_{ix} a_{iz}$. Hence, the Wigner function of a product state can be represented as a product of single-qubit Wigner functions.

B. Frame changing rules (Observation 1)

We explain the frame-changing rules under the Clifford operations and the corresponding transformation of the Wigner function. Suppose an n-qubit quantum state ρ is positively represented under the frame F_{in}. As we discussed in the main text, after applying a Clifford unitary U, $U\rho U^\dagger$ may have negativity [2] when the frame is fixed. However, we note that the transformation of $T_{\mathbf{a}}$ under any Clifford unitary U has the following form [1]:

$$U T_{\mathbf{a}} U^\dagger = (-1)^{P(\mathbf{a})} T_{S(\mathbf{a})}, \tag{3}$$

where symplectic matrices S and phase functions $P(\mathbf{a})$ for each Clifford gate are given in Table I. This leads to

$$\begin{aligned}
U\rho U^\dagger &= \frac{1}{2^n} \sum_{\mathbf{u}, \mathbf{a} \in V_n} W_\rho^{F_{\text{in}}}(\mathbf{u})\, (-1)^{[\mathbf{u}, \mathbf{a}] + F_{\text{in}}(\mathbf{a})}\, U T_{\mathbf{a}} U^\dagger &(4)\\
&= \frac{1}{2^n} \sum_{\mathbf{u}, \mathbf{a}} W_\rho^{F_{\text{in}}}(\mathbf{u})\, (-1)^{[\mathbf{u}, \mathbf{a}] + F_{\text{in}}(\mathbf{a}) + P(\mathbf{a})}\, T_{S(\mathbf{a})} &(5)\\
&= \frac{1}{2^n} \sum_{\mathbf{u}, \mathbf{a}} W_\rho^{F_{\text{in}}}(\mathbf{u})\, (-1)^{[S(\mathbf{u}), \mathbf{a}] + F_{\text{in}}(S^{-1}(\mathbf{a})) + P(S^{-1}(\mathbf{a}))}\, T_{\mathbf{a}} &(6)\\
&= \frac{1}{2^n} \sum_{\mathbf{u}, \mathbf{a}} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}))\, (-1)^{[\mathbf{u}, \mathbf{a}] + F_{\text{in}}(S^{-1}(\mathbf{a})) + P(S^{-1}(\mathbf{a}))}\, T_{\mathbf{a}} &(7)\\
&= \frac{1}{2^n} \sum_{\mathbf{u}, \mathbf{a}} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}))\, (-1)^{[\mathbf{u}, \mathbf{a}] + F(\mathbf{a})}\, T_{\mathbf{a}} &(8)\\
&= \frac{1}{2^n} \sum_{\mathbf{u}} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u})) A^F(\mathbf{u}). &(9)
\end{aligned}$$

By noting that $U\rho U^\dagger = \frac{1}{2^n} \sum_{\mathbf{u}} W_{U\rho U^\dagger}^F(\mathbf{u}) A^F(\mathbf{u})$ in the new frame $F(\mathbf{a}) = F_{\text{in}}(S^{-1}\mathbf{a}) + P(S^{-1}\mathbf{a})$, we obtain $W_{U\rho U^\dagger}^{F_{\text{in}}}(\mathbf{u}) = W_\rho^F(S^{-1}(\mathbf{u}))$. This proves Observation 1.

Clifford gate	S	$P(\mathbf{a})$
$CNOT_{i\to j}$-gate	$a_{iz}\longleftarrow a_{iz}+a_{jz}$ $a_{jx}\longleftarrow a_{ix}+a_{jx}$	$a_{jz}a_{ix}(a_{iz}+a_{jx}+1)$
H_i-gate	$a_{ix}\longleftarrow a_{iz}$ $a_{iz}\longleftarrow a_{ix}$	$a_{iz}a_{ix}$
S_i-gate	$a_{iz} \longleftarrow a_{ix}+a_{iz}$	$a_{iz}a_{ix}$

TABLE I. A table that shows the symplectic transformation (S) of elementary Clifford gates and corresponding phase function ($P(\mathbf{a})$). $A \leftarrow B$ means A is transformed to B.

We further note that all linear terms within the frame $F(\mathbf{a})$ can be replaced by a translation in the Wigner function. By noting that linear terms can be expressed as $[\mathbf{v},\mathbf{a}]$ for some $\mathbf{v}\in V_n$, we obtain

$$W_\rho^F(\mathbf{u}) = \frac{1}{2^n}\sum_{\mathbf{a}\in V_n}(-1)^{[\mathbf{u},\mathbf{a}]+F(\mathbf{a})}\mathrm{Tr}[\rho T_{\mathbf{a}}] \tag{10}$$

$$= \frac{1}{2^n}\sum_{\mathbf{a}\in V_n}(-1)^{[\mathbf{u}+\mathbf{v},\mathbf{a}]+(F(\mathbf{a})+[\mathbf{v},\mathbf{a}])}\mathrm{Tr}[\rho T_{\mathbf{a}}] \tag{11}$$

$$= \frac{1}{2^n}\sum_{\mathbf{a}\in V_n}(-1)^{[\mathbf{u}+\mathbf{v},\mathbf{a}]+F'(\mathbf{a})}\mathrm{Tr}[\rho T_{\mathbf{a}}] \tag{12}$$

$$= W_\rho^{F'}(\mathbf{u}+\mathbf{v}), \tag{13}$$

where $F'(\mathbf{a}) = F(\mathbf{a}) + [\mathbf{v},\mathbf{a}]$. In other words, if a frame F has a linear term, then its Wigner function of σ follows by translating the arguments of the original Wigner function.

C. Time and memory complexities of frame changing

We discuss the time and memory complexities of the proposed simulation algorithm. We first discuss the memory cost for storing the frame functions. Suppose we have a product state input ρ which is positively represented under the frame $F_{\mathrm{in}} = \sum_{i=1}^n b_i a_{ix} a_{iz}$ with $b_i \in \{0,1\}$. We recall that the final frame after the Clifford operation has the following transformation rule, $F(\mathbf{a}) = F_{\mathrm{in}}(S^{-1}\mathbf{a}) + P(S^{-1}\mathbf{a})$. Since all Clifford operations can be generated by gates in the set $\{CNOT, H, S\}$ shown in Table. I with phase functions of degree up to 3 and linear transformation S^{-1} does not raise the degree of frame function, the resulting frame must have up to the third degree. In light of those facts, we can formalize the final frame as the following cubic binary valued polynomial,

$$F(\mathbf{a}) = \sum_\mu c_\mu a_\mu + \sum_{\mu,\nu} c_{\mu\nu} a_\mu a_\nu + \sum_{\mu,\nu,\omega} c_{\mu\nu\omega} a_\mu a_\nu a_\omega \pmod 2, \tag{14}$$

where $\mu,\nu,\omega \in \{1x,\dots,nx,1z,\dots,nz\}$. To store that information of the frame, we need $\mathcal{O}(n^3)$-memory to contain all coefficients of possible monomials.

We then discuss the time and memory costs for updating the frames for each Clifford gate acting on at most two qubits. With $\mathcal{O}(1)$-time and memory complexity, we can find the symplectic matrix S and phase function P for this gate. Given a frame F to be changed, we collect all monomials having variables in $\{a_{ix}, a_{iz}, a_{jx}, a_{jz}\}$. As we collect each monomial, we linearly transform it via S^{-1} and obtain the set of newly generated monomials. Then we add this set of monomials to F, and we add constant-sized monomials of $P(S^{-1}(\mathbf{a}))$. Since we need at most $\mathcal{O}(n^3)$ memory to record arbitrary cubic frame functions and the above steps do not raise the degree of the output frame, newly generated monomials can be recorded in another $\mathcal{O}(n^3)$-memory. Moreover, we can obtain the set of generated monomials in at most $\mathcal{O}(n^3)$-time by putting or deleting the generated monomial in the new memory, as we transform the selected monomial in F with constant time. The union with the generated set can be done in time complexity with the same scaling of memory. Therefore, the total time complexity is at most $\mathcal{O}(\mathrm{poly}(n))$ given that we have poly(n)-number of 2-qubit Clifford gates.

After getting through all the Clifford gates, by the last argument of Section I B, we can always choose $\mathbf{v}_F \in V_n$ for the final frame without linear terms by applying an additional translation to the Wigner function to be $W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))$, i.e., $W_{U\rho U^\dagger}^F(S(\mathbf{u})+\mathbf{v}_F) = W_\rho^{F_{\mathrm{in}}}(\mathbf{u})$. Also, this translation does not affect the scale of total time complexity. From now on, for convenience, we will always assume that the final frame has no linear terms.

D. Weak simulation

Now, we discuss sufficient conditions of weak simulation via the framed Wigner function. Suppose the frame F satisfies $F(\mathbf{0}_x, \mathbf{a}_z) = 0$. We then note that $P^F(\mathbf{x}|\mathbf{u})$ with $\mathbf{x} \in \mathbb{Z}_2^n$ can be expressed as

$$\begin{aligned} P^F(\mathbf{x}|\mathbf{u}) &= \langle \mathbf{x}|A^F(\mathbf{u})|\mathbf{x}\rangle && (15)\\ &= \frac{1}{2^n} \sum_{\mathbf{a}\in V_n} (-1)^{[\mathbf{u},\mathbf{a}]+F(\mathbf{a})} \langle \mathbf{x}|T_{\mathbf{a}}|\mathbf{x}\rangle && (16)\\ &= \frac{1}{2^n} \sum_{\mathbf{a}\in V_n} (-1)^{[\mathbf{u},\mathbf{a}]+F(\mathbf{a})} \delta_{\mathbf{a}_x,0} (-1)^{\mathbf{a}_z\cdot\mathbf{x}} && (17)\\ &= \frac{1}{2^n} \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} (-1)^{\mathbf{a}_z\cdot(\mathbf{x}+\mathbf{u}_x)} && (18)\\ &= \delta_{\mathbf{x},\mathbf{u}_x}. && (19) \end{aligned}$$

Next, we express the Born probability $p(\mathbf{x}) = \mathrm{Tr}(U\rho U^\dagger |\mathbf{x}\rangle\langle\mathbf{x}|)$ in terms of the framed Wigner function. When the output state $U\rho U^\dagger$ is positively represented as $W^F_{U\rho U^\dagger}(\mathbf{u}) = W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))$, we observe that

$$\begin{aligned} \mathrm{Tr}(U\rho U^\dagger |\mathbf{x}\rangle\langle\mathbf{x}|) &= \sum_{\mathbf{u},\mathbf{a}\in V_n} W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F)) \langle \mathbf{x}|A^F(\mathbf{u})|\mathbf{x}\rangle && (20)\\ &= \sum_{\mathbf{u},\mathbf{a}} W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))\delta_{\mathbf{x},\mathbf{u}_x} && (21)\\ &= \sum_{\mathbf{u}_z\in\mathbb{Z}_2^n,\mathbf{a}\in V_n} W_\rho^{F_{in}}(S^{-1}((\mathbf{x}+(\mathbf{v}_F)_x, \mathbf{u}_z+(\mathbf{v}_F)_z)). && (22) \end{aligned}$$

By the above result, we can make a weak simulation scheme, which samples outcomes $\mathbf{x}$ following the probability distribution $p(\mathbf{x})$, as follows:

1. Sample the phase point $\mathbf{u} \in V_n$ from $W_\rho^{F_{\mathrm{in}}}(\mathbf{u})$ with the initial frame F_{in}.
2. Update $\mathbf{u} \leftarrow S(\mathbf{u})$
3. Update $\mathbf{u} \leftarrow \mathbf{u} + \mathbf{v}_F$
4. Output $\mathbf{u}_x$.

Even if the resulting frame does not satisfy the condition $F(\mathbf{0}_x, \mathbf{a}_z) = 0$, we could find marginal measurements in which the reduced frame satisfies that condition. We explain this in more detail here. Without losing the generality, assume that we measure only the first to $k(\leq n)$-th qubits and then trace out the others. The marginal measurement probability to obtain $\mathbf{x}' \in \mathbb{Z}_2^k$ then becomes

$$\begin{aligned} p(\mathbf{x}') &= \sum_{\mathbf{x}''\in\mathbb{Z}_2^{n-k}} \mathrm{Tr} U\rho U^\dagger |\mathbf{x}'\oplus\mathbf{x}''\rangle\langle\mathbf{x}'\oplus\mathbf{x}''| && (23)\\ &= \sum_{\mathbf{x}''\in\mathbb{Z}_2^{n-k}} \sum_{\mathbf{u},\mathbf{a}\in V_n} W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v})) \langle \mathbf{x}'\oplus\mathbf{x}''|A^F(\mathbf{u})|\mathbf{x}'\oplus\mathbf{x}''\rangle && (24)\\ &= \frac{1}{2^k} \sum_{\mathbf{u}} W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v})) \sum_{\mathbf{a}'_z\in\mathbb{Z}_2^k} (-1)^{\mathbf{u}_x\cdot(\mathbf{a}'_z\oplus\mathbf{0}'')+\mathbf{a}'_z\cdot\mathbf{x}'+F(\mathbf{0},\mathbf{a}'_{\mathbf{z}}\oplus\mathbf{0}'')}. && (25) \end{aligned}$$

Hence, if the $F'(\mathbf{0}_x, \mathbf{a}'_z) = F(\mathbf{0}_x, \mathbf{a}'_{\mathbf{z}} \oplus \mathbf{0}'') = 0$, the last equation becomes $\frac{1}{2^k}\sum_{\mathbf{u}} W_\rho^{F_{\mathrm{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))\delta_{\mathbf{x}',\mathbf{u}'_x}$. Then, we can efficiently measure the outcome $\mathbf{x}'$ by similar steps to the main algorithm. We just need to replace $\mathbf{u}_x$ with $(u_{1x}, \ldots, u_{kx}, 0, \ldots, 0)$. In the same way, if the resulting frame after marginalizing arbitrary k-qubits satisfies $F'(\mathbf{0}'_x, \mathbf{a}'_z) = 0$, we can efficiently measure the marginal outcome. We note that after marginalizing $n-1$ qubits, the reduced frame must become zero.

Now, let us recollect the results obtained through this section to encapsulate the proof. We assume that a input state is a product state $\rho = \bigotimes_{i=1}^n \rho_i$ and each ρ_i is positively represented under a single qubit frame $F_i = 0$ or $F_i = a_{ix}a_{iz}$. Then ρ can be positively represented under $F_{\mathrm{in}} = \sum_{i=1}^n b_i a_{ix} a_{iz}$ $(\forall b_i \in \{0,1\})$. As we discussed in the previous section, the time complexity of frame changing is up to poly(n) as well as obtaining S [1] with at most $\mathcal{O}(n^3)$ memory cost. Marginalizing the resulting frame until it becomes linear takes at most $\mathcal{O}(n^4)$-time. This is because checking if a given frame has non-linear terms takes $\mathcal{O}(n^3)$-time, and the reduced frame must be zero after the marginalization of $n-1$ qubits. Also, updating $\mathbf{u}$ to $\mathbf{u}'$ is a simple matrix multiplication which takes $\mathcal{O}(n^2)$ time. This completes the proof of Theorem 1. In Section II, we provide a systematic program to solve this problem by solving the graph theoretical problem.

E. Efficient simulation of Pauli measurements to stabilizer states

If the depth of the circuit becomes high, the resulting frame may contain many quadratic and cubic terms. Hence, only a small number of qubits might be efficiently simulatable. However, we show that if the input is a stabilizer state, any non-adaptive Clifford circuit can be transformed to the *CH-form* [3], which satisfies the efficient sampling condition. This can be shown by the following Lemma:

Lemma 1. *[Bruhat Decomposition [4, 5]] (i) An arbitrary n-qubit Clifford circuit can be rewritten by layers* $\mathrm{hF'}-\mathrm{SW}-\mathrm{H}-\mathrm{hF}$*, where* H *is a layer of Hadamard gates,* SW *is a layer of SWAP gates (hence of CNOT gates) and* $\mathrm{hF},\mathrm{hF'}$ *are CNOT-CZ-S-Pauli layered circuits. This decomposition can be done with poly(n)-time.*

(ii) Starting from the zero frame $F_{\text{in}}=0$, the changed frame F after $\mathrm{Pauli}-\mathrm{H}-\mathrm{hF}$ *section satisfies $F(\mathbf{0}_x,\mathbf{a}_z)=0$.*

Proof. The proof of (i) can be found in Refs. [4, 5]. We show (ii) by noting that the phase functions (see Table. I) of $H, S, CNOT$ gates do not have quadratic or cubic monomials with only a_{iz} terms, and the symplectic transforms of S and $CNOT$ gates do not change a_{ix} to a_{jz}. Furthermore, we can easily note that the phase function of the Pauli operator is linear, and the symplectic operation is identity. Hence, the final frame $F(\mathbf{0},\mathbf{a}_z)$ must be linear, and those linear terms can be converted into translation following the last arguments of Section I C. □

We can represent stabilizer states as zero state input rotated by a Clifford operation. Also, by Lemma 1, this operation can be transformed to $\mathrm{hF'}-\mathrm{S}-\mathrm{H}-\mathrm{hF}$ form. However, the first CNOT-CZ-S part of hF' section does not affect to zero state. Hence, we have a zero state followed by $\mathrm{Pauli}-\mathrm{H}-\mathrm{hF}$ sections. Note the zero states can be positively represented under zero frame, and the resulting frame satisfies $F(\mathbf{0}_x,\mathbf{a}_z)=0$. Therefore, all the n-qubit measurement outcomes $\mathbf{x}$ can be efficiently simulated via the framed Wigner function.

F. Simulation for a resulting frame of second degree

When the resulting frame $F'(\mathbf{0}_x,\mathbf{a}_z)$ is quadratic, we cannot directly measure the outcome. However, we can still obtain some information about those outcomes.

Proposition 1. *Let ρ be positively represented under a single frame F_{in}, and the final frame is F. We take I_F such that $F(\mathbf{a}_x=\mathbf{0},\mathbf{a}_z)\big|_{a_{iz}=0\text{ for }i\notin I_F}$ is a quadratic Boolean function. Then we can simulate to obtain at least $\lfloor\frac{|I_F|+1}{2}\rfloor$ number of Boolean function values with the arguments of $|I_F|$-marginal measurement outcome.*

Proof. We first assume that $F(\mathbf{a}_x=\mathbf{0},a_z)\big|_{a_{iz}=0\text{ for }i\notin I_F}$ only has quadratic terms. We choose one element from $i_1\in[n]\backslash I$ and rewrite $F(\mathbf{a}_x=\mathbf{0},a_z)\big|_{a_{iz}=0\text{ for }i\notin I_F}$ as $a_{i_1z}(L_{\{i_1\}}(\mathbf{a}_z))+Q_{\{i_1\}}(\mathbf{a}_z)$, where $L_{\{j_1,j_2,\dots\}}$ denotes a linear Boolean function that does not have variables $\{a_{j_1z},a_{j_2z},\dots\}$ and $Q_{\{j_1,j_2,\dots\}}$ denotes a quadratic Boolean function not having variables $\{a_{j_1z},a_{j_2z},\dots\}$. Now, we choose one another variable $i_2\neq i_1$ in $L_{\{i_1\}}$ and find an invertible linear transform S_1 that transforms $a_{i_1z}L_{\{i_1\}}$ to $a_{i_1z}a_{i_2z}$ $(i_1\neq i_2)$ and $Q_{\{i_1\}}$ to another quadratic polynomial $Q^{(1)}_{\{i_1\}}$ still not having variable a_{i_1z}. This is possible by taking S_1 which transforms a_{i_2} to $L_{\{i_1\}}(\mathbf{a}_z)$ and leaves the other variables unchanged. Then, S_1 is linear and invertible.

After that, $a_{i_1z}(L_{\{i_1\}}(\mathbf{a}_z))+Q_{\{i_1\}}(\mathbf{a}_z)$ is transformed to $a_{i_1z}a_{i_2z}+Q^{(1)}_{\{i_1\}}(\mathbf{a}_z)$. Next, we decompose $Q^{(1)}_{\{i_1\}}$ so that $a_{i_1z}a_{i_2z}+Q^{(1)}_{\{i_1\}}(\mathbf{a}_z)$ is transformed to $a_{i_1z}a_{i_2z}+a_{i_2z}L_{\{i_1,i_2\}}+Q^{(1)}_{\{i_1,i_2\}}(\mathbf{a}_z)$. If $Q^{(1)}_{\{i_1\}}$ does not have a_{i_2z} hence $L_{\{i_1,i_2\}}=0$, we set S_2 as $n\times n$ identity and choose $i_3\in[n]\backslash\{i_1,i_2\}$ and decompose $Q^{(1)}_{\{i_1\}}$ starting with i_3 as we do with i_1. Otherwise, if $L_{\{i_1,i_2\}}$ is non-zero, then we again take a linear transform S_2 that converts the above equation to $a_{i_1z}a_{i_2z}+a_{i_2z}a_{i_3z}+Q^{(2)}_{\{i_1,i_2\}}(\mathbf{a}_z)$. After repeating this, we obtain the final resulting polynomial $a_{i_1z}a_{i_2z}+c_2a_{i_2z}a_{i_3z}+\dots+c_pa_{i_pz}a_{i_{p+1}z}$ $(p\in\mathbb{N}$ and, $c_2,\dots c_p\in\{0,1\})$.

From these arguments, the marginal outcome probabilities $p(\mathbf{x}')$ on the subset of qubits I_F under U(with symplectic transform S) is

$$p(\mathbf{x}') = \sum_{\mathbf{x}''} \mathrm{Tr}(\left|\mathbf{x}' \oplus \mathbf{x}''\right\rangle \left\langle \mathbf{x}' \oplus \mathbf{x}''\right| U\rho U^{\dagger}) \tag{26}$$

$$= \sum_{\mathbf{u}} \left(\sum_{\substack{\mathbf{a}_z \in \mathbb{Z}_2^n, \\ a_{iz}=0 \text{ for } i\in[n]\setminus I_F}} \frac{1}{2^{|I_F|}} W_{\rho}^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))\,(-1)^{\left((\mathbf{u}_x+(\mathbf{x}'\oplus 0))\cdot \mathbf{a}_z + F'(\mathbf{a}_x=\mathbf{0},\mathbf{a}_z)\right)} \right) \tag{27}$$

$$= \sum_{\mathbf{u}} \left(\sum_{\substack{\mathbf{a}_z \in \mathbb{Z}_2^n, \\ a_{iz}=0 \text{ for } i\in[n]\setminus I_F}} \frac{1}{2^{|I_F|}} W_{\rho}^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))\,(-1)^{((\mathbf{u}_x+(\mathbf{x}'\oplus 0))\cdot(S_1S_2\ldots S_p)(\mathbf{a}_z)+a_{i_1z}a_{i_2z}+c_2a_{i_2z}a_{i_3z}+\ldots+c_pa_{i_pz}a_{i_{p+1}z})} \right) \tag{28}$$

$$= \sum_{\mathbf{u}} \left(\sum_{\substack{\mathbf{a}_z \in \mathbb{Z}_2^n, \\ a_{iz}=0 \text{ for } i\in[n]\setminus I_F}} \frac{1}{2^{|I_F|}} W_{\rho}^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))(-1)^{(S_1S_2\ldots S_p)^T(\mathbf{u}_x+(\mathbf{x}'\oplus 0))\cdot\mathbf{a}_z+a_{i_1z}a_{i_2z}+c_2a_{i_2z}a_{i_3z}+\ldots+c_pa_{i_pz}a_{i_{p+1}z}} \right). \tag{29}$$

Therefore, we conclude that (note that $S_1S_2\ldots S_p$ acts as an identity on the subset of qubits $[n]\setminus I_F$)

$$\sum_{\mathbf{x}''} p\left(\left((S_1S_2\ldots S_p)^T\right)^{-1}(\mathbf{x}'\oplus\mathbf{x}'')\right) \tag{30}$$

$$= \sum_{\mathbf{u}} \left(\sum_{\substack{\mathbf{a}_z \in \mathbb{Z}_2^n, \\ a_{iz}=0 \text{ for } i\in[n]\setminus I_F}} \frac{1}{2^{|I_F|}} W_{\rho}^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))(-1)^{\left((S_1S_2\ldots S_p)^T(\mathbf{u}_x)+(\mathbf{x}'\oplus 0)\right)\cdot\mathbf{a}_z+a_{i_1z}a_{i_2z}+c_2a_{i_2z}a_{i_3z}+\ldots+c_pa_{i_pz}a_{i_{p+1}z}} \right). \tag{31}$$

Now, we further trace out qubits in $\{i_2, i_4, \ldots, i_p\}$ if p is even and $\{i_2, i_4, \ldots, i_{p+1}\}$ if p is odd until the remaining frame becomes linear, then use the simulation algorithm of Section I D. However, after the step 3, we must take $\mathbf{u}_x$ to $(S_1S_2\ldots S_p)^T(\mathbf{u}_x)$. Consequently, given that p is even (routine is similar for odd p), the outcome string is $\left(\left((S_1S_2\ldots S_p)^T(\mathbf{u}_x)\right)_i\right)_{i\in I_F\setminus\{i_2,i_4,\ldots,i_p\}}$. The worst case happens when all c_k $(k\in[n])$ is 1 and $p = |I_F - 1|$ so that the number of measurable qubits is $\lfloor\frac{|I_F|+1}{2}\rfloor$. Time to obtain $(S_1S_2\ldots S_p)^T$ is at most poly(n)-time, and then measuring outcome takes $\mathcal{O}(n^2)$-time. Since we rotate $\mathbf{u}_x$ once more by $(S_1S_2\ldots S_p)^T$, the measured outcome is partial elements of $(S_1S_2\ldots S_p)^T\left((S_1S_2\ldots S_p)^T\right)^{-1}(\mathbf{x}')$ that are the linear Boolean function values of direct measurement outcome $\left((S_1S_2\ldots S_p)^T\right)^{-1}(\mathbf{x}')$ (see Eq. (30)). □

II. FINDING EFFICIENTLY SIMULATABLE QUBITS BY SOLVING THE VERTEX COVER PROBLEM

In the main text, we discuss that the k-marginal qubits are efficiently simulatable when tracing out the $(n-k)$ qubits until the reduced frame meets the condition $F'(\mathbf{0}_x, \mathbf{a}_z') = 0$. In this section, we discuss how this can be translated into a graph theoretical problem, known as *the vertex cover problem* in more detail.

A. Basic notation of graph theory

Here, we introduce a formal definition of hypergraph and the vertex cover problem.

Definition 1 (Hypergraph). *(i) Let V be a non-empty set. We say a tuple $G(V,E)$ is a* hypergraph *if and only if E is a set of subsets $e \in V$ of V. We call each element in E an* edge*. From now on, we always assume $\forall e \in E, |e| > 1$.*

Let $G(V, E)$ be a hypergraph.
(ii) We say G is of kth-degree ($k \in \mathbb{N}$) if all edges in G contain at most k vertices.
*(iii) If all elements of E have ($k \in \mathbb{N}$)-number of elements in V, then we call $G(V, E)$ as a k-*uniform hypergraph *or simply a k-*graph*. Also, a 2-graph is just called a* graph*.*

Next, we define several properties of a hypergraph.

Definition 2. *Let $G(V, E)$ be a hypergraph.*
i) $V' \subset V$ is a vertex cover *if all edges in E contain some elements in V'. $A \subset V$ is the* minimal vertex cover *if every vertex cover $V' \subset V$ satisfies $|V'| \geq |A|$.*
ii) $S' \subset V$ is an independent set *if any two elements in S' are not contained in same edge in E. $B \subset V$ is the* maximal independent set *if every independent set $S' \subset V$ satisfies $|S'| \leq |B|$.*
iii) Let A be a minimal vertex cover of G and B be a maximal independent set in G. Then we denote $\nu(G) \equiv |A|$ and $\triangle(G) \equiv |B|$. We note that minimal(maximal resp.) vertex cover(independent set) could not be unique, but $\nu(G)$ and $\triangle(G)$ are unique.
iv) For $v \in V$, order *of v, $d(v)$ is the number of edges containing v.*
v) Maximal order *of the graph, $d(G)$ is* $\max_{v \in V} \{d(v)\}$.

The *vertex cover problem* is to find the minimal vertex cover of a given hypergraph. Now, we obtain the following result.

Corollary 1. *For any hypergraph $G(V, E)$, $\nu(G) + \triangle(G) \leq |V|$.*

Proof. Consider a maximal independent set $S \subset V$ ($|S| = \triangle(G)$) and suppose $|V \backslash S| = |V| - \triangle(G) < \nu(G)$. Then $V \backslash S$ must not be the vertex cover. Hence, there exists $e \in E$ such that e does not have any elements in $V \backslash S$. Since e is non-zero, without loss of generality, say $e = \{v_1^e, v_2^e, \ldots, v_k^e\} \subset S$ ($k \geq 2$). Since S is independent, $|e| = 1$, which contradicts that $k \geq 2$. In conclusion, $|V \backslash S| = |V| - \triangle(G) \geq \nu(G) \Rightarrow \nu(G) + \triangle(G) \leq |V|$. □

If the graph representation is 2-graph (resulting frame is quadratic), then it is known that $\triangle G = |V| - \nu(G)$.

The vertex cover problem is an NP-hard problem [6], but several efficient and approximative algorithms are valid [7]. These algorithms may obtain vertex covers such that the size is larger than the minimal cover but is within a reasonable scale factor. The typical example we use throughout this paper is a *greedy algorithm.* The detailed procedure of the algorithm is as follows. Suppose we have a hypergraph $G(V, E)$.

1. For each vertex $v \in V$ of G, count $d(v)$ (*order of* v), the number of edges containing v.
2. Take $v' = \text{argmax}_{v \in V} \{d(v)\}$.
3. Remove v' from G and also remove all edges containing v'.
4. Repeat the above sequences with at most $|V|$ times until no edges are left.

Step 1 takes at most $\mathcal{O}(|V||E|)$-time, and Step 2 takes $\mathcal{O}(|V|)$-time. Step 3 takes at most $\mathcal{O}(|E|)$-time, which is the time complexity of set subtraction. Since we repeat these steps at most $|V|$-time, the total time complexity of the greedy algorithm is at most $\mathcal{O}(|V|^2|E|)$.

B. Graph representation of the frame function and marginalization

Now, we show how to connect finding simulatable marginal qubits and the vertex cover problem of the hypergraph. We recall the brief explanation of the graph representation of the frame function in the main text. We shall call this a *frame graph.*

Definition 3. *Suppose we have a frame function F of at most 3rd-degree such that $F(\mathbf{0}_x, \mathbf{a}_z) = \sum_{(i,j) \in \mathcal{E}_2} a_{iz} a_{jz} + \sum_{(i,j,k) \in \mathcal{E}_3} a_{iz} a_{jz} a_{kz}$ (mod 2) for proper index set $\mathcal{E}_2 \subset [n]^{\otimes 2}, \mathcal{E}_3 \subset [n]^{\otimes 3}$. Frame graph G_F of F is a hypergraph $G(V, E)$ where V is a set of vertex $\{a_{1z}, a_{2z}, \ldots, a_{nz}\}$ and $E = \mathcal{E}_2 \bigcup \mathcal{E}_3$.*

From the Section I D, we know that whenever we marginalize the i-th qubit, we substitute $a_{iz} = 0$ to the representing frame $F'(\mathbf{0}_x, \mathbf{a}_z)$. In other words, all monomials containing a_{iz} vanish. In a graphical notation, this means that starting from the frame graph of $F'(\mathbf{0}, \mathbf{a}_z)$, we eliminate both the i-th vertex and all connecting hyperedges. Therefore, tracing the qubits to make the resulting frame function zero is equivalent to finding vertex cover: eliminating vertices and connecting edges until all edges vanish. We can do this using the greedy algorithm and note that $|V|$ is at most n and $|S|$ is within $\mathcal{O}(n^3)$. From the arguments in Section II A, the total time complexity is at most $\mathcal{O}(n^4)$.

Solving the vertex cover problem of the final frame enables us to search simulatable qubits from a given highly entangled circuit that is hard to pick by hand. Also, we can use various modern approximation techniques to find more qubits over the greedy algorithm [6].

We can find the largest number of simulatable qubits if we find the minimal vertex cover. Also, we note that the independent set of the frame graph is also a set of simulatable qubits. However, Corollary 1 says that finding minimum vertex cover and tracing out the qubits corresponding to the vertices produces a larger set of simulatable qubits than finding the maximal independence set.

III. SIMULATIONS ON LOG-DEPTH CLIFFORD CIRCUITS

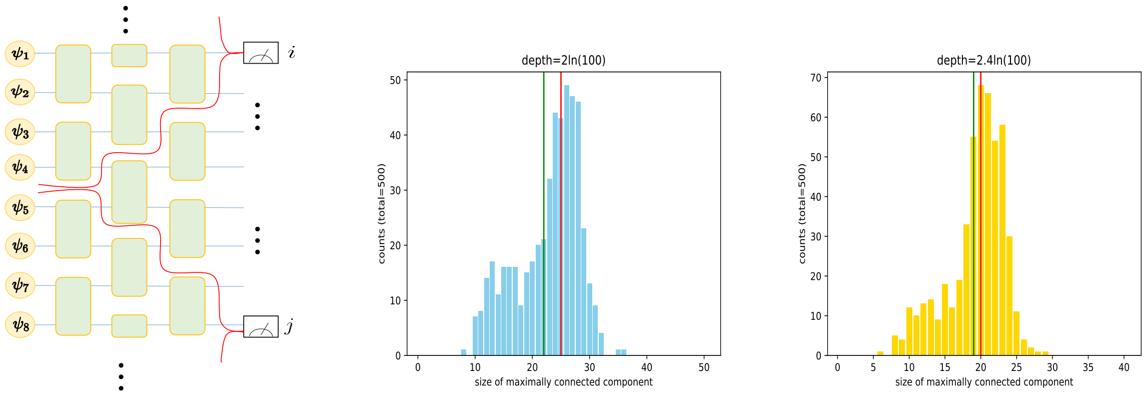
A. Circuit architecture

We first briefly explain the definitions of several n-qubit Clifford circuit architectures [8]. One is the *1D* architecture, which consists of alternating layers with 2-qubit random Clifford gates between neighboring qubits (see Fig. 1(a)). We also regard the Clifford gates connecting the first and the last qubits as a neighboring gate. The other is the *complete graph* architecture, where we put a random single qubit gate to each qubit, and then random Clifford gates are applied between randomly chosen two qubits, regardless of their locations. *Gate count* is the total number of 2-qubit random Clifford gates. In both architectures, random Clifford gates are uniformly chosen [8], and we enact each gate until the gate count reaches the designated value. The *depth* of the circuit is defined as the minimum value of the number of layers in which a set of 2-qubit gates can be applied in parallel (also, see Ref. [8] for more detail). Furthermore, the authors in Ref. [8] showed that in both cases, there exists sufficient and necessary scaling of gate count $\mathcal{O}(n\log(n))$ such that outcome probability distribution of random circuit sampling (including random unitary gates) satisfies the anti-concentration condition [9].

B. On the inseparability of efficiently measurable qubits found from the greedy algorithm for 1D circuits

For the log-depth 1D architecture, even if we do not use the framed Wigner formalism, we can always find many qubits on which measurements are simulatable via brute-forced matrix calculation. We briefly explain how to do this and numerically show that simulatable qubits found by our method do not fall to this case. Suppose we have a d-depth 1D circuit. Now, we pick $i \in [n]$ and choose one group of locations of qubits, $\left\{i - \lfloor\frac{\beta}{2}\log_2(n)\rfloor, i - (\lfloor\frac{\beta}{2}\log_2(n)\rfloor - 1), \ldots, i, \ldots, i + (\lceil\frac{\beta}{2}\log_2(n)\rceil - 1), i + \lceil\frac{\beta}{2}\log_2(n)\rceil\right\}$. Then if we only measure this subset of qubits, we can efficiently simulate it with rotating Pauli operators via Clifford operations [10] with at most $\mathcal{O}(n^{\beta+1}\log_2(n))$-time. Because one method is to calculate the Born probability exactly. To do so, we expand the target binary state by $2^{\beta\log_2(n)} = n^\beta$ number of coherent Z operators and then obtain all traces between the input product state and Pauli operators, which is backward-evolved by Clifford circuit starting from those Z operators. We note that each expectation is obtained in $\mathcal{O}((\log_2(n))^2)$-time [1, 10]. Furthermore, if we choose another $i' \in [n]$ such that $\left\{j - \lfloor\frac{\beta}{2}\log(n)\rfloor, j - (\lfloor\frac{\beta}{2}\log(n)\rfloor - 1), \ldots, j, \ldots, j + (\lceil\frac{\beta}{2}\log(n)\rceil - 1), j + \lceil\frac{\beta}{2}\log(n)\rceil\right\}$ is $2d$-far away from has a distance of $2d$ between the previous group (see Fig. 1 for 3-depth case), then we can also efficiently simulate these measurements by same time complexity because gates involved in two simulations are totally separated. By repeating the same procedure, we find the $\frac{n}{2d+\beta\log_2(n)}$-number of groups of simulatable qubits. Hence, given $d = \alpha\log_2(n)$, the total number of simulatable qubits is $\frac{\beta n}{2\alpha+\beta}$ with total simulation time $\mathcal{O}(n^{\beta+1}(\log_2(n))^2)$.

However, this trivial method only finds distant groups with neighboring qubits. This means that the simulatable qubits should be picked from each group, which always has a distance larger than $2d$ each other. In contrast, our methods also find simulatable qubits that are not far from each other, which can be numerically checked. More precisely, given a non-adaptive Clifford circuit with the Clifford unitary U, let $A_U \equiv \left\{i_1, i_2, \ldots, i_{|A_U|}\right\} \subset [n]$ be a set of locations of simulatable qubits. Now, let Z_i be an n-qubit Paul operator, which affects the Z-operation to the i-th qubit and identity to the other qubits. We calculate the set of Pauli operators $P_{A_U} \equiv \left\{U^\dagger Z_i U | i \in A_U\right\}$ which can be obtained efficiently [10]. We then define the 2-graph $G(A_U, E_{A_U})$ where the set of vertex is A_U, and E_{A_U} is a set of edges which connects $i, j \in A_U$ if and only if two Pauli strings $U^\dagger Z_i U$ and $U^\dagger Z_j U$ have non-trivial (not identity, not need to be same) Pauli operation on the same qubit locations. Now, we denote $\mathcal{C}(G(A_U, E_{A_U})) \subset A_U$ as a set of connected components of G, i.e., vertices consisting of connected subgraphs such that each subgraph is not connected with the others. We note that measurement on the set of qubits with location $C' \in \mathcal{C}(G(A_U, E_{A_U}))$ is independent



(a) (b) (c)

FIG. 1. (a) Schematic illustration of a 3-depth 1D circuit. Measurement on the i-th qubit does not influence the measurement outcome of the j (6-far away from i). If we only simulate these two measurements, we can separate this circuit into two portions sided by the red line. (b,c) The population of the size of maximally connected components for 500 numbers of 100-qubit 1D shallow Clifford samples. The green line represents the average size of maximally connected components, and the red line indicates the average value of total simulatable qubits of each sample. (b): Results of depth $= 2\ln(100)$ 1D circuits (green line:22, red line:25). (c): Results of depth $= 2.4\ln(100)$ 1D circuits (green line:19, red line:20).

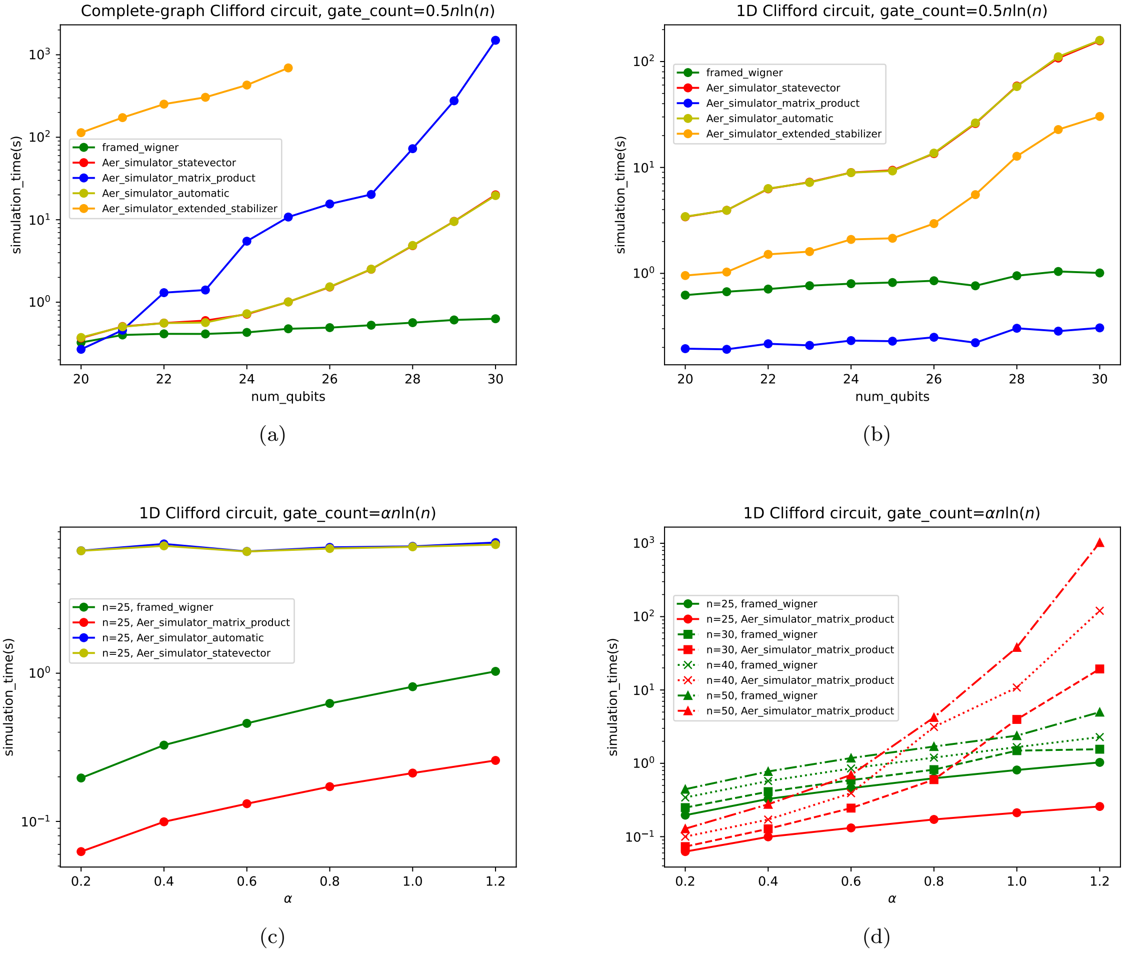
of the measurement outcome on the set of other locations in $\mathcal{C}(G(A_U, E_{A_U}))$. Hence, the time complexity of weak simulation is upper bounded by $\mathcal{O}\left(\exp\left(\max_{C\in\mathcal{C}(G(A_U,E_{A_U}))}(|C|)\right)\right)$, which can be achieved by the similar method with the first paragraph. Now we see Fig. 1 (b) and (c). We randomly sample 500 numbers of 100-qubit 1D Clifford circuit U with zero frame input and find $\max_{C\in\mathcal{C}(G(A_U,E_{A_U}))}(|C|)$ efficiently via Python NetworkX packages, and we observed that most of the samples have many connected Pauli operators $U^\dagger Z_i U$ ($i \in A_U$) and hence such a trivial decomposition (in the first paragraph) is not applied to them.

C. Simulation time comparison with Qiskit

In this section, we show two graphs of the simulation speed of shallow non-adaptive Clifford circuits (see Fig. 2). We compare the simulation time between our simulator and the Qiskit Aer_simulators. For the Wigner function method, simulation time includes the frame changing and finding simulatable qubits, as well as sampling and rotating the phase point. In both simulators, Wigner and Qiskit, we measure the marginal outcome only once. The time complexity $\mathcal{O}(\alpha\text{poly}(n))$ in the main text is obtained by changing the frame for each Clifford gate, and hence total time complexity is $\mathcal{O}(n^3)$ multiplied by the gate count $\alpha n\ln n$. For 1D case, by Sec. II A, time complexity for solving vertex cover problem is $\mathcal{O}\left(\alpha^3 n^3(\ln(n))^3\right)$ ($\because |E| = \mathcal{O}(\alpha^3 n(\ln(n))^3)$), lower than frame changing time complexity for large n.

In Fig. 2 (a,b), we observe that our simulator executes the marginal sampling with the polynomial scaling of the time costs by increasing the number of qubits, which can be compared to the Aer_simulators whose time complexity, except for Aer_matrix_product_state (Aer_mps), increases exponentially by increasing the number of qubits. From Fig. 2 (b,c,d), the Aer_mps performs better than framed Wigner when the circuit is low-entangled or has few qubits. Because the Aer_mps employs the tensor network method and is efficient for circuits with large n but with low-entanglement [11]. However, we note that for $n \geq 30$, the simulation time of Aer_mps increases exponentially by increasing the scale factor of gate count, α, hence by increasing the depth. Hence, our method outperforms Aer_mps for this region.

When the number of simulatable qubits is not sufficiently large, there could be other methods, for example, by directly calculating the Born probability to simulate Clifford circuits [1]. However, we expect that the low time scaling of the Wigner function simulator, while keeping a sufficient portion of simulatable qubits, leads to more efficient simulation for larger n compared to the previous methods. In Section III E, we demonstrate that the time complexity can be further improved by utilizing the property of the circuits' shallow depth, at the cost of additional polynomial-sized memory.



(a)

(b)

(c)

(d)

FIG. 2. Comparison of simulation time for the log-depth random Clifford circuits between framed Wigner function method and Qiskit Aer simulators. (a,b) Average time (over 200 random samples) for simulating the log-depth Clifford circuits. Here, Aer_density_matrix and Aer_stabilizer simulators are not functioning. We fixed the gate count scaling factor α, while increasing the number of qubits. (c,d) Average time (over 100 random samples) for simulating the 1D Clifford circuits by using the framed Wigner function method and Qiskit Aer simulators. We took the n-copies of $|A\rangle$ state as an input for both (a) and (b)

D. Finite-sized scaling for log-depth completely connected circuits

Here, we explain the finite-sized scaling (FSS) analysis of Fig. 3 (e) in the main text. For the completely connected random Clifford circuits, the average number of measurable qubits ($n_{\rm sim}$) has two different scaling on n for $\alpha > \alpha_c$ and $\alpha < \alpha_c$ with some critical point α_c. In order to explore the critical point, we model the scaling function of $n_{\rm sim}$ in terms of α and n as,

$$n_{\rm sim}(\alpha, n) - n_{\rm sim}(\alpha_c, n) = f((\alpha - \alpha_c), n), \tag{32}$$

for some function f with two different scalings at $\alpha < \alpha_c$ and $\alpha > \alpha_c$. It naturally follows that $f(0, n) = 0$ for all n at the critical point. In order to estimate the critical values, we apply the FSS method to the data set with various α and n values. We take the ansatz $f((\alpha - \alpha_c)n^{\frac{1}{\nu}})$ for some $\nu \in \mathbb{R}$ which is commonly found in the FSS literature [12]. By numerically optimizing the parameter of α_c and ν from the data set, we obtain a good collapse of data as in Fig. 3 (e) in the main text with the optimal parameter $\alpha_c = 0.81$ and $\nu = 1.28$. After we find the (α_c, ν), we observe $n_{\rm sim}(\alpha, n) - n_{\rm sim}(\alpha_c, n) \sim C(\alpha - \alpha_c)n^{\frac{1}{\nu}}$ $(C \in \mathbb{R}^+)$ when $\alpha < \alpha_c$. On the other hand, for $\alpha > \alpha_c$, $n_{\rm sim}(\alpha, n)$ shows almost flat behavior when increasing n (see Fig. 3(d) in the main text).

E. Faster frame changing and finding the vertex cover in shallow depth circuits

We already know that frame changing and finding the vertex cover of the final frame can be done in poly(n)-time. In this subsection, we show that the time complexity can be further reduced for shallow circuits with depth $\mathcal{O}(\alpha \ln(n))$. We also realize that frame changing of uniformly sampled Clifford circuit has time complexity within $\mathcal{O}(n^4)$.

To do so, we further define the equivalent expression of the hypergraph.

Definition 4 (Pivoted graph)**.** *(i) Given a graph $G(V,E)$,* Pivoted graph *of G is a set* $\mathrm{Piv}_G \equiv \left\{(\mathrm{Piv}_1, |\mathrm{Piv}_1|), (\mathrm{Piv}_2, |\mathrm{Piv}_2|), \ldots, (\mathrm{Piv}_{|V|}, |\mathrm{Piv}_{|V|}|)\right\}$ *where for $i \in [|V|]$, the* pivoted set Piv_i *is an indexed set* $\left\{e_j^{(i)}\right\}_{j\in[|\mathrm{Piv}_i|]}$*, which is a subset of E whose edges contain the i-th vertex.*
(ii) A pivoted frame graph *of a frame F is* Piv_{G_F}*.*

Indexing is necessary to search for a specific edge in constant time. Since each pivoted set has a maximal size upper-bounded by $\mathcal{O}(n^2)$, it needs $\mathcal{O}(n^3)$ to represent the frame as its pivoted frame graph.

Next, we review one simple lemma.

Lemma 2. *The time complexity to multiply arbitrary $n \times n$ matrix X and $A \oplus I$ where A is 2×2 matrix and I is $(n-2)\times(n-2)$ identity is $\mathcal{O}(n)$.*

Proof. We can rewrite those two matrices as block matrix forms,

$$X = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}, A \oplus I = \begin{pmatrix} A & O \\ O & I \end{pmatrix}. \tag{33}$$

Therefore,

$$X(A\oplus I) = \begin{pmatrix} C_1 A & C_2 \\ C_3 A & C_4 \end{pmatrix}. \tag{34}$$

Hence, we only need to calculate C_1A and C_3A, which takes only $\mathcal{O}(n)$ time complexity, given that A has a constant size and $C_{1(3)}$ has $\mathcal{O}(n)$ size. □

Now, we elaborate on this faster frame-changing algorithm below.

Proposition 2. *Suppose we start from the frame $F_{\mathrm{in}} = \sum_{i=1}^n b_i a_{ix} a_{iz}$, where $\forall i,\ b_i \in \{0,1\}$.*

(i) If the given circuit has 1D architecture and depth d, then obtaining a resulting frame function (and its pivoted frame graph) takes at most $\min\left\{\mathcal{O}(dn^3), \mathcal{O}(d^4 n + dn^2)\right\}$. For a complete graph architecture with depth d, it takes at most $\min\left\{\mathcal{O}(dn^3), \mathcal{O}(8^d \cdot dn + dn^2)\right\}$. To do so, we need $\mathcal{O}(dn^2 + n^3)$-memory.

(ii) There exists a method to uniformly randomly choose a Clifford circuit such that obtaining a resulting pivoted frame graph takes at most $\mathcal{O}(n^4)$.

Proof. (i) Suppose we transform the frame F_0 under a 2-qubit Clifford gate which acts on the i-th and j-th qubits. If we know the pivoted frame graph of F_0, then we just search newly generated monomials from Piv_i, Piv_j, and phase functions. Updating its pivoted frame graph takes $\mathcal{O}(n^2)$-time because the size of the pivoted set is upper bounded by $\mathcal{O}(n^2)$ and updating by generated monomials which come from a single monomial takes constant-time. Then frame changing after a single depth operation takes $\mathcal{O}(n^3)$-time because each depth has $\lfloor \frac{n}{2} \rfloor$ number of neighboring two-qubit gates and changing the pivoted frame graph for each gate takes $\mathcal{O}(n^2)$-time. Hence, the total changing time is at most $\mathcal{O}(dn^3)$, which holds for both 1D and complete graph architecture. Next, let us assume that for each stage $1 \le i \le d$, we act the Clifford operation $U_i \equiv \bigotimes_{j=1}^{k_i} U_{ij}$ where $k_i \in \mathbb{N}, k_i \le \lfloor \frac{n}{2} \rfloor$ and U_{ij} is 2-qubit Clifford operation. We can obtain the symplectic matrix S_i and phase function P_i in $\mathcal{O}(n)$-time because, for each j, the symplectic transform of 2-qubit operation does not affect other qubit pairs. Now, from the arguments in Eq. (9) and Eq. (3), we easily note that resulted symplectic transform S and phase function P is,

$$S = S_d S_{d-1} \ldots S_1, \tag{35}$$

$$P(\mathbf{a}) = P_1(\mathbf{a}) + P_2(S_1(\mathbf{a})) + P_3(S_2(S_1(\mathbf{a}))) + \cdots + P_d(S_{d-1}(S_{d-2}\cdots(S_2(S_1(\mathbf{a})))\cdots)). \tag{36}$$

Hence, the resulting frame function K becomes,

$$\begin{aligned} K(\mathbf{a}) &= F_{\text{in}}(S^{-1}(\mathbf{a})) + P(S^{-1}(\mathbf{a})) && (37)\\ &= P_1(S_1^{-1}(S_2^{-1}\cdots(S_{d-1}^{-1}(S_d^{-1}(\mathbf{a})))\cdots)) + P_2(S_2^{-1}(S_3^{-1}\cdots(S_{d-1}^{-1}(S_d^{-1}(\mathbf{a})))\cdots)) && (38)\\ &\qquad + \cdots + P_{d-1}(S_{d-1}^{-1}((S_d^{-1}(\mathbf{a})))) + P_d(S_d^{-1}(\mathbf{a})) + F(S_1^{-1}(S_2^{-1}\cdots(S_{d-1}^{-1}(S_d^{-1}(\mathbf{a})))\cdots)). && (39) \end{aligned}$$

Each S_i can be expressed as a tensor product $\bigotimes_{j=1}^{k_i} S_{ij}$ of 4×4 matrices, which leads to $S_i^{-1} = \bigotimes_{j=1}^{k_i} S_{ij}^{-1}$. The time complexity to multiply arbitrary $2n\times 2n$ matrix and $A\oplus I_3\oplus\cdots\oplus I_n$, where A is a 4×4 matrix and $I_3,\ldots,I_n$ are 2×2 identities, is $\mathcal{O}(n)$ by the Lem. 2. Therefore, starting from S_d^{-1} and calculating up to $S_1^{-1}(S_2^{-1}\cdots(S_{d-1}^{-1}(S_d^{-1}(\mathbf{a})))\cdots)$ takes $\mathcal{O}(dn^2)$-time. By multiplying each S_i^{-1}'s, we record all $d-1$ output matrices. Storing each output matrix takes $\mathcal{O}(n^2)$-time and therefore we need $\mathcal{O}(dn^2)$-memory and additional $\mathcal{O}(dn^2)$-time.

Now, we prepare another $\mathcal{O}(n^3)$-memory (say M) to represent the pivoted frame graph of zero frame. We will update the graph in a way that the resulting pivoted frame graph is the desired final pivoted frame graph.

For the 1D case, for $m\in[n]$, we easily note that $S^{-1}(\mathbf{a})_{mx(or\ mz)}$ does not have variable $a_{qx(or\ qz)}$ where $|m-q|\ (mod\ n) > d$. If $S^{-1}(\mathbf{a})_{mx(or\ mz)}$ has such variables, two-qubit operation blocks must have propagated from the q-th qubit to the m-th qubit, but this is not the case for the 1D case. Since each P_i is at most of 3rd-degree and has at most $\mathcal{O}(n)$ monomials, expanding $P_i(S_i^{-1}(S_{i+1}^{-1}\cdots(S_2^{-1}(S_1^{-1}(\mathbf{a})))\cdots))$ takes at most $\mathcal{O}((2d)^3 n)$-time. This time complexity is possible because during the expansion, for each obtained single term, we must update the pivoted graph by adding (subtracting resp.) the corresponding edge and adding (subtracting) the order of each pivoted set of target vertices. This step takes constant time. We repeat these steps for d times so that the total time cost is at most $\mathcal{O}(d^4 n)$. Also, in the same manner, adding $F_{\text{in}}(S_1^{-1}(S_2^{-1}\cdots(S_{d-1}^{-1}(S_d^{-1}(\mathbf{a})))\cdots))$ takes $\mathcal{O}((2d)^3 n)$-time.

For a complete graph case, the problem becomes more complicated. Each Clifford gate may entangle two qubits far from each other, and then each qubit can be further affected by different long-ranged Clifford gates. As a results, $S^{-1}(\mathbf{a})_{mx(or\ mz)}$ have the number of variable $a_{qx(or\ qz)}$ upper bounded by 2^{d+1}, so expanding $P_i(S_i^{-1}(S_{i+1}^{-1}\cdots(S_2^{-1}(S_1^{-1}(\mathbf{a})))\cdots))$ takes at most $\mathcal{O}(2^{3d+3}n)$-time. Then we update M in the same way with 1D-case.

(ii) From Ref. [5], we can efficiently sample random Clifford operation in $\mathcal{O}(n^2)$-time. This form always has the layers $F'-S-H-F$, where H is a layer of Hadamard gates, S is a layer of SWAP gates (hence of CNOT gates), and F, F' are CNOT-CZ-S-Pauli layered circuits. CNOT circuit can be decomposed as Clifford bases with depth at most $\mathcal{O}(\frac{n}{\log(n)})$ with at most $\mathcal{O}(n^3)$-time [1, 13]. Also, the depth of the CZ-layer can be upper bounded by $\mathcal{O}(n)$, with $\mathcal{O}(n^3)$-time [14]. Therefore, randomly chosen Clifford circuits can be decomposed to have a depth at most $\mathcal{O}(n)$ (in long-range form). Hence, the total time complexity of frame changing is at most $\mathcal{O}(n^4)$. □

Proposition 2 states that for the complete graph with $\alpha\log(n)$-depth or 1D with n^α-depth where $\alpha < \frac{2}{3}$, we can find another changing algorithm with a reduced order of n. Since the above frame changing is only given by rotations of phase and the argument of the Pauli operator, the application of those algorithms is wider than the scope of the main text.

Next, we discuss solving the vertex cover problem on the pivoted graph Piv_{G_F} of the frame graph G_F. We recall the algorithm of the Section II A. From the pivoted graph, we already know the information on the order of each vertex. Hence step 1 and step 2 takes $\mathcal{O}(|V|)$-time. Now, suppose we eliminate one edge having the vertex v'. Note that this edge has at most another 2 vertices, so when we delete this edge, we also subtract this edge from each pivoted set of those two vertices and adjust the order. We note that this can be done in $\mathcal{O}(1)$-time; hence, getting an updated pivoted graph takes at most $\mathcal{O}(d(G))$-time. Since we repeat these steps for at most $|V|$-time, the total time complexity is at most $\mathcal{O}(|V|d(G)+|V|^2)$.

We summarize these arguments as the following corollary.

Corollary 2. *Suppose we have hypergraph $G(V,E)$ and its pivoted graph* Piv_G. *Then the time complexity of the greedy algorithm is $\mathcal{O}(|V|^2+|V|d(G))$.*

Given an d-depth Clifford circuit, the total time complexity of sampling the initial phase point and obtaining the resulting point after matrix multiplication takes $\mathcal{O}(dn)$-time because the transform of the single qubit part of the phase point under the corresponding two-qubit Clifford block takes constant time. Consider a $\alpha\log(n)$-depth 1D circuit. We note that the total time for the sampling algorithm is at most $\mathcal{O}(\alpha n\log(n))$ because we sample the phase point from the initial framed Wigner function in $\mathcal{O}(n)$-time. Before that, we need to change the frame and solve the vertex cover problem. However, we do not need to do those things over once. Furthermore, by Proposition 2, frame changes (and obtaining its pivoted frame graph) in at most $\min\left\{\mathcal{O}(dn^3), \mathcal{O}(\alpha^4 n(\log(n))^4)+\alpha n^2\log(n)\right\}$-time, and the greedy algorithm can be done in $\mathcal{O}(\alpha^2 n(\log(n))^2+n^2)$-time which is easily derived by Corollary 2 and locality of edges of resulting frame graph. Therefore, even the first trial has a shorter time than a method in the first paragraph of Section III B given that $n^\beta \gg n$.

For each Clifford operation at a specific depth, $\mathcal{O}(n)$ number of new hyperedges are attached. Also, existing edges undergo symplectic transform hence yielding other hyperedges. For the complete graph case, with the worst case, the rate of the number of hyperedges is at most proportional to the number of existing hyperedges. Therefore, the number of hyperedges increases exponentially and the vertex cover size to trace out also increases by the depth. However, if the depth sufficiently increases such that all qubits are interleaved by some edges, then some existing edges rather vanish by the newly generated edges. We expect that this phenomenon will loosen the decreasing rate of vertex cover size and explain the transition of $n_{\rm sim}$ (see Fig. 3 (d) of the main text) by the depth. Whereas, for the 1D case, symplectic transform and hyperedge generation occur locally. Hence the decrease of $n_{\rm sim}$ is much weaker than the complete-graph case, and $\Omega(\frac{n}{\log(n)})$ number of vertex cover is guaranteed.

IV. MORE GENERAL FRAME FORMALISM AND BORN PROBABILITY ESTIMATION

A. Wigner representation using multiple frames

In this section, we further generalize the framed Wigner function formalism by taking multiple frame functions to represent a quantum state. In particular, we show that an arbitrary product state can be positively represented by using multiple quadratic frame functions.

We recall that a single qubit state can be expressed by either zero frame ($F = 0$) or dual frame ($F = a_{1x}a_{1z}$). By combining the phase space operators corresponding to these two frames, one can express any single qubit states by the convex sum of these operators. Hence, if ρ is a product state, it is positively represented under a set of frames $\mathcal{F} \equiv \{\mathbf{b}\cdot(a_{1x}a_{1z}, a_{2x}a_{2z}, \ldots, a_{nx}a_{nz}) | \mathbf{b} \in \mathbb{Z}_2^n\}$. More precisely, for $\rho = \bigotimes_{i=1}^n \rho_i$, we express each ρ_i as

$$\rho_i = \sum_{\mathbf{u}_i \in \mathbb{Z}_2^2} \left(w^0_{\rho_i}(\mathbf{u}_i) A^0(\mathbf{u}_i) + w^{a_{ix}a_{iz}}_{\rho_i}(\mathbf{u}_i) A^{a_{ix}a_{iz}}(\mathbf{u}_i) \right), \tag{40}$$

using eight phase space operators $\{A^0(\mathbf{u}_i), A^{a_{ix}a_{iz}}(\mathbf{u}_i)\}$, where $\mathbf{u}_i \equiv (u_{ix}, u_{iz}) \in \mathbb{Z}_2^2$. Here, w^0 and $w^{a_{ix}a_{iz}}$ are non-negative functions and are different from the Wigner functions $W^F_\rho(\mathbf{u})$ in the main text. We note that summation over phase point of $w^0_{\rho_i}(\mathbf{u}_i)$, or $w^{a_{ix}a_{iz}}_{\rho_i}(\mathbf{u}_i)$ solely does not give unity, but $\sum_{\mathbf{u}_i} \left(w^0_{\rho_i}(\mathbf{u}_i) + w^{a_{ix}a_{iz}}_{\rho_i}(\mathbf{u}_i) \right) = 1$. We also note that these two functions cannot be obtained by inversion in Eq. (2) of the main text because we now have eight phase point operators, which are overcomplete, and hence, their coefficients are not unique. However, we can still efficiently find these two functions because the convex polytope by 8-phase point operators as extreme points contain the Bloch sphere (see Ref. [2]). Hence, solving the constant-sized system of linear equations leads to the following expression of ρ,

$$\rho = \bigotimes_{i=1}^n \rho_i = \sum_{\mathbf{b} \in \mathbb{Z}_2^n} \sum_{\mathbf{u} \in V_n} \left(\prod_{i=1}^n w^{b_i a_{ix} a_{iz}}_{\rho_i}(\mathbf{u}_i) \right) \left(\bigotimes_{i=1}^n A^{b_i a_{ix} a_{iz}}(\mathbf{u}_i) \right), \tag{41}$$

where $\mathbf{u} = \bigoplus_{i=1}^n(\mathbf{u}_i)$. From the definition, $\bigotimes_{i=1}^n A^{b_i a_{ix} a_{iz}}(\mathbf{u}_i)$ is an n-qubit phase point operators with a frame function $F = \mathbf{b}\cdot(a_{1x}a_{1z}, a_{2x}a_{2z}, \ldots, a_{nx}a_{nz})$. Hence, we can rewrite Eq. (41) as

$$\rho = \sum_{F \in \mathcal{F}} \sum_{\mathbf{u} \in V_n} \left(\prod_{i=1}^n w^{b_i a_{ix} a_{iz}}_{\rho_i}(\mathbf{u}_i) \right) (A^F(\mathbf{u})). \tag{42}$$

Therefore, the desired Wigner function is

$$W^F_\rho(\mathbf{u}) = \prod_{i=1}^n w^{b_i a_{ix} a_{iz}}_i(\mathbf{u}_i). \tag{43}$$

Although there could not be a unique expression, the same phase point sampling protocol can be applied to the generalized Wigner functions with multiple frames whenever they are non-negative. This is because the non-negative function W^F_ρ is a probability distribution with random variables of not only $\mathbf{u}$ but also F, so that we can sample both $\mathbf{u}$ and F from $W^F_\rho(\mathbf{u})$. For this case, we say ρ is positively represented under a *frame set* $\mathcal{F}$. Since the Wigner function has a product form and for each $i \in [n]$, we sample $\mathbf{u}_i$ and b_i from $W^{b_i a_{ix} a_{iz}}_i(\mathbf{u}_i)$. The resulting sampling outcome then becomes $\mathbf{u} = \bigoplus_i^n(\mathbf{u}_i)$ and $F = \mathbf{b}\cdot(a_{1x}a_{1z}, a_{2x}a_{2z}, \ldots, a_{nx}a_{nz})$.

B. Generalization of weak simulation results

With the above generalization of using multiple frames representation, we can also obtain a more general statement on the weak simulation. We will discuss this in detail in the next theorem.

Theorem 2. *Suppose that we have a product state $\rho = \bigotimes_{i=1}^{n} \rho_i$ as an input and a non-adaptive Clifford operation U and Z-measurements. Then ρ is positively represented under a frame set $\mathcal{F} \equiv \{\mathbf{b} \cdot (a_{1x}a_{1z}, a_{2x}a_{2z}, \ldots, a_{nx}a_{nz}) | \mathbf{b} \in \mathbb{Z}_2^n\}$. We denote a resulting frame function via the Clifford circuit starting from $F_{\text{in}} \in \mathcal{F}$ as F. Also, let the $I \subset [n]$ satisfies that for all $F_{\text{in}} \in \mathcal{F}$, $F(\mathbf{a}_x = \mathbf{0}, \mathbf{a}_z)\big|_{a_{iz}=0 \text{ for } i \notin I_F}$ is zero. We then can classically simulate $|I|$-number of measurements.*

Proof. We start from Eq. (9). Probability to measure $\mathbf{x} \in \mathbb{Z}_2^n$ is

$$\mathrm{Tr}(|\mathbf{x}\rangle \langle \mathbf{x}| U\rho U^\dagger) = \sum_{\mathbf{u}, F_{\text{in}} \in \mathcal{F}, \mathbf{a}_z \in \mathbb{Z}_2^n} \frac{1}{2^n} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}))\,(-1)^{(\mathbf{u}+\mathbf{x})\cdot \mathbf{a}_z + F_{\text{in}}(S^{-1}(\mathbf{0}_x, \mathbf{a}_z)) + P(S^{-1}(\mathbf{0}_x, \mathbf{a}_z))} \tag{44}$$

$$= \sum_{\mathbf{u}, F_{\text{in}} \in \mathcal{F}, \mathbf{a}_z \in \mathbb{Z}_2^n} \frac{1}{2^n} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}))\,(-1)^{((\mathbf{u}+\mathbf{x})\cdot \mathbf{a}_z + F(\mathbf{0}_x, \mathbf{a}_z))}\,. \tag{45}$$

Now, consider measuring a subset I of qubits. The probability of measuring a marginal string $\mathbf{x}'$ (with arbitrary qubit locations) is as follows. There exists a set of $\mathbf{v}_F \in V_n$ $(F_{\text{in}} \in \mathcal{F})$ such that

$$p(\mathbf{x}') = \sum_{\mathbf{x}''} \mathrm{Tr}(|\mathbf{x}' \oplus \mathbf{x}''\rangle \langle \mathbf{x}' \oplus \mathbf{x}''| U\rho U^\dagger) \tag{46}$$

$$= \sum_{\mathbf{u}, F_{\text{in}} \in \mathcal{F}} \left(\sum_{\substack{\mathbf{a}_z \in \mathbb{Z}_2^n \\ a_{iz}=0 \text{ for } i \in ([n]\setminus I)}} \frac{1}{2^{|I|}} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))\,(-1)^{((\mathbf{u}_x + (\mathbf{x}'\oplus 0))\cdot \mathbf{a}_z)} \right) \tag{47}$$

$$= \sum_{\mathbf{u}, F \in \mathcal{F}} W_\rho^{F_{\text{in}}}(S^{-1}((\mathbf{u}+\mathbf{v}_F))) \prod_{i \in I} \delta_{x_i u_{ix}}\,. \tag{48}$$

Therefore, we obtain the following simulation scheme given that the conditions in Theorem 2 for the final frame hold.

1. Sample a phase space point $\mathbf{u} \in V_n$ and $F_{\text{in}} \in \mathcal{F}$ from $W_\rho^{F_{\text{in}}}(\mathbf{u})$.

2. Change the input frame under the given Clifford operation and obtain both final frame F and $\mathbf{v}_F$

3. Update $\mathbf{u} \leftarrow \mathbf{u}' \equiv S(\mathbf{u})$.

4. Update $\mathbf{u} \leftarrow \mathbf{u} + \mathbf{v}_F$

5. Desired outcome is a marginal string $\mathbf{u}'_x$.

□

We can see that by Theorem 2 (i), the larger the frame set for quantum state input we represent, the fewer the number of measurable qubits. For example, n-copies of *equatorial state*, $|E_\phi\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right)$, can have non-negative representation by 2^n-numbers of frame [2]. Whereas, the n-copies of $|A\rangle = \cos(\theta/2)|0\rangle + e^{i(\pi/4)}\sin(\theta/2)|1\rangle$ with $\theta = \cos^{-1}(1/\sqrt{3})$ [15] need only zero frame [2] for non-negative representation. Hence, when we take equatorial states as an input, we have, in general, fewer simulatable qubits than that for $|A\rangle$. In other words, we can expect that equatorial states have more computational power in non-adaptive Clifford circuits. We can see a similar conjecture in universal computing [16]. Here, we can always make a (non-Clifford) T-gate by acting Clifford gates and measurements to $|E_{\frac{\pi}{4}}\rangle$ and we post-process depending on measurement outcome. However, given a quantum state $|A\rangle$ to make a similar non-Clifford gate, we need two copies of $|A\rangle$ and might fail to implement depending on coherent measurement outcome, with fairly high probability. Interestingly, for approximate simulation, there exists an algorithm that marginally simulates a large fraction of circuits with $|E_{\frac{\pi}{4}}\rangle^{\otimes n}$ as an input efficiently but not for $|A\rangle$ state input [17], which has Pauli rank 4.

C. Born probability estimation

We consider the Born probability estimation of a quantum circuit with outcome $\mathbf{x} \in \mathbb{Z}_2^n$ within additive error ϵ. Suppose a given quantum state ρ is positively represented under the frame F_{in}. From Eq. (13), we have

$$\mathrm{Tr}(U\rho U^\dagger |\mathbf{x}\rangle\langle\mathbf{x}|) = \frac{1}{2^n} \sum_{\mathbf{u}\in V_n, F\in\mathcal{F}} \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))(-1)^{(\mathbf{u}_x+\mathbf{x})\cdot\mathbf{a}_z+F(\mathbf{0}_x,\mathbf{a}_z)}, \tag{49}$$

for some $\mathbf{v}_F \in V_n$. The first method is to uniformly choose $\mathbf{a}_z$ and take an estimator,

$$\hat{p}(\mathbf{x}) = \sum_{\mathbf{u}\in V_n, F\in\mathcal{F}} W_\rho^{F_{\text{in}}}(\mathbf{u})(-1)^{(S(\mathbf{u})_x+(\mathbf{v}_F)_x+\mathbf{x})\cdot\mathbf{a}_z+F(\mathbf{0}_x,\mathbf{a}_z)} = \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} (-1)^{\mathbf{a}_z\cdot\mathbf{x}} \left(\mathrm{Tr}\left(U\rho U^\dagger T_{(\mathbf{0},\mathbf{a}_z)}\right)\right). \tag{50}$$

This estimator can be simulated classically if $W_\rho^{F_{\text{in}}}(\mathbf{u})$ has a product form. However, we also have another expression,

$$\mathrm{Tr}(U\rho U^\dagger |\mathbf{x}\rangle\langle\mathbf{x}|) = \frac{1}{2^n} \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} (-1)^{\mathbf{a}_z\cdot\mathbf{x}} \left(\mathrm{Tr}\left(U\rho U^\dagger T_{(\mathbf{0},\mathbf{a}_z)}\right)\right) = \frac{1}{2^n} \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} (-1)^{\mathbf{a}_z\cdot\mathbf{x}} \left(\mathrm{Tr}\left(\rho U^\dagger T_{(\mathbf{0},\mathbf{a}_z)} U\right)\right). \tag{51}$$

Hence, we may just uniformly randomly choose $\mathbf{a}_z$ and find $T'_{(\mathbf{0}_x,\mathbf{a}_z)} \equiv U^\dagger T_{(\mathbf{0},\mathbf{a}_z)} U$ by using the stabilizer tableau [10], and then take an estimator $\hat{p}_s(\mathbf{x}) = (-1)^{\mathbf{a}_z\cdot\mathbf{x}}\mathrm{Tr}(T'_{(\mathbf{0}_x,\mathbf{a}_z)}\rho)$. Therefore, the estimators $\hat{p}(\mathbf{x})$ and $\hat{p}_s(\mathbf{x})$ have same value for given sampled variable $\mathbf{a}_z$. Hence, both estimators have the same mean squared error, which is,

$$\begin{aligned}
\mathrm{Var}_{\mathrm{Pauli}}(\mathbf{x}) &= \frac{1}{2^n} \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} \left(\mathrm{Tr}\left(\rho U^\dagger T_{(\mathbf{0},\mathbf{a}_z)} U\right)\right)^2 - p(\mathbf{x})^2 && (52)\\
&= \frac{1}{4^n} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{a}_z,\mathbf{b}_z\in\mathbb{Z}_2^n} (-1)^{(\mathbf{a}_z+\mathbf{b}_z)\cdot\mathbf{x}} \left(\mathrm{Tr}\left(\rho U^\dagger T_{(\mathbf{0},\mathbf{a}_z)} U\right)\right)\left(\mathrm{Tr}\left(\rho U^\dagger T_{(\mathbf{0},\mathbf{b}_z)} U\right)\right) - p(\mathbf{x})^2. && (53)\\
&= \left(\sum_{\mathbf{x}\in\mathbb{Z}_2^n} p(\mathbf{x})^2\right) - p(\mathbf{x})^2 = Z_{U,\rho} - p(\mathbf{x})^2, && (54)
\end{aligned}$$

where $Z_{U,\rho} \equiv \sum_{\mathbf{x}\in\mathbb{Z}_2^n} p(\mathbf{x})^2$ is the so-called collision probability [8].

The above schemes do not use the probabilistic property of the Wigner function. We introduce another estimation method by sampling phase points from the Wigner function. We enclose it in the following result.

Theorem 3. *Assume $\rho = \bigotimes_{i=1}^n \rho_i$ is a product state, which is positively represented under a frame set $\mathcal{F} \equiv \{\mathbf{b}\cdot(a_{1x}a_{1z}, a_{2x}a_{2z}, \dots, a_{nx}a_{nz}) | \mathbf{b} \in \mathbb{Z}_2^n\}$. Also, let F_0 be the resulting frame via a given circuit starting from a zero frame. Now, we assume that $I_{F_0} \subset [n]$ satisfies that $F_0(\mathbf{a}_x = \mathbf{0}, \mathbf{a}_z)\big|_{a_{iz}=0 \text{ for } i\notin I_{F_0}}$ is a quadratic polynomial, or has $\mathcal{O}(\log(n))$-sized vertex cover of subgraph of G_{F_0} having only third-degree terms. Then there exists an efficient algorithm for estimation of marginal measurement probability $p(\mathbf{x}')$, where $\mathbf{x}'$ is a target string on qubits located on $I_{F'_0}$. Also, averaged variance over uniform outcomes is $(1-Z_{U,\rho}^{(k)})/2^k$. Hence if we uniformly randomly choose a binary string $\mathbf{x}'$, $\mathrm{Var}(\mathbf{x}') \le \frac{a(k)}{2^k} - p(\mathbf{x}')^2$ with probability at least $\left(1 - \frac{1}{a(k)}\right)$, where $a(k)$ is a non-negative function of k.*

Proof. We first consider the Born probability estimation of full string $\mathbf{x} \in \mathbb{Z}_2^n$. In the same manner as Eq.(13), we obtain that

$$\mathrm{Tr}(U\rho U^\dagger |\mathbf{x}\rangle\langle\mathbf{x}|) = \frac{1}{2^n} \sum_{\mathbf{u}\in V_n, F_{\text{in}}\in\mathcal{F}} \sum_{\mathbf{a}_z\in\mathbb{Z}_2^n} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))(-1)^{(\mathbf{u}_x+\mathbf{x})\cdot\mathbf{a}_z+F(\mathbf{0}_x,\mathbf{a}_z)}. \tag{55}$$

Now, we set the Born probability estimation algorithm of $P(\mathbf{x}) \equiv \mathrm{Tr}(U\rho U^\dagger |\mathbf{x}\rangle\langle\mathbf{x}|)$. Here's the scheme.

1. Sample a phase space point $\mathbf{u} \in V_n$ and $F_{\text{in}} \in \mathcal{F}$ from $W_\rho^{F_{\text{in}}}(\mathbf{u})$.
2. Change the input frame under the given Clifford operation and obtain both final frame F and $\mathbf{v}_{F_{\text{in}}}$
3. Update $\mathbf{u} \leftarrow S(\mathbf{u})$ and then update $\mathbf{u} \leftarrow \mathbf{u} + \mathbf{v}_F$

4. Desired estimation value for each trial is $\hat{p}(\mathbf{x}) \equiv \frac{1}{2^n} \sum_{\mathbf{a}_z} (-1)^{(\mathbf{u}_x+\mathbf{x})\cdot\mathbf{a}_z + F(\mathbf{0}_x,\mathbf{a}_z)}$, where F is a final frame starting from F_{in}.

5. Repeat step 2 $\sim$ step 4 to obtain many $\hat{p}(\mathbf{x})$'s. The final estimation will be the sample mean of those $\hat{p}(\mathbf{x})$'s.

Unfortunately, this is not an efficient algorithm. Because at the third stage, $F(\mathbf{0}_x, \mathbf{a}_z)$ is in general of third-order. The exact calculation is #P-Hard problem [18]. However, in the cases where the size of the vertex cover of a hypergraph with terms of third-degree in $F(\mathbf{0}_x, \mathbf{a}_z)$ is $\mathcal{O}(\log(n))$, we can do this efficiently [19]. Therefore, if we do not estimate the probability of all measurements, we can trace some qubits until the resulting frame is such a form. This is a more relaxed condition than one of weak simulation in Section I D. If the final frames (after tracing) become quadratic, then $\hat{p}(\mathbf{x})$ becomes an exponential sum of quadratic binary polynomials, which is efficiently calculated in $\mathcal{O}(k^3)$-time [3].

For every initial second-ordered frame we sampled from, all resulting frames (after we take $\mathbf{a}_x = 0$) have the same third-ordered terms. Because third-ordered terms are obtained only from phase functions of Clifford gates and symplectic transforms, which do not raise the order of the polynomial, therefore the vertex cover problem may be solved only once for the resulting frame starting from $F_{\text{in}} = 0$.

Now, we only see the marginal outcome string $\mathbf{x}'$. The mean squared error $\text{Var}(\mathbf{x}')$ is given as,

$$\text{Var}(\mathbf{x}') = \frac{1}{4^k} \sum_{\mathbf{u}\in V_n, F_{\text{in}}\in\mathcal{F}} \sum_{\mathbf{a}'_z,\mathbf{b}'_z} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F))(-1)^{(\mathbf{u}'_x+\mathbf{x}')\cdot(\mathbf{a}'_z+\mathbf{b}'_z)+F(\mathbf{0}_x,\mathbf{a}'_z\oplus 0)+F(\mathbf{0}_x,\mathbf{b}'_z\oplus 0)} - p(\mathbf{x}')^2, \tag{56}$$

where $\sum_{\mathbf{a}'_z,\mathbf{b}'_z}$ is the sum over strings at which the same marginalization is applied as $\mathbf{x}'$. Let us denote the first term of the right side as $\mathbb{E}(\hat{p}(\mathbf{x}')^2)$. When we take the uniform average to this over binary strings $\mathbf{x}'$,

$$\overline{\mathbb{E}(\hat{p}(\mathbf{x}')^2)}^{\mathbf{x}'} = \frac{1}{2^k} \sum_{\mathbf{u},F_{\text{in}}} W_\rho^{F_{\text{in}}}(S^{-1}(\mathbf{u}+\mathbf{v}_F)) = \frac{1}{2^k}. \tag{57}$$

(Note that $\overline{\text{Var}(\mathbf{x}')}^{\mathbf{x}'} = 1/2^k - Z_{U,\rho}^{(k)}/2^k$, where $Z_{U,\rho}^{(k)} \equiv \sum_{\mathbf{x}'\in\mathbb{Z}_2^k} p(\mathbf{x}')^2$.) Hence, by Markov's inequality, when we uniformly randomly sample $\mathbf{x}'$, the probability of $\mathbb{E}(\hat{p}(\mathbf{x}')^2)$ being larger than $\frac{a(k)}{2^k}$ is,

$$\Pr\left(\mathbb{E}(\hat{p}(\mathbf{x}')^2) \geq \frac{a(k)}{2^k}\right) \leq \frac{2^k\overline{\mathbb{E}(\hat{p}(\mathbf{x}')^2)}^{\mathbf{x}'}}{a(k)} = \frac{1}{a(k)}. \tag{58}$$

We note that $\text{Var}(\mathbf{x}') = \mathbb{E}(\hat{p}(\mathbf{x}')^2) - p(\mathbf{x}')^2$. Hence if we uniformly randomly choose $\mathbf{x}'$, the probability of $\text{Var}(\mathbf{x}') \leq \frac{a(k)}{2^k} - p(\mathbf{x}')^2$ is at least $\left(1 - \frac{1}{a(k)}\right)$. □

Suppose that we use product state input. We need to find the final (and marginal) frame from each initial frame, which can be sampled in $\mathcal{O}(n)$-time. Moreover, all $\mathcal{O}(k^2)$ number of coefficients of second-ordered terms in a final (and marginal) frame can be rewritten by a boolean linear function with the argument $\mathbf{b} \in \mathbb{Z}_2^n$ which represents the input frame sample $F_{\text{in}} = \sum_{\mathbf{b}\in\mathbb{Z}_2^n} b_i a_{ix} a_{iz}$. These functions can be found before the sampling. Therefore, the total time for each trial is $\mathcal{O}(nk^2)$.

Whereas, we can easily derive that from Eq. (51), $\text{Var}_{\text{Pauli}}(\mathbf{x}') = Z_{U,\rho}^{(k)} - p(\mathbf{x}')^2$ and calculation of $\hat{p}_s(\mathbf{x}')$ takes $\mathcal{O}(n)$-time given that $T'_{(\mathbf{0}_x,\mathbf{a}'_z)} \equiv U^\dagger T_{(\mathbf{0},\mathbf{a}'_z)} U$ is known.

The mean squared error is connected to the required number of samples to achieve additive estimation error ϵ with probability larger than $1-\delta$, given by $\mathcal{O}\left(\frac{\text{Var}(\mathbf{x})}{\epsilon^2}\log\left(\frac{1}{\delta}\right)\right)$ [20, 21]. Suppose that the input state is a product state. Using Theorem 3, we note that for any choice of a non-negative function $a(k) \geq 1$ at least $2^k(1-\frac{1}{a(k)})$-number of binary strings $\mathbf{x}'$ can be estimated with $\mathcal{O}\left(\frac{a(k)/2^k - p(\mathbf{x}')^2}{\epsilon^2}\log\left(\frac{1}{\delta}\right)\right)$ samples using the Wigner function approach. In contrast, Ref. [22] requires $\mathcal{O}\left(\frac{Z_{U,\rho}^{(k)} - p(\mathbf{x}')^2}{\epsilon^2}\log\left(\frac{1}{\delta}\right)\right)$ samples for any string $\mathbf{x}'$. The total time to simulate is the product of the sample number and the time taken to run the estimator once. From the above arguments, if the input state is a product (by ignoring the time for the first trial) we have a time improvement for $2^k(1-\frac{1}{a(k)})$-number of strings when the collision probability $Z_{U,\rho}^{(k)} \geq \mathcal{O}(\frac{a(k)k^2}{2^k})$. The one of such cases is when $k \sim \beta n$ ($\beta \in (0,1)$, n is large) and the k-marginal probability distribution is far from *anti-concentration*, $Z_{U,\rho}^{(k)} \sim \frac{1}{2^{\alpha k}}$ ($\alpha \in (0,1)$) in which we take improvements for $2^k(1-\frac{1}{poly(k)})$ number of strings.

[1] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, Phys. Rev. A **70**, 052328 (2004).
[2] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega, Contextuality and wigner-function negativity in qubit quantum computation, Phys. Rev. A **95**, 052334 (2017).
[3] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Simulation of quantum circuits by low-rank stabilizer decompositions, Quantum **3**, 181 (2019).
[4] D. Maslov and M. Roetteler, Shorter stabilizer circuits via bruhat decomposition and quantum circuit transformations, IEEE Trans. Inf. Theory **64**, 4729 (2018).
[5] S. Bravyi and D. Maslov, Hadamard-free circuits expose the structure of the clifford group, IEEE Trans. Inf. Theory **67**, 4546 (2021).
[6] E. Halperin, Improved approximation algorithms for the vertex cover problem in graphs and hypergraphs, SIAM J. Comput. **31**, 1608 (2002).
[7] V. Guruswami and S. Sandeep, Approximate hypergraph vertex cover and generalized tuza's conjecture, arXiv:2008.07344 (2020).
[8] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits anticoncentrate in log depth, PRX Quantum **3**, 010333 (2022).
[9] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, Nat. Phys. **15**, 159 (2019).
[10] D. Gottesman, The heisenberg representation of quantum computers, arXiv:quant-ph/9807006 (1998).
[11] G. Vidal, Efficient classical simulation of slightly entangled quantum computations, Phys. Rev. Lett. **91**, 147902 (2003).
[12] B. Skinner, J. Ruhman, and A. Nahum, Measurement-induced phase transitions in the dynamics of entanglement, Phys. Rev. X **9**, 031009 (2019).
[13] J. Jiang, X. Sun, S.-H. Teng, B. Wu, K. Wu, and J. Zhang, Optimal space-depth trade-off of cnot circuits in quantum logic synthesis, arXiv:1907.05087 (2022).
[14] J. Misra and D. Gries, A constructive proof of vizing's theorem, Inf. Process. Lett. **41**, 131 (1992).
[15] H. Qassim, H. Pashayan, and D. Gosset, Improved upper bounds on the stabilizer rank of magic states, Quantum **5**, 606 (2021).
[16] S. Bravyi and A. Kitaev, Universal quantum computation with ideal clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).
[17] K. Bu and D. E. Koh, Efficient classical simulation of clifford circuits with nonstabilizer input states, Phys. Rev. Lett. **123**, 170502 (2019).
[18] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-case complexity versus approximate simulation of commuting quantum computations, Phys. Rev. Lett. **117**, 080501 (2016).
[19] A. Montanaro, Quantum circuits and low-degree polynomials over, J. Phys. A: Math. Theor. **50**, 084002 (2017).
[20] L. G. V. M. R. Jerrum and V. V. Vazirani, Theor. Comput. Sci. **43**, 169 (1986).
[21] B. Charles, SIAM Rev. **27**, 264 (1985).
[22] H. Pashayan, S. D. Bartlett, and D. Gross, From estimation of quantum probabilities to simulation of quantum circuits, Quantum **4**, 223 (2020).

Bosonic randomized benchmarking with passive transformations

Extended abstract

Mirko Arienzo[1] * Dmitry Grinko[3 4 5] Martin Kliesch[1] Markus Heinrich[2 3 5]

[1] *Institute for Quantum Inspired and Quantum Optimization, Hamburg University of Technology, Hamburg, Germany*

[2] *Quantum Technology Group, Heinrich Heine University, Düsseldorf, Germany*

[3] *QuSoft, Amsterdam, The Netherlands*

[4] *University of Amsterdam, Amsterdam, The Netherlands*

[5] *Centrum Wiskunde & Informatica, Amsterdam, The Netherlands*

Keywords: bosonic randomized benchmarking, passive Gaussian transformations, LOP.

Bosonic quantum systems play a major role for the design of quantum computing platforms. Most prominently, this includes photonic quantum computing as a popular proposal for real world implementations of quantum computers [1–4]. The biggest advantages of this model rely on the implementation of particle sources, detectors, and linear optical circuits on the same integrated chips [5–8], and access to mixed schemes for quantum error correction [9]. Bosonic systems also offer interesting non-universal models of computation to test quantum supremacy, such as boson sampling [10] and Gaussian boson sampling [11, 12].

The characterization of quantum devices, and, in particular, of the involved unitary gates, is a fundamental task in quantum information processing [13, 14]. While this is a well-studied field for discrete variable systems, a similar standing for continuous variable (CV) systems has not yet been achieved, as the first rigorous guarantees for learning CV quantum states have been proved only very recently [15, 16]. Tomographic protocols provide, in principle, a complete description of experimentally implemented gates [17, 18]. However, the number of measurements required is beyond concrete applications [19–23]. In particular, full quantum process tomography is not feasible in practice since it requires either an unpractical number of different input states [20, 21] or entangling the input state with an ancilla [24, 25]. Moreover, standard versions of the protocol suffer from state preparation and measurement (SPAM) errors.

For bosonic systems, additional challenges arise due to particularities of the infinite-dimensional Hilbert space [19, 26]. For instance, characterization protocols that rely on scrambling techniques via unitary designs are notably challenging to implement, since Gaussian unitaries only form a unitary 1-design [27, 28], and, more dramatically, unitary 2-designs for CV systems cannot exist, unless rigged Hilbert spaces are taken into account [29]. Such issues constraint the characterization of quantum gates to very specific settings, where implemented unitary operators (which may include non-Gaussian single-mode unitaries) are only benchmarked w.r.t. the input ensembles [30].

For discrete variable systems, randomized benchmarking (RB) [31–40] is the most widespread family of protocols for the estimation of average gate fidelities. Its popularity is due to its robustness against SPAM errors and its rather low demands on the measurement effort [41]. Recent efforts led to general guarantees for RB protocols with finite or compact groups [42, 44–47]. This generality is important when considering RB for CV systems, since unitary 2-designs, as in the standard formulation of RB, are not available [27–29]. For general groups, the RB signal consists of a linear combination of exponential decays, labelled by the relevant irreducible subrepresentations (irreps) [40, 42–44]. In the CV setting, we however expect many irreps and isolating the decay rates is likely infeasible in practice [44, 47]. These issues can be resolved using the recently proposed filtered RB protocol [42, 44, 47], which isolates contributions associated to individual irreps by performing a suitable post-processing of the data.

In this work, we introduce the first RB protocol for bosonic systems: *bosonic passive RB* (or passive RB for simplicity). Our protocol benchmarks passive (Gaussian) transformations – identified with the

[*] `mirko.arienzo@tuhh.de`

unitary group over m modes $\mathrm{U}(m)$ [48]. We perform the necessary representation-theoretic computations and evaluate relevant moments of $\mathrm{U}(m)$ to exploit the general guarantees of filtered RB [47]. From this perspective, Gaussian input states and measurements seems unfavorable due to infinitely many relevant irreps and thus decay rates. Instead, we consider experiments that start with the preparation of a Fock state $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$, and end with either a particle number resolving (PNR) measurement or a balanced heterodyne measurement at the end of each mode.

Our passive RB protocol. Repeat the following steps L times, for different sequence lengths $m \in \mathbb{M}$: Prepare $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$, and apply passive transformations $g_1, \ldots, g_m$ drawn i.i.d. from the Haar probability measure on $\mathrm{U}(m)$. Lastly, measure the output state, and store the outcome $\boldsymbol{x} \in \Omega$ together with the sampled unitaries. In the post-processing, we compute the estimator $\hat{F}_\lambda(m) = \frac{1}{L}\sum_{i=1}^{L} f_\lambda(\boldsymbol{x}^{(i)}, g_1^{(i)} \cdots g_m^{(i)})$ where f_λ is the *filter function* defined as

$$f_\lambda(\boldsymbol{x}, g) := \frac{1}{s_\lambda}\langle \boldsymbol{x}\,|\omega(g) \circ P_\lambda(\rho)|\boldsymbol{x}\rangle\,, \qquad (1)$$

where

$$s_\lambda = \frac{1}{\dim\lambda}\int_\Omega d\boldsymbol{x}\,\langle \boldsymbol{x}\,|P_\lambda(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)|\boldsymbol{x}\rangle\,. \qquad (2)$$

Here, ω is the representation of $\mathrm{U}(m)$ on density operators and P_λ is the projector onto an irrep λ of interest. Fit the data $(m, \hat{F}_\lambda(m))_{m\in\mathbb{M}}$ to an exponential model $A_\lambda\varphi_\lambda^m$ and report the *decay rates* φ_λ, which are a measure of the quality of the implementation [44, 47].

Importantly, the choice of ρ ensures that we can restrict the representation of $\mathrm{U}(m)$ to the invariant subspace of n particles. Hence, we consider the representation $\omega_n^M := \tau_n^m(\cdot)\tau_n^{m\dagger}$, where τ_n^m is the totally symmetric irrep of $\mathrm{U}(m)$ supported on the n-particle subspace. We show that ω_n^M decomposes as $\omega_n^M = \bigoplus_{k=0}^n \lambda_k$, where all λ_k are distinct, $\lambda_0 \equiv \mathbf{1}$ is the trivial irrep and $\lambda_1 \equiv \mathrm{Ad}$ is the adjoint irrep. The proof is based on an iterative procedure, using Young diagrams of τ_n^m and its dual, to compute the decomposition of ω_n^m for arbitrary n's and m's via Littlewood-Richardson's rules [49].

Main results. The general results of the filtered RB framework [47] directly guarantee that the expected signal $F_\lambda(m) = \mathbb{E}[\hat{F}_\lambda(m)]$ is well-approximated by an exponential decay, $F_\lambda(m) \approx A_\lambda\varphi_\lambda^m$. In particular, the approximation error decays exponentially in m (and faster than φ_λ^m). From the discrete variable setting, we expect that already very short sequences are sufficient to suppress this error and expose the decay. A crucial step in the post-processing is the evaluation of the filter function (1). Its computation is generally a hard problem, as it can be reduced to the computation of permanents or Hafnians, which lie at the heart of the complexity of (Gaussian) boson sampling.

Theorem 1. *Consider an input state $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ and either PNR or balanced heterodyne measurements. Then, we can evaluate the filter function* (1) *as a linear combination of permanents or Hafnians, respectively.*

We prove this result by applying a generalized Clebsch-Gordan decomposition to $\omega_n^m \simeq \tau_n^m \otimes \bar{\tau}_n^m$, resulting in an explicit block-diagonalization of ω_n^m [50, 51]. The projection onto an irrep λ then selects the relevant terms in the Clebsch-Gordan decomposition. Similarly, s_λ in Eq. (1) can be evaluated in terms of Clebsch-Gordan coefficients.

For the sample complexity of passive RB we can use Chebyshev's inequality to ensure $|\hat{F}_\lambda(m) - F_\lambda(m)| < \epsilon$ with probability $1-\delta$ given $L \geq \epsilon^{-2}\delta^{-1}\mathbb{E}[f_\lambda^2]$ samples. Using results in Ref. [47] we can reduce the computation of $\mathbb{E}[f_\lambda^2]$ to the noiseless second moment.

Theorem 2 (Variance bound)**.** *Assume that the input state of passive RB is a Fock state $|\boldsymbol{n}\rangle$ and we use either PNR or balanced heterodyne measurements, and the SPAM noise is non-malicious. Then*

$$\mathbb{E}[f_\lambda^2] \leq \mathbb{E}[f_\lambda^2]_{\text{ideal}} = \frac{\mathcal{C}}{s_\lambda^2}\,, \qquad (3)$$

where $\mathcal{C}$ is a suitable linear combination of Clebsch-Gordan coefficients.

The proof of this result relies on expressing the second moment $\mathbb{E}[f_\lambda^2]_{\text{ideal}}$ as a suitable integral of the representations $\lambda^{\otimes 2}$ and ω_n^m over $\mathrm{U}(m)$ [40, 47]. Schur's lemma then implies that the non-trivial contributions to this integral are given by the irreducible representations (irreps) of $\lambda^{\otimes 2}$ which are also contained in ω_n^m. We determine these irreps which allows us to finally write $\mathbb{E}[f_\lambda^2]_{\text{ideal}}$ in terms of suitable Clebsch-Gordan coefficients.

Finally, in the case $m = 2$ and PNR measurements, the latter admits a bound of the form $\mathbb{E}[f_{\lambda_k}^2] = O(d_\lambda^2 n^2)$. The latter upper bound can also be generalized to $m > 2$, by taking into account the additional multiplicities appearing in this case. However, we expect that these bounds are very loose and the variance is much smaller in practice.

References

[1] E. Knill, R. Laflamme, and G. J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature **409**, 46 (2001).

[2] M. Koashi, T. Yamamoto, and N. Imoto, *Probabilistic manipulation of entangled photons*, Phys. Rev. A **63**, 030301 (2001).

[3] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Linear optical quantum computing with photonic qubits*, Rev. Mod. Phys. **79**, 135 (2007).

[4] S.-H. Tan and P. P. Rohde, *The resurgence of the linear optics quantum interferometer — recent advances & applications*, Reviews in Physics **4**, 100030 (2019).

[5] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, *Silica-on-Silicon Waveguide Quantum Circuits*, Science **320**, 646 (2008).

[6] Sprengers et al., *Waveguide superconducting single-photon detectors for integrated quantum photonic circuits*, Applied Physics Letters **99**, 181110 (2011).

[7] Silverstone et al., *On-chip quantum interference between silicon photon-pair sources*, Nature Photonics **8**, 104 (2014).

[8] T. Meany, M. Gräfe, R. Heilmann, A. Perez-Leija, S. Gross, M. J. Steel, M. J. Withford, and A. Szameit, *Laser written circuits for quantum photonics*, Laser & Photonics Reviews **9**, 363 (2015).

[9] Bourassa et al., *Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer*, Quantum **5**, 392 (2021), arxiv:2010.02905 [quant-ph].

[10] S. Aaronson and A. Arkhipov, *The Computational Complexity of Linear Optics*, arxiv:1011.3245 [quant-ph] (2010).

[11] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, *Gaussian Boson Sampling*, Phys. Rev. Lett. **119**, 170501 (2017), arxiv:1612.01199 [quant-ph].

[12] L. Chakhmakhchyan and N. J. Cerf, *Boson sampling with gaussian measurements*, Physical Review A **96**, 10.1103/physreva.96.032326 (2017).

[13] M. Kliesch and I. Roth, *Theory of quantum system certification*, PRX Quantum **2**, 010201 (2021), tutorial, arXiv:2010.05925 [quant-ph].

[14] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Quantum certification and benchmarking*, Nat. Rev. Phys. **2**, 382 (2020), arXiv:1910.06343 [quant-ph].

[15] Y.-D. Wu, G. Chiribella, and N. Liu, arxiv:2303.05097 [quant-ph] (2023).

[16] F.A. Mele et al., *Learning quantum states of continuous variable systems*, arxiv:2405.01431 [quant-ph] .

[17] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Complete characterization of a quantum process: The two-bit quantum gate*, Physical Review Letters **78**, 390–393 (1997).

[18] M. Mohseni, A. T. Rezakhani, and D. A. Lidar, *Quantum-process tomography: Resource analysis of different strategies*, Physical Review A **77**, 10.1103/physreva.77.032322 (2008).

[19] A. I. Lvovsky and M. G. Raymer, *Continuous-variable optical quantum-state tomography*, Reviews of Modern Physics **81**, 299–332 (2009).

[20] C. C. López, A. Bendersky, J. P. Paz, and D. G. Cory, *Progress toward scalable tomography of quantum maps using twirling-based methods and information hierarchies*, Phys. Rev. A **81**, 062113 (2010).

[21] C. T. Schmiegelow, A. Bendersky, M. A. Larotonda, and J. P. Paz, *Selective and Efficient Quantum Process Tomography without Ancilla*, Phys. Rev. Lett. **107**, 100502 (2011).

[22] A. Bendersky and J. P. Paz, *Selective and efficient quantum state tomography and its application to quantum process tomography*, Phys. Rev. A **87**, 012122 (2013).

[23] R. Namiki, *Schmidt-number benchmarks for continuous-variable quantum devices*, Phys. Rev. A **93**, 052336 (2016).

[24] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White, *Ancilla-Assisted Quantum Process Tomography*, Phys. Rev. Lett. **90**, 193601 (2003).

[25] G. Bai and G. Chiribella, *Test One to Test Many: A Unified Approach to Quantum Benchmarks*, Phys. Rev. Lett. **120**, 150502 (2018).

[26] K. Sharma and M. M. Wilde, *Characterizing the performance of continuous-variable Gaussian quantum gates*, Phys. Rev. Research **2**, 013126 (2020), arxiv:1810.12335 [quant-ph].

[27] R. Blume-Kohout and P. S. Turner, *The curious nonexistence of gaussian 2-designs*, Communications in Mathematical Physics **326**, 755–771 (2014).

[28] Q. Zhuang, T. Schuster, B. Yoshida, and N. Y. Yao, *Scrambling and Complexity in Phase Space*, Phys. Rev. A **99**, 062334 (2019), arxiv:1902.04076.

[29] J. T. Iosue, K. Sharma, M. J. Gullans, and V. V. Albert, *Continuous-variable quantum state designs: Theory and applications* (2022), arxiv:2211.05127 [math-ph, physics:physics, physics:quant-ph].

[30] R. M. S. Farias and L. Aolita, *Certification of continuous-variable gates using average channel-fidelity witnesses*, Quantum Sci. Technol. **6**, 035014 (2021), arxiv:1812.01968.

[31] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators*, J. Opt. B **7**, S347 (2005), arXiv:quant-ph/0503243.

[32] B. Lévi, C. C. López, J. Emerson, and D. G. Cory, *Efficient error characterization in quantum information processing*, , arXiv:quant-ph/0608246 [quant-ph].

[33] C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and approximate unitary 2-designs and their application to fidelity estimation*, Phys. Rev. A **80**, 012304 (2009), arXiv:quant-ph/0606161 [quant-ph].

[34] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, *Symmetrized characterization of noisy quantum processes*, Science **317**, 1893 (2007), arXiv:0707.0685 [quant-ph].

[35] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Phys. Rev. A **77**, 012307 (2008), arXiv:0707.0963 [quant-ph].

[36] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and robust randomized benchmarking of quantum processes*, , arXiv:1009.3639 [quant-ph].

[37] E. Magesan, J. M. Gambetta, and J. Emerson, *Characterizing quantum gates via randomized benchmarking*, Phys. Rev. A **85**, 042311 (2012), arXiv:1109.6887.

[38] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout, *What randomized benchmarking actually measures*, arXiv:1702.01853 [quant-ph].

[39] J. J. Wallman, *Randomized benchmarking with gate-dependent noise*, Quantum **2**, 47 (2018), arXiv:1703.09835 [quant-ph].

[40] S. T. Merkel, E. J. Pritchett, and B. H. Fong, *Randomized Benchmarking as Convolution: Fourier Analysis of Gate Dependent Errors*, arxiv:1804.05951 [quant-ph].

[41] R. Harper, I. Hincks, C. Ferrie, S. T. Flammia, and J. J. Wallman, *Statistical analysis of randomized benchmarking*, Phys. Rev. A **99**, 052350 (2019), arXiv:1901.00535 [quant-ph].

[42] J. Helsen, X. Xue, L. M. K. Vandersypen, and S. Wehner, *A new class of efficient randomized benchmarking protocols*, arxiv:1806.02048 [quant-ph].

[43] D. S. França and A.-L. Hashagen, *Approximate Randomized Benchmarking for Finite Groups*, J. Phys. A: Math. Theor. **51**, 395302 (2018), arxiv:1803.03621.

[44] J. Helsen, I. Roth, E. Onorati, A. Werner, and J. Eisert, *General framework for randomized benchmarking*, PRX Quantum **3**, 020357 (2022).

[45] J. Helsen, M. Ioannou, J. Kitzinger, E. Onorati, A. H. Werner, J. Eisert, and I. Roth, *Shadow estimation of gate-set properties from random sequences*, Nature Communications **14**, 10.1038/s41467-023-39382-9 (2023).

[46] L. Kong, *A framework for randomized benchmarking over compact groups* (2021), arxiv:2111.10357 [quant-ph] .

[47] M. Heinrich, M. Kliesch, and I. Roth, *Randomized benchmarking with random quantum circuits* (2023), presented at QIP 2023 as a talk, arxiv:2212.06181 [quant-ph].

[48] Arvind, B. Dutta, N. Mukunda, and R. Simon, *The Real Symplectic Groups in Quantum Mechanics and Optics*, Pramana - J Phys **45**, 471 (1995), arxiv:quant-ph/9509002.

[49] S. Sternberg, *Group theory and physics*, Cambridge University Press (1994).

[50] A. Alex, M. Kalus, A. Huckleberry, and J. von Delft, *A numerical algorithm for the explicit calculation of SU(N) and* $SL(n, \mathbb{C})$ *clebsch–gordan coefficients*, Journal of Mathematical Physics **52**, 10.1063/1.3521562 (2011).

[51] A. Alex, *Non-Abelian Symmetries in the Numerical Renormalization Group*, Ph.D. thesis, Ludwig-Maximilians-Universität Münich (2009).

Randomize benchmarking with bosonic passive transformations

Mirko Arienzo[1] * Dmitry Grinko[3 4 5] Martin Kliesch[1] Markus Heinrich[2 3 5]

[1] *Institute for Quantum Inspired and Quantum Optimization, Hamburg University of Technology, Hamburg, Germany*

[2] *Quantum Technology Group, Heinrich Heine University, Düsseldorf, Germany*

[3] *QuSoft, Amsterdam, The Netherlands*

[4] *University of Amsterdam, Amsterdam, The Netherlands*

[5] *Centrum Wiskunde & Informatica, Amsterdam, The Netherlands*

Abstract. Randomized benchmarking (RB) is the most commonly employed protocol for the characterization of unitary gates in (discrete variable) quantum circuits due to its reasonable experimental requirements and robustness against state preparation and measurement (SPAM) errors. In this work, we introduce the first RB protocol for passive Gaussian transformations based on the recently developed filtered RB framework by Heinrich et al. [1]. We suggest a setting consisting of a Fock input state and either particle number resolving or heterodyne detectors. We provide a detailed procedure to post-process the experimental data and derive an analytical formula for the sampling complexity.

Keywords: bosonic randomized benchmarking, passive Gaussian transformations, LOP.

1 Introduction

Bosonic quantum systems play a major role for the design of quantum computing platforms. Most prominently, this includes photonic quantum computing as a popular proposal for real world implementations of quantum computers [2–7]. The biggest advantages of this model rely on the implementation of particle sources, detectors, and linear optical circuits on the same integrated chips [8–11], and access to mixed schemes for quantum error correction [12]. Bosonic systems also offer interesting non-universal models of computation to test quantum supremacy, such as boson sampling [13] and Gaussian boson sampling [14–18].

The characterization of quantum devices, and, in particular, of the involved unitary gates, is a fundamental task in quantum information processing [19, 20]. While this is a well-studied field for discrete variable systems, a similar standing for continuous variable (CV) systems has not yet been achieved, as the first rigorous guarantees for learning CV quantum states have been proved only very recently [21, 22]. Tomographic protocols provide, in principle, a complete description of experimentally implemented gates [23, 24]. However, the number of measurements required is beyond concrete applications [25–29]. In particular, full quantum process tomography is not feasible in practice since it requires either an unpractical number of different input states [26, 27] or entangling the input state with an ancilla [30, 31]. Moreover, standard versions of the protocol suffer from state preparation and measurement (SPAM) errors.

For bosonic systems, most challenges can be attributed to the particularities of the infinite-dimensional Hilbert space [25, 32]. For instance, characterization protocols that rely on scrambling techniques via unitary designs are notably challenging to implement, since Gaussian unitaries only form a unitary 1-design [33, 34], and, more dramatically, unitary 2-designs for CV systems cannot exist, unless rigged Hilbert spaces are taken into account [35]. Such issues constraint the characterization of quantum gates to very specific settings, where implemented unitary operators (which may include non-Gaussian single-mode unitaries) are only benchmarked w.r.t. the input ensembles [36].

For discrete variable systems, randomized benchmarking (RB) [37–46] is the most widespread family of protocols for the estimation of average gate fidelities. Its popularity is due to its robustness against SPAM errors and its rather low demands on the measurement effort [47]. The standard RB protocol is as follows: To a fixed initial state, apply a sequence of Haar-random (Clifford) unitaries, followed by a final *inversion gate* cancelling the action of the entire sequence. Then, the success probability of restoring the initial state decays exponentially with the length of the sequence, and the decay rate is a proxy for the average gate fidelity of the gate set. However, many variations of this theme exist.

Recent efforts led to general guarantees for RB protocols with finite or compact groups [1, 48–51]. This generality is important when considering RB of CV systems, since unitary 2-designs, as in the standard formulation of RB, are not available. However, these protocols still suffer from two crucial problems: First, the computation and experimental implementation of the inversion gate is generally challenging. Second, it is known that the RB signal consists of a linear combination of exponential decays, in correspondence with the relevant irreducible subrepresentations (irreps) of the used group [49, 52]. Isolating the decay rates is already difficult in practice if more than a few irreps are involved [1, 49], and may become impossible in the CV setting. To resolve these issues, filtered RB has been recently proposed [1, 48, 49]. This protocol omits the inversion gate and instead performs a suitable post-processing of the data. During the post-processing, contributions associated to individual ir-

*mirko.arienzo@tuhh.de

reps can be isolated in a SPAM-robust way, allowing to handle compact groups with many irreps.

In this work, we introduce the first RB protocol for bosonic systems: *bosonic passive RB* (or passive RB for simplicity). Our protocol benchmarks passive (Gaussian) transformations and allows to deduce statements about their average quality. We consider experiments where the input state is a Fock basis state and analyze two common measurement scenarios: Either the total number of particles is measured in each mode with a particle number resolving (PNR) detector, or each mode is measured with a (balanced) heterodyne detector. In these cases, passive RB resembles either boson sampling or Gaussian boson sampling experiments [13–15]. Arguably, the simplest experimental setting would instead involve Gaussian input states and measurements. In this case, however, we encounter infinitely many relevant irreps and thus decay rates, and it is unclear whether a meaningful analysis is possible.

By performing the necessary representation-theoretic computations, we can then rely on the general framework of filtered RB [1]. In particular, we derive explicit formulas for the so-called *filter function* used in the classical post-processing of the experimental data. Moreover, we give exact expressions and bounds on the variance of our estimators, thereby characterizing the sampling complexity of our protocol.

The classical post-processing essentially involves the simulation of (Gaussian) boson sampling experiments. This is akin to the discrete setting which requires the simulation of random circuits [1, 53]. Both settings thus involve computationally hard problems which, generically, cannot be avoided. However, specific choices of the initial Fock state may help to reduce the computational effort of the classical post-processing [54].

The remainder of this work is structured as follows: In Section 2 we highlight our main results. In particular, in Section 2.2 we spell out passive RB in full details, and discuss the different experimental settings. In Section 2.3 we show our performance guarantees including results on the sampling complexity for both PNR and heterodyne measurement schemes. In Section 3 the technical tools are introduced and Section 4 is devoted to the technical part of this manuscript. Section 4.1 is dedicated to the main technical result, i.e. we show the decomposition into irreps of the representation of passive transformations acting on states with a fixed number of particles. This result is used to isolate the signals, and is the main tool from which the general form of the post-processing procedure follows, in Section 4.2. Finally, in Section 4.3, we provide analytical expressions for the optimal sample complexity of filtered RB with bunched input states. Similar results in a setting with heterodyne measurements are discussed in Appendix H.

2 Main results

In the following, we introduce a scalable protocol for benchmarking Gaussian unitaries that preserve the total number of bosons of a quantum system, referred to as *passive transformations* from here on. We discuss different experimental settings which are commonly implemented within the framework of CV systems. In particular, we argue that Gaussian probe states and measurements impose additional challenges on RB-like experiments due the presence of an infinite number of irreps. As a consequence, it is unclear whether a meaningful RB experiment can be formulated on their basis. In contrast, using Fock basis states (or measurements) directly lead to a well-behaved protocol for the characterization of passive unitaries.

2.1 Notation

We consider a bosonic system of $m \in \mathbb{N}$ modes described by a set of pairs of bosonic field operators $\{a_k^\dagger, a_k\}_{k=1}^m$, where a_k and $a_k^\dagger$ are the k-th annihilation and creation operators, respectively, which satisfy the canonical commutation relations (CCRs)

$$[a_k, a_l^\dagger] = \delta_{k,l}\,, \quad [a_k, a_l] = [a_k^\dagger, a_l^\dagger] = 0\,, \quad k,l = 1,\ldots,m\,.$$

Here, $\delta_{k,l}$ is the usual Kronecker delta. Such a system is described by the Fock-Hilbert space $\mathcal{F}_m := \bigoplus_{n=0}^\infty \mathcal{H}_n^m$, where $\mathcal{H}_n^m$ is the subspace of n bosons distributed over m modes spanned by the *Fock* states

$$|\boldsymbol{n}\rangle \equiv |n_1,\ldots,n_m\rangle := \prod_{k=1}^m \frac{1}{\sqrt{n_k!}} a_k^{\dagger n_k} |\boldsymbol{0}\rangle\,, \qquad (1)$$

where $|\boldsymbol{n}| := \sum_{i=1}^m n_i = n$ and $|\boldsymbol{0}\rangle \equiv |0,\ldots,0\rangle$ denotes the vacuum state of m decoupled one-dimensional harmonic oscillators [55]. We shall also consider coherent states, defined as $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^\infty \frac{\alpha^n}{\sqrt{n!}}|n\rangle$ for a single mode, with a straightforward extension to the multimode setting. The set of passive transformations is the group of unitary operators on $\mathcal{F}_m$ that leave the total number of particles invariant. These are exactly the unitaries which induce a transformation of the bosonic operators as $a_k \mapsto \sum_{l=1}^m U_{lk} a_l$ for a unitary matrix $U = (U_{lk})_{l,k=1}^m$. Hence, the group of passive transformations can be identified with the unitary group $\mathrm{U}(m)$ [56]. Practically, these can also be thought as multimode interferometers, which can be decomposed in quadratically many two-modes interferometers and phase shift transformations only [6, 58–61].

2.2 The passive randomized benchmarking protocol

The passive RB protocol is based on the filtered RB protocol [1, 48, 49], which consists of a *data collection phase* and a *post-processing phase*. We briefly state the protocol and justify it afterwards.

Description of the protocol. The passive RB protocol is based on the filtered RB protocol [1, 48, 49], which consists of a *data collection phase* and a *post-processing phase*. We briefly state the protocol in the bosonic case.

(I) **Data collection.** We propose to use a fixed number state $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ as input and perform particle number resolving (PNR) measurements described by the positive operator-valued measure (POVM) $\{|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\}_{\boldsymbol{x}\in\mathbb{N}^m}$. For different sequence lengths $l \in \mathbb{L}$, repeat the following steps N times,

(i) Prepare the state ρ.

(ii) Apply passive transformations $g_1, \dots, g_l$ drawn i.i.d. from the Haar probability measure on $\mathrm{U}(m)$.

(iii) Measure the output state and store the outcome together with the sampled unitaries.

(II) **Post-processing.** Assuming the data $\{(\boldsymbol{x}^{(i)}, g_1^{(i)}, \dots, g_l^{(i)})\}_{i=1}^N$ has been gathered, compute the following mean estimator of a later-to-be-defined *filter function* f_λ, parametrized by suitable irreducible representations (irreps) λ of $\mathrm{U}(m)$:

$$\hat{F}_\lambda(l) = \frac{1}{N}\sum_{i=1}^{N} f_\lambda(\boldsymbol{x}^{(i)}, g_1^{(i)}, \dots, g_l^{(i)})\,. \tag{2}$$

We refer to the data series $(l, \hat{F}_\lambda(l))_{l\in\mathbb{L}}$ as the (filtered) *RB signal*. Finally, perform an exponential fit according to the model $\hat{F}_\lambda(l) = A_\lambda \varphi_\lambda^l$ to extract the *decay rates* $\{\varphi_\lambda\}_\lambda$.

The reasons for our choice of initial state and measurements are laid out in the discussion below, and possible variations are discussed at the end of this subsection (in particular Gaussian states and measurements).

We would like to emphasize that Haar-random sampling from $\mathrm{U}(m)$ can be substituted by any distribution which converges sufficiently fast to the Haar measure [1]. For the main part of this paper, we resort to the Haar measure to simplify the presentation.

Decay rates and fidelities. The decay rates can be combined into an average performance measure for passive transformations on the n-particle subspace using the formula [49]

$$F = (\dim \mathcal{H}_n^m)^{-2} \sum_\lambda d_\lambda \varphi_\lambda\,, \tag{3}$$

where the sum runs over all relevant irreps λ with dimensions d_λ, see Section 2.3. Although commonly done, we remind the reader that caution is advised if F is interpreted as the average *entanglement fidelity* of passive transformations. This is due to the inherent *gauge freedom* of RB, see Refs. [44, 49] for a detailed discussion. In particular, whether such an interpretation is justified or not cannot be deduced from RB results alone. We take the point of view of Ref. [49] in that RB decays rates and F in Eq. (3) should be regarded as quantities in the own right which serve as a benchmark for the average quality of the used unitaries. Besides the mentioned interpretational issues, RB decay rates for discrete variable systems are usually identified with *average gate fidelities* by a suitable affine transformation of Eq. (3). The concept of average gate fidelity is however not meaningful in the CV context due to divergent integrals in the definition. Nevertheless, the entanglement fidelity can still be defined for quantum channels restricted to finite-dimensional subspaces.

2.2.1 Discussion of the protocol

In the following, we justify the made choices based on the blueprint for filtered RB [1]. First, we identify the relevant unitary representation ω_n^m of the group $\mathrm{U}(m)$, which describes the ideal action of the unitaries as quantum channels. ω_n^m is called the *reference representation* in the RB literature and its irreps will play a central role. While the reference representation in the discrete setting is typically set as $\omega(g) = U_g(\,\cdot\,)U_g^\dagger$, where $g \mapsto U_g$ is the defining representation [1], there is a richer plethora of representations for CV systems. Moreover, this choice may also be related to the choice of initial state and measurement. In particular, the most straightforward –and experimentally simplest– RB protocol would involve an entirely Gaussian experiment with Gaussian state and measurement (the CV analogue of the usual stabilizer setting in discrete variables). In this case, the reference representation is however ill-behaved for the following reason: Any passive transformation can be described on $\mathcal{F}_m$ by a unitary representation $\tau^m : \mathrm{U}(m) \to \mathrm{U}(\mathcal{F}_m)$, where $\mathrm{U}(\mathcal{F}_m)$ is the group of unitary operators on $\mathcal{F}_m$. Since $\mathrm{U}(m)$ is compact, τ^m is completely reducible, and decomposes into infinitely many finite-dimensional irreps acting on the boson number subspaces [62]. Similarly, the reference representation $\omega \equiv \tau^m(\,\cdot\,)\tau^{m\dagger}$ decomposes into infinitely many irreps, which are not all supported on the number subspaces. This means we find infinitely many decay rates (each associated to one irrep) and it is unclear how to truncate those with a regularization argument, as the irreps lack a clear physical interpretation. On top of that, the decomposition of ω is not multiplicity-free[1], which complicates the post-processing and affects its numerical stability [49].

Before moving forward, we comment on the choice of the ensemble: Broadly speaking, *active* Gaussian transformations play a fundamental role in CV systems, for instance in the implementation of Gaussian boson sampling experiments [14, 15, 63]. However, benchmarking non-passive transformations pose many challenging issues, that head to the group of Gaussian transformations –that corresponds to the symplectic group $\mathrm{Sp}(2m,\mathbb{R})$ on m modes– being *non-compact*. This would imply that the general framework of filtered RB cannot be applied as it is, since it is specifically designed to deal with compact groups [1], and a generalization to the case of locally compact groups would be necessary. In particular, this would rise many technical challenges. Among them, and most prominently, one can find the non-existence of a probability Haar measure (since, by standard results in harmonic analysis, the Haar measure of a non-compact group cannot be finite) not clear to deal with. Similarly, the action

[1] Note that ω restricted to $\mathcal{B}(\mathcal{H}_n^m)$ is equal to ω_n^M and by Eq. (4), each λ_k appears in all ω_n^M for $n \geq k$.

of active transformations is determined by the full metaplectic representation of $\mathrm{Sp}(2m, \mathbb{R})$, which decomposes into infinite dimensional irreps only [64]. A priori, it is not clear how the conjugate action of such representation decomposes into irreps. On the other hand, naive extensions of standard RB to the group of active transformations will probably lead to experimental data which are too hard to analyze, as the contribution coming from different irreps would be 'entangled' and isolating it will likely be rather hard.

Hence, we consider an experiment where the initial state is supported on a finite-dimensional subspace of $\mathcal{F}_m$ such that there are finitely many relevant irreps of $\mathrm{U}(m)$. More precisely, we assume that an arbitrary Fock basis state can be prepared to avoid the problem of multiplicities (as e.g. for core states). Assuming the input state is $|\boldsymbol{n}\rangle$, with $n = \sum_{j=1}^{M} n_j$, any passive transformation acts on $|\boldsymbol{n}\rangle$ according to the totally symmetric irrep $\tau_n^m \colon \mathrm{U}(m) \to \mathrm{U}(\mathcal{H}_n^m)$. As we show in Section 4.1, the reference representation $\omega_n^M := \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$ is multiplicity-free, and we find

$$\omega_n^M = \bigoplus_{k=0}^{n} \lambda_k\,, \quad \lambda_0 \equiv \mathbf{1}\,,\ \lambda_1 \equiv \mathrm{Ad}\,, \tag{4}$$

where $\mathbf{1}$ denotes the trivial irrep and Ad the adjoint representation of $\mathrm{U}(m)$.

For our protocol, we consider two possible measurement settings. The first one consists of particle number resolving (PNR) detectors, implementing the POVM described by projectors onto Fock states, i.e. $\{|\boldsymbol{k}\rangle\langle\boldsymbol{k}|\}_{\boldsymbol{k}\in\mathbb{N}^m}$ [65, 66]. In this case, the experiment resembles -up to the choice of the input state and the POVM element- the Boson Sampling (BS) experiment originally proposed by Aaronson and Arkhipov [13]. In the second setting – discussed in Appendix H– we consider a balanced heterodyne measurement at the end of each mode, formally described by the coherent states POVM $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\}_{\boldsymbol{\alpha}\in\mathbb{C}^m}$. This setup is similar to a Gaussian Boson Sampling (GBS) experiment [14, 15, 67].

Finally, we introduce the *filter function* which isolates the exponential decays for each irrep $\lambda = \lambda_k$ in the post-processing of the collected data. Let P_λ be the projector on the carrier space of λ and let d_λ be its dimension. Then, given the measurement channel $\mathcal{M}(A) := \int_\Omega d\boldsymbol{x}\, \langle \boldsymbol{x}\,|A|\boldsymbol{x}\rangle |\boldsymbol{x}\rangle\langle\boldsymbol{x}|$, we define the filter function as [1]

$$f_\lambda(\boldsymbol{x}, g) := s_\lambda^{-1} \langle \boldsymbol{x}\,|\omega_n^m(g)^\dagger \circ P_\lambda(\rho)\,|\boldsymbol{x}\rangle\,, \tag{5}$$

with

$$s_\lambda := \frac{1}{d_\lambda}\,\mathrm{Tr}[P_\lambda \mathcal{M}] \in \mathbb{R}_{\geq 0}\,. \tag{6}$$

Notably, s_λ can be zero if the measurement POVM augmented by passive transformations is not informationally complete. In this case, we formally set $f_\lambda = 0$ as there will be no contribution from this irrep and no post-processing is necessary.

A remaining open question is how to choose the input state $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$. This choice influences the overall magnitude of the RB signal since the latter scales with the overlap of the initial state with the irrep of interest [1]. For RB on discrete variable systems, the input state is typically chosen to be the all-zeros state $|0^n\rangle$, and, in fact, the choice of input state plays a minor role in this case. The underlying reason is that we typically have a single non-trivial irrep with respect to which all states are essentially equivalent. For CV systems, this is a more subtle question, as many more non-trivial irreps exist, and it seems that there is no clear preferred choice in this case. As the protocols is – beyond the scaling with overlap – independent of the choice of initial state, the input state should be chosen by practical considerations. Generating higher Fock states can be a challenging task [68–70], and it seems that Fock states with $n \leq m$ photons evenly distributed across all modes may be preferable from a practical point of view.

2.3 Performance guarantees

The filtered RB framework [1] implies a number of guarantees for the passive RB protocol under the *implementation map* model. In the latter, the noise is modeled by replacing the representation ω_n^M with an implementation map ϕ_n^M on $\mathrm{U}(m)$, which takes values in the set of quantum channels on $\mathcal{H}_n^M$. This model allows for highly gate-dependent noise, which, however, needs to be stationary and Markovian.

2.3.1 Signal form

Let us define the expected signal as $F_\lambda(m) := \mathbb{E}[\hat{F}_\lambda(m)]$. In the absence of noise, the expected signal is simply constant and of the form [1]:

$$F_\lambda(m) = \begin{cases} \mathrm{Tr}\,[\rho P_\lambda(\rho)] & \text{if } s_\lambda \neq 0\,, \\ 0 & \text{else}\,. \end{cases} \tag{7}$$

In the presence of noise, $F_\lambda(m)$ is no longer constant, but well-approximated by an exponential decay:

Proposition 1 ([1, Thm. 8], informal)**.** *Suppose that the noise is sufficiently weak (in a precise sense). Then, we have*

$$F_\lambda(m) \approx A_\lambda \varphi_\lambda^m\,, \tag{8}$$

up to an additive error $\alpha \geq 0$ which is suppressed exponentially in m, and $A_\lambda \in \mathbb{R}$, $\varphi_\lambda \leq 1$.

In fact, the filtered RB framework [1] gives some more precise conditions on the error suppression in the expected signal. In particular, it is sufficient to choose the sequence length as

$$m \geq \log \frac{d_\lambda}{s_\lambda} + 2 \log \frac{1}{\alpha} + 4\,, \tag{9}$$

where d_λ is the dimension of the irrep and s_λ is as in Eq. (5). Later in Sec. 4, we give an explicit formula for s_λ in terms of Clebsch-Gordan coefficients of $\mathrm{SU}(m)$, however, it is generally difficult to give bounds which are better than $s_\lambda^{-1} = O(d_\lambda)$. We later show that $d_{\lambda_k} \leq \binom{k+m-1}{k}^2$ (c.f. Proposition 5), which would yield sequences of length $O(k \log \frac{k+m-1}{k})$. However, we expect that none of these bounds is particularly tight (in fact, Eq. (9) is not tight in the first place [1]). Based on the performance of discrete RB, we expect that already very short sequences (of constant length) are in fact sufficient.

2.3.2 Evaluation of the filter function

At the heart of the post-processing phase lies the evaluation of the filter function (5). Clearly, for Gaussian input state and measurements, the latter can be simulated in polynomial time. However, such a setting may not be favorable in the context of RB as argued in the last section. Instead, we consider the setting described in Section 2.2, involving Fock input states and either PNR or balanced heterodyne measurements. Then, we show the following:

Theorem 2 (filter function – informal)**.** *Consider an input state of the form $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ and either PNR or balanced heterodyne measurements. Then, the filter function (5) is a suitable linear combination of permanents or Hafnians, respectively.*

Note that the computational complexity of evaluating permanents (or Hafnians) is central to the complexity-theoretic arguments for boson sampling (and Gaussian boson sampling). In fact, even approximating any of the two is known to be computationally hard [13–15, 71]. Nevertheless, these quantities can be computed efficiently in some scenarios [54, 67, 72–77].

We prove Theorem 2 in Section 4.2. Here, we briefly sketch the central steps: Note that the reference representation can be written as $\omega_n^m \simeq \tau_n^m \otimes \bar{\tau}_n^m$, where $\bar{\tau}_n^m$ is the dual (or contragredient) representation of τ_n^m. The irrep decomposition of $\tau_n^m \otimes \bar{\tau}_n^m$ has a natural interpretation as the generalization of the Clebsch-Gordan decomposition for the sum of two angular momenta in quantum mechanics [78]. Informally, there exists a unitary matrix CG –the *Clebsch-Gordan* matrix– that block-diagonalizes ω_n^m [79], such that

$$|\boldsymbol{n}, \boldsymbol{n}\rangle = \sum_{\lambda} \sum_{M\in\lambda} C^{M}_{\boldsymbol{n},\bar{\boldsymbol{n}}} |M\rangle \,, \tag{10}$$

where $\bar{\boldsymbol{n}}$ denotes the dual of $\boldsymbol{n}$ in a sense to be specified later, λ is an irrep of ω_n^m, M's form a basis in which ω_n^m is block diagonal, and $C^M_{\boldsymbol{n},\bar{\boldsymbol{n}}}$ is a (generalized) SU(m) Clebsch-Gordan coefficient. We refer to Section 3 for a discussion on dual vectors and the Clebsch-Gordan series for SU(m) and to Section 4.1 for the irrep decomposition of ω_n^m.

Then, the projection onto a specific irrep λ acts by eliminating all terms in Eq. (10) which do not correspond to the filtering irrep λ . In a similar fashion, the coefficient s_λ in Eq. (5) can be evaluated – for a fixed measurement setting – in terms of Clebsch-Gordan coefficients.

In general, the result of Theorem 2 does not guarantee that the filter function can be computed efficiently. This is due to the fact that any basis vector in the coupled basis generally decomposes into a linear combination of essentially all Fock states in $\mathcal{H}_n^m$, using the inverse Clebsch-Gordan matrix. While some terms may be simulated efficiently, there is no hope that, in general, all inner products can be evaluated efficiently, as, for instance, bosons may be scattered across all modes, making simulation algorithms scale exponentially with the number of bosons [54].

In the case of PNR measurements, we give an alternative expression for f_λ in Section 4.2 as a linear combination of matrix elements of the irrep λ. In the bosonic realization of the Lie algebra $\mathfrak{su}(m)$, these also correspond to permanents [81], however, of a different dimension.

2.3.3 Sampling complexity

Finally, we discuss the sample complexity of passive RB, i.e. the number of samples needed to guarantee that the estimator $\hat{F}_\lambda(m)$ is ϵ-close to its expected value $F_\lambda(m)$ with high probability. Recall from Eq. (2) that $\hat{F}_\lambda(m)$ is a mean estimator for the filter function f_λ. Since the latter is only poorly bounded, we intend to compute the variance $\mathrm{Var}[\hat{F}_\lambda(m)] = \mathrm{Var}[f_\lambda]/L$ (here the variance is still taken over length-m sequences). Then, we can use Chebyshev's inequality to ensure $|\hat{F}_\lambda(m) - F_\lambda(m)| < \epsilon$ with probability $1-\delta$ given $L \geq \epsilon^{-2}\delta^{-1}\,\mathrm{Var}[f_\lambda]$ samples.

In general, analyzing the variance $\mathrm{Var}[f_\lambda]$ can be quite cumbersome, as the underlying probability distribution is given by Born probabilities involving the noisy input state, the noisy transformations, and the noisy measurements. In the filtered RB framework [1] it is shown that –as long as the SPAM-noise is non-malicious– this problem can be reduced to analyzing the second moment $\mathbb{E}[f_\lambda^2]_{\text{ideal}}$ in the ideal, noiseless case. In other words, the presence of noise cannot decrease the efficiency of filtered RB. Here, non-malicious means that the overall effect of SPAM noise is to reduce the magnitude of the signal, measured by the SPAM constants.[2] Using $\mathrm{Var}[f_\lambda] \leq \mathbb{E}[f_\lambda^2]$, the following result then establishes a bound on the sampling complexity of passive RB:

Theorem 3 (Second moment of f_λ – informal)**.** *Assume that the input state is a Fock state $|\boldsymbol{n}\rangle$, we use either PNR or balanced heterodyne measurements, and the SPAM noise is non-malicious. Then, we have*

$$\mathbb{E}[f_\lambda^2] \leq \mathbb{E}[f_\lambda^2]_{\text{ideal}} = \frac{\mathcal{C}}{s_\lambda^2} \,, \tag{11}$$

where $\mathcal{C}$ is a suitable linear combination of Clebsch-Gordan coefficients.

The proof of Theorem 3 is postponed to Section 4.3 for PNR measurements and to Appendix H for Gaussian measurement. It relies on expressing the second moment $\mathbb{E}[f_\lambda^2]_{\text{ideal}}$ as a suitable integral of the representations $\lambda^{\otimes 2}$ and ω_n^m over the compact group G [1, 46]. Schur's lemma then implies that the non-trivial contributions to this integral are given by the irreps of $\lambda^{\otimes 2}$ which are also contained in ω_n^m. We determine these irreps which allows

[2] This is necessary as specially engineered noise can drastically change the behavior of the RB signal, for instance by relabeling the measurement outcomes. Similar assumptions can be found throughout the RB literature [47, 82].

us to finally write $\mathbb{E}[f_\lambda^2]_{\text{ideal}}$ in terms of suitable Clebsch-Gordan coefficients.

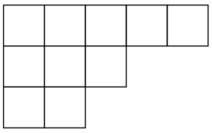
As we generally have $s_\lambda^{-1} \leq d_\lambda$, we have a naive upper bound $\mathbb{E}[f_{\lambda_k}^2] = O(s_{\lambda_k}^{-2})$. We however expect that these bounds are very loose and the variance is much smaller in practice.

3 Technical preliminaries

In this section, we review the main technical tools used in the proofs of our main results, shown in Section 4. First, we review irreps of SU(m) and the Clebsch-Gordan decomposition in terms of Gelfand–Tsetlin patterns, then we briefly review additional technical details concerning filtered randomized benchmarking.

3.1 Representations of SU(m)

Let $n \geq 0$ be a non-negative integer and let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be a partition of n, i.e. $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m \geq 0$ with $\sum_{i=0}^m \lambda_i = n$. Any such partition can be identified with a *Young diagram*, namely a collection of boxes arranged in left-justified rows with a weakly decreasing number of boxes in each row, where the i-th row contains λ_i boxes, e.g.



(12)

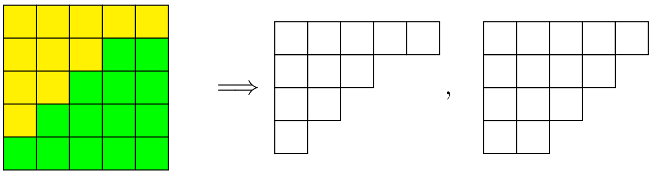
corresponds to $\lambda = (5, 3, 2)$. A *semi-standard Young tableaux* is a filling of a Young diagram with entries taken from any totally ordered set (here, $\mathbb{N}$) such that the entries are weakly increasing across each row and strictly increasing down each column. For instance,

$$\begin{array}{ccccc} 1 & 1 & 2 & 2 & 3 \\ 2 & 2 & 3 & & \\ 3 & 4 & & & \end{array}, \quad \begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 3 & & \\ 3 & 4 & & & \end{array} \tag{13}$$

are semi-standard Young of shape $\lambda = (5, 3, 2)$.

By the theorem of the highest weight [84, Thms. 9.4 and 9.5], Young diagrams uniquely determine irreps of SU(m) up to constant shifts, namely, $(\lambda_1, \ldots, \lambda_m)$ and $(\lambda_1 + c, \ldots, \lambda_m + c)$ identify the same irrep for any integer c. Therefore, as the rank of SU(m) is $m - 1$, by convention we assume $\lambda_m = 0$ without loss of generality. In the following we will not distinguish between Young diagrams and the corresponding irreps, unless otherwise specified.

For a given irrep λ, the *dual (or contragredient)* representation λ^* defined as $\lambda(g) := \lambda(g^{-1})^T$ for each $g \in$ SU(m) is also irreducible, see [84, Prop 4.22]. In a fixed orthonormal basis, we also have $\lambda^* \cong \bar{\lambda}$, where $\bar{\lambda}(g) := \overline{\lambda(g)}$ for each $g \in$ SU(m) denotes the complex conjugate representation of λ. For any irrep $\lambda = (\lambda_1, \ldots, \lambda_m)$, this implies λ^* is identified by the *dual* Young diagram $\bar{\lambda} := (\lambda_1 - \lambda_m, \lambda_1, -\lambda_{m-1}, \ldots, \lambda_2 - \lambda_1, 0)$. More practically, $\bar{\lambda}$ is constructed by completing λ to a $(m-1) \times \lambda_1$ rectangle-shaped Young diagram: The newly added boxes form $\bar{\lambda}$. For instance,



(14)

are dual Young diagrams in SU(5).

For a fixed irrep λ of SU(m), semistandard Young tableaux of shape λ label an orthonormal basis of λ, sometimes referred as the *Weyl basis*. For instance, the Young tableaux

$$\begin{array}{cc} 1 & 1 \\ 2 & \end{array}, \quad \begin{array}{cc} 1 & 1 \\ 3 & \end{array}, \quad \begin{array}{cc} 1 & 2 \\ 2 & \end{array}, \quad \begin{array}{cc} 1 & 2 \\ 3 & \end{array},$$
$$\begin{array}{cc} 1 & 3 \\ 2 & \end{array}, \quad \begin{array}{cc} 1 & 3 \\ 3 & \end{array}, \quad \begin{array}{cc} 2 & 2 \\ 3 & \end{array}, \quad \begin{array}{cc} 2 & 3 \\ 3 & \end{array}.$$

identify an orthonormal basis for the SU(3) adjoint irrep $\lambda = (2, 1)$.

3.1.1 Gelfand-Tsetlin patterns

A more convenient way of labeling basis vectors for any irrep $\lambda = (\lambda_1, \ldots, \lambda_m)$ of SU(m) is by *Gelfand–Tsetlin (GT) patterns*. A GT pattern M of shape λ and length m is represented by a triangular table with m rows, the i-th row containing i integers (counting from the bottom to the top)

$$M = \begin{pmatrix} M_{1,m} & & M_{2,m} & & \cdots & & M_{m-1,m} & & M_{m,m} \\ & M_{1,m-1} & & M_{2,m-1} & \cdots & M_{m-2,m-1} & & M_{m-1,m-1} & \\ & & \ddots & & \vdots & & \cdot^{\cdot^{\cdot}} & & \\ & & & M_{1,2} & & M_{2,2} & & & \\ & & & & M_{1,1} & & & & \end{pmatrix}, \tag{15}$$

where $M_{i,m} = \lambda_i$ for every $i \in [m]$ (and, in particular, $M_{m,m} = 0$ by convention) and the entries satisfy the *interlacing* or *inbetweenness* condition:

$$M_{i,j+1} \geq M_{i,j} \geq M_{i+1,j+1} \tag{16}$$

for every $i \in [m-1]$ and $j \in [m-1]$. We denote the set of GT patterns of shape λ by GT(λ).

An orthonormal basis for λ –referred as the Gelfand–Tsetlin basis– is given by state vectors $\{|M\rangle\}$, where M is a valid GT patterns M with top row $\boldsymbol{M}_1 \equiv (M_{1,1}, \ldots, M_{1,m}) = \lambda$. Hence, the dimension of λ is equal to the number of such states, for which the following formula holds:

$$\dim\lambda = \prod_{1\leq i\leq j\leq m}\left(1+\frac{M_{i,m}-M_{j,m}}{j-i}\right) . \tag{17}$$

In terms of the GT basis, the highest weight vector of λ is identified by the pattern maximizing the inbetweenness conditions, namely

$$M_0 = \begin{pmatrix} M_{1,m} & & M_{2,m} & & \cdots & & M_{m-1,m} & & M_{m,m} \\ & M_{1,m} & & M_{2,m} & \cdots & M_{m-2,m} & & M_{m-1,m-1} & \\ & & \ddots & & \vdots & & \cdot^{\cdot^{\cdot}} & & \\ & & & M_{1,m} & & M_{2,m} & & & \\ & & & & M_{1,m} & & & & \end{pmatrix} \tag{18}$$

(likewise, the lowest weight vector of λ is obtained by minimizing the inbetweenness conditions).

GT patterns are in one-to-one correspondence with semi-standard Young tableaux. In fact, for a given Young tableau T of shape λ, the shape of the corresponding GT pattern M is the same shape as T and the $M_{j,k}$-th entry of M is given by the number of entries in the j-th row of T which are less or equal than k. Conversely, given a GT pattern M of shape λ, the shape of the corresponding Young tableau T is determined by the first row of M and $m_{j,k} - m_{j,k-1}$ is the number of k's in the j'th row of T. Throughout this work, we assume that all illegal coefficients are set to 0. For instance, the Young tableaux in Eq. (13) corresponds to the following GT patterns:

$$\begin{pmatrix} 5 & & 3 & & 2 & & 0 \\ & 5 & & 3 & & 2 & \\ & & 4 & & 2 & & \\ & & & 2 & & & \end{pmatrix}, \quad \begin{pmatrix} 5 & & 3 & & 2 & & 0 \\ & 5 & & 3 & & 1 & \\ & & 5 & & 2 & & \\ & & & 5 & & & \end{pmatrix}, \tag{19}$$

For a given GT pattern M, the *weight* of $|M\rangle$ is a $(m-1)$-ple defined as $w_M := (w_1^{(M)}, \ldots, w_{m-1}^{(M)})$, where each $w_i^{(M)}$ can be determined by M:

$$w_j^{(M)} = \sum_{i=1}^{j} M_{i,j} - \frac{1}{2}\left[\sum_{i=1}^{j-1} M_{i,j-1} + \sum_{i=1}^{j+1} M_{i,j+1}\right] , \tag{20}$$

which generalizes the notion of the magnetic quantum number m for SU(2) in the quantum theory of angular momentum to arbitrary many modes.

Notably, unlike the SU(2) case, weights do not uniquely identify the weight vectors, as the associated weight spaces may not be 1-dimensional [98–100]: Consider the tableau weight $w^T = (w_1^T, \ldots, w_m^T)$, where T is the semi-standard Young tableau associated with M and

$$w_i^T := \sum_{i=1}^{j} M_{i,j} - \sum_{i=1}^{j-1} M_{i,j-1} \tag{21}$$

is the total number of i entries in T. The weights w_M and w^T are clearly related since

$$w_i^{(M)} = \frac{1}{2}\left(w_i^T - w_{i+1}^T\right) \tag{22}$$

Then, for instance,

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 2 \\ \hline 3 & 3 & \\ \cline{1-2}\end{array}\,, \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & \\ \cline{1-2}\end{array}\,.$$

have clearly the same (tableau) weight for the SU(3) irrep $\lambda = (3, 2)$.

For a weight w, the dimension of the weight space is the *inner multiplicity* of such weight, and corresponds to the number of GT states (or, equivalently, to the number of semi-standard Young tableaux) with weight w. These amount to Kostka's numbers, and can be computed e.g. with recursive algorithms [95].

Dual GT patterns. For a given GT pattern M of shape λ, we define the *dual* GT pattern $\bar{M}$ of shape $\bar{\lambda}$ as the pattern with entries satisfying the relation

$$\bar{M}_{i,l} := M_{1,m} - M_{l-i+1,l} \, , \tag{23}$$

namely $\bar{M}$ is the GT pattern obtained by a constant shift of size $M_{1,m}$ of the GT pattern obtained by flipping all the elements of each row of M, with opposite sign. By construction, $\bar{M}$ is a basis state for the dual irrep $\lambda^* \cong \bar{\lambda}$ of λ. The conjugate operation is also such that each state $|M\rangle$ of λ is associated with a unique conjugate state $|\bar{M}\rangle$ of $\bar{\lambda}$. Specifically, the conjugation operation is such that [100]

$$|M\rangle = (-1)^{\varphi(M)}|\bar{M}\rangle \, , \tag{24}$$

for a suitable phase function that can be determined as follows: For a GT pattern M, define the function

$$s_M(k) = \sum_{j=1}^{k}\sum_{i=1}^{j} M_{i,j} \, , \tag{25}$$

which corresponds to the sum of the labels of M in the first k rows (counting from bottom to top). Then [100],

$$\varphi(M) = s_M(m-1) - s_{M_0}(m-1) \, , \tag{26}$$

where M_0 is defined in Eq. (18).

3.1.2 Symmetric irreps in SU(m)

In this section, we summarize a few basic facts concerning symmetric irreps of SU(m), as they are of central importance throughout this work.

By construction, the space of n particles over m modes is maximally symmetric under permutations over the modes. This implies that the action of $g \in$ SU(m) on such space is described by the irrep

$$\tau_n^m \equiv (n, \underbrace{0, \ldots, 0}_{m-1}) = \underbrace{\square\cdots\square}_{n} \, , \tag{27}$$

where the number of boxes has the interpretation of the number of particles in the system. Formally, the Young diagram on the r.h.s. labels the maximally symmetric irrep in $\mathrm{SU}(m)$. Notably, the weights of the maximally symmetric irreps uniquely identify GT basis elements, as it can be easily checked via the associated tableaux weights.

In $\mathcal{H}_n^m$, a common orthonormal basis is the *Fock basis*, given by Fock states $\{|\boldsymbol{n}\rangle \mid \boldsymbol{n} \in \mathbb{N}^m, \sum_{i=1}^m n_i = n\}$. We remark that the GT basis, as well as the Weyl basis, labels the same set of orthonormal vectors as the Fock basis. In fact, for symmetric irreps, $\boldsymbol{n}$ is exactly the tableau weight of the corresponding Young tableau, i.e. n_i is the number of boxes filled with i for each $i \in [m]$, e.g.

$$|3,2,1\rangle = \left|\begin{array}{|c|c|c|c|c|c|}\hline 1 & 1 & 1 & 2 & 2 & 3 \\ \hline\end{array}\right\rangle , \tag{28}$$

from which it follows the correspondence with the GT basis. In particular, for any Fock state $|\boldsymbol{n}\rangle = |n_1, \ldots, n_m\rangle$, the corresponding GT pattern will be denoted by N, and it is given as follows:

$$N = \begin{pmatrix} n & & & 0 & & \ldots & & 0 & & 0 \\ & \sum_{i=1}^{m-1} n_i & & & 0 & \ldots & 0 & & 0 & \\ & & & \ddots & & \vdots & & \iddots & & \\ & & & & n_1+n_2 & & 0 & & & \\ & & & & & n_1 & & & & \end{pmatrix} . \tag{29}$$

Accordingly, the complex conjugate representation (and therefore the dual representation) acts on the dual space $\hat{\mathcal{H}}_n^m \cong \mathcal{H}_n^m$ and it is identified by the Young diagram

$$\bar{\tau}_n^m = \underbrace{m-1\left\{\begin{array}{ccc} \square & \cdots & \square \\ \vdots & \cdots & \vdots \\ \square & \cdots & \square \end{array}\right.}_{n} . \tag{30}$$

which acts on the dual space $\hat{\mathcal{H}}_n^m \cong \mathcal{H}_n^m$. In this case, we remark that a Fock basis is lacking for $\bar{\tau}_n^m$, as such irrep is not symmetric (and therefore it is not physical w.r.t. bosonic systems). However, the GT basis exists for each irrep and, in this case, the basis elements are labeled by GT patterns $\bar{N}$ of the form

$$\bar{N} = \begin{pmatrix} n & & n & & \ldots & & & n & & 0 \\ & n & & n & \ldots & & n & & n_m & \\ & & \ddots & & \vdots & & & \iddots & & \\ & & & n & & \sum_{i=3}^m n_i & & & & \\ & & & & \sum_{i=2}^m n_i & & & & & \end{pmatrix} , \tag{31}$$

Cf. Eqs. (23) and (29).

3.1.3 Clebsch-Gordan coefficients

A crucial step for filtered RB is the decomposition of the reference representation into irreps. In this section, we recap the role of the Clebsch-Gordan series for $\mathrm{SU}(m)$ in the decomposition of any tensor product representation, which will be employed in the remaining of this work. This topic has been investigated extensively over the years due to its relevance in particle physics, so we refer to standard references such as [78, 103, 104] for further details.

For two given irreps π_1, π_2 of $\mathrm{SU}(m)$, we consider the (completely reducible) tensor product representation $\pi_1 \otimes \pi_2 \colon \mathrm{SU}(m) \to \mathrm{U}(\mathcal{H}_{\pi_1} \otimes \mathcal{H}_{\pi_2})$. By the compact version of Maschke's theorem [93, Thm. 5.2], we have

$$\pi_1 \otimes \pi_2 = \bigoplus_{\lambda} \lambda^{\oplus m_\lambda} , \tag{32}$$

where m_λ is the multiplicity of λ in $\pi_1 \otimes \pi_2$. For $\mathrm{SU}(m)$, such decomposition can be computed in terms of Young diagrams with *Littlewood-Richardson's rules* that we summarize in Appendix A.

In the context of second quantization, the decomposition of $\tau_n^m \otimes \bar{\tau}_n^m$ can be interpreted as the generalization of the Clebsch-Gordan decomposition for spin states in Quantum Mechanics to the case of Fock states[3] [79, 80, 85, 86]. Such decomposition implies that there exists a unitary matrix CG –here referred as the *Clebsch-Gordan matrix*– that realizes the basis transformation from the tensor product space to the direct sum space:

$$\mathrm{CG}\left(\tau_n^m \otimes \bar{\tau}_n^m\right) \mathrm{CG}^\dagger = \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} . \tag{33}$$

CG is uniquely defined up to global phases, and by convention it is chosen to be real. Clebsch-Gordan coefficients are the matrix coefficients of the CG realizing such change of basis. In particular, Clebsch-Gordan coefficients describe the basis transformation from the tensor product basis to the direct sum space, spanned by the union of the coupled bases: For GT patterns $M_1 \in \mathrm{GT}(\pi_1), M_2 \in \mathrm{GT}(\pi_2)$, we have

$$|M_1, M_2\rangle = \sum_{M \in \mathrm{GT}(\lambda)} C_{M_1,M_2}^{M,r} |M, r\rangle , \tag{34}$$

where $r \in [m_\lambda]$ denotes the r-th copy of λ in $\pi_1 \otimes \pi_2$. Conversely,

$$|M, r\rangle = \sum_{M_1 \in \mathrm{GT}(\pi_1)} \sum_{M_2 \in \mathrm{GT}(\pi_2)} C_{M_1,M_2}^{M,r} |M_1, M_2\rangle . \tag{35}$$

By unitarity of CG, orthogonality relations hold true:

$$\sum_{M \in \mathrm{GT}(\lambda)} C_{M_1,M_2}^{M,r} C_{M_3,M_4}^{M,r} = \delta_{M_1,M_3} \delta_{M_2,M_4} , \tag{36}$$

$$\sum_{M_1 \in \mathrm{GT}(\pi_1)} \sum_{M_2 \in \mathrm{GT}(\pi_2)} C_{M_1,M_2}^{M,r} C_{M_1,M_2}^{M',r'} = \delta_{M,M'} \delta_{r,r'} . \tag{37}$$

As in the case of $\mathrm{SU}(2)$, selection rules for Clebsch-Gordan coefficients of $\mathrm{SU}(m)$ are available: For GT patterns $M_1 \in \mathrm{GT}(()\pi_1), M_2 \in \mathrm{GT}(()\pi_2), M \in \mathrm{GT}(()\lambda)$, $C_{M_1,M_2}^{M,r} = 0$ if

$$w_M \neq w_{M_1} + w_{M_2} , \tag{38}$$

where $w_{(\cdot)}$ is the weight defined in Eq. (20).

[3] This is true for any tensor product representation $\tau_1 \otimes \tau_2$, where τ_1, τ_2 are irreps of $\mathrm{SU}(m)$ [79].

3.2 Background on filter functions

In Section 2.2, we introduced the filter function (Eq. (5)) to isolate and analyze the exponential decays associated with each irreducible component of the reference representation ω_n^m. In this section, for the sake of completeness, we briefly motivate it in the bosonic case, before delving into the main technical results of this work. For a comprehensive discussion, we refer to [1].

Formally, one defines the filter function (dropping the explicit dependence from the input state ρ) as

$$f_\lambda(\boldsymbol{x}, g) = \langle \boldsymbol{x} \,|\, P_\lambda \circ S^+ \circ \omega_n^m(g)^\dagger(\rho) \,|\, \boldsymbol{x}\rangle\,, \tag{39}$$

where S^+ is the Moore-Penrose pseudo-inverse of the *frame operator* S defined as

$$\begin{aligned} S &:= \int_\Omega d\boldsymbol{x} \int_G d\mu_H(g)\; \mathrm{Tr}[\omega_n^m(g)^\dagger(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)(\cdot)] \\ &\quad \times \omega_n^m(g)(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|) \\ &= \int_G d\mu_H(g)\, \omega_n^M(g)^\dagger \mathcal{M} \omega_n^M(g)\,, \end{aligned} \tag{40}$$

where $\mathcal{M} = \int_\Omega d\boldsymbol{x}\; \mathrm{Tr}[|\boldsymbol{x}\rangle\langle\boldsymbol{x}|(\cdot)]\, |\boldsymbol{x}\rangle\langle\boldsymbol{x}|$ is the (possibly infinite dimensional) measurement channel associated with the POVM $\{|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\}_{\boldsymbol{x}\in\Omega}$.

This choice of filter function is such that, in the ideal case of a noise-free, perfect implementation of the gates, the filtered RB signal is of the form $F_\lambda(m) = \mathrm{Tr}[\rho P_\lambda \circ S^+ \circ S(\rho)]$, where S^+S is the projector onto the span of the POVM. In particular, in the special case of an informationally complete POVM, $F_\lambda(m) = \mathrm{Tr}[\rho P_\lambda(\rho)]$, i.e. the filtered signal is the overlap of ρ with the filtering irrep.

Then, Eq. (5) follows from the following observation: As the reference representation $\omega_n^m := \tau_n^m(\cdot)\tau_n^{m\dagger}$ preserves the number of particles, S act non-trivially on the n-th Fock sector only, i.e.

$$S = \begin{pmatrix} \mathbf{0} & & & & & \\ & \ddots & & & & \\ & & \mathbf{0} & & & \\ & & & S^{(n)} & & \\ & & & & \mathbf{0} & \\ & & & & & \ddots \end{pmatrix}, \tag{41}$$

where $S^{(n)}$ is obtained via the restriction of $\mathcal{M}$ to the subspace of n particles. Moreover, since $\omega_n^m := \tau_n^m(\cdot)\tau_n^{m\dagger}$ decomposes as $\bigoplus_{k=0}^n \lambda_k$, the following decomposition holds [1]:

$$S^{(n)} = \bigoplus_\lambda S_\lambda^{(n)}\,, \quad S_\lambda^{(n)} = s_\lambda \mathbb{1}_\lambda\,, \tag{42}$$

where the direct sum is over all irreps of ω_n^M and, in general [1],

$$s_\lambda = d_\lambda^{-1}\, \mathrm{Tr}[P_\lambda \mathcal{M}] = d_\lambda^{-1} \int_\Omega d\boldsymbol{x}\, \mathrm{Tr}[|\boldsymbol{x}\rangle\langle\boldsymbol{x}| P_\lambda(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)]\,. \tag{43}$$

Here, $d_\lambda \equiv \dim \mathcal{H}_\lambda$, with $\lambda \in \{\lambda_k\}_{k=0}^n$, and P_λ is the corresponding projector onto its carrier space. In the second step, we used the fact that the Bochner integral commutes with the trace since the latter is a continuous linear operator in the trace norm and the trace of $[|\boldsymbol{x}\rangle\langle\boldsymbol{x}|P_\lambda(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)]$ is finite.

3.3 Further notations

As the Clebsch-Gordan decomposition is naturally related with the direct sum decomposition of an Hilbert space of the form $\mathcal{H}_1 \otimes \mathcal{H}_2$, it will be convenient to introduce a vectorized notation for operators and superoperators on $\mathcal{H}_n^m$.

We consider the basis of linear operators $L(\mathcal{H}_n^m)$ given by $\Phi = \{|\boldsymbol{n}\rangle\langle\boldsymbol{m}|\}_{\boldsymbol{n},\boldsymbol{m}\in\mathbb{N}^m}$ with $\sum_{i=1}^m n_i = \sum_{i=1}^m m_i = n$. Any linear operator $A \in L(\mathcal{H}_n^m)$ can be vectorized to an element $|A\rangle \in \mathcal{H}_n^m \otimes \mathcal{H}_n^m$ w.r.t. Φ as

$$|A\rangle = \sum_{\boldsymbol{n},\boldsymbol{m}} \mathrm{Tr}[|\boldsymbol{m}\rangle\langle\boldsymbol{n}|A]|\boldsymbol{n},\boldsymbol{m}\rangle\,, \quad |\boldsymbol{n},\boldsymbol{m}\rangle \equiv |\boldsymbol{n}\rangle \otimes |\boldsymbol{m}\rangle\,. \tag{44}$$

Under vectorization, we have $\tau_n^m(\cdot)\tau_n^{m\dagger} \mapsto \tau_n^m \otimes \bar{\tau}_n^m$, where $\bar{\tau}_n^m$ denotes the complex conjugate representation of τ_n^m. Moreover, as long as it is clear from the context, we will not distinguish between super-operators and their corresponding quantities acting on $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Hence, the filter function defined in Eq. (5) becomes

$$f_\lambda(\boldsymbol{x}, g) = \frac{1}{s_\lambda}\langle \boldsymbol{n},\boldsymbol{n} \,|\, P_\lambda(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger \,|\, \boldsymbol{x},\boldsymbol{x}\rangle\,, \tag{45}$$

with $s_\lambda = (\dim\lambda)^{-1} \sum_{\boldsymbol{x}\in\mathbb{N}^m} \langle \boldsymbol{x},\boldsymbol{x} \,|\, P_\lambda \,|\, \boldsymbol{x},\boldsymbol{x}\rangle$.

4 Passive RB with Fock states and measurements

Here, we provide proofs for the theorems introduced in Section 2: In Section 4.2 we prove Theorem 2 and in Section 4.3 we prove Theorem 3 based on notation and technical tools introduced in Section 3.

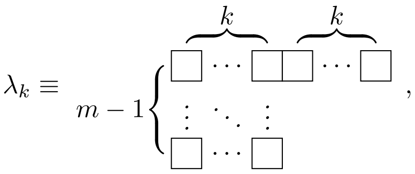
4.1 Clebsch-Gordan decomposition for the reference representation

In this section, we study the irrep decomposition of ω_n^M. As τ_n^m is irreducible, its dual is isomorphic to its complex conjugate representation (w.r.t. the Fock space). In particular, we have

$$\omega_n^M := \tau_n^m(\,\cdot\,)\tau_n^{m\dagger} \cong \tau_n^m \otimes \bar{\tau}_n^m\,. \tag{46}$$

In particular, we will restrict our focus on the irreps of $\mathrm{SU}(m)$ (or, equivalently, its corresponding Lie algebra $\mathfrak{su}(m)$) as τ_n^m can be extended to irreps of $\mathrm{U}(m)$ using nontrivial characters of the unit circle group (roughly speaking, resulting in a multiplication by a global phase), which becomes irrelevant for our aims, since it vanishes as we are interested in its conjugate action on $L(\mathcal{H}_n^m)$. The decomposition of ω_n^m into irreps can be computed using *Littlewood-Richardson's rules*, a general tool to classify the decomposition of tensor product representations. We refer to Appendix A for a brief overview on how they can be employed in the context of $\mathrm{SU}(m)$.

Lemma 4. *Let $\tau_n^m : \mathrm{SU}(m) \to \mathrm{U}(\mathcal{H}_n^m)$ be the irreducible representation of* $\mathrm{SU}(m)$ *on the space of n bosons distributed over m modes as in Eq.* (27). *Define the Young diagram*



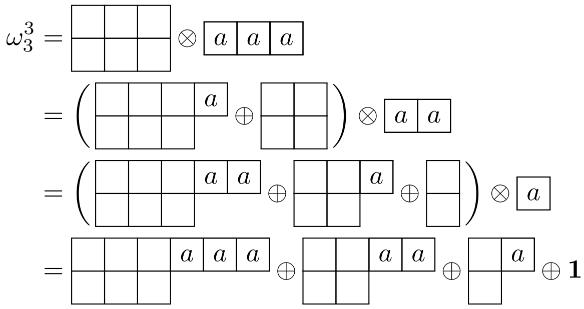
(47)

where λ_0 and λ_1 denote the trivial irrep and the adjoint irrep of $\mathrm{SU}(m)$*, respectively. Then, for any $n, m \in \mathbb{N} \setminus \{0\}$,*

$$\omega_n^M = \bigoplus_{k=0}^{n} \lambda_k \,, \tag{48}$$

where each λ_k, $k = 0, \dots, n$, appears exactly one time.

We prove this result in Appendix B. As an example, we have the following explicit decomposition of the conjugation for $n = m = 3$:



$$= \lambda_3 \oplus \lambda_2 \oplus \lambda_1 \oplus \mathbf{1} = \lambda_3 \oplus \omega_2^3 \,. \tag{49}$$

The dimension of λ_k admits a nice closed-form expression in terms of the dimension of the number subspace:

Proposition 5. *For any $k \in \mathbb{N}$, the following holds:*

$$\dim \lambda_k = \left(1 - \frac{k^2}{(k+m-1)^2}\right) (\dim \mathcal{H}_k^m)^2 \,. \tag{50}$$

We prove this fact in Appendix C.

Hence, we have an easy and algorithmic way to find the decomposition of the action $\tau_n^m \otimes \bar{\tau}_n^m$ into multiplicity-free irreps. We remark that this occurrence is a special case of the completely symmetric representation and its dual: In general, for a fixed representation, the conjugate action will not decompose into multiplicity-free irreps. Moreover, notice that the Young diagrams $\lambda_k, k = 1, \dots, n$ are associated with representations of real type, because each term in the decomposition is self-dual and multiplicity free.

4.2 Filter function for passive RB with PNR measurements

As an irrep decomposition of ω_n^m can be easily computed for any n and m (Cf. Lemma 4), we can evaluate explicit expressions for the filter function. This will provide the proof of Theorem 2.

By construction, $\omega_n^m = \tau_n^m(\cdot)\tau_n^{m\dagger} \cong \tau_n^m \otimes \bar{\tau}_n^m$ acts on elements $|\boldsymbol{n}, \boldsymbol{n}\rangle$ (from here on referred as the uncoupled basis). However, as pointed out in the Section 3.1.1, the second entry shall be suitably interpreted as a basis element of $\bar{\tau}_n^m$, which requires the specification of the relative phases of the states referred by the matrix coefficients. In particular, we have

$$|\boldsymbol{n}\rangle = |N\rangle = (-1)^{\varphi(N)} |\bar{N}\rangle \tag{51}$$

(Cf. Eqs. (23) and (29)). Hence,

$$\begin{aligned} \rho \cong |\boldsymbol{n}, \boldsymbol{n}\rangle &= |N, N\rangle = (-1)^{\varphi(N)} |N, \bar{N}\rangle \\ &= (-1)^{\varphi(N)} \sum_{k=0}^{n} \sum_{M \in \mathrm{GT}(\lambda_k)} C_{N,\bar{N}}^{M} \, |M\rangle \,, \end{aligned} \tag{52}$$

with $\{|N\rangle\}_{N \in \mathrm{GT}(\lambda_k)}$ being an orthonormal basis (referred as the coupled basis from here on) for the carrier space of λ_k. Notice that in Eq. (52) we do not need to specify the multiplicity index of states and Clebsch-Gordan coefficients since λ_k is multiplicity free for each $k = 0, \dots, n$.

Then, for a fixed irrep $\lambda \in \{\lambda_k\}_{k=0}^n$, we have $P_\lambda = X_\lambda X_\lambda^T$ [1], where $X_\lambda \colon \mathcal{H}_n^m \to \mathcal{H}_\lambda$ is an isometry whose matrix representation is given by the Clebsch-Gordan coefficients associated with the irrep λ. This implies

$$P_\lambda = \sum_{M \in \mathrm{GT}(\lambda)} |M\rangle\langle M| \,, \tag{53}$$

and the following relation holds true:

$$\begin{aligned} P_\lambda |N, \bar{N}\rangle &= \sum_{M \in \mathrm{GT}(\lambda)} \langle M | N, \bar{N}\rangle |M\rangle \\ &= \sum_{M \in \mathrm{GT}(\lambda)} C_{N,\bar{N}}^{M} |M\rangle \,, \end{aligned} \tag{54}$$

where, in the second equivalence, we used the identification $C_{N,\bar{N}}^{\lambda M} \equiv \langle \lambda M | N, \bar{N}\rangle$ and that – by the selection rules of Clebsch-Gordan coefficients – the sum is restricted to all the basis vectors such that the associated weight corresponds to the sum of the weights of the states $|N\rangle$ and $|\bar{N}\rangle$, Cf. Eq. (38). Specifically, by Eq. (23), we have

$$\begin{aligned} w_j^{(N)} + w_j^{(\bar{N})} &= \sum_{i=1}^{j} N_{i,j} - \frac{1}{2}\left(\sum_{i=1}^{j-1} N_{i,j-1} + \sum_{i=1}^{j+1} N_{i,j+1}\right) \\ &\quad + \sum_{i=1}^{j} \bar{N}_{i,j} - \frac{1}{2}\left(\sum_{i=1}^{j-1} \bar{N}_{i,j-1} + \sum_{i=1}^{j+1} \bar{N}_{i,j+1}\right) \\ &= \sum_{i=1}^{j} N_{1,m} - \frac{1}{2}\left(\sum_{i=1}^{j-1} N_{1,m} + \sum_{i=1}^{j+1} N_{1,m}\right) \\ &= 0 \,, \end{aligned} \tag{55}$$

which implies $w_N + w_{\bar{N}} = \mathbf{0}$. From the point of view of Young tableaux, this implies that in the tableau T_M –where $M \in \mathrm{GT}(\lambda)$ satisfies the latter selection rules– all the entries appear the same number of times. Moreover, the inner multiplicity $\gamma_{\lambda_k}(\mathbf{0})$ of $\mathbf{0}$ in λ_k for any $k \in \mathbb{N}$ can be easily computed and, in particular,

$$\gamma_{\lambda_k}(\mathbf{0}) = \binom{k+m-2}{k} . \tag{56}$$

We prove this result in Appendix D. This provides the number of non-zero terms in Eq. (54).

With these notations, we can prove the following technical result that will be used extensively in the rest of this work:

Lemma 6. *Let N, X be GT patterns, and let $\bar{N}, \bar{X}$ be their dual, respectively. Let τ_n^m be the n-particles maximally symmetric irrep of* $\mathrm{SU}(m)$ *and consider $\lambda_k \in \omega_n^m = \tau_n^m(\cdot)\tau_n^{m\dagger}$. Let P_{λ_k} be the projector onto λ_k. Then, the following holds:*

$$\begin{aligned}\langle N, \bar{N}\,|P_\lambda(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\,X, \bar{X}\rangle &= \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \\ \times \sum_{M' \in \mathrm{GT}(\lambda_k)} C^{M'}_{X,\bar{X}} \langle M\,|\lambda_k(g)^\dagger|\,M'\rangle \,. &\end{aligned} \tag{57}$$

Proof. By construction, P_{λ_k} selects the λ_k-th component of $|N, \bar{N}\rangle$, which can be conveniently isolated by the Clebsch-Gordan decomposition of $\omega_n^m \cong \tau_n^m \otimes \bar{\tau}_n^m$. This implies

$$\begin{aligned}\langle N, \bar{N}\,|P_\lambda(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\,X, \bar{X}\rangle &= \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \\ \times \langle M\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\,X, \bar{X}\rangle \,. &\end{aligned} \tag{58}$$

To compute the inner product, recall that $\tau_n^m \otimes \bar{\tau}_n^m = \bigoplus_{l=0}^n \lambda_l$ (Cf. Eq. (48)). In particular, observe that M is a basis element in λ_k, which implies the only non trivial contributions from $\tau_n^m \otimes \bar{\tau}_n^m$ are associated with its λ_k-th component. Likewise, the only relevant contributions to the inner product coming from $|X, \bar{X}\rangle$ are associated with its restriction to λ_k that can be expressed as

$$|X, \bar{X}\rangle\big|_{\lambda_k} = \sum_{M' \in \mathrm{GT}(\lambda_k)} C^{M'}_{X,\bar{X}} |M'\rangle \,. \tag{59}$$

Hence,

$$\begin{aligned}\langle M\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\,X, \bar{X}\rangle = &\sum_{M' \in \mathrm{GT}(\lambda_k)} C^{M'}_{X,\bar{X}} \\ &\times \langle M\,|\lambda_k(g)^\dagger|\,M'\rangle \,,\end{aligned} \tag{60}$$

from which the assertion follows. □

A first consequence, is the following explicit expression for the filter function defined in Eq. (5):

Theorem 7 (Restatement of Theorem 2 - PNR version)**.** *Let $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}| \cong |\boldsymbol{n}, \boldsymbol{n}\rangle = |N, N\rangle$ be a m modes state and let $\{|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\}_{\boldsymbol{x}\in\mathbb{N}^m}$ be the Fock state POVM. Then, for a given irrep $\lambda_k \in \hat{\omega}_n^M$, and assuming $s_{\lambda_k} \neq 0$,*

$$\begin{aligned}f_{\lambda_k}(\boldsymbol{x}, g) = \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)+\varphi(X)} &\sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \\ \times \sum_{M' \in \mathrm{GT}(\lambda_k)} C^{M'}_{X,\bar{X}} &\langle M\,|\lambda_k(g)^\dagger|\,M'\rangle \,,\end{aligned} \tag{61}$$

where the sums are restricted to all basis states such that Eq. (55) is satisfied.

Proof. By Eq. (52), and denoting by N and X the GT patterns associated with $\boldsymbol{n}$ and $\boldsymbol{x}$, respectively, the filter function defined in Eq. (5) becomes

$$\begin{aligned}f_{\lambda_k}(X, g) &= \frac{1}{s_{\lambda_k}}\langle N, N\,|P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\,X, X\rangle \\ &= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)+\varphi(X)} \\ &\times \langle N, \bar{N}\,|P_\lambda(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\,X, \bar{X}\rangle \\ &= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)+\varphi(X)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \\ &\times \sum_{M' \in \mathrm{GT}(\lambda_k)} C^{M'}_{X,\bar{X}} \langle M\,|\lambda(g)^\dagger|\,M'\rangle \,.\end{aligned} \tag{62}$$

In the last line, we used Lemma 6. □

Notably, explicit expressions for the matrix elements of irreps of $\mathrm{SU}(m)$ are available, see for instance [89, Chapter 3] for $\mathrm{SU}(2)$ and [90, Chapter 9] for $\mathrm{SU}(m)$. Moreover, numerical implementations using the bosonic realization of the Lie algebra $\mathfrak{su}(m)$ are also available [81].

Alternatively, the f_λ also assumes the following form:

$$\begin{aligned}f_{\lambda_k}(X, g) &= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \\ &\times \langle M\,|(\tau \otimes \bar{\tau})(g)^\dagger|\,X, X\rangle \\ &= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1, N_2 \in \mathrm{GT}(\tau_n^m)} \\ &\times C^M_{N_1,\bar{N}_2} \langle N_1, \bar{N}_2\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\,X, X\rangle \\ &= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1, N_2 \in \mathrm{GT}(\tau_n^m)} \\ &\times (-1)^{\varphi(N_2)} C^M_{N_1,\bar{N}_2} \langle N_1, N_2\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\,X, X\rangle \,,\end{aligned} \tag{63}$$

which is manifestly related to the computation of permanents [87], as each inner product resembles the boson sampling problem when expressed in the Fock basis:

$$\begin{aligned}&\langle N_1, N_2\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\,X, X\rangle = \\ &= \langle \boldsymbol{n}_1, \boldsymbol{n}_2\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\,\boldsymbol{x}, \boldsymbol{x}\rangle \\ &= \langle \boldsymbol{n}_2\,|\tau_n^m(g)|\,\boldsymbol{x}\rangle\langle \boldsymbol{x}\,|\tau_n^m(g)^\dagger|\,\boldsymbol{n}_1\rangle \\ &= \frac{1}{\boldsymbol{x}!\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!}} \operatorname{Per}(\tau_n^m(g)_{\boldsymbol{n}_2,\boldsymbol{x}}) \operatorname{Per}(\tau_n^m(g)^\dagger_{\boldsymbol{x},\boldsymbol{n}_1}) \,,\end{aligned} \tag{64}$$

where $\operatorname{Per}(U_{\boldsymbol{n},\boldsymbol{m}})$ denotes the permanent of the matrix obtained by $\tau_n^m(g)$ by taking m_j copies of the j-th column of U and then by taking n_i copies of the i-th row of the resulting matrix, and we used the multi-index notation $\boldsymbol{n}! := n_1! \ldots n_m!$.

To compute the filter function, we shall provide expressions for the coefficients s_λ. In particular, we have the following result for Eq. (43):

Lemma 8. *Let λ_k be an irrep in ω_n^m. For a PNR measurement setting, the eigenvalues of the frame operator of the passive RB protocol are given by*

$$s_{\lambda_k} = \frac{1}{d_{\lambda_k}} \sum_{X \in \mathrm{GT}(\tau_n^m)} \sum_{M \in \mathrm{GT}(\lambda_k)} |C^M_{X,\bar{X}}|^2 . \tag{65}$$

where $|X\rangle \equiv |\boldsymbol{x}\rangle \in \mathcal{H}_n^m$.

Proof. First, recall that a single mode (ideal) PNR detector measures the number of particles in such mode [66]. In the case of m modes, the (ideal) POVM is therefore given by $\{|\mathbf{x}\rangle\langle\mathbf{x}| \equiv E_{\mathbf{x}}\}_{\mathbf{x}\in\mathbb{N}^m}$ and the (vectorized) measurement channel can be written as

$$\mathcal{M} := \sum_{\mathbf{x}\in\mathbb{N}^m} |\boldsymbol{x},\boldsymbol{x}\rangle\langle\boldsymbol{x},\boldsymbol{x}| = \sum_{n=0}^{\infty}\sum_{X\in\mathrm{GT}(\tau_n^m)} |X,X\rangle\langle X,X|\,. \tag{66}$$

Denoting by P_{λ_k} the projector onto $\lambda_k \in \hat{\omega}_n^M$, we have the following:

$$\begin{aligned} s_{\lambda_k} &= \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{x}\in\mathbb{N}^m} \langle \boldsymbol{x},\boldsymbol{x}\,|P_{\lambda_k}|\boldsymbol{x}\boldsymbol{x}\rangle \\ &= \frac{1}{d_{\lambda_k}} \sum_{X\in\mathrm{GT}(\tau_n^m)} \langle X,X\,|P_{\lambda_k}|X,X\rangle \\ &= \frac{1}{d_{\lambda_k}} \sum_{X\in\mathrm{GT}(\tau_n^m)} (-1)^{2\varphi(X)}\langle X,\bar{X}\,|P_{\lambda_k}|X,\bar{X}\rangle \\ &= \frac{1}{d_{\lambda_k}} \sum_{X\in\mathrm{GT}(\tau_n^m)}\sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{X,\bar{X}}\langle X,\bar{X}|M\rangle \\ &= \frac{1}{d_{\lambda_k}} \sum_{X\in\mathrm{GT}(\tau_n^m)}\sum_{M\in\mathrm{GT}(\lambda_k)} |C^M_{X,\bar{X}}|^2\,, \end{aligned} \tag{67}$$

where in the second step we used the fact that P_{λ_k} acts non-trivially on the n particle subspace, and in the fourth step we used the fact that the phases $\varphi(X)$ introduced in the labeling of GT dual patterns are integers by construction, Cf. Eq. (26). □

Concretely, the time complexity of computing s_{λ_k} heavily relies on the efficient evaluation of the Clebsch-Gordan coefficients, since the sums are restricted to very few terms due to selection rules. In particular, one can evaluate all Clebsch-Gordan coefficients beforehand. Then, since the Clebsch-Gordan matrix is very sparse, the sum in Eq. (65) can be restricted to non-trivial terms only. Hence, as Clebsch-Gordan coefficients can be calculated in polynomial time [79, 92] for ≈ 20 modes before memory overhead limits the application of such algorithms [92], s_{λ_k} can also be evaluated efficiently for a moderate number of modes.

4.3 Moments of the filter function for PNR measurement settings

In this section, we provide explicit expressions for first two moments of probability of the filter function (5) w.r.t the ideal probability distribution $p(\boldsymbol{x}|g) = \langle\boldsymbol{x}\,|\omega_n^m(g)(\rho)|\boldsymbol{x}\rangle$, $\boldsymbol{x}\in\mathbb{N}^m$. In particular, the ideal second moment will provide an upper bound to the sampling complexity of the protocol, Cf. Section 2.3.

The following technical result will be useful:

Lemma 9. *Let N, X be GT patterns, and let $\bar{N}, \bar{X}$ be their dual, respectively. Let τ_n^m be the n-particles maximally symmetric irrep of* SU(m) *and consider $\lambda_k \in \omega_n^m = \tau_n^m(\cdot)\tau_n^{m\dagger}$. Then, the following holds:*

$$\begin{aligned}\langle X,\bar{X}\,|(\tau_n^m\otimes\bar{\tau}_n^m)(g)|N,\bar{N}\rangle = \sum_{j=0}^{n}\sum_{M,M'\in\mathrm{GT}(\lambda_j)} C^M_{X,\bar{X}} \\ \times\, C^{M'}_{N,\bar{N}}\langle M\,|\lambda_j(g)|M'\rangle\,. \end{aligned}\tag{68}$$

Proof. The expression follows immediately from the Clebsch-Gordan decomposition. More specifically, we have

$$|N,\bar{N}\rangle = \sum_{i=0}^{n}\sum_{M\in\mathrm{GT}(\lambda_i)} C^M_{N,\bar{N}}|M\rangle\,, \tag{69}$$

$$|M,\bar{M}\rangle = \sum_{j=0}^{n}\sum_{M'\in\mathrm{GT}(\lambda_j)} C^{M'}_{X,\bar{X}}|M'\rangle\,, \tag{70}$$

$$\tau_n^m\otimes\bar{\tau}_n^m = \bigoplus_{k=0}^{n}\lambda_k\,, \tag{71}$$

Cf. Eq. (52) and Eq. (48). Hence, since M and M' are basis elements of λ_i and λ_j, respectively,

$$\langle M\,|\lambda_k(g)|M'\rangle \neq 0 \tag{72}$$

only if $i = j = k$, from which the assertion follows. □

We will also need the following standard result in the representation theory of compact groups, often referred as Schur's orthogonality relations, see [93, Thm. 5.8]: For a given irrep λ of SU(m) (or, in general, of any compact group G), if $M_1, M_2, M_1', M_2' \in \mathrm{GT}(\lambda)$, then the following relation holds true:

$$\begin{aligned}\int dg\,\langle M_1\,|\lambda(g)|M_1'\rangle\langle M_2\,|\lambda(g)^\dagger|M_2'\rangle \\ = \frac{1}{\dim\lambda}\delta_{M_1,M_2}\delta_{M_1',M_2'}\,,\end{aligned}\tag{73}$$

where dg denotes the Haar measure on G.

Before we prove the main results of this section, it is worth to quickly consider the first moment $\mathbb{E}[f_\lambda]$, as the proof scheme is the same, but in the case of the second moment is hidden behind few additional technical details concerning the representations involved.

Lemma 10. *For a PNR measurement setting, $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ as input state, and an irrep λ_k of $\omega^{(n)} = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$, the following holds:*

$$\mathbb{E}[f_\lambda] = \sum_{M\in\mathrm{GT}(\lambda_k)} |C^M_{N,\bar{N}}|^2\,, \tag{74}$$

where N is the GT pattern associated with $\boldsymbol{n}$, and $\bar{N}$ is its dual.

We prove this result in Appendix E.

In general, finding explicit expressions for the second moment $\mathbb{E}[f_\lambda^2]$ is more involved and the following technical result is necessary:

Lemma 11. *Let λ_k be a Young diagram as in Eq. (47) labeling an irrep of* $\mathrm{SU}(m)$*,* $m \geq 3$*. Then,*

$$\lambda_k \otimes \lambda_k = \bigoplus_{l=0}^{k} \lambda_l^{(l+1)} \oplus \bigoplus_{l=k+1}^{2k} \lambda_l^{(2k-l+1)} \oplus L\,, \tag{75}$$

where $\lambda_0 \equiv \mathbf{1}$, $\lambda_1 \equiv \mathrm{Ad}$, $\lambda_j^{(i)}$ denotes the i-th copy of λ_j in $\lambda_l^{\otimes 2}$, and L is a suitable direct sum of irreps which are not of the form λ_l for any $l \in \mathbb{N}$.

Specifically, all irreps λ_l in $\lambda_k^{\otimes 2}$ are computed by identifying all legal ways of combining two copies of λ_k to a fixed shape using Littlewood-Richardson's rules. This result is presented in Appendix F.

Hence, we derive an explicit expression for $\mathbb{E}[f_\lambda^2]$ using Eq. (73):

Theorem 12. *For a PNR measurement setting, $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ as input state, and an irrep λ_k of $\omega^{(n)} = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$, the following holds:*

$$\mathbb{E}[f_{\lambda_k}^2] = \frac{1}{s_{\lambda_k}^2}(-1)^{\varphi(N)} \sum_{X \in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(X)} g_k(X,N)\,, \tag{76}$$

where $g_k(X,N)$ is a function of Clebsch-Gordan coefficients of the representations $\tau_n^m \otimes \bar{\tau}_n^m$ and $\lambda_k^{\otimes 2}$ given by

$$g_k(X,N) = \sum_{l=0}^{\min\{n,2k\}} \frac{1}{\dim\lambda_l} \sum_{r=1}^{m_l} \sum_{\substack{M,M',L,\\ L' \in \mathrm{GT}(\lambda_k)}} \sum_{R,R' \in \mathrm{GT}(\lambda_l)} \times C_{N,\bar{N}}^{M} C_{N,\bar{N}}^{M'} C_{X,\bar{X}}^{L} C_{X,\bar{X}}^{L'} C_{N,\bar{N}}^{R} C_{X,\bar{X}}^{R'} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \tag{77}$$

where m_l is the multiplicity of λ_l in $\lambda_k^{\otimes 2}$ as in Lemma 11.

We prove this result in in Appendix G.

4.4 A worked out example

In the case of 2 modes systems, Clebsch-Gordan coefficients reduce to the usual ones, and the analysis of the filter function and its moments drastically simplifies. In this section, we show explicit expressions for such a case, which will highlight some technicalities implicit in the general case of $\mathrm{SU}(m)$.

In the $\mathrm{SU}(2)$ case, it is convenient to switch from the bosonic realization of the $\mathrm{SU}(2)$ algebra to its spin realization, where Clebsch-Gordan coefficients are naturally introduced. This task is accomplished by the Jordan-Schwinger map [62]: For given annihilation operators a_1, a_2 acting on a 2 mode system and satisfying the CCRs, the Jordan-Schwinger map is such that

$$J_1 := \frac{1}{2}\left(a_2^\dagger a_1 + a_1^\dagger a_2\right)\,, \tag{78}$$

$$J_2 := \frac{1}{2}\left(a_2^\dagger a_1 - a_1^\dagger a_2\right)\,, \tag{79}$$

$$J_3 := \frac{1}{2}\left(a_1^\dagger a_1 - a_2^\dagger a_2\right)\,, \tag{80}$$

where $[J_i, J_j] = i\epsilon_{ijk}J_k$, ϵ is the Levi-Civita's pseudo-tensor, and

$$J^2 = J_1^2 + J_2^2 + J_3^2 = \frac{n}{2}\left(\frac{n}{2}+1\right)\,, \tag{81}$$

$$n = n_1 + n_2\,, \quad n_i = a_i^\dagger a_i\,. \tag{82}$$

This implies the normalized states $|n_1, n_2\rangle$ correspond to the eigenstates $|jm\rangle$ of J^2 and J_3, with the identification [85, 86]

$$n_1 = j + m\,, \quad n_2 = j - m\,, \tag{83}$$

hence, in this section, we will consider an input state $\rho = |jm\rangle\langle jm|$ and the Fock state POVM becomes $\{|j'm'\rangle\langle j'm'|\}$, where $j' \in \frac{1}{2}\mathbb{N}$ and $m' = -j', \ldots, j'$. A spin state $|jm\rangle$ and its dual are identified by the GT patterns

$$\begin{pmatrix} 2j & & 0 \\ & j-m & \end{pmatrix}, \quad \begin{pmatrix} 2j & & 0 \\ & j+m & \end{pmatrix}, \tag{84}$$

respectively, which implies the following relation:

$$\overline{|jm\rangle} = (-1)^{j+m}|j-m\rangle\,. \tag{85}$$

Moreover, given any irrep λ_J of $\mathrm{SU}(2)$, the following relations hold:

$$P_J = \sum_{M=-J}^{J} |JM\rangle\langle JM|\,, \quad s_J = \frac{1}{2J+1}\,. \tag{86}$$

In particular, the expression for s_J follows from Eq. (65), the fact that the inner multiplicities of $\mathrm{SU}(2)$ basis vectors are 1 (or, equivalently, each weight is uniquely associated with a unique weight vector), and the $\mathrm{SU}(2)$ orthogonality relation $\sum_m |C_{jm,j-m}^{J0}|^2 = 1$.

In this case, with the identification $|x_1, x_2\rangle \mapsto |j\,l\rangle$, Eq. (61) becomes

$$f_J(l,g) = \frac{1}{2J+1}(-1)^{2j+m+l} C_{jm,j-m}^{J0} C_{jl,j-l}^{J0} \times \langle J0\,|\lambda_J(g)^\dagger|\,J0\rangle\,, \tag{87}$$

or, equivalently, it can be expressed as (Cf. Eq. (63))

$$\begin{aligned} f_J(l,g) &= \frac{(-1)^{2j+m}}{2J+1} C_{jm,j-m}^{J0} \sum_{m'=-j}^{j} (-1)^{m'} C_{jm',j-m'}^{J0} \\ &\quad \times \langle jm', j-m'\,|(\tau_n^2 \otimes \bar{\tau}_n^2)(g)^\dagger|\,x_1, x_2\rangle \\ &= \frac{(-1)^{2j+m}}{2J+1} C_{jm,j-m}^{J0} \sum_{m'=-j}^{j} (-1)^{m'} C_{jm',j-m'}^{J0} \\ &\quad \times |\langle x_1, x_2\,|\tau_n^2(g)|\,n_1', n_2'\rangle|^2 \\ &= \frac{(-1)^{2j+m}}{2J+1} \frac{1}{x_1!x_2!} C_{jm,j-m}^{J0} \sum_{m'=-j}^{j} \frac{(-1)^{m'}}{n_1'!n_2'!} \\ &\quad \times C_{jm',j-m'}^{J0} |\mathrm{Per}(\tau_n^2(g)_{(n_1',n_2'),(x_1,x_2)})|^2\,, \end{aligned} \tag{88}$$

where we set $|jm'\rangle = |n_1', n_2'\rangle$ by the inverse Jordan-Schwinger map.

The second moment expression also simplifies significantly. First, notice that, for a given representation

$\lambda_J \otimes \lambda_J$, each λ_K, with $K \in \{0, \dots, 2J\}$, is multiplicity free as all such irreps are clearly maximally symmetric. This implies the decomposition of $\lambda_J^{\otimes 2}$ is formally the same as the one of $\tau_n^2 \otimes \bar{\tau}_n^2$, i.e.

$$\underbrace{\square\cdots\square}_{k} = 1 \oplus \square\square \oplus \square\square\square\square \oplus \cdots \oplus \underbrace{\square\cdots\square}_{2k} \tag{89}$$

and the second moment expression of Theorem 12 simplifies to

$$\begin{aligned}\mathbb{E}[f_J^2] = {} & \frac{1}{s_J^2}(-1)^{2j}|C^{J0}_{jm,j-m}|^2 \sum_{l=-j}^{j}(-1)^{m+l}|C^{L}_{jl,j-l}|^2 \\ & \times \sum_{L=0}^{2\min(J,j)} \frac{1}{2L+1} C^{J0}_{jl,j-l} C^{L0}_{jm,j-m} |C^{L0}_{J0,J0}|^2 \,.\end{aligned} \tag{90}$$

5 Conclusions

Bosonic passive RB is the first RB protocol for the certification of bosonic passive transformations, built on top of general guarantees for filtered RB [1]. Compared to discrete versions of RB, where the defining representation typically determines the reference representation, in passive RB, a broader family of representations, which can be related to the choice of initial state and measurement, is available. This situation complicates the analysis since it made a careful choice of the reference representation necessary.

We analyzed the most common experimental settings for CV systems and argued Gaussian probe states and measurements add additional challenges: First, filtering onto infinitely many irreps appearing in the decomposition of the reference representation would be necessary. They generally present mixed symmetries lacking a clear physical interpretation making it hard to truncate the decomposition with regularization arguments. Also, from a more practical perspective, such irreps are not multiplicity-free, affecting the numerical stability of the post-processing [49]. Moreover, in contrast with RB for discrete variable systems, in CV systems, the choice of the input state influences the RB signal since each number subspace is the carrier space of a non-trivial irrep. We believe Gaussian input states pose additional challenges to RB experiments due to exponentially small overlaps with the number subspaces.

We then identified a well-behaved setting for passive RB with Fock basis states as initial states, ensuring the reference representation decomposes into finitely many multiplicity-free irreps. This allowed a certain degree of freedom in the measurement settings, and we considered the common cases of PNR, or balanced heterodyne detectors. For this setting, we derived explicit formulas needed for the post-processing of the experimental data. Moreover, we analyzed the sampling complexity of the protocol by deriving and bounding the variance of our estimators. Unfortunately, these bounds are quite loose and we expect a much smaller variance in practice.

On the technical side, our analytical results required the Clebsch-Gordan decomposition of ω_n^m, which, for general irreps of $\mathrm{SU}(m)$, is very known to pose significant challenges compared to the standard scenario of $\mathrm{SU}(2)$ [79, 86, 98–100], as irreps with mixed symmetries may appear. However, we found the maximally symmetric irreps are 'regular enough' to carry over a full analysis of the estimators and the sample complexity, as we derived analytical expressions for the frame operators for the POVMs associated with PNR and balanced heterodyne measurements.

A very natural question that arises is whether the passive RB protocol can be extended to active transformations. In this case, many technical difficulties prevent this generalization of filtered RB, as the latter is specifically designed for compact groups, while $\mathrm{Sp}(2m, \mathbb{R})$ (which correspond to the full group of Gaussian transformations) is non-compact (which in turns pose the interesting question of whether a non-compact filtered RB protocol can be formulated). Hence, it is still unclear how to design a meaningful RB protocol for active transformations, as isolating the contributions from different irreps is more challenging.

Finally, we note an analysis of the behavior of passive RB in the presence of *photon distinguishability* is still an open problem, which we believe can be tackled by suitable extensions of the filtered RB framework. However, we leave such problem for future work.

6 Acknowledgements

We would like to thank Ingo Roth, Jonas Helsen, René Sondenheimer, Jan von Delft, Francesco Di Colandrea, and Mattia Walschaers for helpful discussions. This work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – grant numbers 441423094 and 547595784, and by the Fujitsu Services GmbH and the Dataport GmbH as part of the endowed professorship "Quantum Inspired and Quantum Optimization." MH thanks QuSoft and Centrum Wiskunde & Informatica, where part of the research has been conducted.

References

[1] M. Heinrich, M. Kliesch, and I. Roth, *Randomized benchmarking with random quantum circuits* (2023), presented at QIP 2023 as a talk, arxiv:2212.06181 [quant-ph].

[2] E. Knill, R. Laflamme, and G. J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature **409**, 46 (2001).

[3] M. Koashi, T. Yamamoto, and N. Imoto, *Probabilistic manipulation of entangled photons*, Phys. Rev. A **63**, 030301 (2001).

[4] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Linear optical quantum computing with photonic qubits*, Rev. Mod. Phys. **79**, 135 (2007).

[5] T. Rudolph, *Why I am optimistic about the silicon-photonic route to quantum computing*, arXiv:1607.08535 [quant-ph] (2016).

[6] S.-H. Tan and P. P. Rohde, *The resurgence of the linear optics quantum interferometer — recent advances & applications*, Reviews in Physics **4**, 100030 (2019).

[7] K. Alexander et al., *A manufacturable platform for photonic quantum computing*, arxiv:2404.17570 [physics, physics:quant-ph] (2024).

[8] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, *Silica-on-Silicon Waveguide Quantum Circuits*, Science **320**, 646 (2008).

[9] Sprengers et al., *Waveguide superconducting single-photon detectors for integrated quantum photonic circuits*, Applied Physics Letters **99**, 181110 (2011).

[10] Silverstone et al., *On-chip quantum interference between silicon photon-pair sources*, Nature Photonics **8**, 104 (2014).

[11] T. Meany, M. Gräfe, R. Heilmann, A. Perez-Leija, S. Gross, M. J. Steel, M. J. Withford, and A. Szameit, *Laser written circuits for quantum photonics*, Laser & Photonics Reviews **9**, 363 (2015).

[12] Bourassa et al., *Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer*, Quantum **5**, 392 (2021), arxiv:2010.02905 [quant-ph].

[13] S. Aaronson and A. Arkhipov, *The Computational Complexity of Linear Optics*, arxiv:1011.3245 [quant-ph] (2010).

[14] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, *Gaussian Boson Sampling*, Phys. Rev. Lett. **119**, 170501 (2017), arxiv:1612.01199 [quant-ph].

[15] L. Chakhmakhchyan and N. J. Cerf, *Boson sampling with gaussian measurements*, Physical Review A **96**, 10.1103/physreva.96.032326 (2017).

[16] H.-S. Zhong et al., *Quantum computational advantage using photons*, Science **370**, 1460 (2020).

[17] H.-S. Zhong et al., *Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light*, arxiv:2106.15534 [physics:physics, physics:quant-ph].

[18] L.S. Madsen et al., *Quantum computational advantage with a programmable photonic processor*, Nature **606**, 75 (2022).

[19] M. Kliesch and I. Roth, *Theory of quantum system certification*, PRX Quantum **2**, 010201 (2021), tutorial, arXiv:2010.05925 [quant-ph].

[20] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Quantum certification and benchmarking*, Nat. Rev. Phys. **2**, 382 (2020), arXiv:1910.06343 [quant-ph].

[21] Y.-D. Wu, G. Chiribella, and N. Liu, arxiv:2303.05097 [quant-ph] (2023).

[22] F.A. Mele et al., *Learning quantum states of continuous variable systems*, arxiv:2405.01431 [quant-ph] .

[23] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Complete characterization of a quantum process: The two-bit quantum gate*, Physical Review Letters **78**, 390–393 (1997).

[24] M. Mohseni, A. T. Rezakhani, and D. A. Lidar, *Quantum-process tomography: Resource analysis of different strategies*, Physical Review A **77**, 10.1103/physreva.77.032322 (2008).

[25] A. I. Lvovsky and M. G. Raymer, *Continuous-variable optical quantum-state tomography*, Reviews of Modern Physics **81**, 299–332 (2009).

[26] C. C. López, A. Bendersky, J. P. Paz, and D. G. Cory, *Progress toward scalable tomography of quantum maps using twirling-based methods and information hierarchies*, Phys. Rev. A **81**, 062113 (2010).

[27] C. T. Schmiegelow, A. Bendersky, M. A. Larotonda, and J. P. Paz, *Selective and Efficient Quantum Process Tomography without Ancilla*, Phys. Rev. Lett. **107**, 100502 (2011).

[28] A. Bendersky and J. P. Paz, *Selective and efficient quantum state tomography and its application to quantum process tomography*, Phys. Rev. A **87**, 012122 (2013).

[29] R. Namiki, *Schmidt-number benchmarks for continuous-variable quantum devices*, Phys. Rev. A **93**, 052336 (2016).

[30] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White, *Ancilla-Assisted Quantum Process Tomography*, Phys. Rev. Lett. **90**, 193601 (2003).

[31] G. Bai and G. Chiribella, *Test One to Test Many: A Unified Approach to Quantum Benchmarks*, Phys. Rev. Lett. **120**, 150502 (2018).

[32] K. Sharma and M. M. Wilde, *Characterizing the performance of continuous-variable Gaussian quantum gates*, Phys. Rev. Research **2**, 013126 (2020), arxiv:1810.12335 [quant-ph].

[33] R. Blume-Kohout and P. S. Turner, *The curious nonexistence of gaussian 2-designs*, Communications in Mathematical Physics **326**, 755–771 (2014).

[34] Q. Zhuang, T. Schuster, B. Yoshida, and N. Y. Yao, *Scrambling and Complexity in Phase Space*, Phys. Rev. A **99**, 062334 (2019), arxiv:1902.04076.

[35] J. T. Iosue, K. Sharma, M. J. Gullans, and V. V. Albert, *Continuous-variable quantum state designs: Theory and applications* (2022), arxiv:2211.05127 [math-ph, physics:physics, physics:quant-ph] .

[36] R. M. S. Farias and L. Aolita, *Certification of continuous-variable gates using average channel-fidelity witnesses*, Quantum Sci. Technol. **6**, 035014 (2021), arxiv:1812.01968.

[37] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators*, J. Opt. B **7**, S347 (2005), arXiv:quant-ph/0503243.

[38] B. Lévi, C. C. López, J. Emerson, and D. G. Cory, *Efficient error characterization in quantum information processing*, , arXiv:quant-ph/0608246 [quant-ph].

[39] C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and approximate unitary 2-designs and their application to fidelity estimation*, Phys. Rev. A **80**, 012304 (2009), arXiv:quant-ph/0606161 [quant-ph].

[40] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, *Symmetrized characterization of noisy quantum processes*, Science **317**, 1893 (2007), arXiv:0707.0685 [quant-ph].

[41] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Phys. Rev. A **77**, 012307 (2008), arXiv:0707.0963 [quant-ph].

[42] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and robust randomized benchmarking of quantum processes*, , arXiv:1009.3639 [quant-ph].

[43] E. Magesan, J. M. Gambetta, and J. Emerson, *Characterizing quantum gates via randomized benchmarking*, Phys. Rev. A **85**, 042311 (2012), arXiv:1109.6887.

[44] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout, *What randomized benchmarking actually measures*, arXiv:1702.01853 [quant-ph].

[45] J. J. Wallman, *Randomized benchmarking with gate-dependent noise*, Quantum **2**, 47 (2018), arXiv:1703.09835 [quant-ph].

[46] S. T. Merkel, E. J. Pritchett, and B. H. Fong, *Randomized Benchmarking as Convolution: Fourier Analysis of Gate Dependent Errors*, arxiv:1804.05951 [quant-ph].

[47] R. Harper, I. Hincks, C. Ferrie, S. T. Flammia, and J. J. Wallman, *Statistical analysis of randomized benchmarking*, Phys. Rev. A **99**, 052350 (2019), arXiv:1901.00535 [quant-ph].

[48] J. Helsen, X. Xue, L. M. K. Vandersypen, and S. Wehner, *A new class of efficient randomized benchmarking protocols*, arxiv:1806.02048 [quant-ph].

[49] J. Helsen, I. Roth, E. Onorati, A. Werner, and J. Eisert, *General framework for randomized benchmarking*, PRX Quantum **3**, 020357 (2022).

[50] J. Helsen, M. Ioannou, J. Kitzinger, E. Onorati, A. H. Werner, J. Eisert, and I. Roth, *Shadow estimation of gate-set properties from random sequences*, Nature Communications **14**, 10.1038/s41467-023-39382-9 (2023).

[51] L. Kong, *A framework for randomized benchmarking over compact groups* (2021), arxiv:2111.10357 [quant-ph] .

[52] D. S. França and A.-L. Hashagen, *Approximate Randomized Benchmarking for Finite Groups*, J. Phys. A: Math. Theor. **51**, 395302 (2018), arxiv:1803.03621.

[53] Y. Liu, M. Otten, R. Bassirianjahromi, L. Jiang, and B. Fefferman, *Benchmarking near-term quantum computers via random circuit sampling* (2022), arXiv:2105.05232 [quant-ph].

[54] J. Marshall and N. Anand, *Simulation of quantum optics by coherent state decomposition*, Optica Quantum **1**, 78 (2023).

[55] G. Adesso, S. Ragy, and A. R. Lee, *Continuous variable quantum information: Gaussian states and beyond*, Open Syst. Inf. Dyn. **21**, 1440001 (2014), arxiv:1401.4679
.

[56] Arvind, B. Dutta, N. Mukunda, and R. Simon, *The Real Symplectic Groups in Quantum Mechanics and Optics*, Pramana - J Phys **45**, 471 (1995), arxiv:quant-ph/9509002.

[57] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian states in continuous variable quantum information*, arXiv:quant-ph/0503237 [quant-ph] (2005).

[58] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. **73**, 58 (1994).

[59] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, *Universal linear optics*, Science **349**, 711 (2015).

[60] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, *An Optimal Design for Universal Multiport Interferometers* (2017), arxiv:1603.08788 [physics, physics:quant-ph] .

[61] H. de Guise, O. Di Matteo, and L. L. Sanchez-Soto, *Simple factorization of unitary transformations*, Phys. Rev. A **97**, 022328 (2018), arxiv:1708.00735 [quant-ph].

[62] P. Aniello, C. Lupo, and M. Napolitano, *Exploring Representation Theory of Unitary Groups via Linear Optical Passive Devices*, Open Syst. Inf. Dyn. **13**, 415 (2006).

[63] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, *Experimental Scattershot Boson Sampling*, Science Advances **1**, e1400255 (2015), arxiv:1505.03708 [quant-ph].

[64] G. Folland, *Harmonic analysis in phase space*, Annals of Mathematics Studies No. 122 (Princeton Univ Pr, 1989).

[65] F. Marsili, D. Bitauld, A. Gaggero, S. Jahanmirinejad, R. Leoni, F. Mattioli, and A. Fiore, *Physics and application of photon number resolving detectors based on superconducting parallel nanowires*, New J. Phys. **11**, 045022 (2009).

[66] J. Provazník, L. Lachman, R. Filip, and P. Marek, *Benchmarking photon number resolving detectors*, Opt. Express **28**, 14839 (2020), arxiv:2005.02093 [quant-ph].

[67] U. Chabaud, T. Douce, D. Markham, P. van Loock, E. Kashefi, and G. Ferrini, *Continuous-Variable Sampling from Photon-Added or Photon-Subtracted Squeezed States*, Phys. Rev. A **96**, 062307 (2017), arxiv:1707.09245 [quant-ph].

[68] M. Cooper, L. J. Wright, C. Söller, and B. J. Smith, *Experimental generation of multi-photon Fock states*, Optics Express **21**, 5309 (2013), arxiv:1212.4412 [quant-ph].

[69] A. I. Lvovsky, P. Grangier, A. Ourjoumtsev, V. Parigi, M. Sasaki, and R. Tualle-Brouri, *Production and applications of non-Gaussian quantum states of light*, arxiv:2006.16985 [physics, physics:quant-ph] (2020).

[70] M. Walschaers, *Non-Gaussian Quantum States and Where to Find Them*, arxiv:2104.12596 [physics, physics:quant-ph] (2021).

[71] D. Hangleiter and J. Eisert, *Computational advantage of quantum random sampling*, Rev. Mod. Phys. **95**, 035001 (2023).

[72] J. E. Bourassa, N. Quesada, I. Tzitrin, A. Száva, T. Isacsson, J. Izaac, K. K. Sabapathy, G. Dauphinais, and I. Dhand, *Fast simulation of bosonic qubits via Gaussian functions in phase space*, PRX Quantum **2**, 10.1103/prxquantum.2.040315 (2021).

[73] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, *Sufficient Conditions for Efficient Classical Simulation of Quantum Optics*, Phys. Rev. X **6**, 021039 (2016).

[74] N. Heurtel, S. Mansfield, J. Senellart, and B. Valiron, *Strong simulation of linear optical processes*, Computer Physics Communications **291**, 108848 (2023).

[75] W. Roga and M. Takeoka, *Classical simulation of boson sampling with sparse output*, Sci Rep **10**, 14739 (2020), arxiv:1904.05494 [quant-ph].

[76] B. Villalonga, M. Y. Niu, L. Li, H. Neven, J. C. Platt, V. N. Smelyanskiy, and S. Boixo, noop *Efficient approximation of experimental Gaussian boson sampling* (2022), arXiv:2109.11525 [quant-ph] .

[77] M. Liu, C. Oh, J. Liu, L. Jiang, and Y. Alexeev, *Complexity of Gaussian boson sampling with tensor networks* (2023), arxiv:2301.12814 [physics, physics:quant-ph] .

[78] S. Sternberg, *Group theory and physics*, Cambridge University Press (1994).

[79] A. Alex, M. Kalus, A. Huckleberry, and J. von Delft, *A numerical algorithm for the explicit calculation of SU(N) and SL*$(n, \mathbb{C})$ *clebsch–gordan coefficients*, Journal of Mathematical Physics **52**, 10.1063/1.3521562 (2011).

[80] A. Alex, *Non-Abelian Symmetries in the Numerical Renormalization Group*, Ph.D. thesis, Ludwig-Maximilians-Universität Münich (2009).

[81] I. Dhand, B. C. Sanders, and H. de Guise, *Algorithms for su(n) boson realizations and d-functions*, Journal of Mathematical Physics **56**, 10.1063/1.4935433 (2015).

[82] S. T. Flammia and J. J. Wallman, *Efficient estimation of Pauli channels*, ACM Transactions on Quantum Computing **1**, 1 (2020), arxiv:1907.12976.

[83] M. Reed and B. Simon, *Functional Analysis*, Methods of Modern Mathematical Physics, Vol. 1 (Academic Press, New York, San Fransisco, London, 1972).

[84] B. C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, Graduate Texts in Mathematics, Vol. 222 (Springer International Publishing, Cham, 2015).

[85] M. Mathur, I. Raychowdhury, and R. Anishetty, *SU(N) irreducible Schwinger bosons*, Journal of Mathematical Physics **51**, 10.1063/1.3464267 (2010).

[86] M. Mathur, I. Raychowdhury, and T. P. Sreeraj, *Invariants, projection operators and SU(N)×SU(N) irreducible Schwinger bosons*, Journal of Mathematical Physics **52**, 10.1063/1.3660195 (2011).

[87] S. Scheel, *Permanents in linear optical networks* (2004), arxiv:quant-ph/0406127 .

[88] R. Kruse, C. S. Hamilton, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, *Detailed study of Gaussian boson sampling*, Phys. Rev. A **100**, 032326 (2019).

[89] N. Vilenkin and A. Klimyk, *Representation of Lie Groups and Special Functions*, Vol. 1: Simplest Lie Groups, Special Functions and Integral Transforms (Springer, 1993) part of the book series: Mathematics and its Applications.

[90] N. Vilenkin and A. Klimyk, *Representation of Lie Groups and Special Functions*, Vol. 2: Class I Representations, Special Functions, and Integral Transforms (Springer, 1993) part of the book series: Mathematics and its Applications.

[91] G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, *Informationally complete measurements and groups representation*, J. Opt. B: Quantum Semiclass. Opt. **6**, S487 (2004), arxiv:quant-ph/0310013.

[92] A. Alex, L. Everding, P. Littelmann, and J. von Delft, *SU(N) Clebsch-Gordan coefficients and non-Abelian symmetries*, in *APS March Meeting Abstracts*, Vol. 2012 (2012) pp. W26–011.

[93] G. B. Folland, *A Course in Abstract Harmonic Analysis*, 2nd ed. (Chapman and Hall/CRC, New York, 2015).

[94] G. B. Folland, *Harmonic Analysis in Phase Space. (AM-122)* (Princeton University Press, 1989).

[95] R. M. Delaney and B. Gruber, *Inner and Restriction Multiplicity for Classical Groups*, Journal of Mathematical Physics **10**, 252 (1969).

[96] B. Gruber, *Relations between "Inner" and "Outer" multiplicities for the classical groups*, .

[97] J. R. Schmidt, *A unified treatment of SU(N) inner and outer multiplicities*, Journal of Mathematical Physics **27**, 451 (1986).

[98] L. C. Biedenharn, *On the Representations of the Semisimple Lie Groups. I. The Explicit Construction of Invariants for the Unimodular Unitary Group in N Dimensions*, Journal of Mathematical Physics **4**, 436 (2004).

[99] G. E. Baird and L. C. Biedenharn, *On the Representations of the Semisimple Lie Groups. II*, Journal of Mathematical Physics **4**, 1449 (2004).

[100] G. E. Baird and L. C. Biedenharn, *On the representations of the semisimple lie groups. iii. the explicit conjugation operation for SUn*, Journal of Mathematical Physics **5**, 1723 (1964).

[101] W. Fulton, *Young Tableaux: With Applications to Representation Theory and Geometry*, London Mathematical Society Student Texts (Cambridge University Press, Cambridge, 1996).

[102] P. Di Francesco, P. Mathieu, and D. Sénéchal, *Conformal Field Theory*, Graduate Texts in Contemporary Physics (Springer, New York, NY, 1997).

[103] J. F. Cornwell, *Group Theory in Physics*, Vol. 1 (Academic Press, 1984).

[104] J. F. Cornwell, *Group Theory in Physics*, Vol. 2 (Academic Press, 1984).

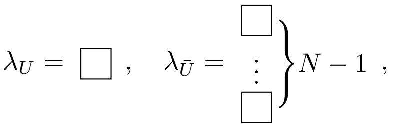
A Littlewood-Richardson's rules

In this section, summarize Littlewood-Richardson's rules for the decomposition into irreps of the tensor product of two irreps of $\mathrm{SU}(m)$. For more details, see for instance [78, Sec. C.3]. In particular, let us consider the unitary irreps $\pi_{\lambda_1}, \pi_{\lambda_2}$ of $\mathrm{SU}(m)$ associated with Young diagrams λ_1, λ_2. Then, the representation

$$\pi_{\lambda_1} \otimes \pi_{\lambda_2} : \mathrm{SU}(m) \ni g \mapsto \pi_{\lambda_1}(g) \otimes \pi_{\lambda_2}(g) \in \mathrm{U}(\mathcal{H}_{\lambda_1} \otimes \mathcal{H}_{\lambda_2}) \tag{91}$$

is in general reducible (in particular, it is completely reducible, since $\mathrm{SU}(m)$ is compact).

For instance, in standard RB [1], one is interested in the irrep $U \otimes \bar{U}$, where $U : \mathrm{SU}(m) \to \mathrm{U}(m)$ is the defining representation and $\bar{U}$ its dual. Diagrammatically, they correspond to

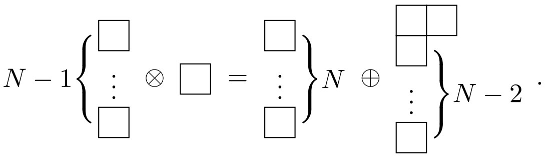


(92)

It is well known that

$$U \otimes \bar{U} = 1 \oplus \mathrm{Ad}, \tag{93}$$

where 1 denotes the trivial irrep and $\mathrm{Ad} : \mathrm{SU}(D) \ni g \mapsto \mathrm{Ad}_g \in \mathrm{Aut}(\mathfrak{su}(D))$ is the adjoint representation. Roughly speaking, the decomposition is achieved by combining the two Young diagrams in all possible ways, and summing up the results. In this case, there are only two possibilities that realize legal Young diagrams: λ_U can be attached on the right of the top row of $\lambda_{\bar{U}}$, or on the bottom of the column, i.e.



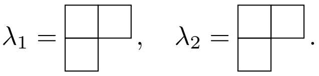
(94)

The first diagram on the r.h.s. is equivalent to the diagram with no boxes associated with the trivial irrep, while the second Young diagram identifies the adjoint representation acting on traceless matrices.

In general, *Littlewood-Richardson's rules* can be used to decompose the tensor product of two arbitrary irreps [78, 101, 102]. To spell out such rules, let us consider two Young diagrams λ_1, λ_2 associated with irreps of $\mathrm{SU}(m)$. The tensor product representation $\lambda_1 \otimes \lambda_2$ can be evaluated algorithmically as follows [102, Sec. 13.5.3] (or also [78, Sec. C.3]):

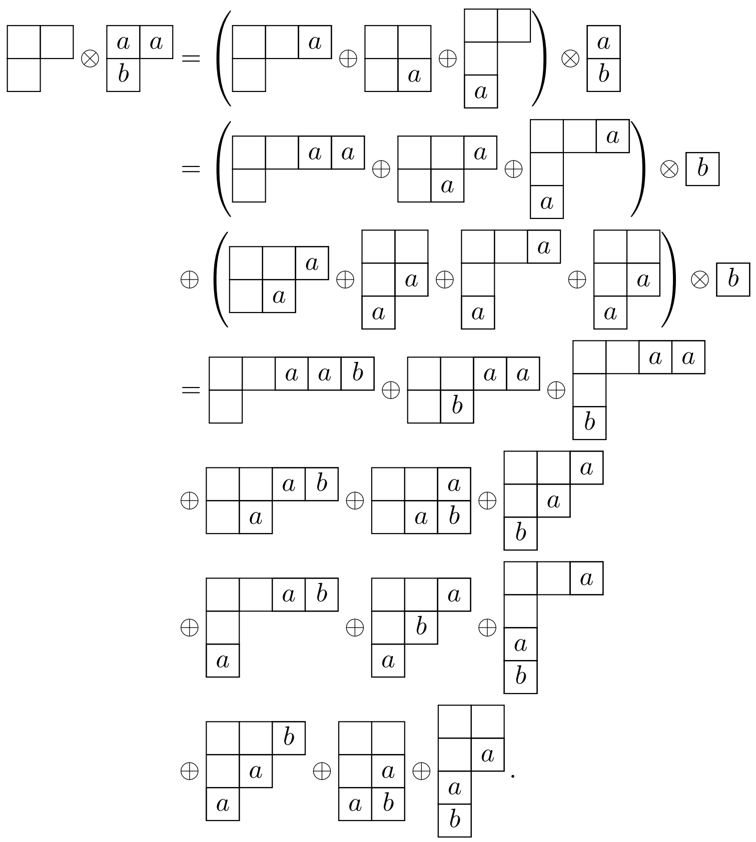
1. Assign distinct labels to boxes in each row of the Young diagram λ_2. For instance, the boxes in the first row will be labeled by 'a', the boxes in the second row by 'b' and so on.
2. Attach boxes labeled by a to λ_1 in all possible ways such that no two a's appear in the same column, and the result is still a proper Young diagram.
3. Repeat the steps above for all rows of λ_2.
4. Elimination rule: For each box, assign numbers n_a = number of a's above and right to it, n_b = number of b's above and right to it, and so on. If, at any point, the relations $n_a \geq n_b \geq n_c \geq n_d \geq \dots$ are not satisfied, discard this diagram.
5. Merging rule. If two diagrams are the same, then they are counted as the same if the labels are the same. Otherwise, they refer to distinct irreps.
6. Cancel columns with m boxes (since they correspond to constant shifts of the highest weight vector).
7. Remove all the labels after the cancellation and the merging steps.

Example 13. Let us consider the following diagrams:



(95)

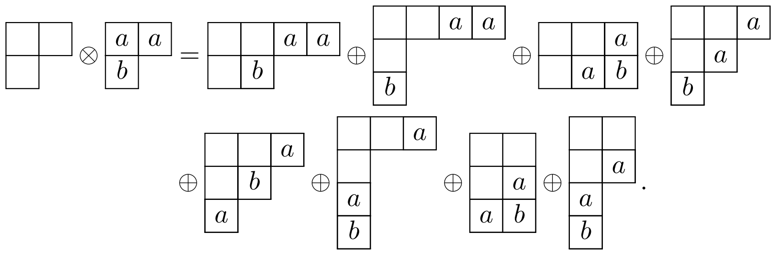
Assigning labels to λ_2 as in rule 1, and using the second and third rules, we get



(96)

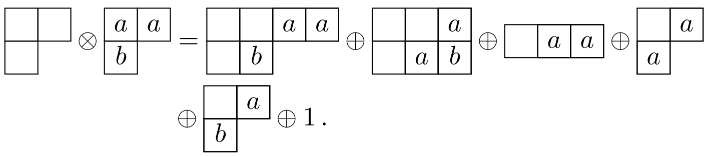
In the second step we got few equivalent diagrams with labels in the same positions, hence they have been merged according to the merging rule. Moreover, we ignored the diagrams with two a's in the same column, in agreement with the symmetric constraint.

By the elimination rule, all the diagrams with a b box attached on the top right shall be eliminated, yielding the following decomposition:

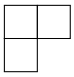


(97)

Finally, suppose for instance that these diagrams are associated with SU(3) irreps. Then, all columns with three boxes can be omitted, while any diagram with more than 3 boxes in a column is not allowed. This yields the following decomposition:



(98)

In the latter, notice that the diagram  appears with multiplicity 2 in the decomposition, as different labels are assigned to the two copies.

In the high energy literature [102], this decomposition is also written in terms of the dimension of the irrep associated with each Young diagram as

$$\mathbf{8}\otimes\bar{\mathbf{8}} = \mathbf{27}\oplus\mathbf{10}\oplus\mathbf{10}'\oplus\mathbf{8}\oplus\mathbf{8}\oplus\mathbf{1}\,. \qquad (99)$$

Here, **10**, **10′** indicates that the two irreps are inequivalent, while repeated dimensions denote the same irrep appear with a non-trivial multiplicity.

B Proof of Lemma 4

Lemma 14 (restatement of Lemma 4)**.** *Let $\tau_n^m : \mathrm{SU}(m) \to \mathrm{U}(\mathcal{H}_n^m)$ be the irreducible representation of $\mathrm{SU}(m)$ on the space of n bosons distributed over m modes as in Eq. (27). Define the Young diagram*

$$\lambda_k \equiv \quad m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{k}\overbrace{\square\cdots\square}^{k} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. , \tag{100}$$

where λ_0 and λ_1 denote the trivial irrep and the adjoint irrep of $\mathrm{SU}(m)$, respectively. Then, for any $n, m \in \mathbb{N} \setminus \{0\}$,

$$\omega_n^M = \bigoplus_{k=0}^{n} \lambda_k \, , \tag{101}$$

where each λ_k, $k = 0, \dots, n$, appears exactly one time.

Proof. We will prove the following equivalent fact by induction:

$$\omega_n^M = \lambda_n \oplus \omega_{n-1}^m \, , \quad \forall n \in \mathbb{N} \setminus \{0\} \, . \tag{102}$$

First, notice that

$$\omega_1^m = \quad m-1\left\{\begin{array}{l} \square\boxed{a} \\ \vdots \\ \square \end{array}\right. \oplus \mathbf{1} \equiv \lambda_1 \oplus \omega_0^m \, , \tag{103}$$

as $\omega_0^m = \mathbf{1}$ trivially.

The conjugate representation is associated with the tensor product of Young diagrams

$$m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{n} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. \otimes \underbrace{\square\cdots\square}_{n} \tag{104}$$

(swapping tensor factors does not influence the result). By Littlewood-Richardson's rules, we first have

$$\begin{aligned} m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{n} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. \otimes \overbrace{\boxed{a}\cdots\boxed{a}}^{n} &= \quad m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{n}\boxed{a} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. \otimes \overbrace{\boxed{a}\cdots\boxed{a}}^{n-1} \\ &\oplus \quad m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{n-1} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. \otimes \overbrace{\boxed{a}\cdots\boxed{a}}^{n-1} \, . \end{aligned} \tag{105}$$

Notice that the second term in the r.h.s. is by definition ω_{n-1}^m. Hence, we shall only prove that

$$m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{n}\boxed{a} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. \otimes \overbrace{\boxed{a}\cdots\boxed{a}}^{n-1} = \oplus_{k=0}^{n} \lambda_k \, . \tag{106}$$

For this purpose, let us consider the factor

$$\tilde{\lambda}_r^{(s)} := \quad m-1\left\{\begin{array}{l} \overbrace{\square\cdots\square}^{r}\overbrace{\boxed{a}\cdots\boxed{a}}^{s} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. . \tag{107}$$

Clearly, $\tilde{\lambda}_r^{(r)} = \lambda_r$ and $\tilde{\lambda}_0^{(0)} = \mathbf{1}$. Notice that

$$\begin{aligned}
\tilde{\lambda}_r^{(s)} \otimes \tau_l^m &= \left(m-1 \left\{ \begin{array}{l} \overbrace{\square \cdots \square}^{r}\overbrace{\boxed{a} \cdots \boxed{a}}^{s+1} \\ \vdots \ \ \ddots \ \ \vdots \\ \square \cdots \square \end{array} \right. \oplus \begin{array}{l} \overbrace{\square \cdots \square}^{r-1}\overbrace{\boxed{a} \cdots \boxed{a}}^{s} \\ \vdots \ \ \ddots \ \ \vdots \\ \square \cdots \square \end{array} \right) \otimes \overbrace{\boxed{a} \cdots \boxed{a}}^{l-1} \\
&= \left(\tilde{\lambda}_r^{(s+1)} \oplus \tilde{\lambda}_{r-1}^{(s)} \right) \otimes \tau_{l-1}^m \,.
\end{aligned} \tag{108}$$

With this notation, expanding the l.h.s. of Eq. (106) we get

$$\begin{aligned}
\tilde{\lambda}_n^{(1)} \otimes \tau_{n-1}^m &= \left(m-1 \left\{ \begin{array}{l} \overbrace{\square \cdots \square}^{n}\boxed{a}\boxed{a} \\ \vdots \ \ \ddots \ \ \vdots \\ \square \cdots \square \end{array} \right. \oplus \begin{array}{l} \overbrace{\square \cdots \square}^{n-1}\boxed{a} \\ \vdots \ \ \ddots \ \ \vdots \\ \square \cdots \square \end{array} \right) \otimes \overbrace{\boxed{a} \cdots \boxed{a}}^{n-2} \\
&= \left(\tilde{\lambda}_n^{(2)} \oplus \tilde{\lambda}_{n-1}^{(1)} \right) \otimes \tau_{n-2}^m \\
&= \left(\tilde{\lambda}_n^{(3)} \oplus \tilde{\lambda}_{n-1}^{(2)} \oplus \tilde{\lambda}_{n-1}^{(2)} \oplus \tilde{\lambda}_{n-2}^{(1)} \right) \otimes \tau_{n-3}^m \\
&= \left(\tilde{\lambda}_n^{(3)} \oplus \tilde{\lambda}_{n-1}^{(2)} \oplus \tilde{\lambda}_{n-2}^{(1)} \right) \otimes \tau_{n-3}^m \\
&\ \ \vdots \\
&= \left(\tilde{\lambda}_n^{(i)} \oplus \tilde{\lambda}_{n-1}^{(i-1)} \oplus \cdots \oplus \tilde{\lambda}_{n-i+1}^{(1)} \right) \otimes \tau_{n-i}^m \\
&\ \ \vdots \\
&= \bigoplus_{i=0}^{n} \tilde{\lambda}_{n-i}^{(n-i)} \\
&= \bigoplus_{k=0}^{n} \lambda_k \,.
\end{aligned} \tag{109}$$

In the latter, we used the merging rule for Young diagrams, see Appendix A.

Therefore, we have

$$\begin{aligned}
\omega_n^M &= \sum_{k=0}^{n} \lambda_k \oplus \omega_{n-1}^m = \sum_{k=0}^{n} \lambda_k \oplus \sum_{l=0}^{n-1} \lambda_l \\
&= \lambda_n \oplus \omega_{n-1}^m \,,
\end{aligned} \tag{110}$$

where we used the merging rule again. □

C Proof of Proposition 5

For convenience, we state again the proposition:

Proposition 15 (restatement of Proposition 5)**.** *For any $k \in \mathbb{N}$, the following holds:*

$$\dim \lambda_k = \left(1 - \frac{k^2}{(k+m-1)^2} \right) \left(\dim \mathcal{H}_k^m \right)^2 \,. \tag{111}$$

Proof. For any irrep $\lambda = (m_1, m_2, \ldots, m_m)$, the following fact holds: [79]

$$\dim \lambda = \prod_{1 \le j < j' \le m} \left(1 + \frac{m_j - m_{j'}}{j' - j} \right) \,. \tag{112}$$

Let us denote the irrep defined in Eq. (47) as $\lambda_k = (2k, k, \ldots, k, 0)$. Hence, notice the following facts:

- For $j = 1$ and $j' = 2, \ldots, m-1$ we obtain the contribution $\prod_{j'=2}^{m-1} \left(1 + \frac{k}{j'-1} \right)$.

- For $j = 1$ and $j' = m$ we obtain the contribution $1 + \frac{2k}{m-1}$.
- For $2 \le j < j' \le m-1$ all the products are equal to 1.
- For $2 \le j \le m-1$ and $j' = m$ we obtain the contribution $\prod_{j=2}^{m-1}\left(1 + \frac{k}{m-j}\right)$.

Using the latter facts, we have

$$\dim \lambda_k = \frac{2k+m-1}{m-1} \prod_{j=2}^{m-1} \frac{k+m-j}{m-j} \prod_{l=2}^{m-1} \frac{k+l-1}{l-1} = \frac{2k+m-1}{m-1} \left(\frac{1}{(M-2)!}\right)^2 \prod_{j=2}^{m-1}(k+m-j) \prod_{l=2}^{m-1}(k+l-1) \tag{113}$$

$$= \frac{2k+m-1}{m-1} \left(\frac{1}{(M-2)!}\right)^2 \left(\frac{1}{k}(k)_{m-1}\right)^2 = \frac{1}{k^2} \frac{2k+m-1}{m-1} \left(\frac{(k)_{m-1}}{(m-2)!}\right)^2 \tag{114}$$

$$= \frac{1}{k^2} \frac{2k+m-1}{m-1} (m-1)^2 \left(\frac{(k)_{m-1}}{(m-1)!}\right)^2 = \frac{(2k+m-1)(m-1)}{k^2} \left(\frac{(k+m-1)!}{k!(m-1)!} \frac{k}{k+m-1}\right)^2 \tag{115}$$

$$= \frac{(2k+m-1)(m-1)}{k^2} \frac{k^2(m-1)}{(k+m-1)^2} \binom{k+m-1}{m-1}^2 = \frac{(2k+m-1)(m-1)}{(k+m-1)^2} \binom{k+m-1}{m-1}^2 \tag{116}$$

$$= \left(1 - \frac{k^2}{(k+m-1)^2}\right) \left(\dim \mathcal{H}_k^m\right)^2 , \tag{117}$$

In Eq. (113) we factorized the denominators and observed that the factors range between 1 and $m-2$. In Eq. (114) we introduced the Pochhammer raising factorial symbol, defined as $(a)_k := a(a+1)\dots(a+k-1)$ for $a, k \in \mathbb{N}$. In Eq. (115) we recognized that, by definition,

$$\frac{(k)_{m-1}}{(m-2)!} = \binom{k+m-2}{m-1} = \frac{(k+m-2)!}{(k-1)!(m-1)!} \cdot \frac{k}{k} . \tag{118}$$

Finally, rearranging the terms and by symmetry of the binomial coefficient, the assertion followed. □

D Proof of Eq. 56

In this section, for convenience, we will say that a box in a Young tableau is a k-box if it is labeled by $k \in [m]$. Let $\mathrm{SSYT}(\lambda_k)$ be the set of semi-standard Young tableaux of shape λ_k and consider the set

$$\mathrm{SSYT}^{(\mathbf{0})}(\lambda_k) := \{T \mid T \in \mathrm{SSYT}(\lambda_k) \text{ s.t. } w_i^T = w_{i+1}^T \, \forall i \in [m-1]\} . \tag{119}$$

It follows that $\gamma_{\lambda_k}(\mathbf{0}) = |\mathrm{SSYT}^{(\mathbf{0})}(\lambda_k)|$ is the inner multiplicity of $\mathbf{0}$ in λ_k.

Clearly, $\gamma(w) = 1$ for each weight w in SU(2), and Eq. (56) holds trivially.

In a similar fashion, counting Young tableaux T_{λ_k} for SU(3) is straightforward: any Young tableau $T \in \mathrm{SSYT}^{(\mathbf{0})}(\lambda_k)$ contains the labels $\{1, 2, 3\}$ exactly k times, with the 1's forced to be placed in the first k boxes of the first row, otherwise T would not be a legal tableau. Then, if we consider a starting Young tableau of the form

$$\begin{array}{cccccc}
\multicolumn{3}{c}{\overbrace{\qquad\qquad}^{k}} & \multicolumn{3}{c}{\overbrace{\qquad\qquad}^{k}} \\
\boxed{1} & \cdots & \boxed{1} & \boxed{2} & \cdots & \boxed{2} \\
\boxed{3} & \cdots & \boxed{3} & & &
\end{array} \tag{120}$$

all remaining $T \in \mathrm{SSYT}^{(\mathbf{0})}(\lambda_l)$ can be obtained by permuting the last 2-box in the first row with the first 3-box in the second row. The total number of allowed swaps is k, which implies $\gamma_{\lambda_k}(\mathbf{0}) = k+1$.

Consider now $m > 3$ and suppose Eq. (56) holds for $k-1, m-1$. As in the previous case, the 1-boxes are fixed to be placed at the beginning of the first row. Suppose the m-boxes are all placed in the $m-1$-th row, i.e. we consider

$$\begin{array}{cccccc}
\multicolumn{3}{c}{\overbrace{\qquad\qquad}^{k}} & \multicolumn{3}{c}{\overbrace{\qquad\qquad}^{k}} \\
\boxed{1} & \cdots & \boxed{1} & \boxed{2} & \cdots & \boxed{2} \\
\vdots & \ddots & \vdots & & & \\
\boxed{m} & \ddots & \boxed{m} & & &
\end{array} . \tag{121}$$

As long as the last row is fixed to contain m-boxes only, the total number of such Young tableaux is $\binom{k+m-3}{k}$. Then, we only have to count the remaining allowed configurations of k-boxes. For this purpose, observe that the remaining allowed positions for m-boxes are only in the first row, and there are k such configurations. Hence, it is enough to count all possible configurations for each placement of m-boxes in the first row, which is given by

$$\binom{k-l+m-2}{k-l}, \tag{122}$$

where l is the number of free boxes in the first row of the tableau. Therefore, the total number of such configurations is

$$\begin{aligned}\sum_{l=1}^{k}\binom{(k-l)+m-2}{k-l} &= \sum_{j=0}^{k-1}\binom{j+m-2}{j} = \sum_{j=0}^{k-1}\binom{j+m-2}{m-2} \\ &= \binom{k+m-3}{k-1},\end{aligned} \tag{123}$$

where we used Fermat's identity

$$\sum_{j=0}^{n}\binom{j+a}{j} = \binom{a+n+1}{n}. \tag{124}$$

Therefore, by Pascal's identity, we have

$$\gamma_{\lambda_k}(\mathbf{0}) = \binom{k+m-3}{k} + \binom{k+m-3}{k-1} = \binom{k+m-2}{k}, \tag{125}$$

from which the assertion follows.

E Proof of Lemma 10

Lemma 16 (Restatement of Lemma 10)**.** *For a PNR measurement setting, $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ as input state, and an irrep λ_k of $\omega^{(n)} = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$, the following holds:*

$$\mathbb{E}[f_\lambda] = \sum_{M\in\mathrm{GT}(\lambda_k)} |C^M_{N,\bar{N}}|^2, \tag{126}$$

where N is the GT pattern associated with $\boldsymbol{n}$, and $\bar{N}$ is its dual.

Proof. Since ρ is an n-particle state and ω_n^m is a passive transformation, the outcome of a PNR measurement must also be an n-particle Fock state. Hence, we have

$$\mathbb{E}[f_{\lambda_k}] := \frac{1}{s_{\lambda_k}}\sum_{\boldsymbol{x}\in\mathcal{H}_n^m}\int dg\,\langle \boldsymbol{n},\boldsymbol{n}\,|P_{\lambda_k}(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger\,|\boldsymbol{x},\boldsymbol{x}\rangle\langle\boldsymbol{x},\boldsymbol{x}\,|(\tau_n^m\otimes\bar{\tau}_n^m)(g)\,|\boldsymbol{n},\boldsymbol{n}\rangle \tag{127}$$

$$= \frac{1}{s_{\lambda_k}}\sum_{X\in\mathrm{GT}(\tau_n^m)}\int dg\,\langle N,\bar{N}\,|P_\lambda(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger\,|X,\bar{X}\rangle\langle X,\bar{X}\,|(\tau_n^m\otimes\bar{\tau}_n^m)(g)\,|N,\bar{N}\rangle \tag{128}$$

$$= \frac{1}{s_{\lambda_k}}\sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}}\sum_{X\in\mathrm{GT}(\tau_n^m)}\int dg\,\langle M\,|\lambda_k(g)^\dagger\,|X,\bar{X}\rangle\langle X,\bar{X}\,|\bigoplus_{j=0}^{n}\lambda_j(g)\,|N,\bar{N}\rangle\,. \tag{129}$$

The second line follows since the relative phases between $|M\rangle$ and $|\bar{M}\rangle$ highlighted in Eq. (24) are integers, and they appear an even number of times. In the third step, projected $|N,\bar{N}\rangle$ onto its λ_k-th component, Cf. Eq. (54). Accordingly, the only non-trivial contribution to the integral is determined by the λ_k-th component of $\tau_n^m\otimes\bar{\tau}_n^m$. Similarly, by orthogonality relations, the integral is non-zero only if $\lambda_j = \lambda_k$. Hence, it is enough to consider the restricted Clebsch-Gordan decomposition to the λ_k-th irrep, and the following holds:

$$\mathbb{E}[f_{\lambda_k}] = \frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{X\in\mathrm{GT}(\tau^m_n)} \int dg \, \langle M \,|\lambda_k(g)^\dagger|\, X,\bar{X}\rangle\langle X,\bar{X}\,|\lambda_k(g)|\,N,\bar{N}\rangle \tag{130}$$

$$= \frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{X\in\mathrm{GT}(\tau^m_n)} \sum_{M_1,M_2,M_3\in\mathrm{GT}(\lambda_k)} C^{M_1}_{X,\bar{X}} C^{M_2}_{X,\bar{X}} C^{M_3}_{N,\bar{N}} \tag{131}$$

$$\times \underbrace{\int dg\, \langle M\,|\lambda_k(g)^\dagger|\,M_1\rangle\langle M_2\,|\lambda_k(g)|\,M_3\rangle}_{=\frac{1}{\dim\lambda_k}\delta_{M,M_3}\delta_{M_1,M_2}} \tag{132}$$

$$= \frac{1}{\dim\lambda_k}\frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} |C^M_{N,\bar{N}}|^2 \sum_{X\in\mathrm{GT}(\tau^m_n)} \sum_{M_1\in\mathrm{GT}(\lambda_k)} |C^{M_1}_{X,\bar{X}}|^2 \tag{133}$$

$$= \sum_{M\in\mathrm{GT}(\lambda_k)} |C^M_{N,\bar{N}}|^2 . \tag{134}$$

In the second step, we expanded $|X,\bar{N}\rangle, |N,\bar{N}\rangle$ in the coupled basis, and restricted the decompositions to the λ_k-th components. In the third step, we used Schur's orthogonality relations to compute the integral, and in the final step we used the definition of the frame operator, and in particular the result in Lemma 8. □

F Proof of Lemma 11

Lemma 17 (Restatement of Lemma 11)**.** *Let λ_k be a Young diagram as in Eq. (47). Then, we have*

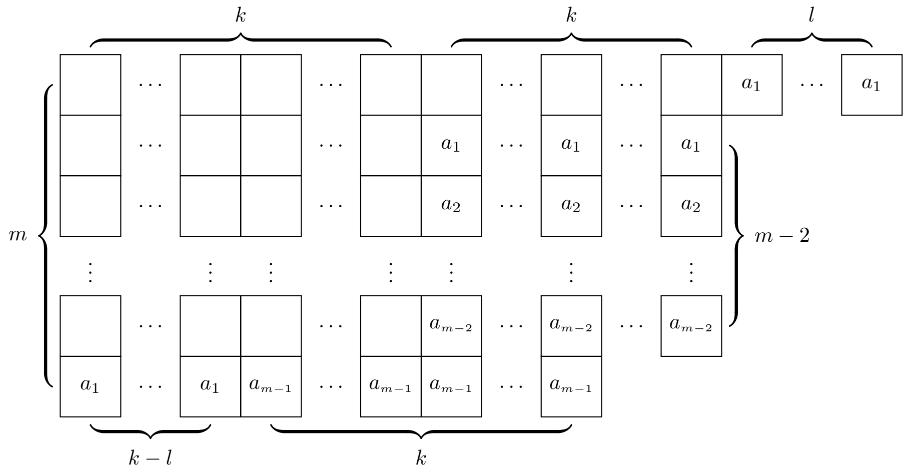
$$\lambda_k \otimes \lambda_k = \bigoplus_{l=0}^{k} \lambda_l^{l+1} \oplus \bigoplus_{l=k+1}^{2k} \lambda_l^{2k-l+1} \oplus L\,, \tag{135}$$

where $\lambda_0 \equiv \mathbf{1}$, $\lambda_1 \equiv \mathrm{Ad}$ as usual, and L is a suitable direct sum of Young diagrams which are not of the form λ_l for any $l \in \mathbb{N}$.

Proof. Consider for any $k \in \mathbb{N}$ the tensor product

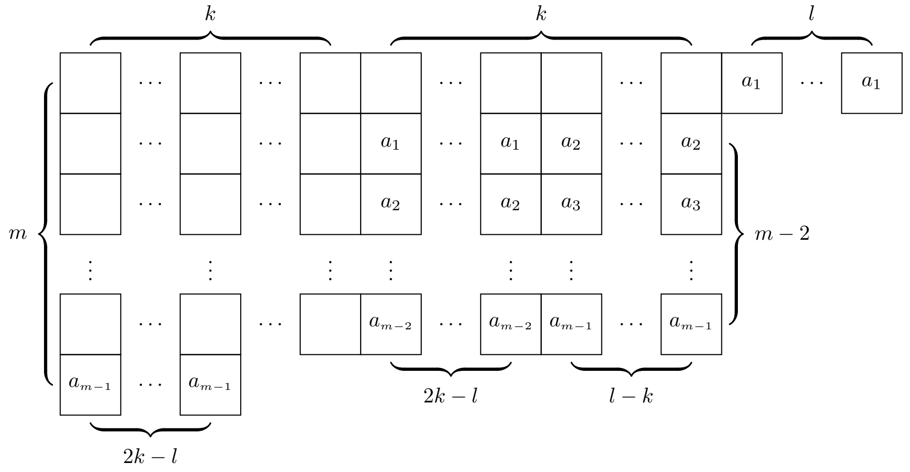
$$\lambda_k \otimes \lambda_k = \begin{array}{cccccc} \boxed{} & \cdots & \boxed{} & \boxed{} & \cdots & \boxed{} \\ \boxed{} & \cdots & \boxed{} & & & \\ \vdots & \cdots & \vdots & & & \\ \boxed{} & \cdots & \boxed{} & & & \end{array} \otimes \begin{array}{cccccc} \boxed{a_1} & \cdots & \boxed{a_1} & \boxed{a_1} & \cdots & \boxed{a_1} \\ \boxed{a_2} & \cdots & \boxed{a_2} & & & \\ \vdots & \cdots & \vdots & & & \\ \boxed{a_{m-1}} & \cdots & \boxed{a_{m-1}} & & & \end{array} . \tag{136}$$

By Littlewood-Richardson's rules, the number of Young diagrams λ_l that can be constructed from $\lambda_k^{\otimes 2}$ is determined by all possible allowed configurations we can attach the a_1 boxes to the first λ_k, since the way the remaining a_i boxes, $i = 2, \dots, m-1$, are attached must follow accordingly. First, notice that only the a_1 boxes can be attached to the first row of the first copy of λ_k due to the elimination rule. Hence, we have two different 'generating' Young diagrams conditioned by whether $l \le k$ or $k+1 \le l \le 2k$. Suppose $l \le k$ at first. The a_1 boxes are attached to the first copy of λ_k as follows: The first l boxes are attached to the first row, the next k boxes are attached to the second row and the remaining $k-l$ boxes are attached to the m-th row. Then, all the a_i boxes, for any $i = 2, 3, \dots, m-2$ are attached to the $i+1$-th row. Finally, the a_{m-1} boxes are attached to the m-th row. The resulting Young diagram is given by


k
k
l
a₁ ⋯ a₁
a₁ ⋯ a₁ ⋯ a₁
a₂ ⋯ a₂ ⋯ a₂
m
m − 2
a_{m−2} ⋯ a_{m−2} ⋯ a_{m−2}
a₁ ⋯ a₁ a_{m−1} ⋯ a_{m−1} a_{m−1} ⋯ a_{m−1}
k − l
k

(137)

Suppose now $l \geq k+1$. The a_1 boxes are attached to the first copy of λ_k as follows: The first l boxes are attached to the first row, while the remaining ones are attached to the second row of λ_k. Then, for the a_i boxes, for any $i = 2, 3, \ldots, m-2$, the first $2k-l$ are attached to the i-th row of λ_k, while the remaining ones are attached to the $i+1$-th row of λ_k. The first a_{m-1} boxes are attached to the $m-1$-th row of T_k and the remaining ones will form the m-th row of the diagram. The resulting Young diagram is



(138)

For notation purpose, let us refer to the latter two Young diagrams as the generating Young diagrams.

At this point, we can generate all the remaining copies of λ_l in the following way:

1. For any $i = 1, \ldots, m-2$, replace the last a_i box in the $i+1$-th row with an a_{i+1} box.

2. Replace the first a_{m-1} box in the m-th row of the diagram with a_1.

It follows that the multiplicity of λ_l in the decomposition of $\lambda_k^{\otimes 2}$ is determined by the number of a_1 boxes in the second row of the generating Young diagram. □

G Proof of Theorem 12

Theorem 18 (Restatement of Theorem 12)**.** *For a PNR measurement setting, $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ as input state, and an irrep λ_k of $\omega^{(n)} = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$, the following holds:*

$$\mathbb{E}[f_{\lambda_k}^2] = \frac{1}{s_{\lambda_k}^2}(-1)^{\varphi(N)} \sum_{X \in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(X)} g_k(X, N)\,, \tag{139}$$

where $g_k(X,N)$ is a function of Clebsch-Gordan coefficients of the representations $\tau_n^m \otimes \bar{\tau}_n^m$ and $\lambda_k^{\otimes 2}$ given by

$$g_k(X,N) = \sum_{l=0}^{\min\{n,2k\}} \frac{1}{\dim \lambda_l} \sum_{r=1}^{m_l} \sum_{\substack{M,M',L,\\ L' \in \mathrm{GT}(\lambda_k)}} \sum_{R,R' \in \mathrm{GT}(\lambda_l)} C^M_{N,\bar{N}} C^{M'}_{N,\bar{N}} C^L_{X,\bar{X}} C^{L'}_{X,\bar{X}} C^R_{N,\bar{N}} C^{R'}_{X,\bar{X}} C^{R,r}_{M,M'} C^{R',r}_{L,L'} \tag{140}$$

where m_l is the multiplicity of λ_l in $\lambda_k^{\otimes 2}$ as in Lemma 11.

Proof. For any irrep $\lambda_k \in \hat{\omega}_n^m$, and by relabeling the second entries as basis elements of the dual irrep $\bar{\tau}_n^m$, the second moment can be expressed as

$$\begin{aligned}
\mathbb{E}[f_{\lambda_k}^2] &:= \frac{1}{s_{\lambda_k}^2} \sum_{\boldsymbol{x}\in\mathcal{H}_n^m} \int dg \,\langle \boldsymbol{n},\boldsymbol{n}\,|P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\,\boldsymbol{x},\boldsymbol{x}\rangle^2 \langle \boldsymbol{x},\boldsymbol{x}\,|\tau_n^m\otimes\tau_n^m(g)|\,\boldsymbol{n},\boldsymbol{n}\rangle \\
&= \frac{1}{s_{\lambda_k}^2} \sum_{X\in\mathrm{GT}(\tau_n^m)} \int dg\,\langle N,N\,|P_{\lambda_k}(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger|\,X,X\rangle^2\langle X,X\,|\tau_n^m\otimes\tau_n^m(g)|\,N,N\rangle \\
&= \frac{1}{s_{\lambda_k}^2} \sum_{X\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N)+\varphi(X)} \int dg\,\langle N,\bar{N}\,|P_{\lambda_k}(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger|\,X,\bar{X}\rangle^2 \\
&\times \langle X,\bar{X}\,|\tau_n^m\otimes\tau_n^m(g)|\,N,\bar{N}\rangle \\
&= \frac{1}{s_{\lambda_k}^2}(-1)^{\varphi(N)} \sum_{X\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(X)} g_k(X,N)\,,
\end{aligned} \tag{141}$$

where

$$g_k(X,N) \equiv \int dg\,\langle N,\bar{N}\,|P_{\lambda_k}(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger|\,X,\bar{X}\rangle^2\langle X,\bar{X}\,|\tau_n^m\otimes\tau_n^m(g)|\,N,\bar{N}\rangle\,. \tag{142}$$

By Lemmas 6 and 9, we obtain

$$\begin{aligned}
g_{k,l}(X,N) = &\sum_{M,M'\in\mathrm{GT}(\lambda_k)} C^{M}_{N,\bar{N}} C^{M'}_{N,\bar{N}} \sum_{L,L'\in\mathrm{GT}(\lambda_k)} C^{L}_{X,\bar{X}} C^{L'}_{X,\bar{X}} \sum_{j=0}^{n} \sum_{J,J'\in\mathrm{GT}(\lambda_j)} C^{J}_{X,\bar{X}} C^{J'}_{N,\bar{N}} \\
&\times \underbrace{\int dg\,\langle M,M'\,|\lambda_k(g)^{\dagger\otimes 2}|\,L,L'\rangle\langle J\,|\lambda_j(g)|\,J'\rangle}_{\equiv I}
\end{aligned} \tag{143}$$

We compute the integral with Schur's orthogonality relations. Specifically, this requires the irrep decomposition of $\lambda_k^{\otimes 2}$: By Lemma 11, we have

$$\langle M,M'\,|\lambda_k(g)^{\dagger\otimes 2}|\,L,L'\rangle = \langle M,M'\,|\bigoplus_{l=0}^{2k}\lambda_k^{\oplus m_l}(g)^\dagger|\,L,L'\rangle\,, \tag{144}$$

where $m_l \in \{0,1,\ldots,k\}$ is the multiplicity of λ_l in $\lambda_k^{\otimes 2}$ worked out in Lemma 11. Then, consider the following Clebsch-Gordan decompositions:

$$|M,M'\rangle = \sum_{i=0}^{2k}\sum_{R\in\mathrm{GT}(\lambda_i)} C^{R,r_i}_{M,M'}|R,r_i\rangle\,,\quad |L,L'\rangle = \sum_{h=0}^{2k}\sum_{R'\in\mathrm{GT}(\lambda_h)} C^{R',r_h}_{L,L'}|R',r_h\rangle\,, \tag{145}$$

where r_i, r_h denote the r_i-th and r_h-th copies of λ_i and λ_h in $\lambda_k^{\otimes 2}$, respectively. By orthogonality of irreps, it follows

$$\langle M,M'\,|\lambda_k(g)^{\dagger\otimes 2}|\,L,L'\rangle = \sum_{l=0}^{2k}\sum_{r=1}^{m_l}\sum_{R,R'\in\mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'}C^{R',r}_{L,L'}\langle R,r\,|\lambda_l^{(r)}(g)^\dagger|\,R',r\rangle\,. \tag{146}$$

By Schur's orthogonality relations, this implies that the only non trivial contributions in I are associated with irreps λ_l which appears in the intersection of the sets of irreps of $\tau_n^m\otimes\bar{\tau}_n^m$ and $\lambda_k\otimes\lambda_k$, i.e. $j=l$ provided that λ_l appears in both decomposition. More specifically,

$$\begin{aligned}
I &= \sum_{l=0}^{2k}\sum_{r=1}^{m_l}\sum_{R,R'\in\mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'}C^{R',r}_{L,L'}\int dg\,\langle R,r\,|\lambda_l^{(r)}(g)^\dagger|\,R',r\rangle\langle J\,|\lambda_j(g)|\,J'\rangle \\
&= \sum_{l=0}^{2k}\delta_{l,j}\sum_{r=1}^{m_l}\sum_{R,R'\in\mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'}C^{R',r}_{L,L'}\int dg\,\langle R,r\,|\lambda_l^{(r)}(g)^\dagger|\,R',r\rangle\langle J\,|\lambda_l(g)|\,J'\rangle \\
&= \sum_{l=0}^{2k}\frac{1}{\dim\lambda_l}\delta_{l,j}\sum_{r=1}^{m_l}\sum_{R,R'\in\mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'}C^{R',r}_{L,L'}\delta_{R,J'}\delta_{R',J}\,.
\end{aligned} \tag{147}$$

Therefore, we have

$$
\begin{aligned}
g_k(X,N) = & \sum_{M,M'\in\mathrm{GT}(\lambda_k)} C^{M}_{N,\bar{N}} C^{M'}_{N,\bar{N}} \sum_{L,L'\in\mathrm{GT}(\lambda_k)} C^{L}_{L,\bar{L}} C^{L'}_{X,\bar{X}} \sum_{j=0}^{n} \sum_{J,J'\in\mathrm{GT}(\lambda_j)} C^{J}_{X,\bar{X}} C^{J'}_{N,\bar{N}} \\
& \times \sum_{l=0}^{2k} \frac{1}{\dim\lambda_l} \delta_{l,j} \sum_{r=1}^{m_l} \sum_{R,R'\in\mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'} C^{R',r}_{L,L'} \delta_{R,J'} \delta_{R',J} \\
= & \sum_{l=0}^{\min n,2k} \frac{1}{\dim\lambda_l} \sum_{r=1}^{m_l} \sum_{M,M'\in\mathrm{GT}(\lambda_k)} C^{M}_{N,\bar{N}} C^{M'}_{N,\bar{N}} \sum_{L,L'\in\mathrm{GT}(\lambda_k)} C^{L}_{L,\bar{L}} C^{L'}_{X,\bar{X}} \\
& \times \sum_{R,R'\in\mathrm{GT}(\lambda_l)} C^{R}_{N,\bar{N}} C^{R'}_{X,\bar{X}} C^{R,r}_{M,M'} C^{R',r}_{L,L'} ,
\end{aligned}
\tag{148}
$$

from which the assertion follows. □

H Passive RB with heterodyne measurement

In this section, we will use the usual multi-index notation [83, Sec. 9.1]: For elements $\boldsymbol{n}_1, \boldsymbol{n}_2 \in \mathcal{H}^m_n$, $\boldsymbol{n}_1 + \boldsymbol{n}_2$ denotes the component-wise sum. The multi-index factorial of $\boldsymbol{n} \in \mathcal{H}^m_n$ is defined as $\boldsymbol{n}! := n_1! \dots n_m!$. Also, for a given $\boldsymbol{\alpha} \in \mathbb{C}^m$, we consider the power $\boldsymbol{\alpha}^{\boldsymbol{n}} := \alpha_1^{n_1} \dots \alpha_m^{n_m}$, and we set $|\boldsymbol{\alpha}|^p := \alpha_1^p + \dots + \alpha_m^p$ for $p \geq 1$. We also use the shorthand notation

$$
\int d^2\boldsymbol{\alpha} \equiv \int d^2\alpha_1 \cdots \int d^2\alpha_m \,, \tag{149}
$$

where $d^2\alpha_i$ is the complex measure on $\mathbb{C}$. With this notation, the multi-mode coherent state $|\boldsymbol{\alpha}\rangle$ can be expanded as

$$
|\boldsymbol{\alpha}\rangle = e^{-|\boldsymbol{\alpha}|^2/2} \sum_{\boldsymbol{n}\in\mathcal{F}_m} \frac{\boldsymbol{\alpha}^{\boldsymbol{n}}}{\sqrt{\boldsymbol{n}!}} |\boldsymbol{n}\rangle \,. \tag{150}
$$

Consider now the following quantity for any $K \in 2\mathbb{N}$:

$$
I(\{\boldsymbol{n}_i\}_{i=1}^K) = \frac{1}{\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!\dots\boldsymbol{n}_K!}} \int d^2\boldsymbol{\alpha}\, e^{-K/2|\boldsymbol{\alpha}|^2} \bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\dots\boldsymbol{n}_{K/2}} \boldsymbol{\alpha}^{\boldsymbol{n}_{K/2+1}+\dots\boldsymbol{n}_K} \,. \tag{151}
$$

The latter can be evaluated writing down the integral in polar coordinates and integrating by parts. Specifically, for the single-mode integral, and for any $c > 0$, we have

$$
\begin{aligned}
\int d^2\alpha\, e^{-c|\alpha|^2} \alpha^{a+b} \bar{\alpha}^{c+d} &= \int_0^\infty dr\, e^{-cr^2} r^{a+b+c+d+1} \int_0^{2\pi} d\theta\, e^{i\theta(a+b-c-d)} \\
&= \pi \left(\frac{a+b+c+d}{2}\right)!\, c^{-\frac{a+b+c+d}{2}} \delta_{a+b,c+d} \,.
\end{aligned}
\tag{152}
$$

Notice that the expression in parenthesis is a proper factorial due to the δ. This implies

$$
I(\{\boldsymbol{n}_i\}_{i=1}^K) = \frac{\pi^m}{(K/2)^n} \frac{(\boldsymbol{n}_1 + \dots + \boldsymbol{n}_{K/2})!}{\sqrt{\boldsymbol{n}_1!\dots\boldsymbol{n}_K!}} \delta_{\boldsymbol{n}_1+\dots+\boldsymbol{n}_{K/2}, \boldsymbol{n}_{K/2+1}+\dots+\boldsymbol{n}_K} \,. \tag{153}
$$

where $\delta_{\boldsymbol{n}_1+\dots+\boldsymbol{n}_{K/2}, \boldsymbol{n}_{K/2+1}+\dots+\boldsymbol{n}_K} = 1$ if $\sum_{i=1}^{K/2} \boldsymbol{n}_i = \sum_{i=K/2+1}^{K} \boldsymbol{n}_i$, and 0 otherwise, and we used the fact that $|\boldsymbol{n}_i| = n$ for each $i = 1, \dots K$.

The coherent state POVM $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\}_{\alpha\in\mathbb{C}^m}$ is informationally complete [91], which implies $s_{\lambda_k} \neq 0$ for any $\lambda_k \in \hat{\omega}^M_n$ [1]. More specifically, we have:

Lemma 19. *Let $\lambda_k \in \hat{\omega}^M_n$. For a balanced heterodyne measurement setting, the eigenvalues of the frame operator of the filtered RB protocol are given by*

$$
s_{\lambda_k} = \frac{1}{d_{\lambda_k}} \frac{\pi^m}{2^n} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2} I_\varphi(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \sum_{M\in\mathrm{GT}(\lambda_k)} C^{M}_{N_{\boldsymbol{n}_1},\bar{M}_{\boldsymbol{m}_1}} C^{M}_{N_{\boldsymbol{n}_2},\bar{M}_{\boldsymbol{m}_2}} \,, \tag{154}
$$

where $N_{\boldsymbol{n}_i}, M_{\boldsymbol{m}_i}$ are the GT patterns associated with $\boldsymbol{n}_1, \boldsymbol{m}_i$, respectively, and I_φ is given by

$$
I_\varphi(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) = (-1)^{\varphi(M_{\boldsymbol{m}_1})+\varphi(M_{\boldsymbol{m}_2})} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \,. \tag{155}
$$

and

$$
I = \frac{\pi^m}{2^n} \sqrt{\frac{\boldsymbol{n}_1!\boldsymbol{n}_2!}{\boldsymbol{m}_1!\boldsymbol{m}_2!}} \binom{\boldsymbol{n}_1+\boldsymbol{n}_2}{\boldsymbol{n}_2} \delta_{\boldsymbol{n}_1+\boldsymbol{n}_2, \boldsymbol{m}_1+\boldsymbol{m}_2} \,. \tag{156}
$$

Proof. For the balanced heterodyne measurement setting the corresponding (ideal) POVM is $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \equiv E_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{C}^m}$, where $|\boldsymbol{\alpha}\rangle = \bigotimes_{i=1}^m |\alpha_i\rangle$ is an m modes coherent state. The associated measurement channel is given by

$$\mathcal{M}(\cdot) := \int_{\mathbb{C}^m} d^2\boldsymbol{\alpha}\, \mathrm{Tr}[|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|(\cdot)]\, |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \,. \tag{157}$$

To evaluate Eq. (42), we use the multi-mode expansion defined in Eq. (150). Moreover, since P_{λ_k} is defined onto a subspace of $\mathcal{H}_n^m$, such expansions of the copies of $\boldsymbol{\alpha}$ are truncated. Hence, by Eq. (151), we have

$$\begin{aligned}
s_{\lambda_k} &= \frac{1}{d_{\lambda_k}} \int d^2\boldsymbol{\alpha}\, \mathrm{Tr}[|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| P_{\lambda_k}(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)] \\
&= \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2)\, \mathrm{Tr}[|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1| P_{\lambda_k}(|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2|)] \\
&= \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \langle \boldsymbol{n}_1, \boldsymbol{m}_1 \,|P_{\lambda_k}|\, \boldsymbol{n}_2, \boldsymbol{m}_2\rangle \\
&= \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \langle N_{\boldsymbol{n}_1}, M_{\boldsymbol{m}_1} \,|P_{\lambda_k}|\, N_{\boldsymbol{n}_2}, M_{\boldsymbol{m}_2}\rangle \\
&= \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m} I_\varphi(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \langle N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1} \,|P_{\lambda_k}|\, N_{\boldsymbol{n}_2}, \bar{M}_{\boldsymbol{m}_2}\rangle \\
&= \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m} I_\varphi(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_{\boldsymbol{n}_1},\bar{M}_{\boldsymbol{m}_1}} C^M_{N_{\boldsymbol{n}_2},\bar{M}_{\boldsymbol{m}_2}} \,,
\end{aligned} \tag{158}$$

where in the last step we used the definition of P_{λ_k} to compute the inner product, i.e.

$$\begin{aligned}
\langle N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1} \,|P_{\lambda_k}|\, N_{\boldsymbol{n}_2}, \bar{M}_{\boldsymbol{m}_2}\rangle &= \sum_{M\in\mathrm{GT}(\lambda_k)} \langle N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1} \,|\, M\rangle\langle M \,|\, N_{\boldsymbol{n}_2}, M_{\boldsymbol{m}_2}\rangle \\
&= \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_{\boldsymbol{n}_1},\bar{M}_{\boldsymbol{m}_1}} C^M_{N_{\boldsymbol{n}_2},\bar{M}_{\boldsymbol{m}_2}} \,.
\end{aligned} \tag{159}$$

By Eq. (153), we have

$$I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) = \frac{\pi^m}{2^n} (\boldsymbol{n}_1 + \boldsymbol{n}_2)!\, \delta_{\boldsymbol{n}_1+\boldsymbol{n}_2, \boldsymbol{m}_1+\boldsymbol{m}_2} \,. \tag{160}$$

Finally, since

$$(\boldsymbol{n}_1 + \boldsymbol{n}_2)! = \boldsymbol{n}_1! \boldsymbol{n}_2! \binom{\boldsymbol{n}_1 + \boldsymbol{n}_2}{\boldsymbol{n}_2} \,, \tag{161}$$

with

$$\binom{\boldsymbol{n}_1 + \boldsymbol{n}_2}{\boldsymbol{n}_2} \equiv \binom{n_{1,1} + n_{2,1}}{n_{2,1}} \cdots \binom{n_{1,m} + n_{2,m}}{n_{2,m}} \,, \tag{162}$$

Eq. (156) follows. □

A result similar to Eq. (63) is available for heterodyne detectors. We remark that, in principle, it could be possible to workout an expression analogous to Eq. (61). However, we find it less intuitive in the interpretation, as it would correspond to a weighted sum of matrix coefficients of λ_k. Instead, we can express the filter function as a linear combination of Hafnians, in agreement with Gaussian boson sampling experiments:

Theorem 20 (Restatement of Theorem 2 - heterodyne version)**.** *Let $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ be a m modes state and let $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\}_{\boldsymbol{\alpha}\in\mathbb{C}^m}$ be the coherent state POVM. Then, for a given irrep $\lambda_k \in \hat{\omega}_n^m$, the filter function is given by*

$$f_{\lambda_k}(\boldsymbol{\alpha}, g) = \frac{(-1)^{\varphi(N)}}{d_{\lambda_k}} \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1,N_2\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_2)} C^M_{N_1,\bar{N}_2} \langle N_1, N_2 \,|\, \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha}\rangle \,. \tag{163}$$

Proof. The proof is analogous to the PNR case. We go through each step again for clarity. By a slight generalization of Lemma 6 to include coherent state measurements, we have

$$f_{\lambda_k}(\boldsymbol{\alpha}, g) = \frac{1}{d_{\lambda_k}} \langle \boldsymbol{n}, \boldsymbol{n} \,|\, P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \tag{164}$$

$$= \frac{1}{d_{\lambda_k}} (-1)^{\varphi(N)} \langle N, \bar{N} \,|\, P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \tag{165}$$

$$= \frac{1}{d_{\lambda_k}} (-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \langle M \,|\, \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \tag{166}$$

$$= \frac{1}{d_{\lambda_k}} (-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1, N_2 \in \mathrm{GT}(\tau_n^m)} C^M_{N_1,\bar{N}_2} \langle N_1, \bar{N}_2 \,|\, \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \tag{167}$$

$$= \frac{1}{d_{\lambda_k}} (-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1, N_2 \in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_2)} C^M_{N_1,\bar{N}_2} \tag{168}$$

$$\times \langle N_1, N_2 \,|\, \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \,, \tag{169}$$

where $\boldsymbol{n}_1, \boldsymbol{n}_2$ are Fock states associated with GT states N_1, N_2, respectively. By writing

$$\langle N_1, N_2 \,|\, \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle = \langle \boldsymbol{n}_2 \,|\, \tau_n^m(g) \,|\, \boldsymbol{\alpha} \rangle \langle \boldsymbol{\alpha} \,|\, \tau_n^m(g)^\dagger \,|\, \boldsymbol{n}_1 \rangle \tag{170}$$

we see that f_{λ_k} is given by a suitable combination of Hafnians [14]. □

H.1 Moments for the heterodyne measurement setting

In this section, we provide explicit expressions for first two moments of probability of the filter function (5) in the case of heterodyne measurements, for which the ideal probability distribution is $p(\boldsymbol{\alpha}|g) = \langle \boldsymbol{\alpha} \,|\, \omega_n^m(g)(\rho) \,|\, \boldsymbol{\alpha} \rangle$, $\boldsymbol{\alpha} \in \mathbb{C}^m$. In particular, the ideal second moment will provide an upper bound to the sampling complexity of the protocol, Cf. Section 2.3. As in Section 4.3, the proofs rely on the application of Schur's orthogonality relations, see Eq. (73).

Lemma 21. *For a heterodyne measurement setting, $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$ as input state, and an irrep λ_k of $\omega^{(n)} = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$, the following holds:*

$$\mathbb{E}[f_{\lambda_k}] = \frac{1}{d_{\lambda_k} s_{\lambda_k}} \sum_{\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{m}_1, \boldsymbol{m}_2} I_\varphi(\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{m}_1, \boldsymbol{m}_2) \sum_{M \in \mathrm{GT}(\lambda_k)} |C^M_{N,\bar{N}}|^2 \sum_{S \in \mathrm{GT}(\lambda_k)} C^S_{N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1}} C^S_{N_{\boldsymbol{n}_2}, \bar{M}_{\boldsymbol{m}_2}} \,, \tag{171}$$

where I_φ is as in Lemma 19.

Proof. As in the proof of Lemma 19, considering the multi-mode expansion of $\boldsymbol{\alpha}$, only the n-particle component provides non-trivial contribution to the first moment, since ω_n^m acts non trivially on $\mathcal{H}_n^m$ only. Recalling Eq. (151), it follows

$$\mathbb{E}[f_{\lambda_k}] = \frac{1}{s_{\lambda_k}} \int d^2\boldsymbol{\alpha} \int dg \ \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{n}| P_{\lambda_k} \circ \omega_n^m(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)] \, \mathrm{Tr}[|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \omega_n^m(g)(|\boldsymbol{n}\rangle\langle\boldsymbol{n}|)] \tag{172}$$

$$= \frac{1}{s_{\lambda_k}} \sum_{\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{m}_1, \boldsymbol{m}_2} I(\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{m}_1, \boldsymbol{m}_2) \int dg \ \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{n}| P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)] \tag{173}$$

$$\times \mathrm{Tr}[|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2| \omega_n^m(g)(|\boldsymbol{n}\rangle\langle\boldsymbol{n}|)] \,. \tag{174}$$

In particular,

$$H \equiv \int dg \ \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{n}| P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)] \, \mathrm{Tr}[|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2| \omega_n^m(g)(|\boldsymbol{n}\rangle\langle\boldsymbol{n}|)] \tag{175}$$

$$= \int dg \, \langle \boldsymbol{n}, \boldsymbol{n} \,|\, P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,|\, \boldsymbol{n}_1, \boldsymbol{m}_1 \rangle \langle \boldsymbol{n}_2, \boldsymbol{m}_2 \,|\, \tau_n^m \otimes \bar{\tau}_n^m(g) \,|\, \boldsymbol{n}, \boldsymbol{n} \rangle \tag{176}$$

$$= (-1)^{\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \int dg \, \langle M \,|\, \lambda_k(g)^\dagger \,|\, N_{\boldsymbol{n}_1}, M_{\boldsymbol{m}_1} \rangle \langle N_{\boldsymbol{n}_2}, M_{\boldsymbol{m}_2} \,|\, \bigoplus_{j=0}^{n} \lambda_j(g) \,|\, N, N \rangle \tag{177}$$

$$= (-1)^{\varphi(M_{\boldsymbol{m}_1}) + \varphi(M_{\boldsymbol{m}_2})} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \int dg \, \langle M \,|\, \lambda_k(g)^\dagger \,|\, N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1} \rangle \tag{178}$$

$$\times \langle N_{\boldsymbol{n}_2}, \bar{M}_{\boldsymbol{m}_2} \,|\, \bigoplus_{j=0}^{n} \lambda_j(g) \,|\, N, \bar{N} \rangle \,. \tag{179}$$

The latter can be computed by slight modifications of Lemmas 6 and 9. In particular, by orthogonality relations, the integral is non-zero only if $j = k$ and for basis vectors of λ_k. In other words, it is enough to restrict the Clebsch-Gordan decompositions to the λ_k-th component:

$$|N_{\boldsymbol{n}_1}, M_{\boldsymbol{m}_1}\rangle|_{\lambda_k} = \sum_{S_1 \in \mathrm{GT}(\lambda_k)} C^{S_1}_{N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1}} |S_1\rangle \,,$$

$$|N_{\boldsymbol{n}_2}, M_{\boldsymbol{m}_2}\rangle|_{\lambda_k} = \sum_{S_2 \in \mathrm{GT}(\lambda_k)} C^{S_2}_{N_{\boldsymbol{n}_2}, \bar{M}_{\boldsymbol{m}_2}} |S_2\rangle \,,$$

$$|N, \bar{N}\rangle|_{\lambda_k} = \sum_{S_3 \in \mathrm{GT}(\lambda_k)} C^{S_3}_{N, \bar{N}} |S_3\rangle \,.$$

Therefore, by Eq. (73), we have

$$H = \frac{1}{d_{\lambda_k}} (-1)^{\varphi(M_{\boldsymbol{m}_1}) + \varphi(M_{\boldsymbol{m}_2})} \sum_{M \in \mathrm{GT}(\lambda_k)} |C^{M}_{N, \bar{N}}|^2 \sum_{S \in \mathrm{GT}(\lambda_k)} C^{S}_{N_{\boldsymbol{n}_1}, \bar{M}_{\boldsymbol{m}_1}} C^{S}_{N_{\boldsymbol{n}_2}, \bar{M}_{\boldsymbol{m}_2}} \tag{180}$$

from which the assertion follows recalling the definition of I_φ. □

Lastly, we have the following explicit expression for the second moment:

Theorem 22. *Consider a passive RB experiment with balanced heterodyne measurement setting, initial Fock state* $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$, *and* λ *is an irrep of* $\omega^M_n = \tau^m_n(\,\cdot\,)\tau^{m\dagger}_n$. *Then, the following holds:*

$$\mathbb{E}[f^2_{\lambda_k}] = \frac{1}{s^2_{\lambda_k}} (-1)^{\varphi(N)} \sum_{\substack{\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{n}_3, \\ \boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3}} (-1)^{\sum_{i=1}^3 \varphi(M_i)} I((\boldsymbol{n}_i), (\boldsymbol{m}_i)) g^{(\varphi)}_k(\boldsymbol{N}, \boldsymbol{M}, N) \,, \tag{181}$$

where $\boldsymbol{N} = (N_1, N_2, N_3), \boldsymbol{M} = (M_1, M_2, M_3)$ *with* $N_i \equiv N(\boldsymbol{n}_i), M_i \equiv M(\boldsymbol{m}_i)$ *are GT patterns associated with* $\boldsymbol{n}_i, \boldsymbol{m}_i$, *respectively,* $I((\boldsymbol{n}_i), (\boldsymbol{m}_i)) \equiv I(\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{n}_3, \boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3)$ *is as in Eq.* (153) *and*

$$\begin{aligned} g_k(\boldsymbol{N}, \boldsymbol{M}, N) = &\sum_{l=0}^{\min\{n,2k\}} \frac{1}{d_{\lambda_k}} \sum_{r=1}^{m_l} \sum_{M, M', L, L' \in \mathrm{GT}(\lambda_k)} \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C^{M}_{N, \bar{N}} C^{M'}_{N, \bar{N}} C^{R,r}_{M, M'} C^{R}_{N, \bar{N}} C^{R'}_{N_3, \bar{M}_3} \\ &\times C^{L}_{N_1, \bar{M}_1} C^{L'}_{N_2, \bar{M}_2} C^{R',r}_{L, L'} \,. \end{aligned} \tag{182}$$

Proof. By Eqs. (150) and (151), we have, for any λ_k,

$$\mathbb{E}[f^2_{\lambda_k}] = \frac{1}{s^2_{\lambda_k}} \int d^2\boldsymbol{\alpha} \int dg \ \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{n}| P_{\lambda_k} \circ \omega^m_n(g)^\dagger (|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)]^2 \, \mathrm{Tr}[|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \omega^m_n(g)(|\boldsymbol{n}\rangle\langle\boldsymbol{n}|)] \tag{183}$$

$$= \frac{1}{s^2_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{n}_3, \\ \boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3}} I((\boldsymbol{n}_i), (\boldsymbol{m}_i)) \int dg \ \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{m}| P_{\lambda_k} \circ \omega^m_n(g)^\dagger (|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)] \tag{184}$$

$$\times \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{n}| P_{\lambda_k} \circ \omega^m_n(g)^\dagger (|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2|)] \, \mathrm{Tr}[|\boldsymbol{n}_3\rangle\langle\boldsymbol{m}_3| \omega^m_n(g)(|\boldsymbol{n}\rangle\langle\boldsymbol{n}|)] \tag{185}$$

$$\equiv \frac{1}{s^2_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{n}_3, \\ \boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3}} I((\boldsymbol{n}_i), (\boldsymbol{m}_i)) g^{(\varphi)}_k(\boldsymbol{N}, \boldsymbol{M}, N) \,. \tag{186}$$

Introducing GT patterns, we have

$$g^{(\varphi)}_k(\boldsymbol{N}, \boldsymbol{M}, N) \equiv \int dg \ \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{m}| P_{\lambda_k} \circ \omega^m_n(g)^\dagger (|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)] \, \mathrm{Tr}[|\boldsymbol{n}\rangle\langle\boldsymbol{n}| P_{\lambda_k} \circ \omega^m_n(g)^\dagger (|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2|)] \tag{187}$$

$$\times \mathrm{Tr}[|\boldsymbol{n}_3\rangle\langle\boldsymbol{m}_3| \omega^m_n(g)(|\boldsymbol{n}\rangle\langle\boldsymbol{n}|)] \tag{188}$$

$$= \int dg \, \langle \boldsymbol{n}, \boldsymbol{n} \,|P_{\lambda_k} \tau^m_n \otimes \bar{\tau}^m_n(g)^\dagger \,|\boldsymbol{n}_1, \boldsymbol{m}_1\rangle\langle \boldsymbol{n}, \boldsymbol{n} \,|P_{\lambda_k} \tau^m_n \otimes \bar{\tau}^m_n(g)^\dagger \,|\boldsymbol{n}_2, \boldsymbol{m}_2\rangle \tag{189}$$

$$\times \langle \boldsymbol{n}_3, \boldsymbol{m}_3 \,|\tau^m_n \otimes \bar{\tau}^m_n(g)|\boldsymbol{n}, \boldsymbol{n}\rangle \tag{190}$$

$$= (-1)^{\varphi(N) + \varphi(M_1) + \varphi(M_2) + \varphi(M_3)} \sum_{M, M' \in \mathrm{GT}(\lambda_k)} C^{M}_{N, \bar{N}} C^{M'}_{N, \bar{N}} \tag{191}$$

$$\times \int dg \, \langle M, M' \,|\lambda_k(g)^{\otimes 2\dagger} \,|N_1, \bar{M}_1, N_2, \bar{M}_2\rangle\langle N_3, \bar{M}_3 \,|\bigoplus_{j=0}^{n} \lambda_j(g)|N, \bar{N}\rangle \tag{192}$$

$$\equiv (-1)^{\varphi(N) + \sum_{i=1}^3 \varphi(M_i)} g_k(\boldsymbol{N}, \boldsymbol{M}, N) \,. \tag{193}$$

We compute the integral as in the proof of Theorem 12: Consider the decomposition of $\lambda_l^{\otimes 2}$ as in Lemma 11. Then, by orthogonality of the matrix coefficients, the non-trivial contributions to the integral come from irreps that appear –with their multiplicities– in both ω_n^m and $\lambda_k^{\otimes 2}$. In this way, the latter integral reduces to

$$\sum_{l=0}^{\min\{n,2k\}} \sum_{r=1}^{m_l} \int dg \, \langle M, M' \, | \lambda_l^{(r)}(g)^\dagger \, | N_1, \bar{M}_1, N_2, \bar{M}_2 \rangle \langle N_3, \bar{M}_3 \, | \lambda_l(g) | N, \bar{N} \rangle \, . \tag{194}$$

Given the Clebsch-Gordan decompositions

$$|M, M'\rangle = \sum_{R \in \mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'} |R, r\rangle \, , \tag{195}$$

$$|N_3, \bar{M}_3\rangle = \sum_{J \in \mathrm{GT}(\lambda_l)} C^{J}_{N_3,\bar{M}_3} |J\rangle \, , \tag{196}$$

$$|N, \bar{N}\rangle = \sum_{J' \in \mathrm{GT}(\lambda_l)} C^{J'}_{N,\bar{N}} |J'\rangle \, , \tag{197}$$

$$|N_1, \bar{M}_1, N_2, \bar{M}_2\rangle = \sum_{L,L' \in \mathrm{GT}(\lambda_k)} C^{L}_{N_1,\bar{M}_1} C^{L'}_{N_2,\bar{M}_2} |L, L'\rangle \, , \tag{198}$$

$$|L, L'\rangle = \sum_{R' \in \mathrm{GT}(\lambda_l)} C^{R' r}_{L,L'} |R', r\rangle \, , \tag{199}$$

from which it follows

$$\int dg \, \langle R, r \, | \lambda_l^{(r)}(g)^\dagger \, | R', r\rangle \langle J \, | \lambda_l(g) | J' \rangle = \frac{1}{d_{\lambda_l}} \delta_{R,J'} \delta_{R',J} \, . \tag{200}$$

Hence,

$$\begin{aligned} g_k(\boldsymbol{N}, \boldsymbol{M}, N) = & \sum_{l=0}^{\min\{n,2k\}} \frac{1}{d_{\lambda_k}} \sum_{r=1}^{m_l} \sum_{M,M',L,L' \in \mathrm{GT}(\lambda_k)} \sum_{R,R' \in \mathrm{GT}(\lambda_l)} C^{M}_{N,\bar{N}} C^{M'}_{N,\bar{N}} C^{R,r}_{M,M'} C^{R}_{N,\bar{N}} C^{R'}_{N_3,\bar{M}_3} \\ & \times C^{L}_{N_1,\bar{M}_1} C^{L'}_{N_2,\bar{M}_2} C^{R',r}_{L,L'} \, , \end{aligned} \tag{201}$$

and the assertion follows with a suitable sorting of all the terms. □

Simulating non-completely-positive Actions via Exponentiation of Hermitian-preserving Maps

Fuchuan Wei, Zhenhuan Liu, Guoding Liu, Zizhao Han, Dong-Ling Deng, and Zhengwei Liu

The full version of this paper can be found at arXiv:2308.07956.

I. INTRODUCTION

Principles of quantum mechanics dictate that quantum operations must act on and output density matrices, which are positive matrices with a unit trace [1]. Thus, a valid quantum operation must be completely positive and trace-preserving (CPTP). As depicted in Fig. 1(a), the set of CPTP maps represents only a small subset of all linear maps [2]. In practical terms, the CPTP constraint limits the performance of many quantum tasks.

In entanglement detection and quantification, positive but not completely positive maps [3] serve as crucial tools. By deciding the positivity of output matrices generated by acting positive maps on subsystems, corresponding entanglement criteria exhibit strong detection capabilities. Moreover, the entanglement negativity, which quantifies the violation of the positive partial transposition criterion, represents an easily computable and operationally meaningful entanglement measure [4]. However, due to their lack of complete positivity, verifying positive map criteria often requires highly joint operations or exponential repetition times [5–7].

In quantum error mitigation [8, 9], the core idea is applying the inverse map of the noise channel to noisy states. However, since the inverse maps of noise channels are always non-completely-positive (non-CP), techniques such as probabilistic error cancellation [10–12] are adopted to statistically realize these inverse maps, recovering only noiseless expectation values rather than noiseless states, limiting the range of applications.

Existing approaches for realizing non-CP maps are restricted in the level of quantum states and aim to prepare outputs of non-CP maps in some indirect ways. Methods based on structural approximation [13, 14] and Petz recovery map [15, 16] employ CPTP maps to approximate non-CP maps. However, the approximate channel may largely deviate from the target non-CP map. The multicopy extension method [17] utilizes a joint CPTP map acting on multiple copies of input states to produce a single output of the non-CP map, making it feasible only when the output remains a density matrix. Probabilistic error cancellation [10–12] decomposes the non-CP map into a linear combination of some CPTP maps, realizing the non-CP map only in a statistical manner.

An effective and practical approach to implementing non-CP maps remains elusive. In this work, we address this crucial problem by proposing a systematic approach to efficiently simulate the actions of all Hermitian-preserving maps.

II. THE ALGORITHM

Although the output of a Hermitian-preserving map, $\mathcal{N}(\rho)$, might not necessarily be a density matrix but rather a general Hermitian matrix, Hermitian matrices still have physical meanings, such as Hamiltonians determining evolutions of physical systems. Therefore, by exponentiating a Hermitian-preserving map $\mathcal{N}(\cdot)$, we define a new map, $e^{-i\mathcal{N}(\cdot)t}$, which maps an input state to a unitary evolution. This new map contains all the information of the Hermitian-preserving map $\mathcal{N}$.

To realize the map $e^{-i\mathcal{N}(\cdot)t}$, we design a quantum algorithm called *Hermitian-preserving map exponentiation* (HME), as depicted in Fig. 1(c). The HME algorithm begins with preparing two quantum systems, the target state ρ will be prepared on the first system, while the second system serves as a quantum memory to keep the state on which the evolution of $e^{-i\mathcal{N}(\rho)t}$ is applied. Based on the desired accuracy, the non-CP map $\mathcal{N}$, and the total evolution time t, one determines an appropriate Hamiltonian H and a short time period Δt. Subsequently, one repeats the following steps for a total of $K = t/\Delta t$ times:

1. Prepare the target state ρ on the first system.

2. Evolve the two systems jointly using $e^{-iH\Delta t}$.

Theorem 1 (Validation of HME). *For a short time period Δt, we have*

$$\mathrm{Tr}_1\left(e^{-iH\Delta t}(\rho\otimes\sigma)e^{iH\Delta t}\right) = e^{-i\mathcal{N}(\rho)\Delta t}\sigma e^{i\mathcal{N}(\rho)\Delta t} + \mathcal{O}(\Delta t^2). \quad (1)$$

Here, Tr_1 denotes the partial trace over the first system, $\mathcal{N}$ represents the target Hermitian-preserving map, $H = \Lambda_{\mathcal{N}}^{T_1}$ with $\Lambda_{\mathcal{N}} = (\mathcal{I}\otimes\mathcal{N})\,|\Phi^+\rangle\langle\Phi^+|$ being the Choi matrix for $\mathcal{N}$, $|\Phi^+\rangle = \sum_i |ii\rangle$ denotes the unnormalized maximally entangled state, and T_1 represents the partial transposition operation on the first system.

The density matrix exponentiation algorithm [18, 19], which has been proved to exhibit exponential speedup compared to single-copy strategies in certain tasks [20], can be regarded as a special case of HME by setting $\mathcal{N}$ to be the identity map. Given that Hermitian-preserving maps are significantly more general than CPTP maps and encompass a wide range of crucial non-CP maps, HME has the potential to be a key tool in various quantum information processing tasks.

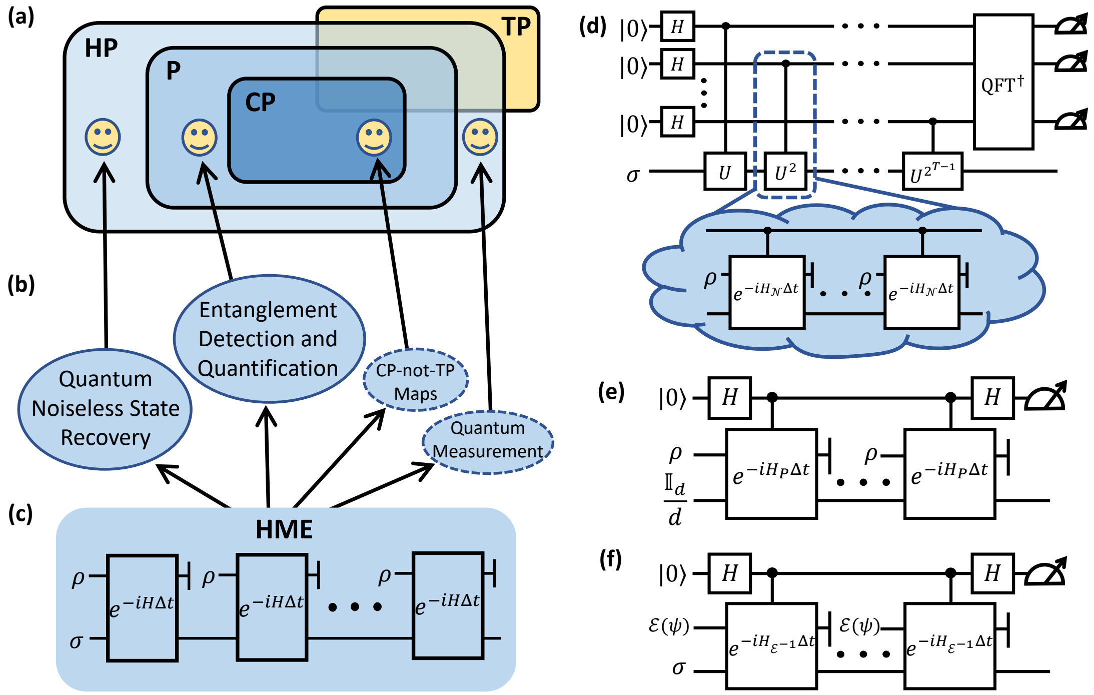


FIG. 1. (a) Diagrammatic representation of different types of maps, including CP (completely positive), P (positive), HP (Hermitian-preserving), and TP (trace-preserving) maps. Physical maps lie in the intersection of CP and TP. The smiling faces represent the maps used in the four applications listed in (b). (c) Circuit diagram for HME, comprising three components: sequential input of identical states ρ, the evolved state σ preserved using quantum memory, and joint Hamiltonian evolution. (d) The circuit of the HME-based entanglement detection protocol, which is constructed by combining the HME and quantum phase estimation algorithms. The controlled unitary evolutions are approximately realized by HME, where $H_{\mathcal{N}}$ is the Hamiltonian for implementing $\mathcal{N} = \mathcal{P}_A \otimes \mathcal{I}_B$. (e) The circuit for estimating entanglement negativity. (f) The circuit of our error mitigation protocol.

III. PERFORMANCE ANALYSIS

HME realizes the evolution of $e^{-i\mathcal{N}(\rho)t}$ by sequentially inputting the target state ρ. Thus, an essential indicator for analyzing the performance of HME is the number of copies needed for realizing the desired evolution with an error up to ϵ. According to Theorem 1, the difference between the ideal and real channels for a single step of the experiment is a second-order term. Thus the error could be suppressed by choosing a shorter time slice Δt, or equivalently, by using more copies of ρ.

Theorem 2 (Upper bound of sample complexity)**.** *Let $\mathcal{N}$ be an arbitrary Hermitian-preserving map, the HME algorithm shown in Fig. 1(c) requires at most*

$$\mathcal{O}\left(\epsilon^{-1}\|H\|_\infty^2 t^2\right) \tag{2}$$

copies of sequentially inputting state ρ to ensure that $\|\mathcal{Q}_t - \mathcal{U}_t\|_\diamond \le \epsilon$ holds for arbitrary ρ. Here, $H = \Lambda_{\mathcal{N}}^{T_1}$, $\mathcal{Q}_t = \mathcal{Q}_{\Delta t}^{\circ K}$ represents the real channel with $\mathcal{Q}_{\Delta t}(\sigma) := \mathrm{Tr}_1\left[e^{-iH\Delta t}(\rho\otimes\sigma)e^{iH\Delta t}\right]$ and $K = t/\Delta t$, $\mathcal{U}_t$ is the ideal evolution channel corresponding to $e^{-i\mathcal{N}(\rho)t}$, and $\|\cdot\|_\diamond$ denotes the diamond norm.

We also analyze the lower bound of sample complexity for exponentiating Hermitian-preserving maps, considering the ability to perform arbitrary physical operations.

Theorem 3 (Lower bound of sample complexity)**.** *Let $\mathcal{N} \in T(\mathcal{H},\mathcal{K})$ be a Hermitian-preserving map and set $0 < \epsilon \le 1/6$, and $t \ge \frac{15\pi\epsilon}{4R_*}$. Even using highly joint operations, the minimum number of ρ needed to realize the evolution of $e^{-i\mathcal{N}(\rho)t}$ with ϵ accuracy in diamond distance satisfies*

$$f_{\mathcal{N}}(\epsilon,t) \ge \Omega\left(\epsilon^{-1}R_*^2 t^2\right), \tag{3}$$

where $R_* := \max\limits_{A\in\mathscr{F}} R\left[\mathcal{N}(A)\right]$. $R[\cdot] = \lambda_{max}(\cdot) - \lambda_{min}(\cdot)$ denotes the spectral gap defined as the difference between the largest and the lowest eigenvalues of the processed matrix. The feasible region $\mathscr{F}$ is defined as $\mathscr{F} = \Big\{A \in L(\mathcal{H}) : A^\dagger = A, \mathrm{Tr}(A) = 0, \|A\|_1 = 1, [\mathcal{N}(A^+),\mathcal{N}(A^-)] = 0\Big\}$, where A^+ and A^- are the positive and negative parts of A.

Combining Theorem 2 and Theorem 3, we can conclude that HME represents the **optimal** protocol for exponentiating certain Hermitian-preserving maps, including the identity map $\mathcal{I}$ and the inverse map of local amplitude damping noise $(\mathcal{E}_\gamma^{\otimes n})^{-1}$.

IV. ENTANGLEMENT DETECTION AND QUANTIFICATION

One direct application of HME lies in entanglement detection and quantification, as positive maps are Hermitian-preserving. In entanglement detection, we incorporate HME into the quantum phase estimation algorithm [1, 21], as shown in Fig. 1(d), to propose a new entanglement detection protocol. We demonstrate through an example that the HME-based protocol can offer **exponential advantages** compared to all single-copy approaches.

Theorem 4 (Informal)**.** *The HME-based protocol requires at most $\mathcal{O}(1)$ copies of ρ to accomplish an entanglement detection task with a success probability of at least $2/3$. In contrast, all single-copy approaches require $\Omega(d^{1/4})$ copies of ρ to achieve the same task with a success probability of at least $2/3$.*

Moreover, by combining the HME and Hadamard test algorithm [22], as illustrated in Fig. 1(e), we develop the **first** protocol to unbiasedly estimate entanglement negativity $N(\rho)$. Compared to the tomography-based protocol which has sample complexity $\theta(\epsilon^{-2}d^4)$, HME-based protocol has sample complexity at most $\widetilde{\mathcal{O}}(\epsilon^{-3}d^3)$. Additionally, the HME-based protocol exhibits an exponential advantage in terms of classical memory requirements.

Theorem 5. *One needs an expected number of $\widetilde{\mathcal{O}}\left(\log(\delta^{-1})\epsilon^{-3}d^2d_A\left\|\rho^{T_A}\right\|_1\right)$ copies of ρ to ensure $\left|\hat{N}(\rho)-N(\rho)\right| \leq \epsilon$ with a probability of at least $1-\delta$. Here, the $\widetilde{\mathcal{O}}$ notation suppresses logarithmic expressions for d and ϵ. Besides, the sampling times scales as $M = \mathcal{O}\left(\log(\delta^{-1})\epsilon^{-2}d\left\|\rho^{T_A}\right\|_1\right)$, and the copies of ρ needed in a single run of circuit in Fig. 1(e) when setting $t=(2l-1)$ scales as $K(l)=\widetilde{\mathcal{O}}(\epsilon^{-1}dd_Al)$.*

V. MANAGING QUANTUM NOISES

Building upon HME, we propose a new protocol to handle quantum noises named *quantum noiseless state recovery*. This protocol enables the recovery of a noiseless state from multiple copies of noisy states, given that the description of the noise channel is known.

We consider a similar setting as quantum error mitigation, where the ideal noiseless state ψ is generated by an ideal noiseless circuit, $\psi = \mathcal{U}(|0\rangle\langle 0|)$, while the existence of noise will change it to $\mathcal{E}(\psi) = \mathcal{E}\circ\mathcal{U}(|0\rangle\langle 0|)$. By sequentially inputting multiple copies of $\mathcal{E}(\psi)$ into the circuit depicted in Fig. 1(c) and choosing an appropriate Hamiltonian, we can approximately realize the evolution of $e^{-i\mathcal{E}^{-1}\circ\mathcal{E}(\psi)t} = e^{-i\psi t}$ with arbitrary accuracy. Using the circuit depicted in Fig. 1(f), we can extract the noiseless state ψ from the evolution $e^{-i\psi\pi}$.

Theorem 6. *Let $\mathcal{E}$ be an invertible noise map. Denote $H_{\mathcal{E}^{-1}} := \Lambda^{T_1}_{\mathcal{E}^{-1}}$ as the Hamiltonian corresponding to the inverse noise channel, and let $F := \langle\psi|\,\sigma\,|\psi\rangle$ be the fidelity between $|\psi\rangle\langle\psi|$ and σ. Then we need at most $\mathcal{O}\left(\log(\delta^{-1})\epsilon^{-1}F^{-2}\|H_{\mathcal{E}^{-1}}\|_\infty^2\right)$ copies of $\mathcal{E}(|\psi\rangle\langle\psi|)$ to approximately produce $|\psi\rangle\langle\psi|$ with trace distance smaller than ϵ and a success probability at least $1-\delta$.*

In contrast to existing methods such as quantum error mitigation and quantum error correction, our protocol can recover the desired noiseless state from multiple noisy states, establishing a new approach for combating quantum noises. Compared to quantum error mitigation, our protocol has the ability to **recover noiseless states**, at the expense of a deeper circuit. Additionally, compared to quantum error correction, our protocol requires fewer ancilla qubits and does not necessitate access to the noiseless state at the beginning.

VI. DISCUSSION

HME has potential in other scenarios, as listed in Fig. 1(b). Utilizing the Hermitian-preserving map $\mathcal{N}_O(\rho) = \mathrm{Tr}(O\rho)\,|1\rangle\langle 1|$, HME enables the encoding of expectation values into relative phases of reference states. One can then measure the reference state to extract the value of $\mathrm{tr}(O\rho)$. This HME-based phase encoding operation may also exhibit some advantages for other applications such as gradient estimation [23, 24]. Consider maps of the form $\mathcal{N}(\rho) = P\rho P^\dagger$, where P can be an arbitrary rectangular matrix. In the task of linear combination of unitaries [25], the matrix P is chosen as the sum of several unitaries, allowing for producing an arbitrary pure state or realizing a desired Hamiltonian evolution. Additionally, in quantum imaginary time evolution [26–28], P is set as $e^{-\beta H}$, where β represents the inverse temperature and H is a Hamiltonian. By increasing β, one can prepare a pure state that approximates the ground state of H to arbitrary precision.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[2] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).

[3] O. Gühne and G. Tóth, Entanglement detection, Physics Reports **474**, 1 (2009).

[4] G. Vidal and R. F. Werner, Computable measure of entanglement, Phys. Rev. A **65**, 032314 (2002).

[5] J. Gray, L. Banchi, A. Bayat, and S. Bose, Machine-learning-assisted many-body entanglement measurement, Phys. Rev. Lett. **121**, 150503 (2018).

[6] Y. Zhou, P. Zeng, and Z. Liu, Single-copies estimation of entanglement negativity, Phys. Rev. Lett. **125**, 200502 (2020).

[7] A. Elben, R. Kueng, H.-Y. R. Huang, R. van Bijnen, C. Kokail, M. Dalmonte, P. Calabrese, B. Kraus, J. Preskill, P. Zoller, and B. Vermersch, Mixed-state entanglement from local randomized measurements, Phys. Rev. Lett. **125**, 200501 (2020).

[8] S. Endo, Z. Cai, S. C. Benjamin, and X. Yuan, Hybrid quantum-classical algorithms and quantum error mitigation, Journal of the Physical Society of Japan **90**, 032001 (2021).

[9] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, Quantum error mitigation, arXiv:2210.00921 (2022).

[10] K. Temme, S. Bravyi, and J. M. Gambetta, Error mitigation for short-depth quantum circuits, Phys. Rev. Lett. **119**, 180509 (2017).

[11] S. Endo, S. C. Benjamin, and Y. Li, Practical quantum error mitigation for near-future applications, Phys. Rev. X **8**, 031027 (2018).

[12] Y. Guo and S. Yang, Quantum error mitigation via matrix product operators, PRX Quantum **3**, 040313 (2022).

[13] P. Horodecki and A. Ekert, Method for direct detection of quantum entanglement, Phys. Rev. Lett. **89**, 127902 (2002).

[14] J. K. Korbicz, M. L. Almeida, J. Bae, M. Lewenstein, and A. Acín, Structural approximations to positive maps and entanglement-breaking channels, Phys. Rev. A **78**, 062105 (2008).

[15] D. Petz, Sufficient subalgebras and the relative entropy of states of a von neumann algebra, Communications in Mathematical Physics **105**, 123 (1986).

[16] A. Gilyén, S. Lloyd, I. Marvian, Y. Quek, and M. M. Wilde, Quantum algorithm for petz recovery channels and pretty good measurements, Phys. Rev. Lett. **128**, 220502 (2022).

[17] Q. Dong, M. T. Quintino, A. Soeda, and M. Murao, Implementing positive maps with multiple copies of an input state, Phys. Rev. A **99**, 052352 (2019).

[18] S. Lloyd, M. Mohseni, and P. Rebentrost, Quantum principal component analysis, Nature Physics **10**, 631 (2014).

[19] M. Kjaergaard, M. E. Schwartz, A. Greene, G. O. Samach, A. Bengtsson, M. O'Keeffe, C. M. McNally, J. Braumüller, D. K. Kim, P. Krantz, M. Marvian, A. Melville, B. M. Niedzielski, Y. Sung, R. Winik, J. Yoder, D. Rosenberg, K. Obenland, S. Lloyd, T. P. Orlando, I. Marvian, S. Gustavsson, and W. D. Oliver, Demonstration of density matrix exponentiation using a superconducting quantum processor, Phys. Rev. X **12**, 011005 (2022).

[20] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, *et al.*, Quantum advantage in learning from experiments, Science **376**, 1182 (2022).

[21] A. Y. Kitaev, Quantum measurements and the abelian stabilizer problem, quant-ph/9511026 (1995).

[22] E. Knill and R. Laflamme, Power of one bit of quantum information, Phys. Rev. Lett. **81**, 5672 (1998).

[23] A. Gilyén, S. Arunachalam, and N. Wiebe, Optimizing quantum optimization algorithms via faster quantum gradient computation, in *Proceedings of the 2019 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)* (Society for Industrial and Applied Mathematics, 2019) pp. 1425–1444.

[24] W. J. Huggins, K. Wan, J. McClean, T. E. O'Brien, N. Wiebe, and R. Babbush, Nearly optimal quantum algorithm for estimating multiple expectation values, Phys. Rev. Lett. **129**, 240501 (2022).

[25] A. Childs and N. Wiebe, Hamiltonian simulation using linear combinations of unitary operations, Quantum Information and Computation **12** (2012).

[26] S. Lu, M. C. Bañuls, and J. I. Cirac, Algorithms for quantum simulation at finite energies, PRX Quantum **2**, 020321 (2021).

[27] D.-B. Zhang, G.-Q. Zhang, Z.-Y. Xue, S.-L. Zhu, and Z. D. Wang, Continuous-variable assisted thermal quantum simulation, Phys. Rev. Lett. **127**, 020502 (2021).

[28] M. Motta, C. Sun, A. T. K. Tan, M. J. O'Rourke, E. Ye, A. J. Minnich, F. G. S. L. Brandão, and G. K.-L. Chan, Determining eigenstates and thermal states on a quantum computer using quantum imaginary time evolution, Nature Physics **16**, 205 (2020).

Integrated spin-wave quantum memory

Zong-Quan Zhou[1] *

[1] *CAS key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China*

Abstract. Optical quantum memory is an essential component for overcoming channel losses in large-scale quantum networks. Now, quantum memories are marching toward miniaturization and integration for large-scale practical applications. I will introduce the state-of-the-art technologies for fabricating integrated quantum memories in rare-earth ions doped crystals [1]. Several achievements from our group will be highlighted, including telecom integrated quantum memories for applications in quantum repeaters [2,3,4], and the integrated spin-wave quantum memories for applications in transportable quantum memories [5,6].

Keywords: quantum memories, quantum repeaters, spin-wave storage

An optical quantum memory is a device that can store photonic quantum information and release it after a controlled time. It is an essential component for overcoming channel losses in large-scale quantum networks. Optical quantum memories have been demonstrated with various physical systems including atomic gases, single atoms in optical cavities, and rare-earth-ion doped solids. Now, quantum memories are marching toward miniaturization and integration for large-scale practical applications. Solid state systems stand as a natural choice due to the physical stability and ease of micro or nano fabrication using well-established techniques. In the past decade, considerable efforts have been devoted to developing photonic integrated quantum memories, that is, quantum memories based on micro/nano-photonic structures manufactured in solids. Remarkable performances have been achieved with integrated quantum memories, with the advantages of lower laser/electric power requirements, small volumes, large storage densities, and easy implementations. In our recent review [1], the basic concepts of optical quantum memories, the state-of-the-art technologies for fabricating integrated quantum memories in rare-earth ions doped crystals, and recent advances are introduced, and the roadmap for developing practically useful devices for applications in quantum networks is discussed.

In particular, I will introduce our recent achievements in two aspects. First, for applications in quantum repeaters [2], we have developed integrated quantum memories at the telecom wavelength using Erbium based material. On-demand storage of photonic qubits [3] and tunable single photon emitter [4] are both demonstrated at the telecom C band. Second, for applications in transportable quantum memories [5], we have developed integrated spin-wave quantum memories using Europium based material [6]. Qubits encoded with single-photon-level inputs are stored as the spin-wave excitation with a fidelity of 94.9 (1.2)%, which is far beyond the maximal fidelity that can be obtained with any classical device. The latest achievements in long-lived spin-wave quantum storage will also be discussed.

References

[1] Z. Q. Zhou, et al., Photonic Integrated Quantum Memory in Rare-Earth Doped Solids. *Laser and Photonics Reviews* 17, 2300257 (2023)

[2] X. Liu, et al., Heralded entanglement distribution between two absorptive quantum memories. *Nature* 594, 41 (2021)

[3] D. C. Liu, et al., On-Demand Storage of Photonic Qubits at Telecom Wavelengths. *Phys. Rev. Lett.* 129, 210501 (2022)

[4] J. Y. Huang, et al., Stark Tuning of Telecom Single-Photon Emitters Based on a Single Er3+ *Chin. Phys. Lett.* 40, 070301 (2023)

[5] Y. Ma, et al., One-hour coherent optical storage in an atomic frequency comb memory. *Nature Communications* 12, 2381 (2021)

[6] T. X. Zhu, et al., Integrated spin-wave quantum memory. *National Science Review* nwae161 (2024), https://doi.org/10.1093/nsr/nwae161

*zq_zhou@ustc.edu.cn

Experimental Quantum State Tomography of Multimode Gaussian States

Chan Roh[1] * Geunhee Gwak[1] Young-Do Yoon[1] Young-Sik Ra[1]

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*

Abstract. We report a quantum state tomography method which can reliably reconstruct multimode Gaussian states. Our method is free from the issue of yielding a non-physical quantum state and exhibits higher reconstruction fidelity than the conventional method. Moreover, we experimentally reconstruct the covariance matrix of the multimode Gaussian states by the method and decompose the covariance matrix to extract full information of the thermal noise and the mulitimode squeezing inside the state.

Keywords: Quantum state tomography, Gaussian state, Maximum-likelihood estimation

A multimode Gaussian state is an essential quantum resource for quantum information processing in continuous variable systems, offering large-scale entanglement in a deterministic manner [1]. Many experimental studies have realized a multimode Gaussian state for quantum computation, quantum communication, and quantum sensing. Moreover, the generation of multimode Gaussian states paves a way to study multimode quantum systems, such as multipartite entanglement. Therefore, to certify generation and investigate quantum features of the multimode Gaussian state, we need to fully characterize the states by quantum state tomography [2].

Quantum state tomography in continuous-variable mostly reconstructs the density operator of the target state by quadrature measurement [3]. However, obtaining density operators of multimode Gaussian states is challenging since the dimension of a density operator grows exponentially with increasing mode number. Fortunately, we can also obtain complete information on the multimode Gaussian state by obtaining the covariance matrix of the state [1]. The dimension of the covariance matrix is proportional to the square of the system size, so reconstructing a covariance matrix is the efficient method for quantum state tomography of the multimode Gaussian state.

The conventional method for reconstructing the covariance matrix is achieved by directly estimating the covariance of quadrature operators from homodyne measurement. Through this direct method, the full covariance matrix of the two-mode squeezed state [4] and some part of the covariance matrix (without $\hat{x}\hat{p}$ correlation) of the 8-mode and 16-mode Gaussian state [5] are obtained experimentally. However, reconstructing full covariance matrices of multimode Gaussian states has remained elusive in experiments. In addition, the direct method can simply acquire the covariance matrix, but statistical errors from a finite number of data reduce fidelity. Even worse, the errors would make the resultant covariance matrix not satisfy the uncertainty principle, which means that the result is unphysical. As for the unphysical consequences, we are unable to analyze the multimode Gaussian state through the covariance matrix.

In this work, we develop an efficient quantum state tomography method for multimode Gaussian states by reconstructing full and physical covariance matrices of the states. We parameterize the covariance matrices to satisfy the uncertainty principle and update the parameters by maximum likelihood estimation (MLE) through quadrature data. The data are gathered from single mode homodyne detection after mode mixer. To substantiate the effectiveness of our method, we conduct benchmarks of the MLE method against the conventional direct reconstruction of covariance matrices. The outcomes of the MLE method always satisfy the uncertainty principle in a limited number of data, while the direct method often fails to satisfy the physical condition. Moreover, our method reconstructs covariance matrices more precisely than the direct method for various target states. These shows that the MLE method can effectively conduct quantum state tomography for multimode Gaussian states.

Our MLE method (Fig. 1) starts with parameterizing a covariance matrix. A covariance matrix $\boldsymbol{V}$ of an M-mode Gaussian state can be decomposed as [7]

$$\boldsymbol{V} = \boldsymbol{S}\mathrm{diag}(\boldsymbol{\lambda},\boldsymbol{\lambda})\boldsymbol{S}^T, \tag{1}$$

where $\boldsymbol{S}$ is a $2M \times 2M$ symplectic matrix, and $\boldsymbol{\lambda} = (\lambda_1, ..., \lambda_M)$. The uncertainty principle for the covariance matrix

$$\boldsymbol{V} + i\boldsymbol{\Omega} \geq 0, \quad \boldsymbol{\Omega} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{I} \\ -\boldsymbol{I} & \boldsymbol{0} \end{bmatrix} \tag{2}$$

is translated to constraints for symplectic eigenvalues $\lambda_m \geq 1$, which can be parameterized as $\lambda_m = \kappa_m^2 + 1$

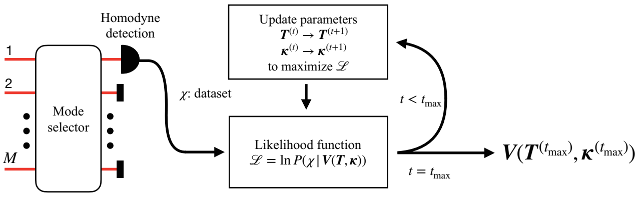

Homodyne detection
1
2
M
Mode selector
χ: dataset
Update parameters
$\boldsymbol{T}^{(t)} \rightarrow \boldsymbol{T}^{(t+1)}$
$\boldsymbol{\kappa}^{(t)} \rightarrow \boldsymbol{\kappa}^{(t+1)}$
to maximize $\mathscr{L}$
Likelihood function
$\mathscr{L} = \ln P(\chi \mid \boldsymbol{V}(\boldsymbol{T},\boldsymbol{\kappa}))$
$t < t_{\max}$
$t = t_{\max}$
$\boldsymbol{V}(\boldsymbol{T}^{(t_{\max})}, \boldsymbol{\kappa}^{(t_{\max})})$

Figure 1: Illustration of the maximum-likelihood estimation method for quantum state tomography of multimode Gaussian state.

[*] croh@kaist.ac.kr

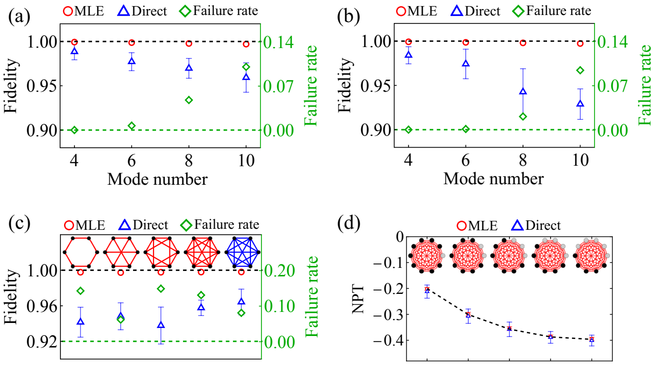


Figure 2: (a) and (b) are performances of MLE and direct reconstruction method depending on the mode number of target states, GHZ state (a), and completely connected cluster state (b), respectively. (c) Performance for various six-mode Gaussian states. The red graphs and the blue graph indicate cluster states and a six-mode GHZ state, respectively. Green points show failure probability of the direct reconstruction method from 1,000 repetitions. We set sampling per measured mode number $N_s = 10,000$. (d) Bipartite entanglement test of 10-mode completely connected cluster state. Reconstructed matrices are used to test entanglement between two subsets (black and white).

for $\kappa_m \in \mathbf{R}$. We parameterize the symplectic matrix $\boldsymbol{S}$ as

$$\boldsymbol{S} = (\boldsymbol{I} + \boldsymbol{\Omega T}/2)(\boldsymbol{I} - \boldsymbol{\Omega T}/2)^{-1}, \tag{3}$$

where $\boldsymbol{T}$ is a $2M \times 2M$ real symmetric matrix. In this way, we can parameterize any multimode covariance matrix under physical constraints. Next, the MLE method updates the parameters $\boldsymbol{T}$ and $\boldsymbol{\kappa} = (\kappa_1, ..., \kappa_M)$. Let us set χ as the dataset of whole measurement results, which contains quadrature data from homodyne measurements in single mode and superposed mode. The dataset χ is used for calculating log-likelihood function $\mathcal{L} = \ln P(\chi|\boldsymbol{V}(\boldsymbol{T}, \boldsymbol{\kappa}))$, which means the logarithm of the conditional probability that χ measured in the Gaussian state with covariance matrix $\boldsymbol{V}(\boldsymbol{T}, \boldsymbol{\kappa})$. The parameters are updated to maximize the likelihood function by the likelihood function by the gradient ascent method.

We further highlight the advantages of our MLE method over the conventional direct reconstruction method for obtaining covariance matrices of multimode Gaussian state. To compare the performances of both methods, we set target multimode Gaussian states and generate measurement data by simulation. We compare the results of reconstructing covariance matrices by the MLE method and the conventional direct. Figure 2(a-b) shows the fidelities of the reconstructed result of MLE and direct method for GHZ states (a) and completely-connected cluster states (b). As the number of modes increases, the fidelity of the direct method decreases. However, the MLE method shows high fidelities close to one. In addition, we compare both methods for various six-mode Gaussian states in Fig. 2 (c). The MLE method outperforms the direct method in terms of fidelity.

Moreover, we implement entanglement test of the 10-mode completely connected cluster state by using reconstructed covariance matrices from MLE method and direct method. Ten modes were divided into two subsets, and the separability between each subset was investigated using Peres-Horodecki separability criterion for continuous variable systems [6]. In Fig. 2 (d), black and white vertexes of the graphs denote biparitite subsets, and the results of test is plotted as red (MLE method) and blue (direct method) dots. MLE method reconstructs covariance matrix of the 10-mode cluster state more precisely, so that make the results of the inseparability test more close to the theoretical values (black line).

Reconstructed covariance matrices can be used for analyzing multimode Gaussian states. Gaussian state can be decomposed by sequence of multimode thermal noise and squeezing operation on the vacuum state, as Fig. 3 (a). If we know the thermal noise and squeezing modes and their respective degrees, we can perfectly understand the Gaussian state that we obtain. In this way, we have analyzed the ten-mode Gaussian state with the covariance matrix obtained through the experiment. We experimentally generate a 10-mode completely connected cluster state and reconstruct its covariance matrix by the MLE method (Fig. 3 (b)). The reconstructed covariance matrix is already expressed by Williamson decomposition as Eq.(1), and we can decompose the symplectic matrix $\boldsymbol{S}$ as

$$\boldsymbol{S} = \boldsymbol{O}_1 \boldsymbol{D}_s \boldsymbol{O}_2 \tag{4}$$

based on Bloch-Messiah decomposition [8]. $\boldsymbol{O_1}$ and $\boldsymbol{O_2}$ are orthogonal symplectic matrices, $\boldsymbol{D}_s = \mathrm{diag}(e^{-r}, ..., e^{-r}, e^{r}, ..., e^{r})$ is the symplectic matrix for the squeezing operation, and r is the squeezing parameter. If we set $\boldsymbol{O}_s = \boldsymbol{O}_1$ and $\boldsymbol{O}_t = \boldsymbol{O}_s\boldsymbol{O}_2$, then the covariance matrix is expressed as

$$\boldsymbol{V} = \boldsymbol{O}_s \boldsymbol{D}_s \boldsymbol{O}_s^T \boldsymbol{O}_t \boldsymbol{\Lambda} \boldsymbol{O}_t^T \boldsymbol{O}_s^T \boldsymbol{D} \boldsymbol{O}_s. \tag{5}$$

O_s and O_t correspond to the multimode linear operations for squeezing modes ($\hat{O}_s$) and thermal noise modes ($\hat{O}_t$) in Fig. 3 (a), respectively. These decomposition elements (5) let us know the thermal noise and squeezing modes and their respective degrees.

Figure 3 (c) shows the thermal noise (up, purple) and squeezing (down, light blue) inside the 10-mode cluster state. Thermal photon number is obtained by $n_m^{\mathrm{th}} = (\lambda_m - 1)/2$, and squeezing level is $10\log_{10}e^{-2r}$. Plus, modes containing each thermal noise (squeezing) can be obtained from $\boldsymbol{O}_t$. $\boldsymbol{O}_t$ is the orthogonal symplectic matrix, so it can be expressed as

$$\boldsymbol{O}_t = \begin{bmatrix} \boldsymbol{X}_t & -\boldsymbol{Y}_t \\ \boldsymbol{Y}_t & \boldsymbol{X}_t \end{bmatrix}. \tag{6}$$

Rows of $\boldsymbol{X}_t - i\boldsymbol{Y}_t$ are the thermal noise (squeezing) modes, and the intensity and phase information of each mode is shown at Fig. 3 (d). Similarly, Fig. 3 (e) shows the squeezing modes obtained from $\boldsymbol{O}_s$.

In this work, we develop an efficient quantum state tomography method for multimode Gaussian states by

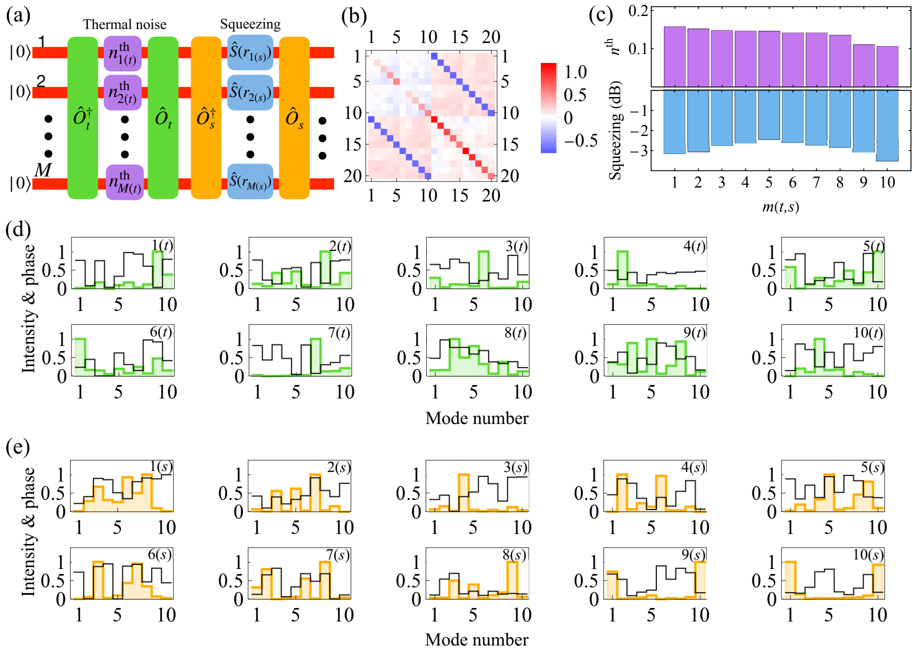


Figure 3: (a) Decomposition of a multimode Gaussian state. Subscripts t and s indicates thermal noise mode and pure squeezing mode, respectively. (b) Experimentally reconstructed covariance matrix of 10-mode completely connected cluster state. Identity matrix is subtracted to remove vacuum noise. (c) Mean photon number of thermal noise (up) and squeezing level (down) of each mode. (d) Thermal noise modes and (e) Pure squeezing mode. Each graph shows the mode in which thermal noise and squeezing operation corresponding to (b) is contained.

reconstructing full and physical covariance matrices of the states. We parameterize the covariance matrices to satisfy the uncertainty principle and update the parameters by maximum likelihood estimation (MLE) through quadrature data. The data are gathered from single mode homodyne detection after mode mixer. To substantiate the effectiveness of our method, we conduct benchmarks of the MLE method against the conventional direct reconstruction of covariance matrices. The outcomes of the MLE method always satisfy the uncertainty principle in a limited number of data, while the direct method often fails to satisfy the physical condition. Moreover, our method reconstructs covariance matrices more precisely than the direct method for various target states. These shows that the MLE method can effectively conduct quantum state tomography for multimode Gaussian states.

We have implemented the multimode quantum state tomography of multimode Gaussian state experimently by the MLE method. We reconstruct the covariance matrix of the 10-mode cluster state and analyze the state by the covariance matrix. We decompose the covariance matrix and extract full information of thermal noise and multimode squeezing inside the state.

Our MLE method will be valuable quantum state tomography method for multimode Gaussian state. Since the MLE method is able to reconstruct covariance matrices of Gaussian state precisely, we can implement analysis for multimode Gaussian states based on covariance matrices, e.g., quantum entanglement test, steering test, calculating quantum fisher information, etc. We expect that the MLE method will facilitate future studies to uncover multimode CV quantum systems.

References

[1] C. Weedbrook *et al.*, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[2] A. I. Lvovsky and M. G. Raymer, Continuous-variable optical quantum-state tomography, Rev. Mod. Phys. **81**, 299 (2009).

[3] A. I. Lvovsky, Iterative maximum-likelihood reconstruction in quantum homodyne tomography, J. Opt. B: Quantum Semiclass. Opt. **6**, 6 (2004).

[4] V. D'Auria *et al.*, Full characterization of Gaussian bipartite entangled states by a single homodyne detector, Phys. Rev. Lett. **102**, 020502 (2009).

[5] Y. Cai *et al.*, Multimode entanglement in reconfigurable graph states using optical frequency combs, Nat. Commun. **8**, 15645 (2017).

[6] R. Simon. Peres-Horodecki separability criterion for continuous variable systems. Phys. Rev. Lett. **84**, 2726 (2000)

[7] J. Williamson, American journal of mathematics **58**, 141–163 (1936)

[8] C. Bloch, and A. Messiah, Nuclear Physics **39**, 95–106 (1962).

Long-distance entanglement-sharing using optical hybrid states between discrete and continuous variables

Soumyakanti Bose[1] * Jaskaran Singh[2 3] † Adán Cabello[2] ‡ Hyunseok Jeong [1] §

[1] *Department of Physics & Astronomy, Seoul National University, Gwanak-ro 1, Gwanak-gu, Seoul 08826, Korea*
[2] *Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[3] *Department of Physics and Center for Quantum Frontiers of Research & Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*

Abstract. We introduce a feasible scheme [arXiv:2305.189006v4] to produce high-rate long-distance entanglement using hybrid-entangled (HE) states between continuous variables (CV) and discrete variables (DV). The key idea is to yield a DV-entangled pair between distant locations by adjusting the CV part to be robust against transmission losses. We also benchmark the shared entanglement in an entanglement-based (EB) quantum key distribution (QKD) protocol. Our results show that HE-states enables EB-QKD with standard telecommunication fibers for 300 km promising an alternative tool for practical long-distance entanglement-sharing that provides a testbed for further applications in quantum information processing.

Keywords: Hybrid states, entanglement sharing, quantum communication.

1 Introduction

Generation of high-rate entanglement between distant locations is crucial for fundamental tests of quantum theory as well as various information processing tasks such as loophole-free Bell tests [1, 2], quantum teleportation [3], device-independent (DI) quantum-key-distribution (QKD) protocol [4, 5, 6]. It also allows to achieve higher detection efficiencies, a crucial requirement in both loophole-free Bell tests and DI-QKD, by means of heralded qubit amplifiers [7] or photonic precertification schemes [8, 9], whose practicality is currently limited by the rates achieved after transmission.

An operational benchmark of the shared entanglement can be set by its performance in a practical task such as, however not limited to, an entanglement-based (EB) QKD protocol. These protocols are traditionally analyzed using two different kinds of physical systems, namely discrete variable (DV) and continuous variable (CV) systems only, which offer their own set of advantages and limitations [10, 11, 12]. Alongside remarkable sucesses with these systems [13, 14, 15], despite an extensive theoretical and experimental analysis, the quest for an optimal physical system to potentially use for sharing high-rate long-distance entanglement still remains open.

Nonetheless, there exists a different class of physical states, with cross-system entanglement between CV and DV systems, which are formally known as hybrid entangled (HE) states [16, 17]. However, despite their generation in a wide range of experimental setups [18, 19, 20] and importance in quantum information science and technology [21, 30, 23, 24, 25, 26], such states remain largely unexplored.

Here, by harnessing these strongly correlated HE states [27, 28, 29], we propose an altenate scheme for sharing high-rate entanglement. We show that two parties who are hundreds of kms apart, can efficiently generate a DV entangled-pair by exploiting entanglement-swapping [30] over the respective CV parts by a third party in the midway. We further access the operationally significance of our HE-state based scheme for long-distance entanglement-sharing in a practical information processing task such EB-QKD with the shared DV entanglement.

Our results indicate that the HE-states enables to achieve secure key rate at a distance of 300 km with practical homodyne detectors (55% efficiency) and on-off detectors (80% efficiency) [31], at telecommunication wavelength (check [31] for further detail). While the long transmission distance stems from the robustness of the coherent state against transmission losses, our scheme offers two major advantages such as (i) elimination of major limiting factors of DV EB-QKD, which include high precision Bell-state-measurement as well as the photon-number-splitting attack by by considering entanglement swapping over the CV system and (ii) elimination of the requirement of near-unit efficiency for the homodyne detectors in CV EB-QKD.

2 Entanglement-sharing with hybrid states

2.1 Hybrid states:

Let $|n\rangle$ and $|\alpha\rangle$ represent to the photon-number-states (PNS) and a coherent state of a quantized light respectively. For the remainder of this paper we denote the PNS as the DV system and the coherent state as the CV system. As a consequence, an HE state is defined [16, 17] as an entangled pair between the DV and CV systems as

$$|\psi\rangle_{a_1a_2} = \frac{1}{\sqrt{2}}\left(|0\rangle_{a_1}|\alpha\rangle_{a_2} + |1\rangle_{a_1}|-\alpha\rangle_{a_2}\right), \qquad (1)$$

where a_1 and a_2 are the two modes pertaining to the DV and CV parts, respectively. Kindly check the [31] for further discussion on the generation of such states.

*soumyakanti.bose09@gmail.com
†jsinghiiser@gmail.com
‡adan@us.es
§h.jeong37@gmail.com

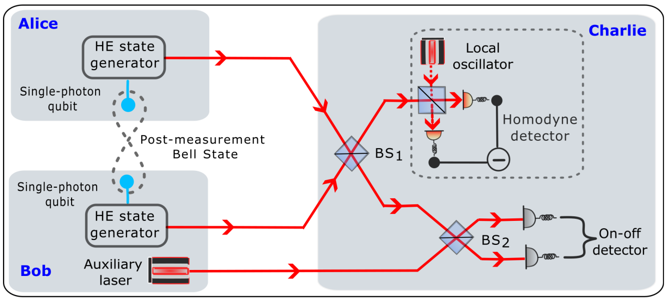


Figure 1: Schematic for generating DV entangled states between Alice and Bob using HE states. Alice and Bob send their CV parts to Charlie, who then mixes the incoming signals at a balanced beam splitter (BS), say BS$_1$. He then mixes one of output signals of (BS$_1$) with the additional coherent signal sent by Bob at a second BS, say BS$_2$, followed by a joint measurement implemented by on-off detectors. The remaining output signal of BS$_1$ is then subjected to homodyne detection. Upon declaration of the results by Charlie, Alice and Bob obtain a DV entangled pair.

2.2 Protocol for entanglement sharing:

Let us consider that two distant parties, say Alice and Bob, each of them having access to bipartite HE-states $|\psi\rangle_{a_1a_2}$ and $|\psi\rangle_{b_1b_2}$ given by Eq. (1). Our scheme for entanglement-sharing, as schematically represented in Fig. 1 (a), (see [31] for detail) proceeds as described below

Step 1: Alice and Bob transmit their CV parts (corresponding to modes a_2 and b_2 respectively) to a third untrusted party, say Charlie, through a lossy quantum channel with transmittance T $(0 \leq T \leq 1)$. Additionally, Bob also sends another coherent state, $|\sqrt{2}\alpha\rangle$, to Charlie separately through a similar quantum channel.

We quantify the impact of the loss in the transmission channel on the HE-states by considering the output entanglement, measured by logarithmic negativity, in Fig. 2, where $0 \leq R \leq 1$ stand for the normalised loss-parameter. We observe that there exists an optimal value of α for a fixed value of photon loss which, in the case of a significantly lossy channel, approaches $\alpha = 0.5$. This behaviour of HE states can be qualitatively understood in terms of the interplay between entanglement and the fragility of the initial HE-state [31].

Step 2: Next, Charlie mixes the two incoming modes via a beam splitter (BS), labelled as BS$_1$. He, then further mixes one of the output modes of BS$_1$ with the additional coherent state, sent by Bob, though a second BS (BS$_2$). Subsequently, he now performs a joint projective measurements on the output of BS$_2$ implemented by on-off detectors and declares the outcome (check [31] for detail). The protocol continues only in the case when both the detectors click, otherwise the parties start afresh.

Step 3: After a successful projective measurement, Charlie now performs a homodyne measurement on the residual output of BS$_1$ announces the results publicly.

Step 4: After receiving of the results of a successful projective measurement and the homodyne measurement by Charlie, Alice and Bob end up with the final normalized single-photon-Bell-state in modes a_1 and b_1 as

$$\rho_{a_1b_1} = \frac{1}{2}\left[\begin{array}{l}|01\rangle\langle 01| + |10\rangle\langle 10| \\ \quad + h\left(g\,|01\rangle\langle 10| + g^*\,|10\rangle\langle 01|\right)\end{array}\right] \quad (2)$$

with probability $P_0 = \frac{\left(1-e^{-\eta_o T\alpha^2}\right)^2}{2}$, where $h = e^{-4(1-T\eta_h)\alpha^2}$, $g = e^{4\mathrm{i}\sqrt{T\eta_h}\alpha p}$ and p is the result of the homodyne measurement. η_h and η_0 are the efficiencies of the homodyne detector and the on-off detectors respectively.

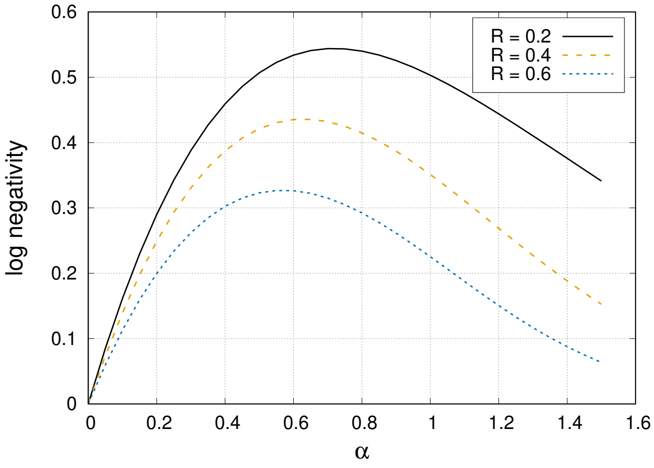


Figure 2: Logarithmic negativity of the HE state undergoing photon-loss over the CV part as a function of the coherent amplitude α.

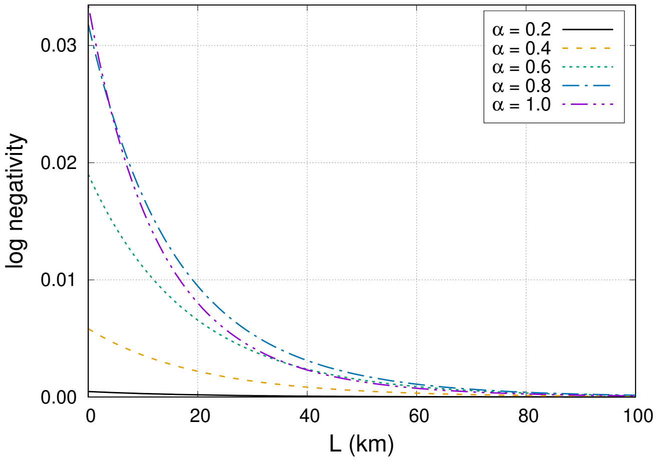


Figure 3: Logarithmic negativity of the state $\rho_{a_1b_1}$ as a function of the transmission distance (L) for different values of coherent amplitude α. We assume $p = \frac{\pi}{2}$.

3 Simulation results on shared entanglement

The final shared entanglement depends on a number of parameters such as the channel transmittance $T = 10^{-l\frac{L/2}{10}}$, where $l = 0.2$ dB/km (standard channel loss at telecommunication wavelength [11]) and L is the

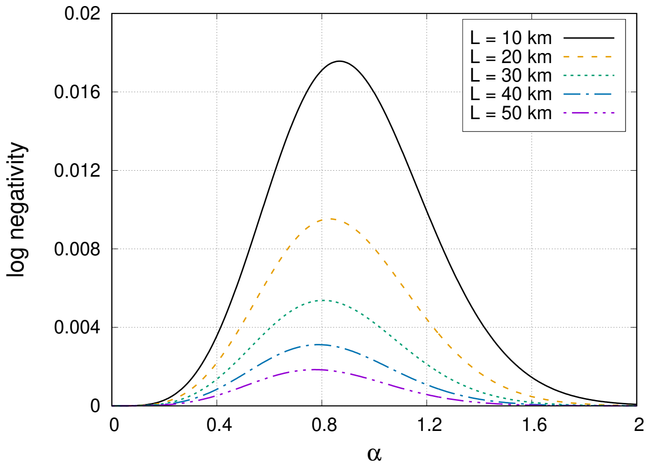


Figure 4: Logarithmic negativity of the state $\rho_{a_1b_1}$ as a function of the transmission distance L for different values of coherent amplitude α. We consider $p = \frac{\pi}{2}$.

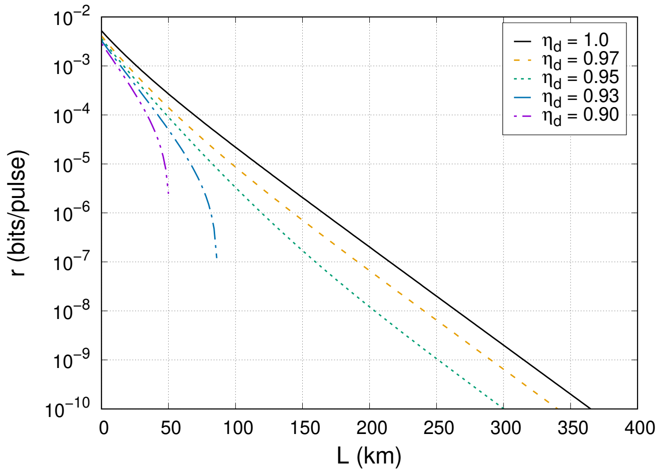


Figure 5: Secure key rate as a function of total transmission distance L for different values of η_d in the optimal case, i.e., $\alpha = 0.5$. $p = \frac{\pi}{2}$.

total transmission distance between Alice and Bob. The detection efficiencies are also set (standard in telecommunication setup) as $\eta_h = 0.55$ and $\eta_0 = 0.8$ [31].

In Figs. 3 and 4 we plot the shared entanglement with the total transmission length (L) and the coherent amplitude (α) respectively. We observe that while the shared entanglement decreases exponentially with L, at a given distance (equivalently loss) there exists an optimal value of α, say α_{opt}. For sufficiently long transmission distance ($L \geq 150$ Km), α_{opt} for sharing entanglement becomes close to 0.5 (not shown in the Fig. 4). It may be noted that, at a given distance, the α_{opt} for shared DV-entanglement may be different than the α_{opt} for the original HE state (Fig. 2).

4 Benchmarking the shared entanglement in EB-QKD

Let us now consider that the efficiency of the single-photon-detectors of Alice and Bob, required for key generation, is given by η_d ($0 \leq \eta_d \leq 1$). With these inefficient detectors, the secure key rate [31] for the shared state (2) is given as

$$\begin{aligned} r &\geq P_0\left[I(A:B) - \chi(A:E)\right] \\ &= P_0\Big\{1 - \eta_d + \frac{1}{2}\left[(1+h)\log_2(1+h) + (1-h)\log_2(1-h)\right] \\ &\quad -\frac{1}{2}\left[(2-\eta_d)\log_2(2-\eta_d) - (1-\eta_d)\log_2(1-\eta_d)\right]\Big\}, \end{aligned} \tag{3}$$

where $I(A:B)$ and $\chi(A:E)$ are the mutual information between Alice and Bob and the Holevo information between Alice and and adversary Eve respectively. For a detail discussion on the assumptions and other requirements kindly look at [31].

Here also, we notice that the optimal value of α that maximizes the secured key rate coincides with the α_{opt} for shared entanglement, i.e., $\alpha = 0.5$ (see [31] for detail). As a consequence, in Fig. 5 we plot the secure key rate as a function of the total transmission distance L for different values of η_d with $\alpha = 0.5$. As it is evident, under low detection errors ($\eta_d = 0.97$ and 0.95), a secure key rate can be achieved for transmission distances around 300 km indicating that the resultant entangled state is useful. However, the maximum achievable distance drastically falls off as η_d is decreased up to $\eta_d = 0.90$ (corresponds to 10% detection error).

5 Conclusion

To summarize, we have proposed a scheme to harness the cross-system correlation in HE-states for sharing long-distance high-rate entanglement that efficiently removes the practical limitations of conventional approaches based on DV only or CV only systems. We have further showcased the efficacy of the shared DV-entanglement in a practical task such as EB-QKD where with a realistic detectors and transmission channel one can obtain a secure key rate of $\sim 10^{-10}$ bits/pulse at a distance of 300 km with 5% detection error at the telecommunication wavelength (1550 nm).

A major limitation of our protocol stems from the non-deterministic generation of the HE states with fidelity ≈ 0.75 for $\alpha = 0.5$ [18]. This could be easily overcome with the use of polarization qubits [32, 33, 34] with a possible deterministic generation of HE-states using quantum walks [35]. It may also be noted that in the current scheme, it is sufficient to consider *loss-only* channel as the general *lossy and noisy* channel closely approximates the former under practical conditions [31].

Nonetheless, current proposal for long-distance entanglement-sharing provides a multipurpose test bed, beyond the paradigm of EB-QKD protocols. This represents HE-states as a promising alternative for practical entanglement distribution that serves as a central core in various information processing applications such as DI-QKD protocols [36], quantum networks [37], network steering [39].

References

[1] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature (London) 526, 682 (2015).

[2] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. Phys. Rev. Lett. 119, 010402 (2017).

[3] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. Nature (London) 489, 269 (2012).

[4] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y. Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal. Experimental quantum key distribution certified by Bell's theorem. Nature (London) 607, 682 (2022).

[5] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C. W. Lim, and H. Weinfurter. A device-independent quantum key distribution system for distant users. Nature 607, 687 (2022).

[6] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan. Toward a photonic demonstration of device-independent quantum key distribution. Phys. Rev. Lett. 129, 050502 (2022).

[7] N. Gisin, S. Pironio, and N. Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. Phys. Rev. Lett. 105, 070501 (2010).

[8] A. Cabello and F. Sciarrino. Loophole-free bell test based on local precertification of photon's presence. Phys. Rev. X 2, 021010 (2012).

[9] E. Meyer-Scott, D. McCloskey, K. Golos, J. Z. Salvail, K. A. G. Fisher, D. R. Hamel, A. Cabello, K. J. Resch, and T. Jennewein. Certifying the presence of a photonic qubit by splitting it in two. Phys. Rev. Lett. 116, 070501 (2016).

[10] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo. Discrete and continuous variables for measurement-device-independent quantum cryptography. Nat. Photonics 9, 772 (2015).

[11] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen. Reply to 'discrete and continuous variables for measurement-device-independent quantum cryptography'. Nat. Photonics 9, 773 (2015).

[12] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan. Practical challenges in quantum key distribution. npj Quantum Inf. 2, 16025 (2016).

[13] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108, 130503 (2012).

[14] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. 117, 190501 (2016).

[15] A. A. Hajomer, H. Q. Nguyen, and T. Gehring. High-rate continuous-variable measurement-device-independent quantum key distribution. 2023 Optical Fiber Communications Conference and Exhibition (OFC) (2023).

[16] H. Jeong. Using weak nonlinearity under decoherence for macroscopic entanglement generation and quantum computation. Phys. Rev. A 72, 034305 (2005).

[17] Y. Li, H. Jing, and M.-S. Zhan. Optical generation of a hybrid entangled state via an entangling single-photon-added coherent state. J. Phys. B: At. Mol. Opt. Phys. 39, 2107 (2006).

[18] H. Jeong, A. Zavatta, M. Kang, S.-W. Lee, L. S. Costanzo, S. Grandi, T. C. Ralph, and M. Bellini. Generation of hybrid entanglement of light. Nat. Photonics 8, 564 (2014).

[19] A. E. Ulanov, D. Sychev, A. A. Pushkina, I. A. Fedorov, and A. I. Lvovsky. Quantum teleportation between discrete and continuous encodings of an optical qubit. Phys. Rev. Lett. 118, 160501 (2017).

[20] D. V. Sychev, A. E. Ulanov, E. S. Tiunov, A. A. Pushkina, A. Kuzhamuratov, V. Novikov, and A. I. Lvovsky. Entanglement and teleportation between polarization and wave-like encodings of an optical qubit. Nat. Commun. 9, 3672 (2018).

[21] Y.-B. Sheng, L. Zhou, and G.-L. Long. Hybrid entanglement purification for quantum repeaters. Phys. Rev. A 88, 022302 (2013).

[22] Y. Lim, J. Joo, T. P. Spiller, and H. Jeong. Loss-resilient photonic entanglement swapping using optical hybrid states. Phys. Rev. A 94, 062337 (2016).

[23] S. Omkar, Y. S. Teo, and H. Jeong. Resource-efficient topological fault-tolerant quantum computation with hybrid entanglement of light. Phys. Rev. Lett. 125, 060501 (2020).

[24] S. Omkar, Y. S. Teo, S.-W. Lee, and H. Jeong. Highly photon-loss-tolerant quantum computing using hybrid qubits. Phys. Rev. A 103, 032602 (2021).

[25] S. Bose and H. Jeong. Quantum teleportation of hybrid qubits and single-photon qubits using Gaussian resources. Phys. Rev. A 105, 032434 (2022).

[26] M. He and R. Malaney. Teleportation of hybrid entangled states with continuous-variable entanglement. Sci. Rep. 12, 17169 (2022).

[27] Z.-B. Chen, G. Hou, and Y.-D. Zhang. Quantum nonlocality and applications in quantum-information processing of hybrid entangled states. Phys. Rev. A 65, 032317 (2002).

[28] K. Park, S.-W. Lee, and H. Jeong. Quantum teleportation between particlelike and fieldlike qubits using hybrid entanglement under decoherence effects. Phys. Rev. A 86, 062301 (2012).

[29] H. Kwon and H. Jeong. Violation of the Bell–Clauser-Horne-Shimony-Holt inequality using imperfect photodetectors with optical hybrid states. Phys. Rev. A 88, 052127 (2013).

[30] Y. Lim, J. Joo, T. P. Spiller, and H. Jeong. Loss-resilient photonic entanglement swapping using optical hybrid states. Phys. Rev. A 94, 062337 (2016).

[31] S. Bose, J. Singh, A. Cabello, H. Jeong. Long-distance entanglement sharing using hybrid states of discrete and continuous variables. arXiv:2305.18906v4 (2024) [accepted in Phys. Rev. Applied].

[32] S. Li, H. Yan, Y. He, and H. Wang. Experimentally feasible generation protocol for polarized hybrid entanglement. Phys. Rev. A 98, 022334 (2018).

[33] K. Huang, H. L. Jeannic, O. Morin, T. Darras, G. Guccione, A. Cavailles, and J. Laurat. Engineering optical hybrid entanglement between discrete and continuous variable states. New J. Phys. 21, 083033 (2019).

[34] J. Wen, I. Novikova, C. Qian, C. Zhang, and S. Du. Hybrid entanglement between optical discrete polarizations and continuous quadrature variables. Photonics 8, 552 (2021).

[35] J. Singh, V. Mittal and S. Bose. Deterministic generation of hybrid entangled states using quantum walks. arXiv:2311.02419 (2023).

[36] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan. Measurement-device-independent quantum key distribution over un-trustful metropolitan network. Phys. Rev. X 6, 011024 (2016).

[37] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. Science 362, eaam9288 (2018).

[38] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan. Experimental quantum digital signature over 102 km. Phys. Rev. A 95, 032334 (2017).

[39] B. D. M. Jones, I. Supi c, R. Uola, N. Brunner, and P. Skrzypczyk. Network quantum steering. Phys. Rev. Lett. 127, 170405 (2021).

Long-distance entanglement sharing using hybrid states of discrete and continuous variables

Soumyakanti Bose,[1, *] Jaskaran Singh,[2, 3, †] Adán Cabello,[2, 4, ‡] and Hyunseok Jeong[1, §]

[1] *Department of Physics & Astronomy, Seoul National University, Gwanak-ro 1, Gwanak-gu, Seoul 08826, Korea*
[2] *Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[3] *Department of Physics and Center for Quantum Frontiers of Research & Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*
[4] *Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain*

We introduce a feasible scheme to produce high-rate long-distance entanglement which uses hybrid entanglement (HE) between continuous variables (CV) and discrete variables (DV). We show that HE can effectively remove the experimental limitations of existing CV and DV systems to produce long range entanglement. We benchmark the resulting DV entangled states using an entanglement-based quantum key distribution (EB-QKD) protocol. We show that, using HE states, EB-QKD is possible with standard telecommunication fibers for 300 km. The key idea is using the CV part, which can be adjusted to be robust against photon losses, for increasing the transmission distance, while using the DV part for achieving high secure key rates. Our results point out that HE states provide a clear advantage for practical long-distance and high-rate entanglement generation that may lead to further applications in quantum information processing.

I. INTRODUCTION

Generation of high-rate entanglement between distant locations is crucial for fundamental tests of quantum theory and many applications. For example, it is needed for extending the current distances and rates of loophole-free Bell tests [1, 2], quantum steering [3], and quantum teleportation [4], which so far are only feasible for relatively short ranges. It is also needed for increasing the transmission distance and the key rate of entanglement-based quantum key distribution (EB-QKD) protocols, most notably device-independent QKD [5–7], which currently suffers from both these issues. Moreover, higher-rates in distant locations will also allow us to achieve higher detection efficiencies (which are needed both for loophole-free Bell tests and device-independent QKD) by means of heralded qubit amplifiers [8] or photonic precertification schemes [9–11], whose practicality is currently limited by the rates achieved after transmission.

A benchmark of high-rate entanglement over long distances, from an operational perspective, can be set by its performance in an information processing task such as an EB-QKD protocol. These protocols can be broadly classified into two distinct classes: (i) those using discrete variable (DV) entangled states and (ii) those that use continuous variable (CV) entangled states, where each class has its own set of advantages and limitations [12–14]. As an example, DV EB-QKD protocols offer composable security proofs with good key rate, but they require precise Bell-state or single-photon measurements at extremely low temperatures, which are hard to perform even in laboratory conditions. On the other hand, CV EB-QKD protocols generally require Gaussian states which are comparatively easier to prepare, but their performance is limited by the requirement of almost ideal homodyne detectors at telecommunication wavelength [13, 15, 16]. As a consequence, despite an extensive theoretical and experimental analysis on both types of systems, the quest for an optimal physical system which can be potentially used to share high-rate entanglement remains open.

Nonetheless, there exists a different class of physical systems where the entanglement is between CV and DV systems and are formally known as hybrid entangled (HE) states [17–22]. These strongly correlated [23–25] cross-system entangled states play a crucial role in various quantum information processing tasks, including quantum computation, communication, and tests of Bell non-locality [25–33], and have been efficiently generated in a wide range of experimental setups [34–38]. Consequently, it becomes interesting to observe whether such hybrid states can be used to share entanglement among distant locations without the limitations faced by CV and DV systems.

Here, we propose a scheme based on HE states as an initial resource which produces high-rate DV entanglement between extremely far apart locations. We provide a characterization of such states and show that it is possible to share entanglement between locations which are hundreds of kms apart. We further assess the quality of shared entanglement in the context of EB-QKD. We show that, by bringing forth the best of both CV and DV systems, with HE states, it is possible to achieve secure key rate at a distance of 300 km by using practical homodyne detectors with efficiency $\eta_h = 0.55$ [39–43] (which is a reasonable value at telecommunication wavelengths [40]) and on-off detectors with efficiency $\eta_0 = 0.8$ [44]. Note that we use the key rates and transmission distances only to quantify the quality of the entanglement; our central goal is to show the advantage of using HE states

[*] soumyakanti.bose09@gmail.com
[†] jaskaran@us.es
[‡] adan@us.es
[§] h.jeong37@gmail.com

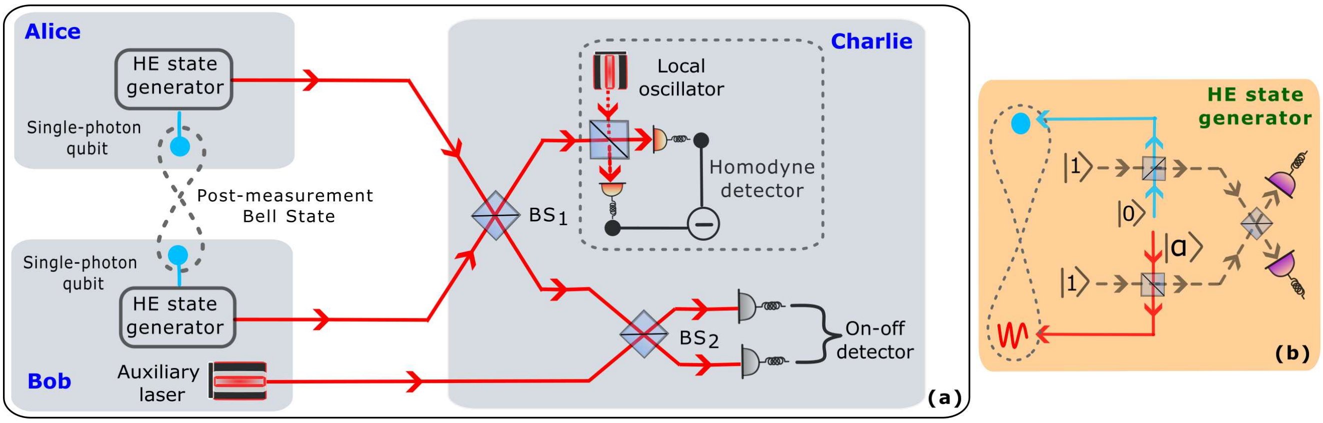


FIG. 1. (a) Scheme for generating DV entangled states between Alice and Bob using HE states. The DV part (cyan) and the CV part (red) of the HE state stand for the single-photon state and coherent state, respectively. Alice and Bob send the CV part of their individual HE states to Charlie, who then mixes the incoming signals at a balanced beam splitter (BS$_1$), and uses one of the output modes for homodyne measurement with efficiency η_h. The other outgoing signal of BS$_1$ is used for a post-selection measurement by on-off detectors with efficiency η_0, after mixing it at another balanced BS (BS$_2$) with the additional coherent signal sent by Bob. Upon declaration of the results by Charlie, Alice and Bob obtain a DV entangled pair which is used for secure key generation. (b) Scheme for generating HE states. Two ancilla single photons (gray, dashed line) are mixed with vacuum and coherent states at the two BSs. The outgoing ancilla photons are then mixed with each other at a second BS. When the detector placed at the output of the second BS clicks, then the HE state between single-photon and the coherent state is obtained.

to achieve entanglement over longer distances, which is a crucial tool enabling a wide range of fundamental tests in physics and quantum information processing applications.

Our scheme hinges on generating a single-photon DV entangled state between two distant parties by exploiting CV entanglement swapping [33] by a third party located midway. It offers three major advantages as compared to earlier CV and DV EB-QKD protocols. These are: (i) Elimination of major limiting factors of DV EB-QKD, which include high precision Bell state or single-photon measurements as well as the photon-number-splitting attack by an eavesdropper by considering entanglement swapping over the CV system. (ii) Elimination of the requirement of near-unit efficiency for the homodyne detectors used for key generation in CV EB-QKD. (iii) Long transmission distance at telecommunication wavelength stemming from the robustness of the multiphoton coherent state against transmission losses and using practical devices.

This article is organized as follows. In Sec. II, we provide some brief introduction to HE states. We then propose a protocol to share DV entanglement among distant locations by using HE states as an initial resource. We also characterize the resulting entanglement using logarithmic negativity and show that it can be non-zero even when the parties are separated hundreds of kilometers apart. In Sec. III, we benchmark the usefulness of the resultant entangled states by demonstrating our scheme as an EB-QKD protocol using practical devices. In Sec. IV, we conclude our results by arguing that our protocol provides a practical solution to the problem long distance entanglement generation which is a central requirement in several information processing tasks.

II. ENTANGLEMENT SHARING WITH HYBRID STATES

In this section we first provide a brief description of HE states. Subsequently, we detail our protocol to share long distance entanglement using these states.

A. Hybrid entangled states

Let $|0\rangle$ and $|1\rangle$ correspond to photon number states in the Fock basis and $|\alpha\rangle$ correspond to a coherent state of a quantized light with coherent amplitude α. For the remainder of this paper we will represent the number of photons as a DV system, while the coherent state represents a CV system. We define a HE state as an entangled pair, where the entanglement is between the DV and CV degrees of freedom. Mathematically, such HE states can be written as

$$|\psi\rangle_{a_1a_2} = \frac{1}{\sqrt{2}}\left(|0\rangle_{a_1}|\alpha\rangle_{a_2} + |1\rangle_{a_1}|-\alpha\rangle_{a_2}\right), \qquad (1)$$

where a_1 and a_2 are the two modes pertaining to the DV and CV parts, respectively.

We stress that HE states with small coherent amplitudes ($\alpha \lesssim 1$) are experimentally available. They have been generated experimentally in various settings such as conditional photon subtraction on a coherent state [34] as well as photon subtraction on two squeezed states [35] (see Appendix A for further details). While these techniques produce HE states with non-unit probability, it should be noted that typical methods to generate standard entangled photon pairs, *e.g.*, the parametric down conversion, also does so non-deterministically. In Fig. 1(b), we outline the linear optics based schematic for generating HE-states as originally described in [34].

B. Protocol for entanglement sharing

We consider two distant parties, Alice and Bob, each of them having access to bipartite HE states $|\psi\rangle_{a_1a_2}$ and $|\psi\rangle_{b_1b_2}$ given by Eq. (1). We consider these as initial resource states which will be used to share a DV entangled state between the parties. We provide a step-by-step description of the protocol, schematically represented in Fig. 1(a), while a detailed mathematical calculation can be found in Appendix B.

Step 1: Alice and Bob generate HE states $|\psi\rangle_{a_1a_2}$ and $|\psi\rangle_{b_1b_2}$ in their respective laboratories. Both parties transmit the CV part of their systems, corresponding to modes a_2 and b_2, respectively, to a third untrusted party, Charlie, who lies midway between them, through a lossy quantum channel with transmittance T $(0 \leq T \leq 1)$. Additionally, Bob also transmits the state $\left|\sqrt{2}\alpha\right\rangle$ to Charlie separately through a similar quantum channel. After passing through channels with transmission losses, Charlie receives the mode a_2 from Alice, the mode b_2 from Bob, and the additional state $\left|\sqrt{2T}\alpha\right\rangle$ from Bob, which we label by mode c. While a general quantum channel between the parties will comprise of both transmission loss and thermal noise, here, for simplicity, we only consider lossy quantum channels with no noise. In Appendix F 4 we demonstrate that the scenario involving a practical level of thermal noise closely matches our current findings.

The effect of a quantum state passing through a noisy channel can be seen as the system undergoing photon loss. In Fig. 2, we plot the logarithmic negativity of the HE state when its CV part undergoes photon loss as a function of the coherent amplitude α (see appendix C for detail). We find that there exists an optimal value of α for a fixed value of photon loss. We denote the photon loss fraction by R such that $R = 0$ and $R = 1$ correspond to no photon loss and complete photon loss, respectively. For a significantly lossy channel, we find that the optimal value of α approaches $\alpha = 0.5$. This value becomes important when we benchmark the resultant DV entangled state by a EB-QKD protocol.

This behaviour of HE states can be qualitatively understood in terms of the interplay between entanglement and the fragility of the initial HE state. Starting from the initial separable state at $\alpha = 0$, the HE state becomes more entangled as α increases. An increase in α also corresponds to an increase in the average number of photons, which can be understood as an increase in the mean energy of the system. However, with an increase in the mean energy, the state becomes more vulnerable to decoherence. This behaviour is similar to what is also shown in Ref. [45] for superposition of coherent states, and the advantage of using small amplitudes under photon losses was demonstrated in the context of teleportation [46]. As a consequence, with increase in α beyond an optimal value, the HE state becomes extremely fragile under noise leading to a drop in entanglement when the multiphoton part passes through a noisy quantum channel.

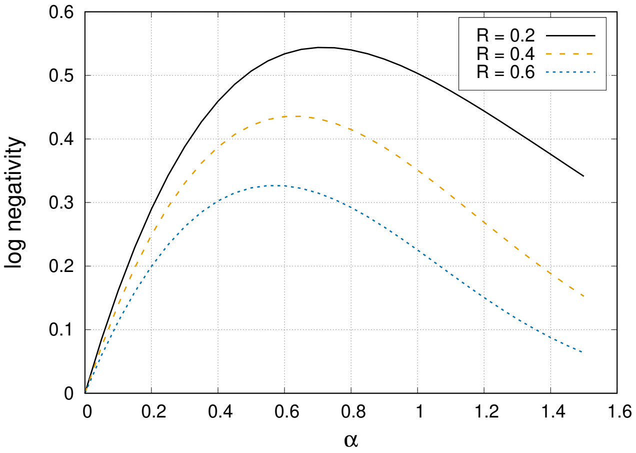


FIG. 2. Logarithmic negativity of the HE state undergoing photon-loss over the CV part as a function of the coherent amplitude α. R $(0 \leq R \leq 1)$ stands for the normalized strength of loss.

Step 2: Next, Charlie mixes the two incoming modes a_2 and b_2 via a beam splitter (BS), labelled as BS$_1$ in Fig. 1 with two output modes which we can label as $a_2^{'}$ and $b_2^{'}$. In our protocol we are specifically interested in the vacuum state contributions from the mode $a_2^{'}$. To extract this contribution, Charlie mixes this mode though a second BS (BS$_2$) with mode c with output modes labelled as $a_2^{''}$ and $c^{'}$. Charlie now performs a projective measurement, $\mathcal{M} = \{\Pi_0, \mathbb{1} - \Pi_0\}$, where $\Pi_0 = (\mathbb{1} - |0\rangle\langle 0|)_{a_2^{''}} \otimes (\mathbb{1} - |0\rangle\langle 0|)_{c^{'}}$. This measurement is accomplished by using on-off detectors (that only detect the presence of photons) on each of the modes $a_2^{''}$ and $c^{'}$. Charlie then publicly announces the outcome of the projective measurement which is considered to be successful only if the result Π_0 is obtained, i.e., both detectors click. In that case, the protocol continues. Otherwise, the measurement is deemed unsuccessful and the parties must repeat the aforementioned steps again. In order to model realistic detectors, we consider imperfect on-off detectors with efficiency η_0.

Step 3: After a successful projective measurement (as dictated in Step 2), Charlie performs a homodyne measurement on mode $b_2^{'}$ and, again, announces the results publicly. We consider that homodyne measurements have efficiency η_h.

Step 4: After a public announcement of the results of a successful projective measurement and the homodyne measurement by Charlie, Alice and Bob end up with the final normalized single-photon-Bell-state in modes a_1 and b_1 as

$$\rho_{a_1b_1} = \frac{1}{2}\left[\begin{aligned} &|01\rangle\langle 01| + |10\rangle\langle 10| \\ &+ h\left(g\,|01\rangle\langle 10| + g^*\,|10\rangle\langle 01|\right)\end{aligned}\right], \tag{2}$$

with probability

$$P_0 = \frac{\left(1 - e^{-\eta_o T\alpha^2}\right)^2}{2}, \tag{3}$$

where $h = e^{-4(1-T\eta_h)\alpha^2}$, $g = e^{4\mathrm{i}\sqrt{T\eta_h}\alpha p}$, g^* is the conjugate of g, and p is the result of the homodyne measurement.

C. Shared DV-entanglement between the parties

The entanglement of the final DV entangled state shared between the parties depends on a number of parameters. However, the quantities of most interest are the transmission length and the coherent amplitude.

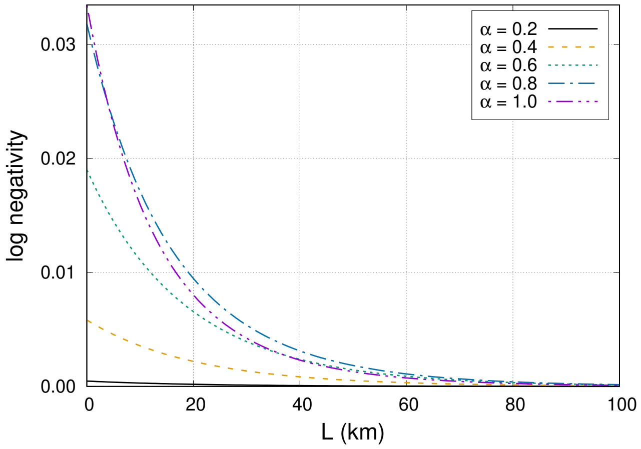


FIG. 3. Logarithmic negativity of the state $\rho_{a_1b_1}$ as a function of the transmission distance (L) for different values of coherent amplitude α. We assume detection efficiencies $\eta_h = 0.55$ for the homodyne detectors, $\eta_0 = 0.8$ for the on-off detectors, and $p = \frac{\pi}{2}$.

In Fig. 4 we plot the logarithmic negativity of the state $\rho_{a_1b_1}$ as a function of the transmission distance for different values of the coherent amplitude α. We assume that the transmittance of both the channels is given by T_A and T_B, respectively, such that, $T_A = 10^{-l\frac{L_{AC}}{10}}$ and $T_B = 10^{-l\frac{L_{BC}}{10}}$, where $l = 0.2$ dB/km is the standard channel loss for telecommunication wavelength [47, 48] and L_{AC} and L_{BC} are the transmission distances between Alice-Charlie and Bob-Charlie respectively. To simplify the scenario, we also assume that Charlie is midway between Alice and Bob such that $L_{AC} = L_{BC} = L/2$ such that the total transmission distance is L. We find that the entanglement of the final state decreases exponentially with the total transmission distance. As an example, at $L = 100$ km the logarithmic negativity is 1.3×10^{-4} for coherent amplitude $\alpha = 0.6$.

Next, in Fig. 3 we plot the logarithmic negativity as a function of the coherent amplitude α for different transmission distances. As it is evident from the Fig. that the shared-entanglement varies non-monotonically on the coherent amplitude (α). We observe that as the transmission distance increases, the optimal value of α becomes less than unity. For higher transmission distance ($L \geq 150$ Km) this optimal value becomes close to $\alpha = 0.5$ (not shown in the Fig.). It is found that there also exists an optimal value of α that offers maximum entanglement at a given distance which may be different than the optimal value of α which maximizes the entanglement of the original HE state (as shown in Fig. 2).

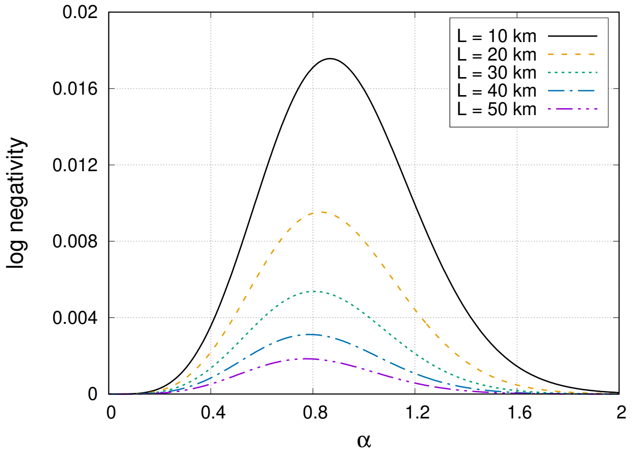


FIG. 4. Logarithmic negativity of the state $\rho_{a_1b_1}$ as a function of the transmission distance L for different values of coherent amplitude α. We assume detection efficiencies $\eta_h = 0.55$ for the homodyne detectors, $\eta_0 = 0.8$ for the on-off detectors, and $p = \frac{\pi}{2}$.

III. QUANTUM KEY DISTRIBUTION USING HE STATES

In this section we benchmark the quality of the shared entangled state in terms of an EB QKD protocol which we set up around the scheme presented in Sec. II B. We also consider an eavesdropper, Eve, who may collaborate with Charlie to determine the secure key that is being shared between Alice and Bob. Additionally, in our protocol we make the following assumptions:

1. We assume that Alice and Bob have access to secure laboratories in which they can perform well characterized measurements. Moreover, the measurement devices of Alice and Bob are assumed to be immune to any side-channel attack since no unwanted system may enter or exit the secure laboratories. In the protocol, the DV modes a_1 and b_1 with Alice and Bob, respectively, are assumed to be in these secure laboratories and do not directly take part in the transmission. On the other hand, the CV modes a_2 and b_2 are not assumed to be in secure laboratories and as such are vulnerable to eavesdropping attacks.

2. We also assume that the quantum channels between Alice-Charlie and Bob-Charlie are characterized by transmission losses only, with no thermal noise. We justify this assumption by demonstrating, in Appendix. F 4, the scenario with no thermal noise approximates the scenario with some practical value of the same with more than 98% fidelity. This assumption is only required to manage the calculation complexity of evaluating the final DV state between Alice and Bob.

3. We also consider a third party, Charlie, who is assumed to be untrusted and can collaborate with an eavesdropper, Eve. In the worst case scenario, we assume that he is identified as Eve herself. The QKD protocol, as described in the main text, dictates that Charlie performs certain measurements and publicly declare the outcomes so that Alice and Bob can share an entangled state. In principle, as an eavesdropper, we assume that Charlie may not perform the operations as dictated by the protocol. However, it is required for him to supply some outcomes to the specified measurements to activate the correlations between Alice and Bob. However, if these outcomes are tampered with or even fabricated, the correlations between Alice and Bob will decrease. It is then possible for Alice and Bob to detect the presence of Eve by various methods including state tomography since the parties know the final state they should potentially share. More details on this assumption and the concept of secure laboratories can be found in Ref. [49].

A. Steps in evaluating key rate

It should be noted that the steps of the QKD protocol directly follow after step 4 in Sec. II B as

Step 5: For the case in which Alice and Bob share $\rho_{a_1 b_1}$, they perform two-outcome measurements $\mathcal{M}_A$ and $\mathcal{M}_B$ on their respective subsystems to generate a raw key. The choice of measurements is made prior to starting the protocol and the information about this choice is usually publicly available. In our protocol, they perform Pauli measurements corresponding to σ_Z on their respective subsystems to generate a raw key. The length of the raw key that the parties can generate is quantified by the mutual information $I(A:B)$ between them for the observable σ_Z.

Step 6: Alice and Bob then estimate the amount of information that an adversary, Eve, can have on their raw key. This information is quantified by the Holevo bound $\chi(A:E)$ between Alice and Eve. In our protocol we consider the Holevo bound to quantify the knowledge about the coherent amplitude α, results of the on-off and homodyne measurement which are publicly declared and are actively used in generating the final state between Alice and Bob. These results can be used by Eve and as such must be taken care of in the security analysis.

B. Simulation results on the secured key rate

Our protocol comprises of two quantum channels: one between Alice and Charlie and another between Bob and Charlie. As before, we consider that the transmittance of both the channels is given by T_A and T_B, respectively, such that, $T_A = 10^{-l\frac{L_{AC}}{10}}$ and $T_B = 10^{-l\frac{L_{BC}}{10}}$, where $l = 0.2$ dB/km is the standard channel loss for telecom wavelength [47, 48] and $L_{AC} = L_{BC} = L/2$ are the transmission distances between Alice-Charlie and Bob-Charlie respectively such that the total transmission distance is L.

Moreover, we consider that the detectors of Alice and Bob have efficiency η_d such that the error rate is given as $Q = 1 - \eta_d$. With these inefficient detectors, the final secure key rate (See Appendix E for a detailed analysis) for the state given in Eq. (2) is given as

$$
\begin{aligned}
r &\geq P_0 \left[I(A:B) - \chi(A:E) \right] \\
&= P_0 \left\{ 1 - \eta_d + \frac{1}{2}\left[(1+h)\log_2(1+h) + (1-h)\log_2(1-h) \right] \right. \\
&\quad \left. - \frac{1}{2}\left[(2-\eta_d)\log_2(2-\eta_d) - (1-\eta_d)\log_2(1-\eta_d) \right] \right\},
\end{aligned}
\tag{4}
$$

where it can be seen that the secure key rate only depends on the parameters h (from Eq. (2)), the detector efficiency of Alice and Bob and the probability with which the final state is prepared.

Generally, for an experimental realization of the QKD protocol, the labs of Alice and Bob are fixed at some distance L. As seen in the main text, α cannot be chosen arbitrarily, as there exists an optimal value which can either maximize the key rate or the total transmission distance. In Fig. 5, we plot the maximum transmission distance as a function of the coherent amplitude for various values of secure key rate with ideal detector $\eta_d = 0$. We observe that there exists an optimal value $\alpha \approx 0.5$ which maximizes the total transmission distance for any value of the secure key rate.

In Fig. 6 we plot the secure key rate as a function of the total transmission distance L for different values

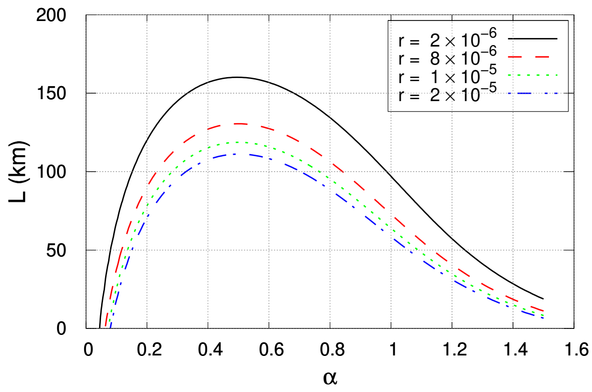


FIG. 5. The total transmission distance as a function of the coherent amplitude for different values of the secure key rate. We fix the channel loss at $l = 0.2$ dB/km which corresponds to losses in standard optical fibres. We also fix $\eta_d = 0$ for this analysis. The optimal value of α which maximizes the transmission distance is found to be the same in each case. The unit for the secure key rate r is bits/pulse.

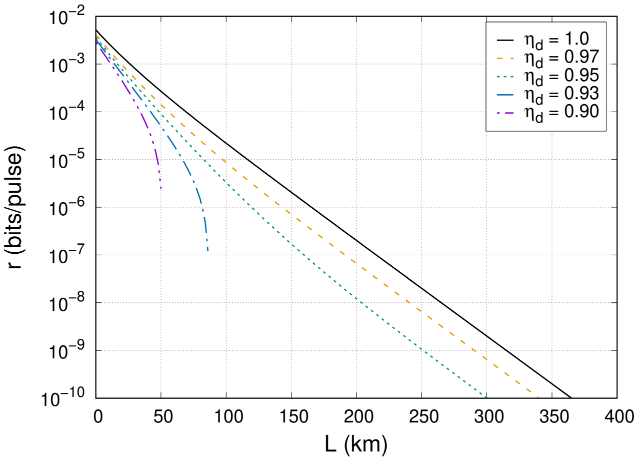


FIG. 6. Secure key rate as a function of total transmission distance L for different values of η_d in the optimal case, i.e., $\alpha = 0.5$. We assume detection efficiencies $\eta_h = 0.55$ for the homodyne detectors, $\eta_0 = 0.8$ for the on-off detectors, and $p = \frac{\pi}{2}$.

of η_d. We choose the parameters $\eta_h = 0.55$, $\eta_0 = 0.8$, and $p = \frac{\pi}{2}$ to be as realistic as possible and simulate the results for a standard telecom fiber with $l = 0.2$dB/km. Furthermore, the value of the coherent amplitude α is chosen to maximize the secure key rate over long transmission distances instead of entanglement. For our analysis we choose $\alpha = 0.5$ to optimize the total distance. It is also approximately the same value that optimizes the logarithmic negativity of an HE state when its CV part undergoes high photon loss. It is seen that under lower errors on Alice's and Bob's side ($\eta_d = 0.97$ and 0.95), a secure key rate can be achieved for transmission distances around 300 km indicating that the resultant entangled state is useful. However, the maximum achievable distance drastically falls off as η_d is increased up to $\eta_d = 0.90$.

IV. DISCUSSION AND CONCLUSION

We have shown that HE states between CV and DV systems provide a robust practical solution to the problem of achieving long-distance high-rate entanglement. Both requirements are fundamental for a number of applications. In this paper we have bench marked the usefulness of the prepared entangled state using an EB-QKD protocol, as it is both a fundamental application and a multipurpose test bed. In an EB-QKD setup, our results indicate that HE states bring forth the best of both CV and DV systems, resulting in a secure key rate of $\sim 10^{-9}$ bits/pulse at a distance of 250 km with 5% detection in-efficiency. This, in itself, represents a significant contribution. All this, without using an ultra low-loss fibre (with channel loss $l = 0.16$ dB/km at 1550 nm [50]), which allowed an earlier result to achieve transmission distances higher than 400 km. With such a fibre, our approach would allow us to achieve $\sim 10^{-10}$ bits/pulse at a distance of 300 km for $\eta_d = 0.95$.

In our analysis, it should be noted that, for the sake of simplicity, we do not consider any thermal noise in the channels. However, one can qualitatively show that incorporating a practical value for such thermal noise will not significantly affect our results (see Appendix F for detail). We leave the detailed quantitative analysis in the presence of thermal noise for future works and acknowledge that it involves lengthy analytical calculations that may have insignificant impact on our findings.

The feasibility of our protocol relies in the fact that HE states with small coherent amplitudes ($\alpha < 1$) can be generated in the lab by several non-deterministic techniques [34, 35] and the generation rate is comparable to the rate of entangled photon pairs in parametric down conversion setups. As an example, it is possible to prepare HE states where CV and DV parts correspond to photon number state and coherent state, respectively, with fidelity ≈ 0.75 for $\alpha = 0.5$ [34]. While the rate of generation in the source is comparable to that of parametric down conversion sources, losses during transmission are reduced, so the effective rate at destination increases. The fidelity of the preparation could be a limiting factor. However, this can be mitigated by using other forms of HE states, most notably with the CV and DV modes corresponding to cat states and polarization, respectively, which offer exceptionally good fidelity of preparation as well as rate of generation [51–55]. We also note that a recent result indicates that it is also possible to deterministically generate HE states with high fidelity [56]

However, it should be noted that there will be effects from phase modulations and phase mismatch in a practical implementation of our scheme. Commercially available lasers, used in generation of HE states, generally do not have well defined phase stabilization while the optical fibres, used for transmission, may introduce non-linear effects on the signals. This causes additional concerns for phase-locking and phase-tracking to ensure successful interference at Charlie's end. Although such issues have been managed in the context of twin-field (TF) QKD [57], it remains unclear to us whether a similar architecture can be useful in our setup as well and we leave it as an open avenue for future discussions.

Our results highlight the significance of HE states as a resource in high-rate remote entanglement generation, which plays a crucial role in enhancing many quantum information processing tasks such as quantum internet [58, 59], quantum digital signature [60, 61], and network steering [62]. We believe that our scheme has the potential to drive a new generation of experimental developments in quantum information technology.

ACKNOWLEDGMENTS

The authors thank Stefano Pirandola and Hua-Lei Yin for their comments on an earlier version of the manuscript. This work is supported by QuantERA grant SECRET, by MCINN/AEI (Project No. PCI2019-111885-2), National Research Foundation of Korea (NRF) grants funded by the Korean government (Grant Nos. NRF-2022M3K4A1097117 and NRF-2023R1A2C1006115) via the Institute of Applied Physics at Seoul National University, and by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (IITP-2021-0-01059 and IITP-2023-2020-0-01606). AC is also supported by MCINN/AEI (Project No. PID2020-113738GB-I00). J. S. also acknowledges the support from the National Science and Technological Council (NSTC) of Taiwan through grant no. NSTC 112-2628-M-006-007-MY4 and NSTC 112-2811-M-006-033-MY4.

[1] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[2] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes, Phys. Rev. Lett. **119**, 010402 (2017).

[3] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering, New J. Phys. **14**, 053030 (2012).

[4] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, Quantum teleportation over 143 kilometres using active feed-forward, Nature (London) **489**, 269 (2012).

[5] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y. Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Experimental quantum key distribution certified by Bell's theorem, Nature (London) **607**, 682 (2022).

[6] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C. W. Lim, and H. Weinfurter, A device-independent quantum key distribution system for distant users, Nature **607**, 687 (2022).

[7] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, Toward a photonic demonstration of device-independent quantum key distribution, Phys. Rev. Lett. **129**, 050502 (2022).

[8] N. Gisin, S. Pironio, and N. Sangouard, Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier, Phys. Rev. Lett. **105**, 070501 (2010).

[9] A. Cabello and F. Sciarrino, Loophole-free bell test based on local precertification of photon's presence, Phys. Rev. X **2**, 021010 (2012).

[10] E. Meyer-Scott, D. McCloskey, K. Gołos, J. Z. Salvail, K. A. G. Fisher, D. R. Hamel, A. Cabello, K. J. Resch, and T. Jennewein, Certifying the presence of a photonic qubit by splitting it in two, Phys. Rev. Lett. **116**, 070501 (2016).

[11] A. Z. Leger, S. Gambhir, J. Légère, and D. R. Hamel, Amplification of cascaded down-conversion by reusing photons with a switchable cavity, Phys. Rev. Res. **5**, 023131 (2023).

[12] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. **2**, 16025 (2016).

[13] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, Discrete and continuous variables for measurement-device-independent quantum cryptography, Nat. Photonics **9**, 772 (2015).

[14] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Reply to 'discrete and continuous variables for measurement-device-independent quantum cryptography', Nat. Photonics **9**, 773 (2015).

[15] C. Kumar, J. Singh, S. Bose, and Arvind, Coherence-assisted non-Gaussian measurement-device-independent quantum key distribution, Phys. Rev. A **100**, 052329 (2019).

[16] J. Singh and S. Bose, Non-Gaussian operations in measurement-device-independent quantum key distribution, Phys. Rev. A **104**, 052605 (2021).

[17] H. Jeong, Using weak nonlinearity under decoherence for macroscopic entanglement generation and quantum computation, Phys. Rev. A **72**, 034305 (2005).

[18] Y. Li, H. Jing, and M.-S. Zhan, Optical generation of a hybrid entangled state via an entangling single-photon-added coherent state, J. Phys. B: At. Mol. Opt. Phys. **39**, 2107 (2006).

[19] J.-Q. Liao, Y. Guo, H.-S. Zeng, and L.-M. Kuang, Preparation of hybrid entangled states and entangled coherent states for a single trapped ion in a cavity, J. Phys. B: At. Mol. Opt. Phys. **39**, 4709 (2006).

[20] B. He, Q. Lin, and C. Simon, Cross-Kerr nonlinearity between continuous-mode coherent states and single photons, Phys. Rev. A **83**, 053826 (2011).

[21] M. Hosseini, S. Rebic, B. M. Sparkes, J. Twamley, B. C. Buchler, and P. K. Lam, Memory-enhanced noiseless cross-phase modulation, Light: Sci. Appl. **1**, e40 (2012).

[22] D. T. Le, W. Asavanant, and N. B. An, Heralded preparation of polarization entanglement via quantum scissors, Phys. Rev. A **104**, 012612 (2021).

[23] Z.-B. Chen, G. Hou, and Y.-D. Zhang, Quantum nonlocality and applications in quantum-information processing of hybrid entangled states, Phys. Rev. A **65**, 032317 (2002).

[24] K. Park, S.-W. Lee, and H. Jeong, Quantum teleportation between particlelike and fieldlike qubits using hybrid entanglement under decoherence effects, Phys. Rev. A **86**, 062301 (2012).

[25] H. Kwon and H. Jeong, Violation of the Bell–Clauser-Horne-Shimony-Holt inequality using imperfect photodetectors with optical hybrid states, Phys. Rev. A **88**, 052127 (2013).

[26] S.-W. Lee and H. Jeong, Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits, Phys. Rev. A **87**, 022326 (2013).

[27] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, Hybrid discrete and continuous-variable quantum information, Nat. Phys. **11**, 713 (2015).

[28] S. Omkar, Y. S. Teo, and H. Jeong, Resource-efficient topological fault-tolerant quantum computation with hybrid entanglement of light, Phys. Rev. Lett. **125**, 060501 (2020).

[29] S. Omkar, Y. S. Teo, S.-W. Lee, and H. Jeong, Highly photon-loss-tolerant quantum computing using hybrid qubits, Phys. Rev. A **103**, 032602 (2021).

[30] S. Bose and H. Jeong, Quantum teleportation of hybrid qubits and single-photon qubits using Gaussian resources, Phys. Rev. A **105**, 032434 (2022).

[31] M. He and R. Malaney, Teleportation of hybrid entangled states with continuous-variable entanglement, Sci. Rep. **12**, 17169 (2022).

[32] Y.-B. Sheng, L. Zhou, and G.-L. Long, Hybrid entanglement purification for quantum repeaters, Phys. Rev. A **88**, 022302 (2013).

[33] Y. Lim, J. Joo, T. P. Spiller, and H. Jeong, Loss-resilient photonic entanglement swapping using optical hybrid states, Phys. Rev. A **94**, 062337 (2016).

[34] H. Jeong, A. Zavatta, M. Kang, S.-W. Lee, L. S. Costanzo, S. Grandi, T. C. Ralph, and M. Bellini, Generation of hybrid entanglement of light, Nat. Photonics **8**, 564 (2014).

[35] O. Morin, K. Huang, J. Liu, L. H. Jeannic, C. Fabre, and J. Laurat, Remote creation of hybrid entanglement between particle-like and wave-like optical qubits, Nat. Photonics **8**, 570 (2014).

[36] A. E. Ulanov, D. Sychev, A. A. Pushkina, I. A. Fedorov, and A. I. Lvovsky, Quantum teleportation between discrete and continuous encodings of an optical qubit, Phys. Rev. Lett. **118**, 160501 (2017).

[37] D. V. Sychev, A. E. Ulanov, E. S. Tiunov, A. A. Pushkina, A. Kuzhamuratov, V. Novikov, and A. I. Lvovsky, Entanglement and teleportation between polarization and wave-like encodings of an optical qubit, Nat. Commun. **9**, 3672 (2018).

[38] T. Darras, B. E. Asenbeck, G. Guccione, A. Cavaillès, H. Le Jeannic, and J. Laurat, A quantum-bit encoding converter, Nat. Photonics **17**, 165 (2023).

[39] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection, Phys. Rev. X **5**, 041009 (2015).

[40] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[41] M. Zou, Y. Mao, and T.-Y. Chen, Rigorous calibration of homodyne detection efficiency for continuous-variable quantum key distribution, Opt. Express **30**, 22788 (2022).

[42] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photonics **13**, 839 (2019).

[43] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[44] While a photon-number-resolving-detector (PNRD) measures the number of photons detected, an on-off detector only indicates whether a photon is detected or not. As a consequence, an on-off detector is much less demanding than a PNRD. Recent advances in technology has led to development of single-photon detectors with efficiencies as high as 0.84–0.91 [63–65] with the use of high-contrast-grating in nanophotonics settings. This, in turn, implies that the efficiency of an on-off detector can be safely approximated up to 0.80 (if not more).

[45] C.-W. Lee and H. Jeong, Quantification of macroscopic quantum superpositions within phase space, Phys. Rev. Lett. **106**, 220401 (2011).

[46] J. S. Neergaard-Nielsen, Y. Eto, C.-W. Lee, H. Jeong, and M. Sasaki, Quantum tele-amplification

with a continuous-variable superposition state, Nat. Photonics **7**, 439 (2013).

[47] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[48] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nat. Photonics **9**, 397 (2015).

[49] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[50] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[51] H. Kwon and H. Jeong, Generation of hybrid entanglement between a single-photon polarization qubit and a coherent state, Phys. Rev. A **91**, 012340 (2015).

[52] S. Li, H. Yan, Y. He, and H. Wang, Experimentally feasible generation protocol for polarized hybrid entanglement, Phys. Rev. A **98**, 022334 (2018).

[53] S. A. Podoshvedov and N. B. An, Designs of interactions between discrete and continuous-variable states for generation of hybrid entanglement, Quant. Inf. Process. **18**, 68 (2019).

[54] K. Huang, H. L. Jeannic, O. Morin, T. Darras, G. Guccione, A. Cavaillès, and J. Laurat, Engineering optical hybrid entanglement between discrete- and continuous-variable states, New J. Phys. **21**, 083033 (2019).

[55] J. Wen, I. Novikova, C. Qian, C. Zhang, and S. Du, Hybrid entanglement between optical discrete polarizations and continuous quadrature variables, Photonics **8**, 552 (2021).

[56] J. Singh and V. Mittal, Deterministic generation of hybrid entangled states using quantum walks, arXiv **2311.02419** (2023).

[57] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, and J.-W. Pan, Twin-field quantum key distribution without phase locking, Phys. Rev. Lett. **130**, 250802 (2023).

[58] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-device-independent quantum key distribution over untrustful metropolitan network, Phys. Rev. X **6**, 011024 (2016).

[59] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, eaam9288 (2018).

[60] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan, Experimental quantum digital signature over 102 km, Phys. Rev. A **95**, 032334 (2017).

[61] W. Zhao, R. Shi, J. Shi, P. Huang, Y. Guo, and D. Huang, Multibit quantum digital signature with continuous variables using basis encoding over insecure channels, Phys. Rev. A **103**, 012410 (2021).

[62] B. D. M. Jones, I. Šupić, R. Uola, N. Brunner, and P. Skrzypczyk, Network quantum steering, Phys. Rev. Lett. **127**, 170405 (2021).

[63] W. Pernice, C. Schuck, O. Minaeva, M. Li, G. Goltsman, A. Sergienko, and H. Tang, High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits, Nat. Commun. **3**, 1325 (2012).

[64] C. Wei, W. Wang, D. Liu, M. Gu, and X. Wu, High-efficiency and large light-receiving area superconducting nanowire single-photon detector integrated with high-contrast grating, Photon. Res. **9**, 2253 (2021).

[65] S. Miki, S. Miyajima, F. China, M. Yabuno, and H. Terai, Photon detection at 1 ns time intervals using 16-element SNSPD array with SFQ multiplexer, Opt. Lett. **46**, 6015 (2021).

[66] S. M. Barnett, D. T. Pegg, and J. Jeffers, Equivalence of a lossless beam splitter and a nondegenerate parametric amplifier in conditional measurements, Opt. Commun. **172**, 55 (1999).

[67] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Volume of the set of separable states, Phys. Rev. A **58**, 883 (1998).

[68] M. B. Plenio, Logarithmic negativity: A full entanglement monotone that is not convex, Phys. Rev. Lett. **95**, 090503 (2005).

[69] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, Quantum Info. Comput. **3**, 535–552 (2003).

[70] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration, Phys. Rev. A **91**, 022320 (2015).

Appendix A: Generation of the hybrid entangled state

In this section we outline a process, using a setup in line with Ref. [34], that can be used to experimentally generate a hybrid entangled (HE) state of the form

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}}\left(|0\rangle_a |\alpha\rangle_b + |1\rangle_a |-\alpha\rangle_b\right) \tag{A1}$$

between modes a and b, where $|0\rangle$ and $|1\rangle$ correspond to photon number states, and $|\alpha\rangle$ is the coherent state with coherent amplitude α.

$|n\rangle$ and $|\alpha\rangle$ correspond to, respectively, the energy eigenstate and coherent state of a quantized electromagnetic field, where n is the number of photons in the state. It is possible to realize the energy eigenstates as a single-photon qubit by only considering the photon number states corresponding to $|0\rangle$ and $|1\rangle$. This is our discrete variable (DV) system and the multiphoton coherent state is our continuous variable (CV) system. The key idea of HE state generation hinges on conditional photon addition and erasing the path information of photon addition. There are several ways of achieving photon addition. This includes a model which uses single photon sources and beam splitters (BS) and another model which uses a parametric-down-converter (PDC) with a weak pump. Since the BS setup and the PDC are equivalent [66], here we use the BS model for photon addition. The following is a step-by-step description of the generation of the HE state in Fig. 1(b) of the main text.

Step 1: A vacuum state $|0\rangle$ in mode a is mixed with a single-photon state $|1\rangle$ in mode c using a BS (BS$_1$) with transmittance T. Similarly, a coherent state $|\alpha\rangle$ in mode c is mixed with another single-photon state in mode d using another BS (BS$_2$) with transmittance T. The output states from each of these two BSs are

$$\begin{aligned}|\psi\rangle^{\mathrm{BS}_1}_{ac} &= \sqrt{1-T}\,|1\rangle_a |0\rangle_c + \sqrt{T}\,|0\rangle_a |1\rangle_c \\ |\psi\rangle^{\mathrm{BS}_2}_{bd} &= \sqrt{1-T}\hat{b}^\dagger\,|\alpha\rangle_b |0\rangle_d + \sqrt{T}\,|\alpha\rangle_b |1\rangle_d\,,\end{aligned} \tag{A2}$$

where $\hat{b}^\dagger$ is the creation operator acting on mode b and $|\psi\rangle^{\mathrm{BS}_1}_{ac}$ is the output state from BS$_1$, while $|\psi\rangle^{\mathrm{BS}_2}_{bd}$ is the output state from BS$_2$. The BS transmittance T can be fine-tuned according to experimental requirements to yield maximum probability for photon addition. Therefore, the 4-mode state at the output of BS$_1$ and BS$_2$ is

$$|\psi\rangle^{\mathrm{BS}_{1,2}}_{ab,cd} = \sqrt{T(1-T)}\left(|1\rangle_a |\alpha\rangle_b \otimes |0\rangle_c |1\rangle_d + |0\rangle_a \hat{b}^\dagger |\alpha\rangle_b \otimes |1\rangle_c |0\rangle_d\right) + (1-T)\,|1\rangle_a \hat{b}^\dagger |\alpha\rangle_b \otimes |0\rangle_c |0\rangle_d + T\,|0\rangle_a |\alpha\rangle_b \otimes |1\rangle_c |1\rangle_d\,. \tag{A3}$$

Step 2: The outgoing single-photon modes (shown by gray dashed-lines in Fig. 1(b) of the main text) from both BS$_1$ and BS$_2$ are mixed with each other using a another BS (BS$_3$) with transmittance τ. This leads to a 4-mode state at the output of BS$_3$ which can be written as

$$\begin{aligned}|\psi\rangle^{\mathrm{BS}_3}_{ab,cd} = \sqrt{T(1-T)}\Big[&|1\rangle_a |\alpha\rangle_b \otimes \Big(-\sqrt{1-\tau}\,|0\rangle_c |1\rangle_d + \sqrt{\tau}\,|1\rangle_c |0\rangle_d\Big) + |0\rangle_a \hat{b}^\dagger |\alpha\rangle_b \otimes \Big(\sqrt{1-\tau}\,|1\rangle_c |0\rangle_d + \sqrt{\tau}\,|0\rangle_c |1\rangle_d\Big)\Big] \\ &+ (1-T)\,|1\rangle_a \hat{b}^\dagger |\alpha\rangle_b \otimes |0\rangle_c |0\rangle_d + T\,|0\rangle_a |\alpha\rangle_b \otimes \Big(\sqrt{1-\tau}\,|2\rangle_c |0\rangle_d + \sqrt{\tau}\,|0\rangle_c |2\rangle_d\Big).\end{aligned} \tag{A4}$$

Step 3: We now detect the output modes of BS$_3$ via single-photon detectors D$_1$ and D$_2$. Since the total photon number at the output of BS$_3$ is 1, it indicates that both D$_1$ and D$_2$ cannot click simultaneously. We post-select the state when only the detector D$_1$ clicks and discard the runs whenever the detector D$_2$ clicks. After post-selection, the state between modes a and b is

$$\begin{aligned}|\psi\rangle^{\mathrm{D}_1}_{ab} &= \langle 1|_c \langle 0|_d\, |\psi\rangle^{\mathrm{BS}_3}_{ab,cd} \\ &= \sqrt{T(1-T)}\left(\sqrt{\tau}\,|1\rangle_a |\alpha\rangle_b + \sqrt{1-\tau}\,|0\rangle_a \hat{b}^\dagger |\alpha\rangle_b\right).\end{aligned} \tag{A5}$$

We can now use the fact that n-photon-added coherent state is a good approximation to another coherent state with amplified amplitude, i.e., $\frac{\hat{b}^{\dagger n}}{\sqrt{N}}|\alpha\rangle \approx |g\alpha\rangle$ [34], where N is the corresponding normalization constant and $g \geq 1$ is the amplification factor. This leads to the result $\hat{b}^\dagger |\alpha\rangle_b \approx \frac{1}{\sqrt{1-\alpha^2}}|g\alpha\rangle_b$, where g is properly chosen. Then, by setting $\tau = \frac{1+\alpha^2}{2+\alpha^2}$ and using the approximation we get,

$$|\psi\rangle^{\mathrm{D}_1}_{ab} \approx \sqrt{\frac{T(1-T)}{2+\alpha^2}}\Big(|1\rangle_a |\alpha\rangle_b + |0\rangle_a |g\alpha\rangle_b\Big). \tag{A6}$$

Step 4: Next, we displace the mode b by performing a displacement operator on this mode given by $D_b\left(-\frac{\alpha+g\alpha}{2}\right) = \exp\left[-\frac{\alpha+g\alpha}{2}(\hat{b}^\dagger - \hat{b})\right]$, where $\hat{b}$ is the annihilation operator. This leads to the final normalized HE state

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}}\left(|0\rangle_a |\alpha_f\rangle_b + |1\rangle_a |-\alpha_f\rangle_b\right), \tag{A7}$$

where $\alpha_f = \frac{(g-1)\alpha}{2}$.

Appendix B: Shared entangled state between Alice and Bob

In this section, we calculate the the state obtained after performing the entanglement swapping operation by Charlie. We also calculate the states obtained after every step of the protocol starting from the initial resource of HE states. The steps of the protocol are detailed in the main manuscript.

1. Initial states and channel transmission

We denote the two hybrid entangled states with Alice and Bob as

$$\begin{aligned}|\psi\rangle_{a_1a_2} &= \frac{1}{\sqrt{2}}\left(|0\rangle_{a_1}|\alpha\rangle_{a_2} + |1\rangle_{a_1}|-\alpha\rangle_{a_2}\right)\\ |\psi\rangle_{b_1b_2} &= \frac{1}{\sqrt{2}}\left(|0\rangle_{b_1}|\alpha\rangle_{b_2} + |1\rangle_{b_1}|-\alpha\rangle_{b_2}\right),\end{aligned} \tag{B1}$$

respectively. The initial 4-mode resource state can be written as

$$\begin{aligned}|\psi\rangle_{\substack{a_1a_2\\b_1b_2}} &= |\psi\rangle_{a_1a_2}|\psi\rangle_{b_1b_2}\\ &= \frac{1}{2}\left(|00\rangle_{a_1b_1}|\alpha\rangle_{a_2}|\alpha\rangle_{b_2} + |11\rangle_{a_1b_1}|-\alpha\rangle_{a_2}|-\alpha\rangle_{b_2}\right.\\ &\quad\left.+|01\rangle_{a_1b_1}|\alpha\rangle_{a_2}|-\alpha\rangle_{b_2} + |10\rangle_{a_1b_1}|-\alpha\rangle_{a_2}|\alpha\rangle_{b_2}\right),\end{aligned} \tag{B2}$$

where $|ij\rangle_{a_1b_1} = |i\rangle_{a_1}|j\rangle_{b_1}\ \forall i,j \in \{0,1\}$.

Alice and Bob both send their multiphoton part (modes a_2 and b_2) to a third distant party Charlie for mixing and subsequent measurements through a noisy/lossy channel with transmittance T. Such channels could be modelled in terms of an effective beam splitter (BS) with transmittance T, where the input state is fed at one of the inputs of the BS while the other input is initialised as a vacuum state. The action of a BS with transmittance T on the input modes is given by a unitary U_T^{ab} implementing the following transformation:

$$\begin{pmatrix}\hat{a}\\ \hat{b}\end{pmatrix} \rightarrow \begin{pmatrix}\hat{a}'\\ \hat{b}'\end{pmatrix} = \begin{pmatrix}\sqrt{T} & \sqrt{1-T}\\ -\sqrt{1-T} & \sqrt{T}\end{pmatrix}\begin{pmatrix}\hat{a}\\ \hat{b}\end{pmatrix}. \tag{B3}$$

$T = \frac{1}{2}$ corresponds to a balanced $(50:50)$ BS. As a consequence, the action of the channel on a coherent state ($|\alpha\rangle$) in mode a is described as $U_T^{ab}|\alpha\rangle_a \otimes |0\rangle_b \rightarrow |\alpha\rangle_{a'} \otimes |0\rangle_{b'} = \left|\sqrt{T}\alpha\right\rangle_a \otimes \left|\sqrt{1-T}\alpha\right\rangle_b$, where U_T^{ab} is the corresponding BS unitary operation. Subsequently, the resultant state is obtained by tracing over the ancillary mode b.

Similarly, the noisy transmission of modes a_2 and b_2 could be described by using two BSs with transmittance T, each one in the paths of modes a_2 and b_2 with ancillary modes given by f_a and f_b, respectively. The resultant noisy/lossy state is obtained by tracing over the ancillary modes (f_a and f_b). Therefore, the total input state to Charlie before mixing is

$$\begin{aligned}|\psi\rangle_{\substack{a_1,b_1;a_2',b_2'\\ f_a',f_b'}} &= U_T^{(a_2,f_a)} \otimes U_T^{(b_2,f_b)}\,|\psi\rangle_{\substack{a_1a_2\\b_1b_2}} \otimes |0\rangle_{f_a}|0\rangle_{f_b}\\ &= \frac{1}{2}\Bigg(|00\rangle_{a_1b_1}\left|\sqrt{1-T}\alpha\right\rangle_{f_a}\left|\sqrt{1-T}\alpha\right\rangle_{f_b}\left|\sqrt{T}\alpha\right\rangle_{a_2}\left|\sqrt{T}\alpha\right\rangle_{b_2} + |11\rangle_{a_1b_1}\left|-\sqrt{1-T}\alpha\right\rangle_{f_a}\left|-\sqrt{1-T}\alpha\right\rangle_{f_b}\left|-\sqrt{T}\alpha\right\rangle_{a_2}\left|-\sqrt{T}\alpha\right\rangle_{b_2}\\ &\quad + |01\rangle_{a_1b_1}\left|\sqrt{1-T}\alpha\right\rangle_{f_a}\left|-\sqrt{1-T}\alpha\right\rangle_{f_b}\left|\sqrt{T}\alpha\right\rangle_{a_2}\left|-\sqrt{T}\alpha\right\rangle_{b_2} + |10\rangle_{a_1b_1}\left|-\sqrt{1-T}\alpha\right\rangle_{f_a}\left|\sqrt{1-T}\alpha\right\rangle_{f_b}\left|-\sqrt{T}\alpha\right\rangle_{a_2}\left|\sqrt{T}\alpha\right\rangle_{b_2}\Bigg),\end{aligned} \tag{B4}$$

where $U_T^{(a_2,f_a)}$ and $U_T^{(b_2,f_b)}$ are the BS unitary operations corresponding to the respective channels with transmittance T. Charlie now mixes the incoming multiphoton modes (a_2 and b_2) through a balanced BS (BS_1) leading to the four mode entangled state

$$
\begin{aligned}
|\psi\rangle^{\mathrm{BS}_1}_{\substack{a_1,b_1;a_2^{''},b_2^{''}\\ f_a^{'},f_b^{'}}} &= U^{(a_2,b_2)}_{\mathrm{BS}_1}\,|\psi\rangle_{\substack{a_1,b_1;a_2^{'},b_2^{'}\\ f_a^{'},f_b^{'}}}\\
&= \frac{1}{2}\Bigg(|00\rangle_{a_1b_1}\left|\sqrt{1-T}\alpha\right\rangle_{f_a}\left|\sqrt{1-T}\alpha\right\rangle_{f_b}|0\rangle_{b_2}\left|\sqrt{2T}\alpha\right\rangle_{a_2}+|11\rangle_{a_1b_1}\left|-\sqrt{1-T}\alpha\right\rangle_{f_a}\left|-\sqrt{1-T}\alpha\right\rangle_{f_b}|0\rangle_{b_2'}\left|-\sqrt{2T}\alpha\right\rangle_{a_2}\\
&\quad+|01\rangle_{a_1b_1}\left|\sqrt{1-T}\alpha\right\rangle_{f_a}\left|-\sqrt{1-T}\alpha\right\rangle_{f_b}\left|\sqrt{2T}\alpha\right\rangle_{b_2}|0\rangle_{a_2}+|10\rangle_{a_1b_1}\left|-\sqrt{1-T}\alpha\right\rangle_{f_a}\left|\sqrt{1-T}\alpha\right\rangle_{f_b}\left|-\sqrt{2T}\alpha\right\rangle_{b_2}|0\rangle_{a_2}\Bigg).
\end{aligned}
\tag{B5}
$$

It can be seen from Eq. (B5) that, in the total 4-mode entangled state after mixing by Charlie, the vacuum state contribution in mode a_2 appears with probability 1/2. Our primary aim is to postselect the state (B5) in $|0\rangle_{a_2}$.

2. State after the on-off measurement

The additional coherent state sent by Bob to Charlie $(|\sqrt{2}\alpha\rangle)$ becomes $\left|\sqrt{2T}\alpha\right\rangle$ as a result of transmission through lossy channel. As is described in [34], for this purpose Charlie first mixes the outgoing a_2 mode with this additional state $\left(\left|\sqrt{2T}\alpha\right\rangle\right)$ in mode c through the second balanced beam splitter (BS$_2$). Consequently, the state after the mixing at BS$_2$ is given by

$$
\begin{aligned}
|\psi\rangle^{\mathrm{BS}_2}_{\substack{a_1,b_1;b_2^{''}\\ f_a^{'},f_b^{'}\\ a_2^{'''},c^{'}}} &= U^{(a_2,c)}_{\mathrm{BS}_1}\,|\psi\rangle^{\mathrm{BS}_1}_{\substack{a_1,b_1;a_2^{''},b_2^{''}\\ f_a^{'},f_b^{'}}}\otimes\left|\sqrt{2T}\alpha\right\rangle_c\\
&= \frac{1}{2}\Bigg(|00\rangle_{a_1b_1}\left|\sqrt{1-T}\alpha\right\rangle_{f_a}\left|\sqrt{1-T}\alpha\right\rangle_{f_b}|0\rangle_{b_2}\left|2\sqrt{T}\alpha\right\rangle_{a_2}|0\rangle_c\\
&\quad+|11\rangle_{a_1b_1}\left|-\sqrt{1-T}\alpha\right\rangle_{f_a}\left|-\sqrt{1-T}\alpha\right\rangle_{f_b}|0\rangle_{b_2}|0\rangle_{a_2}\left|-2\sqrt{T}\alpha\right\rangle_c\\
&\quad+|01\rangle_{a_1b_1}\left|\sqrt{1-T}\alpha\right\rangle_{f_a}\left|-\sqrt{1-T}\alpha\right\rangle_{f_b}\left|\sqrt{2T}\alpha\right\rangle_{b_2}\left|\sqrt{T}\alpha\right\rangle_{a_2}\left|-\sqrt{T}\alpha\right\rangle_c\\
&\quad+|10\rangle_{a_1b_1}\left|-\sqrt{1-T}\alpha\right\rangle_{f_a}\left|\sqrt{1-T}\alpha\right\rangle_{f_b}\left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left|\sqrt{T}\alpha\right\rangle_{a_2}\left|-\sqrt{T}\alpha\right\rangle_c\Bigg).
\end{aligned}
\tag{B6}
$$

As it can be seen from Eq. (B6), if both the detectors at the output of BS$_2$ click then the contribution can arise only from the respective part in (B6), i.e., from the part containing $|0\rangle_{a_2}$. Experimentally, this could be achieved unambiguously by performing the operation $\Pi_0 = (\mathbf{I} - |0\rangle\langle 0|)\otimes(\mathbf{I}-|0\rangle\langle 0|)$ on (B6) using two *on-off* detectors at both the output ports of BS$_2$.

However, here we consider *non-ideal* detectors with efficiency η_o $(0 \le \eta_o \le 1)$. Similar to the case of transmission channels, this could be analysed by considering two additional BS with transmittance η_o and two ancillary modes g_a and g_c for modes a_2 and c, respectively. Therefore, before the *on-off* detectors, the total state is given by

$$
\begin{aligned}
|\psi\rangle^{tot}_{\substack{a_1,b_1;b_2^{''}\\ f_a^{'},f_b^{'},g_a^{'},g_c^{'}\\ a_2^{''''},c^{''}}} &= U_{\eta_o}^{(a_2,g_a)} \otimes U_{\eta_o}^{(c,g_c)} \,|\psi\rangle^{\mathrm{BS}_2}_{\substack{a_1,b_1;b_2^{''}\\ f_a^{'},f_b^{'}\\ a_2^{'''},c^{'}}} \otimes |0\rangle_{g_a} |0\rangle_{g_c} \\
&= \frac{1}{2}\Bigg[|00\rangle_{a_1b_1} |0\rangle_{b_2^{''}} \left|\sqrt{1-T}\alpha\right\rangle_{f_a} \left|\sqrt{1-T}\alpha\right\rangle_{f_b} \left|2\sqrt{T(1-\eta_o)}\alpha\right\rangle_{g_a} |0\rangle_{g_c} \left|2\sqrt{T\eta_o}\alpha\right\rangle_{a_2} |0\rangle_c \\
&\quad + |11\rangle_{a_1b_1} |0\rangle_{b_2} \left|-\sqrt{1-T}\alpha\right\rangle_{f_a} \left|-\sqrt{1-T}\alpha\right\rangle_{f_b} |0\rangle_{g_a} \left|-2\sqrt{T(1-\eta_o)}\alpha\right\rangle_{g_c} |0\rangle_{a_2} \left|-2\sqrt{T\eta_o}\alpha\right\rangle_c \\
&\quad + \Bigg(|01\rangle_{a_1b_1} \left|\sqrt{2T}\alpha\right\rangle_{b_2} \left|\sqrt{1-T}\alpha\right\rangle_{f_a} \left|-\sqrt{1-T}\alpha\right\rangle_{f_b} + |10\rangle_{a_1b_1} \left|-\sqrt{2T}\alpha\right\rangle_{b_2} \left|-\sqrt{1-T}\alpha\right\rangle_{f_a} \left|\sqrt{1-T}\alpha\right\rangle_{f_b} \Bigg) \\
&\qquad \left|\sqrt{T(1-\eta_o)}\alpha\right\rangle_{g_a} \left|-\sqrt{T(1-\eta_o)}\alpha\right\rangle_{g_c} \left|\sqrt{T\eta_0}\alpha\right\rangle_{a_2} \left|-\sqrt{T\eta_o}\alpha\right\rangle_c \Bigg] \\
&= \frac{1}{2}\Bigg[|00\rangle_{a_1b_1} |0\rangle_{b_2} \left|\sqrt{T'}\alpha\right\rangle_{f_a} \left|\sqrt{T'}\alpha\right\rangle_{f_b} \left|2\sqrt{T\eta_o'}\alpha\right\rangle_{g_a} |0\rangle_{g_c} \left|2\sqrt{T\eta_o}\alpha\right\rangle_{a_2} |0\rangle_c \\
&\quad + |11\rangle_{a_1b_1} |0\rangle_{b_2} \left|-\sqrt{T'}\alpha\right\rangle_{f_a} \left|-\sqrt{T'}\alpha\right\rangle_{f_b} |0\rangle_{g_a} \left|-2\sqrt{T\eta_o'}\alpha\right\rangle_{g_c} |0\rangle_{a_2} \left|-2\sqrt{T\eta_o}\alpha\right\rangle_c \\
&\quad + \Bigg(|01\rangle_{a_1b_1} \left|\sqrt{2T}\alpha\right\rangle_{b_2} \left|\sqrt{T'}\alpha\right\rangle_{f_a} \left|-\sqrt{T'}\alpha\right\rangle_{f_b} \;+\; |10\rangle_{a_1b_1} \left|-\sqrt{2T}\alpha\right\rangle_{b_2} \left|-\sqrt{T'}\alpha\right\rangle_{f_a} \left|\sqrt{T'}\alpha\right\rangle_{f_b} \Bigg) \\
&\quad \left|\sqrt{T\eta_o'}\alpha\right\rangle_{g_a} \left|-\sqrt{T\eta_o'}\alpha\right\rangle_{g_c} \left|\sqrt{T\eta_0}\alpha\right\rangle_{a_2} \left|-\sqrt{T\eta_o}\alpha\right\rangle_c \Bigg], \qquad \text{(B7)}
\end{aligned}
$$

where $T' = 1 - T$ and $\eta_o' = 1 - \eta_o$.

Charlie is now supposed to make the measurement of $\Pi_0^{a_2,c} = (\mathbb{1} - |0\rangle\langle 0|)_{a_2} \otimes (\mathbb{1} - |0\rangle\langle 0|)_c$ on the state in Eq. (B7). After the measurement of these operators (Π_0) the total state collapses to $\rho^0_{a_1,b_1;b_2} = \mathrm{tr}_{\substack{f_a,f_b\\ g_a,g_c\\ a_2,c}}\Big(|\psi_0\rangle\langle\psi_0| \Big)/N_0$, where $|\psi_0\rangle = \Pi_0^{a_2,c} |\psi\rangle^{tot}_{\substack{a_1,b_1;b_2^{''}\\ f_a^{'},f_b^{'},g_a^{'},g_c^{'}\\ a_2^{''''},c^{''}}}$ and the normalization constants are $N_0 = \mathrm{tr}_{\substack{a_1,b_1,a_2,b_2,c\\ f_a,f_b,g_a,g_c}}\Big(|\psi_0\rangle\langle\psi_0| \Big)$. It must be noted that the state $\rho^0_{a_1,b_1;b_2}$ is obtained with probability $P_0 = \mathrm{tr}_{\substack{a_1,b_1\\ b_2}}\left(\rho^0_{a_1,b_1;b_2}\right)$.

Let us look at the result first

$$
\begin{aligned}
\Pi_0^{a_2,c} |\alpha\rangle_{a_2} |\beta\rangle_c &= \Big(\mathbb{1}_{a_2} \otimes \mathbb{1}_c - |0\rangle_{a_2}\langle 0| \otimes \mathbb{1}_c - \mathbb{1}_{a_2} \otimes |0\rangle_c\langle 0| + |0\rangle_{a_2}\langle 0| \otimes |0\rangle_c\langle 0| \Big) |\alpha\rangle_{a_2} |\beta\rangle_c \\
&= |\alpha\rangle_{a_2} |\beta\rangle_c - e^{-\alpha^2/2} |0\rangle_{a_2} |\beta\rangle_c - e^{-\beta^2/2} |\alpha\rangle_{a_2} |0\rangle_c + e^{-(\alpha^2+\beta^2)/2} |0\rangle_{a_2} |0\rangle_c . \qquad \text{(B8)}
\end{aligned}
$$

leading to

$$
\begin{aligned}
&\Pi_0^{a_2,c} |\alpha\rangle_{a_2} |0\rangle_c = \Pi_0^{a_2,c} |0\rangle_{a_2} |\alpha\rangle_c = 0 \\
&\Pi_0^{a_2,c} |\alpha\rangle_{a_2} |-\alpha\rangle_c = |\alpha\rangle_{a_2} |-\alpha\rangle_c - e^{-\alpha^2/2} |0\rangle_{a_2} |-\alpha\rangle_c - e^{-\alpha^2/2} |\alpha\rangle_{a_2} |0\rangle_c + e^{-\alpha^2} |0\rangle_{a_2} |0\rangle_c . \qquad \text{(B9)}
\end{aligned}
$$

Deploying the results of Eq. (B9) in Eq. (B7), we obtain

$$
\begin{aligned}
&|\psi_0\rangle = \Pi_0^{a_2,c}\,|\psi\rangle^{tot}_{\substack{a_1,b_1;b_2^{''}\\ f_a^{'},f_b^{'},g_a^{'},g_c^{'}\\ a_2^{''''},c^{''}}}\\
&= \frac{1}{2}\Big[|00\rangle_{a_1b_1}|0\rangle_{b_2}\left|\sqrt{T'}\alpha\right\rangle_{f_a}\left|\sqrt{T'}\alpha\right\rangle_{f_b}\otimes\left|2\sqrt{T\eta_o'}\alpha\right\rangle_{g_a}|0\rangle_{g_c}\times 0\\
&\quad + |11\rangle_{a_1b_1}|0\rangle_{b_2}\left|-\sqrt{T'}\alpha\right\rangle_{f_a}\left|-\sqrt{T'}\alpha\right\rangle_{f_b}\otimes|0\rangle_{g_a}\left|-2\sqrt{T\eta_o'}\alpha\right\rangle_{g_c}\times 0\\
&\quad + \left(|01\rangle_{a_1b_1}\left|\sqrt{2T}\alpha\right\rangle_{b_2}\left|\sqrt{T'}\alpha\right\rangle_{f_a}\left|-\sqrt{T'}\alpha\right\rangle_{f_b} + |10\rangle_{a_1b_1}\left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left|-\sqrt{T'}\alpha\right\rangle_{f_a}\left|\sqrt{T'}\alpha\right\rangle_{f_b}\right)\otimes\left|\sqrt{T\eta_o'}\alpha\right\rangle_{g_a}\left|-\sqrt{T\eta_o'}\alpha\right\rangle_{g_c}\otimes\\
&\quad\left(\left|\sqrt{\eta_oT}\alpha\right\rangle_{a_2}\left|-\sqrt{\eta_oT}\alpha\right\rangle_{c} - e^{-\eta_oT\alpha^2/2}|0\rangle_{a_2}\left|-\sqrt{\eta_oT}\alpha\right\rangle_{c} - e^{-\eta_oT\alpha^2/2}\left|\sqrt{\eta_oT}\alpha\right\rangle_{a_2}|0\rangle_{c} + e^{-\eta_oT\alpha^2}|0\rangle_{a_2}|0\rangle_{c}\right)\Big]\\
&= \frac{1}{2}\left(|01\rangle_{a_1b_1}\left|\sqrt{2T}\alpha\right\rangle_{b_2}\left|\sqrt{T'}\alpha\right\rangle_{f_a}\left|-\sqrt{T'}\alpha\right\rangle_{f_b} + |10\rangle_{a_1b_1}\left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left|-\sqrt{T'}\alpha\right\rangle_{f_a}\left|\sqrt{T'}\alpha\right\rangle_{f_b}\right)\otimes\\
&\quad\left|\sqrt{T\eta_o'}\alpha\right\rangle_{g_a}\left|-\sqrt{T\eta_o'}\alpha\right\rangle_{g_c}\otimes|\Psi\rangle_{a_2c}\,, \qquad \text{(B10)}
\end{aligned}
$$

where

$$
|\Psi\rangle_{a_2c} = \left|\sqrt{\eta_oT}\alpha\right\rangle_{a_2}\left|-\sqrt{\eta_oT}\alpha\right\rangle_{c} - e^{-\eta_oT\alpha^2/2}|0\rangle_{a_2}\left|-\sqrt{\eta_oT}\alpha\right\rangle_{c} - e^{-\eta_oT\alpha^2/2}\left|\sqrt{\eta_oT}\alpha\right\rangle_{a_2}|0\rangle_{c} + e^{-\eta_oT\alpha^2}|0\rangle_{a_2}|0\rangle_{c}\,. \qquad \text{(B11)}
$$

It can be further shown that

$$
\begin{aligned}
&\mathrm{tr}\Big(|\Psi\rangle_{a_2c}\langle\Psi|\Big) = \mathrm{tr}\Big[\Big(\left\langle\sqrt{\eta_oT}\alpha\middle|\sqrt{\eta_oT}\alpha\right\rangle\left\langle-\sqrt{\eta_oT}\alpha\middle|-\sqrt{\eta_oT}\alpha\right\rangle + e^{-\eta_oT\alpha^2}\langle 0|0\rangle\left\langle-\sqrt{\eta_oT}\alpha\middle|-\sqrt{\eta_oT}\alpha\right\rangle\\
&\quad + e^{-\eta_oT\alpha^2}\left\langle\sqrt{\eta_oT}\alpha\middle|\sqrt{\eta_oT}\alpha\right\rangle\langle 0|0\rangle + e^{-2\eta_oT\alpha^2}\langle 0|0\rangle\langle 0|0\rangle\Big) + 2\Big(-e^{-\eta_oT\alpha^2/2}\left\langle 0\middle|\sqrt{\eta_oT}\alpha\right\rangle\left\langle-\sqrt{\eta_oT}\alpha\middle|-\sqrt{\eta_oT}\alpha\right\rangle\\
&\quad - e^{-\eta_oT\alpha^2/2}\left\langle\sqrt{\eta_oT}\alpha\middle|\sqrt{\eta_oT}\alpha\right\rangle\left\langle 0\middle|-\sqrt{\eta_oT}\alpha\right\rangle + e^{-\eta_oT\alpha^2}\left\langle 0\middle|\sqrt{\eta_oT}\alpha\right\rangle\left\langle 0\middle|-\sqrt{\eta_oT}\alpha\right\rangle\Big)\\
&\quad + 2\Big(e^{-\eta_oT\alpha^2}\left\langle\sqrt{\eta_oT}\alpha\middle|0\right\rangle\left\langle 0\middle|-\sqrt{\eta_oT}\alpha\right\rangle - e^{-3\eta_oT\alpha^2/2}\langle 0|0\rangle\left\langle 0\middle|-\sqrt{\eta_oT}\alpha\right\rangle\Big) - 2\,e^{-3\eta_oT\alpha^2/2}\left\langle 0\middle|\sqrt{\eta_oT}\alpha\right\rangle\langle 0|0\rangle\Big]\\
&= \Big(1 + e^{-\eta_oT\alpha^2} + e^{-\eta_oT\alpha^2} + e^{-2\eta_oT\alpha^2}\Big) + 2\Big(-e^{-\eta_oT\alpha^2} - e^{-\eta_oT\alpha^2} + e^{-2\eta_oT\alpha^2}\Big) + 2\Big(e^{-2\eta_oT\alpha^2} - e^{-2\eta_oT\alpha^2}\Big) - 2e^{-2\eta_oT\alpha^2}\\
&= 1 - 2e^{-\eta_oT\alpha^2} + e^{-2\eta_oT\alpha^2} = \Big(1 - e^{-\eta_oT\alpha^2}\Big)^2. \qquad \text{(B12)}
\end{aligned}
$$

Hence

$$
\begin{aligned}
&\mathrm{tr}_{\substack{f_a,f_b\\ g_a,g_c\\ a_2,c}}\Big(\left|\psi_0\right\rangle \left\langle\psi_0\right| \Big)\\
&= \frac{\left(1-e^{-\eta_o T\alpha^2}\right)^2}{4}\mathrm{tr}_{f_a,f_b}\Bigg[\Bigg(\left|01\right\rangle_{a_1b_1}\left\langle 01\right| \otimes \left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right| \otimes \left|\sqrt{T'}\alpha\right\rangle_{f_a}\left\langle\sqrt{T'}\alpha\right| \otimes \left|-\sqrt{T'}\alpha\right\rangle_{f_b}\left\langle-\sqrt{T'}\alpha\right|\\
&\qquad + \left|10\right\rangle_{a_1b_1}\left\langle 10\right| \otimes \left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right| \otimes \left|-\sqrt{T'}\alpha\right\rangle_{f_a}\left\langle-\sqrt{T'}\alpha\right| \otimes \left|\sqrt{T'}\alpha\right\rangle_{f_b}\left\langle\sqrt{T'}\alpha\right|\\
&\qquad + \left|01\right\rangle_{a_1b_1}\left\langle 10\right| \otimes \left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right| \otimes \left|\sqrt{T'}\alpha\right\rangle_{f_a}\left\langle-\sqrt{T'}\alpha\right| \otimes \left|-\sqrt{T'}\alpha\right\rangle_{f_b}\left\langle\sqrt{T'}\alpha\right|\\
&\qquad + \left|10\right\rangle_{a_1b_1}\left\langle 01\right| \otimes \left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right| \otimes \left|-\sqrt{T'}\alpha\right\rangle_{f_a}\left\langle\sqrt{T'}\alpha\right| \otimes \left|\sqrt{T'}\alpha\right\rangle_{f_b}\left\langle-\sqrt{T'}\alpha\right|\Bigg)\Bigg]\\
&\qquad \times \mathrm{tr}_{g_a,g_c}\Big[\left|\sqrt{T\eta_o'}\alpha\right\rangle_{g_a}\left\langle\sqrt{T\eta_o'}\alpha\right| \otimes \left|-\sqrt{T\eta_o'}\alpha\right\rangle_{g_c}\left\langle-\sqrt{T\eta_o'}\alpha\right|\Big]\\
&= \frac{\left(1-e^{-\eta_o T\alpha^2}\right)^2}{4}\Big[\left|01\right\rangle_{a_1b_1}\left\langle 01\right| \otimes \left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right| + \left|10\right\rangle_{a_1b_1}\left\langle 10\right| \otimes \left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right|\\
&\qquad + \Big(\left|01\right\rangle_{a_1b_1}\left\langle 10\right| \otimes \left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right| + \left|10\right\rangle_{a_1b_1}\left\langle 01\right| \otimes \left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right|\Big)e^{-4(1-T)\alpha^2}\Big],
\end{aligned}
\tag{B13}
$$

where $\mathrm{tr}\Big(\left|\alpha\right\rangle \left\langle-\alpha\right| \Big) = e^{-2\alpha^2}$. Corresponding probability and normalization constant are

$$
\begin{aligned}
P_0 = N_0 &= \mathrm{tr}_{\substack{a_1,b_1\\ b_2}}\left[\mathrm{tr}_{\substack{f_a,f_b\\ g_a,g_c\\ a_2,c}}\Big(\left|\psi_0\right\rangle \left\langle\psi_0\right| \Big)\right]\\
&= \frac{\left(1-e^{-\eta_o T\alpha^2}\right)^2}{2}.
\end{aligned}
\tag{B14}
$$

This leads to the normalized state

$$
\begin{aligned}
\rho^0_{a_1,b_1,b_2} &= \frac{1}{N_0}\mathrm{tr}_{\substack{f_a,f_b\\ g_a,g_c\\ a_2,c}}\Big(\left|\psi_0\right\rangle \left\langle\psi_0\right| \Big)\\
&= \frac{1}{2}\Big[\left|01\right\rangle_{a_1b_1}\left\langle 01\right| \otimes \left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right| + \left|10\right\rangle_{a_1b_1}\left\langle 10\right| \otimes \left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right|\\
&\qquad + \Big(\left|01\right\rangle_{a_1b_1}\left\langle 10\right| \otimes \left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right| + \left|10\right\rangle_{a_1b_1}\left\langle 01\right| \otimes \left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right|\Big)e^{-4(1-T)\alpha^2}\Big].
\end{aligned}
\tag{B15}
$$

3. Final state obtained after the homodyne measurement

Charlie now performs the homodyne measurement along the quadrature X_θ on mode b_2. Here also we consider that that the homodyne instruments are not perfect. Rather the efficiency of the homodyne detector is given by η_h. Similar to the earlier cases here also the imperfect homodyne detector could be modeled as a passive beam splitter with transmittance η_h. Now the action of the imperfect homodyne measurement along quadrature X_θ will lead to the resultant unnormalized state $\rho_{\mathrm{un}}^{\mathrm{hom},0} = \left\langle X_\theta\right|_{b_2} \mathrm{tr}_{h_b}\left[\left(U_{\eta_h}^{h_b,b_2}\right)\rho^0_{a_1,b_1;b_2}\otimes\left|0\right\rangle_{h_b}\left\langle 0\right|\left(U_{\eta_h}^{h_b,b_2}\right)^\dagger\right]\left|X_\theta\right\rangle_{b_2}$ with normalization $N_0^{\mathrm{hom}} = \mathrm{tr}_{a_1,b_1}\left(\rho_{\mathrm{un}}^{\mathrm{hom},0}\right)$, where X_θ in a mode a is defined as $X_\theta = (ae^{\mathrm{i}\theta} + a^\dagger e^{-\mathrm{i}\theta})/2$ and with the eigenvalue equation as X_θ defined as $X_\theta\left|X_\theta\right\rangle = x_\theta\left|X_\theta\right\rangle$.

Thus, after the homodyne measurement by Charlie, the residual normalized state between Alice and Bob will be

$$\rho_{a_1,b_1} = \frac{\rho_{\mathrm{un}}^{\mathrm{hom},0}}{N_0^{\mathrm{hom}}}. \tag{B16}$$

In this work we consider the measurement of quadrature operator for the choice of $\theta = \frac{\pi}{2}$, i.e., we consider the *momentum-like* quadrature operator P. Now the measurement of P for a coherent state $|\alpha\rangle$ is $\langle P|\alpha\rangle = \frac{1}{\pi^{1/4}} e^{-p^2/2} e^{-\alpha^2 - \mathrm{i}\sqrt{2}\alpha p}$. Now,

$$\begin{aligned}
&\mathrm{tr}_{h_b}\left[\left(U_{\eta_h}^{h_b,b_2}\right)\rho^0_{a_1,b_1;b_2}\otimes|0\rangle_{h_b}\langle 0|\left(U_{\eta_h}^{h_b,b_2}\right)^\dagger\right] \\
&= \frac{1}{2}\mathrm{tr}_{h_b}\left\{\left(U_{\eta_h}^{h_b,b_2}\right)\left[|01\rangle_{a_1b_1}\langle 01|\otimes\left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right| + |10\rangle_{a_1b_1}\langle 10|\otimes\left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right|\right.\right. \\
&\quad\left.\left. + \left(|01\rangle_{a_1b_1}\langle 10|\otimes\left|\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T}\alpha\right| + |10\rangle_{a_1b_1}\langle 01|\otimes\left|-\sqrt{2T}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T}\alpha\right|\right)e^{-4(1-T)\alpha^2}\right]\otimes|0\rangle_{h_b}\langle 0|\left(U_{\eta_h}^{h_b,b_2}\right)^\dagger\right\} \\
&= \frac{1}{2}\mathrm{tr}_{h_b}\left[|01\rangle_{a_1b_1}\langle 01|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right|\otimes\left|\sqrt{2T\eta_h'}\alpha\right\rangle_{h_b}\left\langle\sqrt{2T\eta_h'}\alpha\right|\right. \\
&\quad + |10\rangle_{a_1b_1}\langle 10|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right|\otimes\left|-\sqrt{2T\eta_h'}\alpha\right\rangle_{h_b}\left\langle-\sqrt{2T\eta_h'}\alpha\right| \\
&\quad + \left(|01\rangle_{a_1b_1}\langle 10|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right|\otimes\left|\sqrt{2T\eta_h'}\alpha\right\rangle_{h_b}\left\langle-\sqrt{2T\eta_h'}\alpha\right|\right. \\
&\quad\left.\left. + |10\rangle_{a_1b_1}\langle 01|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right|\otimes\left|-\sqrt{2T\eta_h'}\alpha\right\rangle_{h_b}\left\langle\sqrt{2T\eta_h'}\alpha\right|\right)e^{-4(1-T)\alpha^2}\right] \\
&= \frac{1}{2}\left[|01\rangle_{a_1b_1}\langle 01|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right| + |10\rangle_{a_1b_1}\langle 10|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right|\right. \\
&\quad\left. + \left(|01\rangle_{a_1b_1}\langle 10|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right| + |10\rangle_{a_1b_1}\langle 01|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right|\right)e^{-4T(1-\eta_h')\alpha^2}e^{-4(1-T)\alpha^2}\right] \\
&= \frac{1}{2}\left[|01\rangle_{a_1b_1}\langle 01|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right| + |10\rangle_{a_1b_1}\langle 10|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right|\right. \\
&\quad\left. + \left(|01\rangle_{a_1b_1}\langle 10|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right| + |10\rangle_{a_1b_1}\langle 01|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right|\right)e^{-4(1-T\eta_h)\alpha^2}\right],
\end{aligned} \tag{B17}$$

which leads to

$$\begin{aligned}
\rho_{\mathrm{un}}^{\mathrm{hom},0} &= \langle P|_{b_2}\,\mathrm{tr}_{h_b}\left[\left(U_{\eta_h}^{h_b,b_2}\right)\rho^0_{a_1,b_1;b_2}\otimes|0\rangle_{h_b}\langle 0|\left(U_{\eta_h}^{h_b,b_2}\right)^\dagger\right]|P\rangle_{b_2} \\
&= \frac{1}{2}\langle P|_{b_2}\left[|01\rangle_{a_1b_1}\langle 01|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right| + |10\rangle_{a_1b_1}\langle 10|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right|\right. \\
&\quad\left. + \left(|01\rangle_{a_1b_1}\langle 10|\otimes\left|\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle-\sqrt{2T\eta_h}\alpha\right| + |10\rangle_{a_1b_1}\langle 01|\otimes\left|-\sqrt{2T\eta_h}\alpha\right\rangle_{b_2}\left\langle\sqrt{2T\eta_h}\alpha\right|\right)e^{-4(1-T\eta_h)\alpha^2}\right]|P\rangle_{b_2} \\
&= \frac{e^{-p^2}}{2\sqrt{\pi}}\left[|01\rangle_{a_1b_1}\langle 01|\,e^{-4T\eta_h\alpha^2} + |10\rangle_{a_1b_1}\langle 10|\,e^{-4T\eta_h\alpha^2}\right. \\
&\quad\left. + \left(|01\rangle_{a_1b_1}\langle 10|\,e^{-4T\eta_h\alpha^2-4\mathrm{i}\sqrt{T\eta_h}\alpha p} + |10\rangle_{a_1b_1}\langle 01|\,e^{-4T\eta_h\alpha^2+4\mathrm{i}\sqrt{T\eta_h}\alpha p}\right)e^{-4(1-T\eta_h)\alpha^2}\right] \\
&= \frac{e^{-p^2}e^{-4T\eta_h\alpha^2}}{2\sqrt{\pi}}\left[|01\rangle_{a_1b_1}\langle 01| + |10\rangle_{a_1b_1}\langle 10| + \left(|01\rangle_{a_1b_1}\langle 10|\,e^{-4\mathrm{i}\sqrt{T\eta_h}\alpha p} + |10\rangle_{a_1b_1}\langle 01|\,e^{4\mathrm{i}\sqrt{T\eta_h}\alpha p}\right)e^{-4(1-T\eta_h)\alpha^2}\right],
\end{aligned} \tag{B18}$$

with $N_0^{\mathrm{hom}} = \mathrm{tr}_{a_1,b_1}\left(\rho_{\mathrm{un}}^{\mathrm{hom},0}\right) = \frac{e^{-p^2}e^{-4T\eta_h\alpha^2}}{\sqrt{\pi}}$.

Therefore,

$$\begin{aligned}\rho_{a_1,b_1} &= \frac{\rho_{\rm un}^{\rm hom,0}}{N_0^{\rm hom}}\\ &= \frac{1}{2}\left[|01\rangle_{a_1b_1}\langle 01| + |10\rangle_{a_1b_1}\langle 10| + \left(|01\rangle_{a_1b_1}\langle 10|\, e^{-4\mathrm{i}\sqrt{T\eta_h}\alpha p} + |10\rangle_{a_1b_1}\langle 01|\, e^{4\mathrm{i}\sqrt{T\eta_h}\alpha p}\right) e^{-4(1-T\eta_h)\alpha^2}\right]\\ &= \frac{1}{2}\left[|01\rangle_{a_1b_1}\langle 01| + |10\rangle_{a_1b_1}\langle 10| + h\left(g\,|01\rangle_{a_1b_1}\langle 10| + g^*\,|10\rangle_{a_1b_1}\langle 01|\right)\right], \end{aligned} \tag{B19}$$

where $h = e^{-4(1-T\eta_h)\alpha^2}$ and $g = e^{-4\mathrm{i}\sqrt{T\eta_h}\alpha p}$. The probability of obtaining this final state is given by (B14) $P_0 = \frac{\left(1-e^{-\eta_o T\alpha^2}\right)^2}{2}$.

Appendix C: Logarithmic negativity of hybrid entangled states undergoing photon loss

In our protocol we use the CV part of the HE state for transmission via a lossy quantum channel. It can be shown that under photon losses in the CV part, an HE state can still retain correlations for a particular value of α.

We analyse the amount of correlations that a HE state retains after its CV system is transmitted via a lossy quantum channel. Upon transmission the CV part undergoes photon loss which is directly dependent on the value of α chosen. We show that the correlations in a HE state after its CV part has undergone transmission loss is a non-monotonic function of its coherent amplitude. Specifically, we evaluate the logarithmic negativity [67, 68] of the initial HE state as a function of transmission loss. We find that for $\alpha \approx 0.5$, the HE state is highly robust against noise.

Let us consider the HE state

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}}\Big(|0\rangle_a|\alpha\rangle_b + |1\rangle_a|{-\alpha}\rangle_b\Big). \tag{C1}$$

Suppose that the mode b undergoes photon loss. The process of photon loss can be equivalently modeled as passage through a beam splitter with reflectivity R ($0 \leq R \leq 1$) while the other input to the beam splitter is taken to be vacuum. In such a case, the beam splitter matrix is $\begin{pmatrix}\sqrt{1-R} & \sqrt{R}\\ -\sqrt{R} & \sqrt{1-R}\end{pmatrix}$, where $R = 0$ and $R = 1$ stand for zero photon loss and complete photon loss, respectively. To that end, let us consider that the mode b passes through such a beam splitter while the other input is at $|0\rangle$ in mode c. As a consequence, the total state after passage through the beam splitter becomes

$$|\psi\rangle_{ab}\otimes|0\rangle_c \xrightarrow{\text{bs}} \frac{1}{\sqrt{2}}\left(|0\rangle_a\left|\sqrt{1-R}\alpha\right\rangle_b\left|\sqrt{R}\alpha\right\rangle_c + |1\rangle_a\left|-\sqrt{1-R}\alpha\right\rangle_b\left|-\sqrt{R}\alpha\right\rangle_c\right). \tag{C2}$$

Subsequently, the two-mode state in modes a and b after photon loss is obtained by tracing over the ancillary mode c as

$$\begin{aligned}\rho_{ab}^{\rm loss} &= \mathrm{tr}_c\left[\frac{1}{2}\left(\left|0,\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 0,\sqrt{1-R}\alpha\right|\otimes\left|\sqrt{R}\alpha\right\rangle_c\left\langle\sqrt{R}\alpha\right| + \left|1,-\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 1,-\sqrt{1-R}\alpha\right|\otimes\left|-\sqrt{R}\alpha\right\rangle_c\left\langle-\sqrt{R}\alpha\right|\right.\right.\\ &\quad\left.\left.+\left|0,\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 1,-\sqrt{1-R}\alpha\right|\otimes\left|\sqrt{R}\alpha\right\rangle_c\left\langle-\sqrt{R}\alpha\right| + \left|1,-\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 0,\sqrt{1-R}\alpha\right|\otimes\left|-\sqrt{R}\alpha\right\rangle_c\left\langle\sqrt{R}\alpha\right|\right)\right]\\ &= \frac{1}{2}\left(\left|0,\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 0,\sqrt{1-R}\alpha\right| + \left|1,-\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 1,-\sqrt{1-R}\alpha\right| + e^{-2R\alpha^2}\left|0,\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 1,-\sqrt{1-R}\alpha\right|\right.\\ &\quad\left.+e^{-2R\alpha^2}\left|1,-\sqrt{1-R}\alpha\right\rangle_{ab}\left\langle 0,\sqrt{1-R}\alpha\right|\right)\\ &= \frac{1}{2}\left[|0\rangle_a\langle 0|\otimes\left|\sqrt{1-R}\alpha\right\rangle_b\left\langle\sqrt{1-R}\alpha\right| + |1\rangle_a\langle 1|\otimes\left|-\sqrt{1-R}\alpha\right\rangle_b\left\langle-\sqrt{1-R}\alpha\right|\right.\\ &\quad\left.+e^{-2R\alpha^2}\left(|0\rangle_a\langle 1|\otimes\left|\sqrt{1-R}\alpha\right\rangle_b\left\langle-\sqrt{1-R}\alpha\right| + |1\rangle_a\langle 0|\otimes\left|-\sqrt{1-R}\alpha\right\rangle_b\left\langle\sqrt{1-R}\alpha\right|\right)\right].\end{aligned} \tag{C3}$$

In order to evaluate the entanglement content in this state, we use logarithmic negativity as a measure of entanglement. For a bipartite state $\rho_{ab}^{\rm loss}$ it is defined as $E_N\left(\rho_{ab}^{\rm loss}\right) = \log_2\left|\left|\left(\rho_{ab}^{\rm loss}\right)^{\rm P.T.}\right|\right|_1$, where $||.||_1$ is the trace norm and P.T. stands for partial transpose over any one of the modes a or b. We evaluate the logarithmic negativity for the state after photon loss in Eq. (C3) numerically and is shown in the main text.

Appendix D: Logarithmic negativity of the shared entangled states

In order to evaluate the entanglement content in this state, we use logarithmic negativity as a measure of entanglement. For a bipartite state $\rho_{a_1b_1}$ it is defined as $E_N\left(\rho_{a_1b_1}\right) = \log_2 \left|\left|\rho^{\text{P.T.}}_{a_1b_1}\right|\right|_1$, where $||.||_1$ is the trace norm and P.T. stands for partial transpose over any one of the modes a_1 or b_1. Here, we evaluate the logarithmic negativity for the shared entangled state between Alice and Bob (B19) under partial transposition over mode b_1. The resultant state after the partial transpose is written as

$$\rho^{\text{P.T.}}_{a_1,b_1} = \frac{1}{2}\left[\left|01\right\rangle_{a_1b_1}\left\langle 01\right| + \left|10\right\rangle_{a_1b_1}\left\langle 10\right| \right. \\ \left. + h\left(g\left|00\right\rangle_{a_1b_1}\left\langle 11\right| + g^{*}\left|11\right\rangle_{a_1b_1}\left\langle 00\right|\right)\right], \tag{D1}$$

where $h = e^{-4(1-T\eta_h)\alpha^2}$ and $g = e^{-4\mathrm{i}\sqrt{T\eta_h}\alpha p}$. This leads to the eigenvalues of $\rho^{\text{P.T.}}_{a_1,b_1}$ as $\lambda_1 = \lambda_2 = \frac{1}{2}$, $\lambda_3 = \frac{h}{2}$ and $\lambda_4 = -\frac{h}{2}$. As a consequence, the logarithmic negativity of $\rho_{a_1b_1}$ is given as

$$E_N\left(\rho_{a_1b_1}\right) = \log_2\left(\sum_{k=1}^{4}\left|\lambda_k\right|\right) = \log_2\left(1+h\right). \tag{D2}$$

However, it should be noted that the final state, $\rho_{a_1b_1}$, is only produced with a probability P_0. Consequently, the entanglement between the parties is effectively given as $E_n\left(\rho_{a_1b_1}\right) = P_0\log_2\left(1+h\right)$. The reason for multiplying with the probability P_0 is because it determines the rate of generation of the resultant entangled state. As an example consider $\alpha = 0$, the HE state (A1) is effectively a separable state and therefore cannot yield any correlations after swapping. This behavior is captured by the fact that the final entangled state is produced with probability 0. However, if we only look at the state $\rho_{a_1b_1}$, we find that it is maximally entangled with logarithmic negativity equal to 1. Therefore, it is necessary to include the rate of production in the analysis of entanglement of the final state.

Appendix E: Analysis of secure key rate

In this section we first provide a description of the optimal strategy of an eavesdropper Eve, namely an entangling cloner attack. Next, provide a detailed analysis of the secure key rate under this strategy by Eve.

1. Evaluating the secured key rate

In order to evaluate the secure key rate, we assume the existence of an eavesdropper Eve with system E. We assume that Eve can potentially collaborate with the untrusted party Charlie while also having access to the two quantum channels which are used to transmit the CV systems. We also consider that Eve can perfrom an entangling cloner attack on each of two the quantum channels [48, 69, 70]. However, the most general attack strategy with Eve is a two-mode correlated attack (one mode for each quantum channel). Since, Alice and Bob use a CV system for transmission purposes, the aforementioned attacks have been shown to be the optimal choices in such a case. Moreover, since the quantum channels are assumed to be non-interacting and spatially well separated, the two-mode correlated attack reduces to two independent single-mode entangling cloner attacks.

Specifically, a single mode entangling cloner attack assumes that Eve can split the incoming CV states in both the channels independently using a BS with transmittance T which equal to the loss of the Alice-Charlie and Bob-Charlie channels (assuming that the loss in both the channels is same). The two input modes for this BS correspond to the quantum state being transmitted and a vacuum state (or a thermal state if we consider thermal noise in the channels). Eve, then stores the reflected states in a quantum memory while the transmitted states are sent to Charlie via identity channels having no loss. Subsequently, Eve can then perform a joint measurement on the two retained states (corresponding to Alice-Charlie and Bob-Charlie channels) which are stored in a quantum memory and try to guess the key of Alice or Bob based on the outcomes observed. However, Alice and Bob can estimate the transmission losses of their respective channels given by T. As a consequence, the maximum information that can obtained by Eve becomes a function of the channel loss parameter T and the publicly declared results by Charlie which in turn is bounded by the Holevo bound $\chi(A:E)$ [48, 70].

Since, Alice and Bob share the state $\rho_{a_1b_1}$ with probability for a detailed derivation) P_0, the secure key rate r between Alice and Bob is then given as

$$r \geq P_0\left[I(A:B) - \chi(A:E)\right] \ \ \text{s.t.} \ \ \mathrm{P}_0 = \frac{\left(1-\mathrm{e}^{-\eta_o \mathrm{T}\alpha^2}\right)^2}{2}. \tag{E1}$$

Evaluating the mutual information between Alice and Bob is relatively simple and is accomplished by using their observed joint statistics. If Alice and Bob perform a measurement corresponding to observables A and B, the mutual information between the two parties sharing a state ρ_{ab} is given as $I(A:B) = H(A)+H(B)-H(A,B)$, where $H(A)$ (and $H(B)$) is the Shannon entropy corresponding to the observable A (and B) measured on the state $\rho_a = \mathrm{tr}_b\left(\rho_{ab}\right)$ and, $H(A,B)$ is the Shannon entropy of the observables jointly measured on the state ρ_{ab}.

2. Calculation of $I(A:B)$ and $\chi(A:E)$

In order to evaluate the mutual information we first look at the final state that is shared between Alice and Bob which is given as

$$\begin{aligned}\rho_{a_1b_1} = \frac{1}{2}\Big[&\left|01\right\rangle_{a_1b_1}\left\langle 01\right| + \left|10\right\rangle_{a_1b_1}\left\langle 10\right| \\ &+h\left(g\left|01\right\rangle_{a_1b_1}\left\langle 10\right| + g^*\left|10\right\rangle_{a_1b_1}\left\langle 01\right|\right)\Big], \end{aligned} \tag{E2}$$

where $h = e^{-4(1-T\eta_h)\alpha^2}$ and $g = e^{-4\mathrm{i}\sqrt{T\eta_h}\alpha p}$ with the reduced states of Alice and Bob as

$$\rho_{a_1} = \rho_{b_1} = \frac{1}{2}\left(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|\right). \tag{E3}$$

In the QKD protocol we consider that both Alice and Bob choose the observable $M = \sigma_Z$ to generate a key. The corresponding projective measurement can then be written as $\{\Pi_0, \Pi_1\}$, where $\Pi_0 = \left|0\right\rangle\left\langle 0\right|$ and $\Pi_1 = \mathbb{1} - \Pi_0 = \left|1\right\rangle\left\langle 1\right|$. We also consider that the photon number detectors are imperfect having efficiency η_d. A general m-photon detector with efficiency η_d is described by the measurement operators

$$\Pi_m(\eta_d) = \eta_d^m \sum_k (1-\eta_d)^k \left|k+m\right\rangle\left\langle k+m\right|. \tag{E4}$$

In view of the fact that in our scheme we have only two outcomes (corresponding to Π_0 and $\mathbb{1}-\Pi_0$), an imperfect measurement of σ_Z then corresponds to measurement operators

$$\Pi_0(\eta_d) = \left|0\right\rangle\left\langle 0\right| + (1-\eta_d)\left|1\right\rangle\left\langle 1\right|, \tag{E5a}$$

$$\Pi_1(\eta_d) = \mathbb{1} - \Pi_0 = \eta_d\left|1\right\rangle\left\langle 1\right|. \tag{E5b}$$

We first consider the imperfect measurement of σ_Z on Alice's reduced state ρ_{a_1}. The outcome $\Pi_0(\eta_d)$ occurs with probability $p_0 = \frac{1}{2}\left[1 + (1-\eta_d)\right] = \frac{2-\eta_d}{2}$ while the outcome $\Pi_1(\eta_d)$ occurs with probability $p_1 = 1 - p_0 = \frac{\eta_d}{2}$. As a consequence, the Shannon entropy of imperfectly measuring σ_Z on Alice's reduced state is given as

$$\begin{aligned} H(\sigma_3) &= -p_0\log_2 p_0 - p_1\log_2 p_1 \\ &= -\left(\frac{2-\eta_d}{2}\right)\log_2\left(\frac{2-\eta_d}{2}\right) - \frac{\eta_d}{2}\log_2\frac{\eta_d}{2}. \\ &= 1 - \frac{2-\eta_d}{2}\log_2(2-\eta_d) - \frac{\eta_d}{2}\log_2\eta_d \end{aligned} \tag{E6}$$

Similarly, it can be seen that the same expression also holds true for the imperfect measurement of σ_Z on Bob's reduced state. The measurement operators corresponding to the case when Alice and Bob jointly (and imperfectly) measure σ_Z on their respective reduced states are

$$\begin{aligned}\Pi_{00}(\eta_d) = {}&\left|00\right\rangle\left\langle 00\right| + (1-\eta_d)^2\left|11\right\rangle\left\langle 11\right| + (1-\eta_d)\left|01\right\rangle\left\langle 01\right| \\ &+ (1-\eta_d)\left|10\right\rangle\left\langle 10\right|, \end{aligned} \tag{E7a}$$

$$\Pi_{01}(\eta_d) = \eta_d\left|01\right\rangle\left\langle 01\right| + \eta_d(1-\eta_d)\left|11\right\rangle\left\langle 11\right|, \tag{E7b}$$

$$\Pi_{10}(\eta_d) = \eta_d\left|10\right\rangle\left\langle 10\right| + \eta_d(1-\eta_d)\left|11\right\rangle\left\langle 11\right|, \tag{E7c}$$

$$\Pi_{11}(\eta_d) = \eta_d^2\left|11\right\rangle\left\langle 11\right|, \tag{E7d}$$

which occur with probabilities $p_{00} = 1-\eta_d$, $p_{01} = \frac{\eta_d}{2}$, $p_{10} = \frac{\eta_d}{2}$, and $p_{11} = 0$, respectively. As a consequence, the Shannon entropy for the joint measurement becomes

$$\begin{aligned} H(\sigma_Z,\sigma_Z) &= -p_{00}\log_2 p_{00} - p_{01}\log_2 p_{01} - p_{10}\log_2 p_{10} - p_{11}\log_2 p_{11} \\ &= -(1-\eta_d)\log_2(1-\eta_d) - \eta_d\log_2\frac{\eta_d}{2} = \eta_d - (1-\eta_d)\log_2(1-\eta_d) - \eta_d\log_2\eta_d. \end{aligned} \tag{E8}$$

The mutual information between Alice and Bob cab then be written as

$$\begin{aligned} I(A:B) &= H(\sigma_Z) + H(\sigma_Z) - H(\sigma_Z,\sigma_Z) \\ &= (2-\eta_d) - \left[(2-\eta_d)\log_2(2-\eta_d) - (1-\eta_d)\log_2(1-\eta_d)\right]. \end{aligned} \tag{E9}$$

Evidently, in absence of any imperfection ($\eta_d = 1$) one obtains perfect correlation, i.e, $\lim_{\eta_d\to 1} I(A:B) = 1$. Next, we evaluate the Holevo bound $\chi(A:E)$.

In order to evaluate the Holevo bound, we assume that Eve has access to a purification of the state $\rho_{a_1b_1}$, which we denote by $\rho_{a_1b_1E}$, such that $\rho_e = \mathrm{tr}_{a_1b_1}(\rho_{a_1b_1e})$ is the reduced state of Eve. Moreover, we also assume that Alice's measurement outcomes are represented by rank-1 operators. Since $\rho_{a_1b_1e}$ is pure by definition, we have $S(\rho_{a_1b_1}) = S(\rho_e)$, where $S(X)$ is the Von Neumann entropy of a system X. Moreover, if Alice's measurement outcomes are represented by rank-1 operators, then the reduced state of Bob and Eve conditioned on Alice's outcome x, given by $\rho_{b_1e|x}$, is also pure. Therefore, by definition of Von Neumann entropy, we have $S(\rho_{e|x}) = S(\rho_{b_1|x})$, where $\rho_{b_1|x}$ is the reduced state of Bob conditioned on Alice's outcome x. In this case, the Holevo bound can then be written as [49]

$$\chi(A:E) = S(\rho_{a_1b_1}) - \sum_x p_x S\left(\rho_{b_1|x}\right). \tag{E10}$$

For the state $\rho_{a_1b_1}$ as given in Eq. (E2), its eigenvalues are given as $\lambda_\pm = \frac{1\pm h}{2}$ leading to the von-Neumann entropy as

$$\begin{aligned} S(\rho_{a_1b_1}) &= -\lambda_+ \log_2 \lambda_+ - \lambda_- \log_2 \lambda_- \\ &= -\left(\frac{1+h}{2}\right)\log_2\left(\frac{1+h}{2}\right) - \left(\frac{1-h}{2}\right)\log_2\left(\frac{1-h}{2}\right) \\ &= 1 - \frac{1}{2}\left[(1+h)\log_2(1+h) + (1-h)\log_2(1-h)\right]. \end{aligned} \tag{E11}$$

On the other hand, the reduced states of Bob corresponding to the two outcomes of the imperfect measurement of σ_Z by Alice are given as

$$\begin{aligned} \rho_{b_1|0} &= \frac{\mathrm{tr}_{a_1}\left[\rho_{a_1b_1}\Pi_0(\eta_d)\right]}{\mathrm{tr}\left[\rho_{a_1b_1}\Pi_0(\eta_d)\right]} \\ &= \frac{1}{2-\eta_d}\left(|1\rangle\langle 1| + (1-\eta_d)|0\rangle\langle 0|\right), \end{aligned} \tag{E12a}$$

$$\rho_{b_1|1} = \frac{\mathrm{tr}_{a_1}\left[\rho_{a_1b_1}\Pi_1(\eta_d)\right]}{\mathrm{tr}\left[\rho_{a_1b_1}\Pi_1(\eta_d)\right]} = |1\rangle\langle 1|, \tag{E12b}$$

that lead to

$$\begin{aligned} \sum_{x=0}^{1} p_x S\left(\rho_{b_1|x}\right) &= \frac{2-\eta_d}{2}\left[-\left(\frac{1}{2-\eta_d}\right)\log_2\left(\frac{1}{2-\eta_d}\right)\right. \\ &\left. - \left(\frac{1-\eta_d}{2-\eta_d}\right)\log_2\left(\frac{1-\eta_d}{2-\eta_d}\right)\right] \\ &= \frac{1}{2}\left[(2-\eta_d)\log_2(2-\eta_d) - (1-\eta_d)\log_2(1-\eta_d)\right]. \end{aligned} \tag{E13}$$

As a consequence, the Holevo bound can be written as

$$\begin{aligned} \chi(A:E) &= S(\rho_{a_1b_1}) - \sum_x p_x S\left(\rho_{b_1|x}\right) \\ &= 1 - \frac{1}{2}\left[(1+h)\log_2(1+h) + (1-h)\log_2(1-h)\right] \\ &- \frac{1}{2}\left[(2-\eta_d)\log_2(2-\eta_d) - (1-\eta_d)\log_2(1-\eta_d)\right]. \end{aligned} \tag{E14}$$

By plugging the mutual information given in Eq. (E9) and the Holevo bound, given in Eq. (E14), in the secure key rate, given by Eq. (E1), we obtain

$$\begin{aligned} r &\geq p_0\left[I(A:B) - \chi(A:E)\right] \\ &= p_0\left\{1 - \eta_d + \frac{1}{2}\left[(1+h)\log_2(1+h) + (1-h)\log_2(1-h)\right]\right. \\ &\left. - \frac{1}{2}\left[(2-\eta_d)\log_2(2-\eta_d) - (1-\eta_d)\log_2(1-\eta_d)\right]\right\}. \end{aligned} \tag{E15}$$

Appendix F: Fidelity between the HE states passed through loss-only and lossy+noise channels

In this section, we analyze the impact of thermal noise present in the quantum channel between Alice (Bob) and Charlie. We show that the final state after a loss-only channel is almost equivalent to the final state after passing through a channel characterized by loss and thermal noise. Using this result, we aim to reduce the complexity of the calculation by only focusing on loss-only quantum channels connecting all the parties.

1. General state after channel transmission

Let us consider that an incoming signal passes through a lossy channel having transmittance T with additional thermal noise. Mathematically, the channel transmission can be written as $U_{\mathrm{ch}} : \rho_{\mathrm{s,in}} \to \rho_{\mathrm{s,out}}$, where $\rho_{\mathrm{s,in}}$ ($\rho_{\mathrm{s,in}}$) is input (output) state of the channel. Such transmission can be modeled as follows. First, the incoming state (in mode a) is mixed with an ancilla initialized in a thermal state (in mode b) via a beam splitter (BS) with transmittance T and two output modes. Subsequently, output of the quantum channel is obtained by tracing out the outgoing ancilla mode of the BS.

The action of a BS with transmittance T is described in terms of a unitary operation U_T^{ab} on the input modes a and b that leads to the transformation matrix between the input and the output modes, labelled by a' and b', as

$$\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \to \begin{pmatrix} \hat{a}' \\ \hat{b}' \end{pmatrix} = \begin{pmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{pmatrix}\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}, \tag{F1}$$

where $\hat{a}$ corresponds to the annihilation operator for the mode a and $T = 0.5$ represents a balanced (50 : 50) BS. As a consequence, the action of the channel on a coherent state ($|\alpha\rangle$) in mode a is described as $U_T^{ab}|\alpha\rangle_a \otimes |\beta\rangle_b \to |\alpha\rangle_{a'} \otimes |\beta\rangle_{b'} = \left|\sqrt{T}\alpha + \sqrt{1-T}\beta\right\rangle_a \otimes \left|\sqrt{T}\beta - \sqrt{1-T}\alpha\right\rangle_b = \left|\sqrt{T}\alpha + \sqrt{1-T}\beta, \sqrt{T}\beta - \sqrt{1-T}\alpha\right\rangle_{ab}$.

Let us consider that, in the coherent state basis, the incoming signal is in the quantum state given by $\rho_{\mathrm{s,in}} = \int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}C(\alpha,\beta)|\alpha\rangle_a\langle\beta|$ while the ancilla thermal state described as $\rho_{\mathrm{anc,th}} = (1-x)\sum_k x^k |k\rangle_b\langle k| = (1-x)\int\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}e^{-\frac{|\eta|^2+|\zeta|^2}{2}+x\eta^*\zeta}|\eta\rangle_b\langle\zeta|$, where $x = \frac{\bar{n}}{1+\bar{n}}$ such that $\bar{n}$ is the average number of thermal photon. In view of the action of a BS on the coherent states, one can easily show that

$$\begin{aligned}
\rho_{\text{out}} &= U_T^{ab}\rho_{\text{s,in}} \otimes \rho_{\text{anc,th}} \left(U_T^{ab}\right)^\dagger \\
&= (1-x)\int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}C(\alpha,\beta)e^{-\frac{|\eta|^2+|\zeta|^2}{2}+x\eta^*\zeta}\left[U_T^{ab}\left|\alpha,\eta\right\rangle_{ab}\left\langle\beta,\zeta\right|\left(U_T^{ab}\right)^\dagger\right] \\
&= (1-x)\int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}C(\alpha,\beta)e^{-\frac{|\eta|^2+|\zeta|^2}{2}+x\eta^*\zeta}\left|\sqrt{T}\alpha+\sqrt{1-T}\eta,\sqrt{T}\eta-\sqrt{1-T}\alpha\right\rangle \\
&\quad \otimes\left\langle\sqrt{T}\beta+\sqrt{1-T}\zeta,\sqrt{T}\zeta-\sqrt{1-T}\beta\right|. \qquad \text{(F2)}
\end{aligned}$$

Consequently, the channel output signal state becomes

$$\begin{aligned}
&U_{\text{ch}}:\rho_{\text{s,in}}\to\rho_{\text{s,out}}=\text{Tr}_{\text{anc}}\left(\rho_{\text{out}}\right) \\
&= (1-x)\int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}C(\alpha,\beta)e^{-\frac{|\eta|^2+|\zeta|^2}{2}+x\eta^*\zeta}\left|\sqrt{T}\alpha+\sqrt{1-T}\eta\right\rangle_a\left\langle\sqrt{T}\beta+\sqrt{1-T}\zeta\right| \\
&\quad\times\left\langle\sqrt{T}\zeta-\sqrt{1-T}\beta\middle|\sqrt{T}\eta-\sqrt{1-T}\alpha\right\rangle \\
&= (1-x)\int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}C(\alpha,\beta)e^{-\frac{1-T}{2}\left(|\alpha|^2+|\beta|^2\right)+(1-T)\alpha\beta^*}e^{-\frac{1+T}{2}\left(|\eta|^2+|\zeta|^2\right)+x\eta^*\zeta+T\eta\zeta^*} \\
&\quad\times e^{\sqrt{T(1-T)}\left[\frac{\alpha^*\eta+\alpha\eta^*}{2}+\frac{\beta^*\zeta+\beta\zeta^*}{2}-(\beta^*\eta+\alpha\zeta^*)\right]}\left|\sqrt{T}\alpha+\sqrt{1-T}\eta\right\rangle_a\left\langle\sqrt{T}\beta+\sqrt{1-T}\zeta\right| \\
&= (1-x)\int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}C(\alpha,\beta)e^{-\frac{1-T}{2}\left(|\alpha|^2+|\beta|^2\right)+(1-T)\alpha\beta^*}e^{-\frac{1+T}{2}\left(|\eta|^2+|\zeta|^2\right)+x\eta^*\zeta+T\eta\zeta^*} \\
&\quad\times e^{\sqrt{T(1-T)}\left[\frac{\alpha^*\eta+\alpha\eta^*}{2}+\frac{\beta^*\zeta+\beta\zeta^*}{2}-(\beta^*\eta+\alpha\zeta^*)\right]}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}\left|\lambda\right\rangle\left\langle\omega\right|\left\langle\lambda\middle|\sqrt{T}\alpha+\sqrt{1-T}\eta\right\rangle\left\langle\sqrt{T}\beta+\sqrt{1-T}\zeta\middle|\omega\right\rangle \\
&= (1-x)\int \frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}C(\alpha,\beta)e^{-\frac{1-T}{2}\left(|\alpha|^2+|\beta|^2\right)+(1-T)\alpha\beta^*}e^{-\frac{1+T}{2}\left(|\eta|^2+|\zeta|^2\right)+x\eta^*\zeta+T\eta\zeta^*} \\
&\quad\times e^{\sqrt{T(1-T)}\left[\frac{\alpha^*\eta+\alpha\eta^*}{2}+\frac{\beta^*\zeta+\beta\zeta^*}{2}-(\beta^*\eta+\alpha\zeta^*)\right]}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}\left|\lambda\right\rangle\left\langle\omega\right|e^{-\frac{|\lambda|^2+|\sqrt{T}\alpha+\sqrt{1-T}\eta|^2}{2}+\lambda^*\left(\sqrt{T}\alpha+\sqrt{1-T}\eta\right)} \\
&\quad\times e^{-\frac{|\omega|^2+|\sqrt{T}\beta+\sqrt{1-T}\zeta|^2}{2}+\left(\sqrt{T}\beta^*+\sqrt{1-T}\zeta^*\right)\omega} \\
&= (1-x)\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}}\left|\lambda\right\rangle\left\langle\omega\right|\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}C(\alpha,\beta)e^{-\frac{|\alpha|^2+|\beta|^2}{2}+(1-T)\alpha\beta^*+\sqrt{T}(\lambda^*\alpha+\omega\beta^*)} \\
&\quad\times\int\frac{d^2\eta}{\pi}\frac{d^2\zeta}{\pi}e^{-\left(|\eta|^2+|\zeta|^2\right)+x\eta^*\zeta+T\eta\zeta^*}e^{-\sqrt{T(1-T)}(\beta^*\eta+\alpha\zeta^*)+\sqrt{1-T}(\lambda^*\eta+\omega\zeta^*)} \\
&= \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\left|\lambda\right\rangle\left\langle\omega\right|\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}C(\alpha,\beta)e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\frac{1-T}{1-Tx}\alpha\beta^*+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\beta^*)}. \qquad \text{(F3)}
\end{aligned}$$

In the case of a loss-only channel, i.e., in absence of additional thermal noise ($x=0$), Eq. (F3) reduces to

$$\begin{aligned}
&\lim_{x\to0}U_{\text{ch}}:\rho_{\text{s,in}}\to\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}C(\alpha,\beta)e^{-\frac{1-T}{2}\left(|\alpha|^2+|\beta|^2\right)+(1-T)\alpha\beta^*}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2+T\left(|\alpha|^2+|\beta|^2\right)}{2}+\sqrt{T}(\lambda^*\alpha+\omega\beta^*)}\left|\lambda\right\rangle\left\langle\omega\right| \\
&=\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}C(\alpha,\beta)e^{-\frac{1-T}{2}\left(|\alpha|^2+|\beta|^2\right)+(1-T)\alpha\beta^*}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}\left|\lambda\right\rangle\left\langle\lambda\middle|\sqrt{T}\alpha\right\rangle\left\langle\sqrt{T}\beta\middle|\right\rangle\omega\left\langle\omega\right| \\
&=\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}C(\alpha,\beta)e^{-\frac{1-T}{2}\left(|\alpha|^2+|\beta|^2\right)+(1-T)\alpha\beta^*}\left|\sqrt{T}\alpha\right\rangle\left\langle\sqrt{T}\beta\right|. \qquad \text{(F4)}
\end{aligned}$$

2. Hybrid state after channel transmission

In our protocol, each party transmits a coherent state through a quantum channel which may have transmission loss as well as thermal noise. In the following, we evaluate all possible terms that may arise when the parties transmit the continuous variable part through the aforementioned channel. In such a case, Eq. (F3) leads to

$$\begin{aligned} U_{\mathrm{ch}}: |\gamma\rangle\langle\gamma| \rightarrow & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\delta^2\left(\beta-\gamma\right)\delta^2\left(\alpha-\gamma\right) \\ & \times e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\frac{1-T}{1-Tx}\alpha\beta^*+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\beta^*)} \\ = & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\times e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma+\omega\gamma^*)} \\ = & e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2}\frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma+\omega\gamma^*)}\,|\lambda\rangle\langle\omega|\,, \end{aligned} \tag{F5}$$

$$\begin{aligned} U_{\mathrm{ch}}: |\gamma\rangle\langle-\gamma| \rightarrow & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\delta^2\left(\beta+\gamma\right)\delta^2\left(\alpha-\gamma\right) \\ & \times e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\frac{1-T}{1-Tx}\alpha\beta^*+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\beta^*)} \\ = & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\times e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma-\omega\gamma^*)} \\ = & e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2}\frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma-\omega\gamma^*)}\,|\lambda\rangle\langle\omega|\,, \end{aligned} \tag{F6}$$

$$\begin{aligned} U_{\mathrm{ch}}: |-\gamma\rangle\langle\gamma| \rightarrow & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\delta^2\left(\beta-\gamma\right)\delta^2\left(\alpha+\gamma\right) \\ & \times e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\frac{1-T}{1-Tx}\alpha\beta^*+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\beta^*)} \\ = & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\times e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2+\frac{\sqrt{T}(1-x)}{1-Tx}(-\lambda^*\gamma+\omega\gamma^*)} \\ = & e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2}\frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma-\omega\gamma^*)}\,|\lambda\rangle\langle\omega|\,, \end{aligned} \tag{F7}$$

$$\begin{aligned} U_{\mathrm{ch}}: |-\gamma\rangle\langle-\gamma| \rightarrow & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\int\frac{d^2\alpha}{\pi}\frac{d^2\beta}{\pi}\delta^2\left(\beta+\gamma\right)\delta^2\left(\alpha+\gamma\right) \\ & \times e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\frac{1-T}{1-Tx}\alpha\beta^*+\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\beta^*)} \\ = & \frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\times e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma+\omega\gamma^*)} \\ = & e^{-\frac{T(1-x)}{1-Tx}|\gamma|^2}\frac{1-x}{1-Tx}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\gamma+\omega\gamma^*)}\,|\lambda\rangle\langle\omega|\,. \end{aligned} \tag{F8}$$

A hybrid-entangled (HE) state (A7) defined as

$$|\psi\rangle_{\mathrm{he}} = \frac{1}{\sqrt{2}}\left(|0,\alpha\rangle + |1,-\alpha\rangle\right), \tag{F9}$$

for which the multiphoton coherent state part is transmitted through a general (both lossy and noisy) channel. Using the results obtained above it can be seen that, after the transmission, the final state is

$$\begin{aligned}\rho^{\mathrm{ch,he}}(T,x) &= U_{\mathrm{ch}} : \rho_{\mathrm{he}} = U_{\mathrm{ch}} : \frac{1}{2}\left(|0\rangle\langle 0| \otimes |\alpha\rangle\langle\alpha| + |0\rangle\langle 1| \otimes |\alpha\rangle\langle -\alpha| + |1\rangle\langle 0| -\alpha\rangle\langle\alpha| + |1\rangle\langle 1| \otimes |-\alpha\rangle\langle -\alpha|\right)\\ &= \frac{e^{-\frac{T(1-x)}{1-Tx}|\alpha|^2}}{2}\frac{1-x}{1-Tx}\int \frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi} e^{-\frac{|\lambda|^2+|\omega|^2}{2}+\frac{x(1-T)}{1-Tx}\lambda^*\omega}\,|\lambda\rangle\langle\omega|\\ &\otimes\left[e^{\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\alpha^*)}\,|0\rangle\langle 0| + e^{\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha-\omega\alpha^*)}\,|0\rangle\langle 1| + e^{-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha-\omega\alpha^*)}\,|1\rangle\langle 0| + e^{-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\alpha^*)}\,|1\rangle\langle 1|\right].\end{aligned}\tag{F10}$$

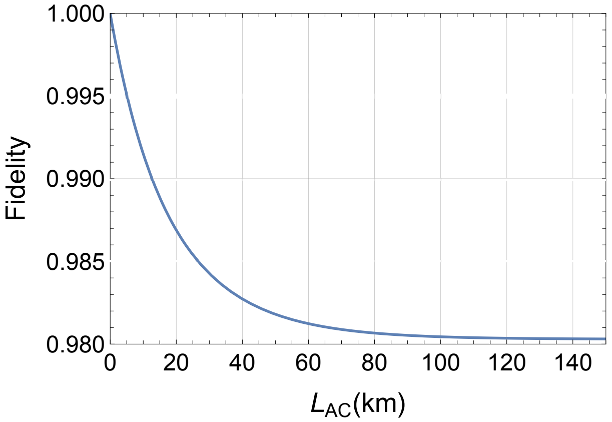


FIG. 7. Dependence of fidelity between the states obtained from initial HE state after transmission through loss-only and both loss+noise channels.

3. HE-state at Charlie's end after transmission through loss-only channel and a general channel

Let us consider that Alice and Bob prepare their individual HE states $|\psi\rangle_{a_1a_2}$ and $|\psi\rangle_{b_1b_2}$ as

$$|\psi\rangle_{a_1a_2} = \frac{1}{\sqrt{2}}\left(|0,\alpha\rangle_{a_1a_2} + |1,-\alpha\rangle_{a_1a_2}\right) \tag{F11a}$$

$$|\psi\rangle_{b_1b_2} = \frac{1}{\sqrt{2}}\left(|0,\alpha\rangle_{b_1b_2} + |1,-\alpha\rangle_{b_1b_2}\right), \tag{F11b}$$

where $|0,\alpha\rangle_{a_1a_2} = |0\rangle_{a_1}|\alpha\rangle_{a_2}$. Using Eq. (F10) one can show that total 4-mode state at the input of Charlie after passing through a general channel is given by

$$\begin{aligned}
&\rho_{\text{in,tot}}(T,x)=\rho^{\text{ch}}_{a_1a_2}\otimes\rho^{\text{ch}}_{b_1b_2}\\
&=\frac{e^{-\frac{2T(1-x)}{1-Tx}|\alpha|^2}}{4}\left(\frac{1-x}{1-Tx}\right)^2\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}\frac{d^2\chi}{\pi}\frac{d^2\xi}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2+|\chi|^2+|\xi|^2}{2}+\frac{x(1-T)}{1-Tx}(\lambda^*\omega+\chi^*\xi)}\left|\lambda\right\rangle_{a_2}\left\langle\omega\right|\otimes\left|\chi\right\rangle_{b_2}\left\langle\xi\right|\\
&\otimes\left[e^{\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\alpha^*)}\left|0\right\rangle_{a_1}\left\langle0\right|+e^{\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha-\omega\alpha^*)}\left|0\right\rangle_{a_1}\left\langle1\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha-\omega\alpha^*)}\left|1\right\rangle_{a_1}\left\langle0\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}(\lambda^*\alpha+\omega\alpha^*)}\left|1\right\rangle_{a_1}\left\langle1\right|\right]\\
&\otimes\left[e^{\frac{\sqrt{T}(1-x)}{1-Tx}(\chi^*\alpha+\xi\alpha^*)}\left|0\right\rangle_{b_1}\left\langle0\right|+e^{\frac{\sqrt{T}(1-x)}{1-Tx}(\chi^*\alpha-\xi\alpha^*)}\left|0\right\rangle_{b_1}\left\langle1\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}(\chi^*\alpha-\xi\alpha^*)}\left|1\right\rangle_{b_1}\left\langle0\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}(\chi^*\alpha+\xi\alpha^*)}\left|1\right\rangle_{b_1}\left\langle1\right|\right]\\
&=\frac{e^{-\frac{2T(1-x)}{1-Tx}|\alpha|^2}}{4}\left(\frac{1-x}{1-Tx}\right)^2\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}\frac{d^2\chi}{\pi}\frac{d^2\xi}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2+|\chi|^2+|\xi|^2}{2}+\frac{x(1-T)}{1-Tx}(\lambda^*\omega+\chi^*\xi)}\left|\lambda,\chi\right\rangle_{a_2b_2}\left\langle\omega,\xi\right|\\
&\otimes\Bigg[\Bigg(e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle0,0\right|+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle0,1\right|\\
&+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle0,0\right|+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle0,1\right|\Bigg)\\
&+\Bigg(e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle1,1\right|\\
&+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle1,1\right|\Bigg)\\
&+\Bigg(e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle0,0\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle0,1\right|\\
&+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle0,0\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle0,1\right|\Bigg)\\
&+\Bigg(e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*-\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle1,1\right|\\
&+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda^*+\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle1,1\right|\Bigg)\Bigg].
\end{aligned}\tag{F12}$$

It should be noted, in absence of the additional thermal noise ($x\to0$) the transmission channel simply becomes simply a loss-only channel and the state at the input of Charlie (after transmission) can be written as

$$\begin{aligned}
&\rho_{\text{in,tot}}(T)=\lim_{x\to0}\rho_{\text{in,tot}}(T,x)\\
&=\frac{e^{-2T|\alpha|^2}}{4}\int\frac{d^2\lambda}{\pi}\frac{d^2\omega}{\pi}\frac{d^2\chi}{\pi}\frac{d^2\xi}{\pi}e^{-\frac{|\lambda|^2+|\omega|^2+|\chi|^2+|\xi|^2}{2}}\left|\lambda,\chi\right\rangle_{a_2b_2}\left\langle\omega,\xi\right|\\
&\otimes\Bigg[\Bigg(e^{\sqrt{T}[(\lambda^*+\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle0,0\right|+e^{\sqrt{T}[(\lambda^*+\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle0,1\right|+e^{\sqrt{T}[(\lambda^*-\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle0,0\right|\\
&+e^{\sqrt{T}[(\lambda^*-\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle0,1\right|\Bigg)+\Bigg(e^{\sqrt{T}[(\lambda^*+\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{\sqrt{T}[(\lambda^*+\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|0,0\right\rangle_{a_1b_1}\left\langle1,1\right|\\
&+e^{\sqrt{T}[(\lambda^*-\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{\sqrt{T}[(\lambda^*-\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|0,1\right\rangle_{a_1b_1}\left\langle1,1\right|\Bigg)\\
&+\Bigg(e^{-\sqrt{T}[(\lambda^*-\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle0,0\right|+e^{-\sqrt{T}[(\lambda^*-\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle0,1\right|+e^{-\sqrt{T}[(\lambda^*+\chi^*)\alpha-(\omega+\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle0,0\right|\\
&+e^{-\sqrt{T}[(\lambda^*+\chi^*)\alpha-(\omega-\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle0,1\right|\Bigg)+\Bigg(e^{-\sqrt{T}[(\lambda^*-\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{-\sqrt{T}[(\lambda^*-\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|1,0\right\rangle_{a_1b_1}\left\langle1,1\right|\\
&+e^{-\sqrt{T}[(\lambda^*+\chi^*)\alpha+(\omega-\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle1,0\right|+e^{-\sqrt{T}[(\lambda^*+\chi^*)\alpha+(\omega+\xi)\alpha^*]}\left|1,1\right\rangle_{a_1b_1}\left\langle1,1\right|\Bigg)\Bigg].
\end{aligned}\tag{F13}$$

4. Fidelity between HE-states at Charlie's end after transmission through loss-only channel and a general channel

In this subsection we evaluate how different the state given in Eq. (F12) is from the one given in Eq. (F13) for a given loss and thermal noise. In order to estimate it we evaluate the fidelity between the states given by Eq. (F12) and Eq. (F13) as

$$
\begin{aligned}
F &= \mathrm{tr}\left[\rho_{\mathrm{in,tot}}(\mathrm{T})\rho_{\mathrm{in,tot}}(\mathrm{T,x})\right]\\
&= \frac{e^{-2T\frac{2-x(1+T)}{1-Tx}|\alpha|^2}}{16}\left(\frac{1-x}{1-Tx}\right)^2\int\frac{d^2\Lambda_i}{\pi^8}e^{-\left(|\lambda_1|^2+|\omega_1|^2+|\chi_1|^2+|\xi_1|^2+|\lambda_2|^2+|\omega_2|^2+|\chi_2|^2+|\xi_2|^2\right)+(\omega_2^*\lambda_1+\xi_2^*\chi_1+\omega_1^*\lambda_2+\xi_1^*\chi_2)}\\
&\quad\times\Bigg[\Bigg(e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha+(\omega_1+\xi)\alpha_1^*]+\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha+(\omega_2+\xi_2)\alpha^*]}+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha+(\omega_1-\xi)\alpha_1^*]+\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha+(\omega_2+\xi_2)\alpha^*]}\\
&\quad+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha+(\omega_1+\xi)\alpha_1^*]+\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha+(\omega_2-\xi_2)\alpha^*]}+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha+(\omega_1-\xi)\alpha_1^*]+\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha+(\omega_2-\xi_2)\alpha^*]}\Bigg)\\
&\quad+\Bigg(e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha-(\omega_1-\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha-(\omega_2+\xi_2)\alpha^*]}+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha-(\omega_1+\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha-(\omega_2+\xi_2)\alpha^*]}\\
&\quad+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha-(\omega_1-\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha-(\omega_2-\xi_2)\alpha^*]}+e^{\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha-(\omega_1+\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha-(\omega_2-\xi_2)\alpha^*]}\Bigg)\\
&\quad+\Bigg(e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha-(\omega_1+\xi_1)\alpha^*]+\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha-(\omega_2-\xi_2)\alpha^*]}+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha-(\omega_1-\xi_1)\alpha^*]+\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha-(\omega_2-\xi_2)\alpha^*]}\\
&\quad+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha-(\omega_1+\xi_1)\alpha^*]+\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha-(\omega_2+\xi_2)\alpha^*]}+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha-(\omega_1-\xi_1)\alpha^*]+\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha-(\omega_2+\xi_2)\alpha^*]}\Bigg)\\
&\quad+\Bigg(e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha+(\omega_1-\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha+(\omega_2-\xi_2)\alpha^*]}+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*-\chi_1^*)\alpha+(\omega_1+\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha+(\omega_2-\xi_2)\alpha^*]}\\
&\quad+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha+(\omega_1-\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*-\chi_2^*)\alpha+(\omega_2+\xi_2)\alpha^*]}+e^{-\frac{\sqrt{T}(1-x)}{1-Tx}[(\lambda_1^*+\chi_1^*)\alpha+(\omega_1+\xi_1)\alpha^*]-\sqrt{T}[(\lambda_2^*+\chi_2^*)\alpha+(\omega_2+\xi_2)\alpha^*]}\Bigg)\Bigg],
\end{aligned}
\tag{F14}
$$

where $d^2\Lambda_i = d^2\lambda_i d^2\omega_i d^2\chi_i d^2\xi_i$ $(i = 1, 2)$.

Let us now consider a generic integral as

$$
\begin{aligned}
I_1 &= \frac{e^{-2T\frac{2-x(1+T)}{1-Tx}|\alpha|^2}}{16}\left(\frac{1-x}{1-Tx}\right)^2\int\frac{d^2\Lambda_i}{\pi^8}e^{-\left(|\lambda_1|^2+|\omega_1|^2+|\chi_1|^2+|\xi_1|^2+|\lambda_2|^2+|\omega_2|^2+|\chi_2|^2+|\xi_2|^2\right)+(\omega_2^*\lambda_1+\xi_2^*\chi_1+\omega_1^*\lambda_2+\xi_1^*\chi_2)}\\
&\quad\times e^{[(A_1\lambda_1^*+B_1\chi_1^*)\alpha+(C_1\omega_1+D_1\xi_1)\alpha_1^*]+[(A_2\lambda_2^*+B_2\chi_2^*)\alpha+(C_2\omega_2+D_2\xi_2)\alpha^*]}\\
&= \frac{e^{-2T\frac{2-x(1+T)}{1-Tx}|\alpha|^2}}{16}\left(\frac{1-x}{1-Tx}\right)^2\int\frac{d^2\lambda_1}{\pi}\frac{d^2\omega_1}{\pi}\frac{d^2\chi_1}{\pi}\frac{d^2\xi_1}{\pi}e^{-\left(|\lambda_1|^2+|\omega_1|^2+|\chi_1|^2+|\xi_1|^2\right)+(A_1\lambda_1^*+B_1\chi_1^*)\alpha+(C_1\omega_1+D_1\xi_1)\alpha_1^*}\\
&\quad\times\int\frac{d^2\lambda_2}{\pi}\frac{d^2\omega_2}{\pi}\frac{d^2\chi_2}{\pi}\frac{d^2\xi_2}{\pi}e^{-\left(|\lambda_2|^2+|\omega_2|^2+|\chi_2|^2+|\xi_2|^2\right)+(\omega_2^*\lambda_1+\xi_2^*\chi_1+\omega_1^*\lambda_2+\xi_1^*\chi_2)+(A_2\lambda_2^*+B_2\chi_2^*)\alpha+(C_2\omega_2+D_2\xi_2)\alpha^*}\\
&= \frac{e^{-2T\frac{2-x(1+T)}{1-Tx}|\alpha|^2}}{16}\left(\frac{1-x}{1-Tx}\right)^2\int\frac{d^2\lambda_1}{\pi}\frac{d^2\omega_1}{\pi}\frac{d^2\chi_1}{\pi}\frac{d^2\xi_1}{\pi}e^{-\left(|\lambda_1|^2+|\omega_1|^2+|\chi_1|^2+|\xi_1|^2\right)+(A_1\lambda_1^*+B_1\chi_1^*)\alpha+(C_1\omega_1+D_1\xi_1)\alpha_1^*}\\
&\quad\times e^{(A_2\omega_1^*+B_2\xi_1^*)\alpha+(C_2\lambda_1+D_2\chi_1)\alpha^*}\\
&= \frac{e^{-2T\frac{2-x(1+T)}{1-Tx}|\alpha|^2}}{16}\left(\frac{1-x}{1-Tx}\right)^2 e^{[(A_1C_2+A_2C_1)+(B_1D_2+B_2D_1)]|\alpha|^2}.
\end{aligned}
\tag{F15}
$$

Using the result of the generic integral (F15), from (F14) we get

$$
\begin{aligned}
F &= \frac{e^{-2T\frac{2-x(1+T)}{1-Tx}|\alpha|^2}}{16}\left(\frac{1-x}{1-Tx}\right)^2\times 16e^{4T\frac{(1-x)}{1-Tx}}\\
&= e^{-\frac{2Tx(1-T)}{1-Tx}|\alpha|^2}\left(\frac{1-x}{1-Tx}\right)^2.
\end{aligned}
\tag{F16}
$$

This analysis is important because a fully general calculation, in which we consider the quantum channels to be characterized by transmission loss and thermal noise is far more involved and lengthy to perform than if we only consider the quantum channels to be characterized by transmission loss only. This can be seen from the form of the 4-mode states at Charlie's input before the entanglement-swapping operation. In view of the result represented in Fig. 7, we believe that a consideration of such a general channel may not yield any significantly different result from a loss-only channel at the cost of a very difficult, lengthy and complicated calculation. It may be noted that in the case of a loss-only channel the ancilla thermal state is replaced by a vacuum state. This simplifies the calculation greatly as now we can proceed with a pure state approach in which the total state is a pure state. In this case, it is possible to take a partial trace over the ancilla after Charlie's operations. This simplifies the overall calculation. However, such a simplification is not possible when we consider an ancilla in the thermal state for which the overall state is mixed. This increases the number of terms to be calculated by four times in comparison with the pure state approach.