Posters

August 26, 2024 (Mon.) [Poster Session I]

Evidence-Based Quantum-Information Processing: Applications on Photonic Quantum Systems

Y. S. Teo[1] * S. U. Shringarpure[1] † H. Jeong[1] ‡ N. Prasannan[2] B. Brecht[2]
C. Silberhorn[2] M. Evans[3] § D. Mogilevtsev[4] L. L. Sánchez-Soto[5 6]

[1] *Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea*
[2] *Integrated Quantum Optics Group, Applied Physics, University of Paderborn, 33098 Paderborn, Germany*
[3] *Department of Statistical Sciences, University of Toronto, Toronto, Ontario, M5S 3G3, Canada*
[4] *B. I. Stepanov Institute of Physics, NAS of Belarus, Nezavisimosti ave. 68, 220072 Minsk, Belarus*
[5] *Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain*
[6] *Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany*

Abstract. The relative-belief inference method that is purely data-evidence-based is introduced to quantum information. It can ascertain the effective dimension of any optical mode, reliably evaluate the quality of a multiphoton source and track nontrivially encoded interacting degrees of freedom, amongst other possible applications.

Keywords: statistical inference, quantum optics

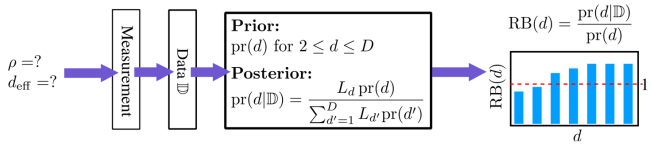


Figure 1: The relative-belief dimension certification scheme.

1 Introduction

Despite residing in an infinite-dimensional Hilbert space, a physical quantum state of light ϱ usually possesses distribution tails that permits its description with a smaller truncated subspace. Ascertaining the effective dimension d_{eff} needed to fully contain ϱ is thus crucial in quantum-information processing. The paradigm of relative belief (RB) [1], developed by Evans for statistical inference, is introduced to quantum information in this work to unambiguously determine which dimensions are plausible according to the experimental data as evidence. To each possible Hilbert-space dimension d, one first assigns prior probabilities reflecting one's prior conviction concerning the dimension of the unknown state ϱ. After experimental data are obtained, the plausible dimensions are those for which the respective posterior probabilities (defined by maximized likelihoods L_d) are larger than the prior ones [$\text{RB}(d) > 1$]. The effective dimension $d_{\text{eff}} = d_{\text{RB}}$ is then the smallest dimension such that $\text{RB}(d) > 1$. Figure 1 below schematically describes such a relative-belief dimension certification (RBDC). The technical version is found in [2].

*ys_teo@snu.ac.kr
†saurabh.s@snu.ac.kr
‡h.jeong37@gmail.com
§mevansthree.evans@utoronto.ca

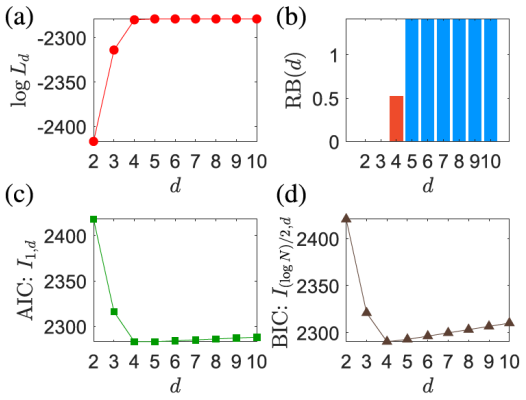


Figure 2: (a) Log-likelihood values for various d that lead to the performances of uniform-prior-based RBDC (red and blue bars refer to RB ratios smaller and greater than one), (b) AIC and (c) BIC based on a single-von Neumann-basis dataset from measuring $N = 1000$ copies of the unknown ten-dimensional $\varrho \mathrel{\widehat{=}} \text{diag}(1,1,1,1,1,1,0,0,0,0)/6$. The respective effective dimensions selected by each of these three methods may be readily read off as $d_{\text{RB}} = 5$ and $d_{\text{AIC}} = 4 = d_{\text{BIC}}$ from the graphs. The red RB-ratio bar also indicates that evidence is found against the smaller d_{AIC} and d_{BIC} values.

2 Key idea

The key idea is that RB measures the belief strengths that ϱ is contained in a d-dimensional space before and after the experiment. The posterior tells us how strongly we should believe that $d_{\text{eff}} = d_{\text{RB}}$. Being a Bayesian framework, RB accepts additional assumptions that are either incorporated into the prior distribution or likelihood model to be collectively and systematically tested, so no spurious or unverified assumptions are invoked.

We show that in general, RB never quotes a d_{eff} that is smaller than those by a large class of information cri-

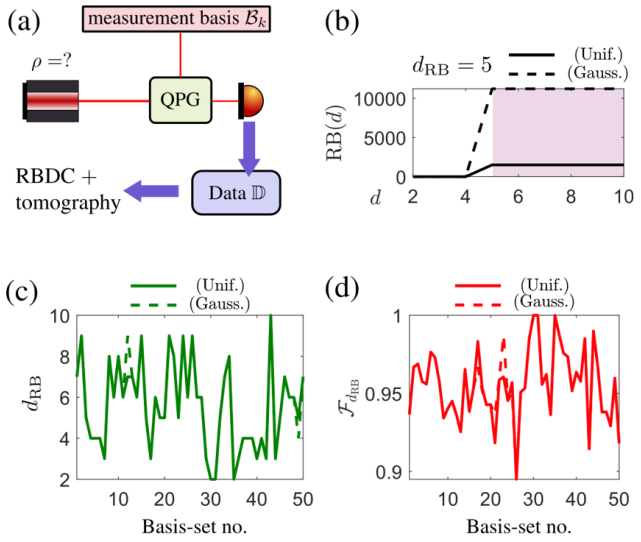


Figure 3: RBDC on 50 random 11-bases experimental datasets (each of sample size 10^4). (b) A particular noisy dataset gives $d_{\rm RB} = 5$ and RB values for various dimensions d (shaded marks RB > 1). (c,d) The $d_{\rm RB}$'s and fidelities for all 50 datasets are shown.

teria (including Akaike's and Bayesian information criteria) and is thus a very conservative methodology for hypothesis evaluation (see Fig. 2). The RB framework is also more operational than regular hypothesis testing as it does not require the additional arbitrary assignment of significance levels and avoids using the generally erroneous p value that could result in wrong statistical conclusions [3].

3 Results and applications

Dimension verification of quantum states in the time-frequency domain:

One important application of RBDC would be to determine the correct truncation dimension for a given optical state, which is essential when any numerical computation from experimental data is to be carried out. Figure 3 shows an example where RBDC is used in optical-state reconstruction in the spectral-temporal domain, where a quantum pulse gate (QPG) [4] is used to shape signal states coming from a laser source and measurement bases. Using both uniform and Gaussian prior distributions of d as examples, we see that RBDC can systematically extract information from the experimental data and ascertain the effective dimension of a quantum state, which in this case is the degree-one temporal Hermite–Gaussian (HG1) state.

Quality assessment of multiphoton sources:

Since RB is a general statistical inference method that is grounded on solid Bayesian statistical foundations, it can be applied to other quantum-information processing tasks in general. One important area is the quality

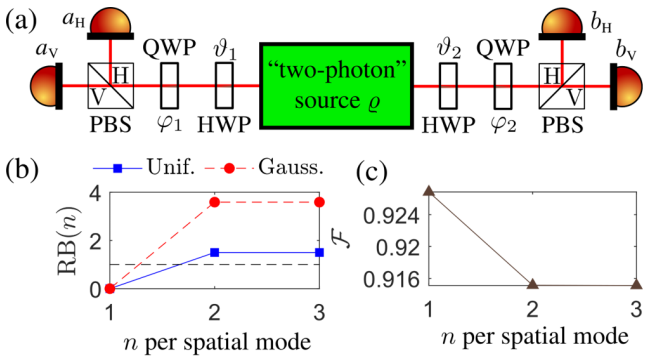


Figure 4: (a) Polarimetry setup for assessing the quality of a two-spatial-mode photon source. (b,c) RB and fidelity values for various n per spatial mode for a dataset, where each combination of waveplate settings is measured with a simulation-data sample size of 10^4.

assessment of multiphoton sources. Given a supposed "two-photon" source emitting photons into two spatial modes, RBDC can be used to find out whether there is strong evidence in favor of the source emitting just $n = 1$ photon in each spatial mode or other higher numbers. Figure 4 shows an example of an SPDC-Type-II two-mode squeezed vacuum state, at 2.1 dB squeezing strength, masquerading as a "two-photon" source. From the measurement data obtained, RBDC is able to unambiguously detect the presence of $n = 2$ photons per mode with high belief strengths (RB > 1).

Tracking nontrivial interacting degrees of freedom :

We go beyond dimension certification and discuss more general model certification with relative belief. In particular, we answer the question of whether a purely evidence-based Bayesian reasoning can assist in ascertaining the number of external degrees of freedom in an interacting environment with an accessible physical system without directly measuring and obtaining explicit information about the external environment. We found that under the premise that information concerning the interacting environment is carried over to the measured physical system after tracing over the external degrees of freedom and that these degrees of freedom are sufficiently small to be precisely accounted for using mathematical models, the relative-belief methodology can certify which interaction models out of a finite set most plausibly describe the given system-environment interaction.

This is illustrated with the Tavis–Cummings (TC) model, where a photon-field interacts with $n_{\rm abs}$ two-level absorber atoms, with a coupling strengths g_j with the jth atom under the rotating-wave approximation. Several other models of this kind include the $n_{\rm abs} = 1$ Rabi model and the more general Dicke model when off-resonant terms are included. These models helped establish the foundation of superradiance in quantum optics. Figure 5 demonstrated that RB is versatile for tracking

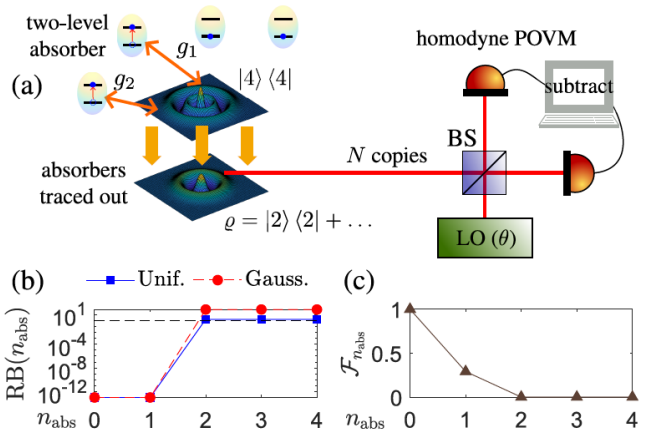


Figure 5: Optical absorption TC model certification with RB, where (a) the Fock state $|4\rangle\langle 4|$ couples to two absorber molecules with equal strengths ($g_1 = 1 = g_2$). Multiple copies of the resulting optical state are then sent to a standard homodyne setup, where the phase θ of the local oscillator (LO) determines the quadrature angle. Both the Hilbert space of ϱ and number of angles are set to $d = 9$ and 10. A total of 10^6 copies are measured using all these settings. The (b) RB ratios (all greater than 1 for $n_{\rm abs} > 1$) for both uniform and Gaussian priors are shown, and (c) fidelity with the ideal Fock state drops gradually to almost zero as RB approaches the correct number of absorbers $n_{\rm abs}$, since the actual mixed state is given by $\varrho \mathrel{\widehat{=}} \mathrm{diag}(0, 0, 0.8159, 0.1822, 0.0019, 0, 0, 0, 0) \cong |2\rangle\langle 2|$, which is almost completely orthonormal to $|4\rangle\langle 4|$.

interacting degrees of freedom for such a model by comparing prior and posterior belief strengths.

Note that not always can such interaction information be available to us through data inference. We emphasize that this works only when nontrivial information concerning the interacting degrees of freedom is encoded into the measurement data and this is interaction-model dependent. As an example, data from measuring an atom that interacts with multiple photon-field modes, on the other hand, will contain no information about the number of photon fields that are coupled to the atom. This is because mathematically, the ladder operators of all independent photon modes may be combined into a single ladder operator that possesses exactly the same commutation relation and other properties. Hence, no information about the photon coupling can be extracted from the atomic reduced state.

References

[1] M. Evans. *Measuring Statistical Evidence Using Relative Belief*. Chapman & Hall, New York, 2015.

[2] Y. S. Teo, H. Jeong, N. Prasannan, B. Brecht, C. Silberhorn, M. Evans, D. Mogilevtsev, and L. L. Sánchez-Soto. Evidence-based certification of quantum dimensions. *arXiv*:2401.01562, 2024.

[3] R. L. Wasserstein and N. A. Lazar. The ASA Statement on p-Values: Context, Process, and Purpose. *Am. Stat.* 70, 129, 2016.

[4] Jano Gil-Lopez, Yong Siah Teo, Syamsundar De, Benjamin Brecht, Hyunseok Jeong, Christine Silberhorn, and Luis L. Sánchez-Soto. Universal compressive tomography in the time-frequency domain. *Optica* 8, 1296-1305, 2021.

On the generic increase of observational entropy in isolated systems

Teruaki Nagasawa[1] * Kohtaro Kato[1] † Eyuri Wakakuwa[1] ‡ Francesco Buscemi[1] §

[1] *Department of Mathematical Informatics, Nagoya University, Furo-cho Chikusa-ku, Nagoya 464-8601, Japan*

Abstract. The concept of observational entropy, which unifies various forms of entropy, including Boltzmann's, Gibbs's, von Neumann's macroscopic entropy, and the diagonal entropy, has recently been proposed as a pivotal element in a contemporary formulation of statistical mechanics. In this study, we employ algebraic techniques derived from Petz's theory of statistical sufficiency and a Levy-type concentration bound to demonstrate rigorous theorems. These theorems illustrate how the observational entropy of a system undergoing a unitary evolution chosen at random tends to increase with overwhelming probability and to reach its maximum very quickly. We demonstrate that for any observation that is sufficiently coarse with respect to the size of the system, the random evolution renders the system's state practically indistinguishable from the uniform distribution (i.e., maximally mixed) with a probability approaching one as the system size increases. This is true regardless of the initial state of the system, whether pure or mixed. The same conclusion is applicable not only to random evolutions sampled according to the unitarily invariant Haar distribution, but also to approximate 2-designs, which are regarded as a more physically reasonable means of modelling random evolutions.

Keywords: Observational entropy, von Neumann entropy, H-theorem

Introduction.—In his book on the mathematical foundations of quantum theory [1], John von Neumann introduces and offers an operational motivation for a quantity that is now known as *von Neumann entropy*. However, he notes that this quantity is not the most appropriate to consider in the context of statistical mechanics.

In order to address this challenge, von Neumann put forth the concept of *macroscopic entropy*, which considers not only the intrinsic uncertainty inherent to the microscopic state of the system but also the supplementary uncertainty associated with the coarse-grained, macroscopic observation with which the system is being monitored.

Since von Neumann's proposal, macroscopic entropy has been largely eclipsed by its more famous and eponymous sibling. Notwithstanding, recent years have witnessed a resurgence of interest in von Neumann's macroscopic entropy and its extension, known as *observational entropy*. This is evidenced by a number of recent publications, including [2–6]. In connection with the mathematical and conceptual foundations of statistical mechanics, as well as various applications, the following sources are recommended for further reading: [7–20]. In a similar manner, this study examines the evolution of observational entropy in unitarily evolving systems, with a particular emphasis on its generic behavior when the system's evolution is selected at random.

In this paper, we are motivated by Ref. [7], which shows that the observational entropy of an isolated system initialized in a state fully known to the observer cannot decrease. We first provide an explicit characterization of all situations in which the observational entropy undergoes a strict increase with time. Such a characterization is based on Petz's theory of statistical sufficiency [21–24]. We then proceed to consider the case of arbitrary initial states. Based on a Lévy-type concentration bound [25, 26] that we prove for the observational entropy, we arrive at a statement analogous to von Neumann's H-theorem. This states that for any observation that is "sufficiently coarse-grained" with respect to the size of the system, under the action of Haar-random evolution, the observational entropy approaches its maximum. The system's state becomes essentially indistinguishable from the maximally mixed (uniform) state, regardless of its initial state. Finally, by applying a number of derandomization techniques, as outlined in the references [27–30], we demonstrate that the same conclusion holds when the Haar distribution is replaced by an approximate 2-design. This represents a more realistic model, both physically and computationally, for random evolutions.

Observational entropy.—The observational entropy (OE) of a microscopic state, represented by the density matrix ρ, with respect to a positive operator-valued measure (POVM) $\boldsymbol{P} = \{P_x\}_{x\in\mathcal{X}}$ is defined as follows [2–7]:

$$S_{\boldsymbol{P}}(\rho) = -\sum_x p_x \log \frac{p_x}{V_x} \,,$$

where $p_x = \mathrm{Tr}[P_x\,\rho]$ and $V_x = \mathrm{Tr}[P_x]$. The fundamental bound of OE is given by the inequality $S_{\boldsymbol{P}}(\rho) \geq S(\rho)$, where $S(\rho)$ is the von Neumann entropy [5].

A state that saturates the bound, namely a state ρ such that $S_{\boldsymbol{P}}(\rho) = S(\rho)$, is defined as a macroscopic state for $\boldsymbol{P}$. The reason for this name is that the condition $S_{\boldsymbol{P}}(\rho) = S(\rho)$ holds if and only if [5]

$$\rho = \sum_x \mathrm{Tr}[P_x\,\rho]\,\frac{P_x}{V_x} \,,$$

which implies that the state ρ can be perfectly reconstructed [31–33] solely from the knowledge of the measurement $\boldsymbol{P}$ and its outcome statistics p_x, i.e., information that is entirely accessible to a macroscopic observer [5].

OE increase in macroscopic states.—As previously stated in the introduction, one of the primary reasons

*teruaki.nagasawa@nagoya-u.jp
†kokato@i.nagoya-u.ac.jp
‡e.wakakuwa@gmail.com
§buscemi@nagoya-u.jp

to consider OE is that it can increase even in isolated systems, in contrast to von Neumann entropy, which, in contrast, remains constant. In this study, we begin by considering the behavior of OE when the initial state of the system is macroscopic, as motivated by Ref. [7].

Let us thus consider an isolated system evolving in time from $t = t_0$ to $t = t_1 > t_0$. Let ρ_0 be the initial state of the system, U describe the time evolution from t_0 to t_1, and $\rho_1 = U\rho_0 U^\dagger$ be the state of the system at t_1. Let us also assume that, at time t_0, the system's state is macroscopic for $\boldsymbol{P}$. While the von Neumann entropy $S(\rho_t)$ of the system remains constant, for the OE we have:

$$S_{\boldsymbol{P}}(\rho_1) \geq S(\rho_0) = S_{\boldsymbol{P}}(\rho_0) = S(\rho_1) \ .$$

The final inequality holds because ρ_0 is macroscopic for $\boldsymbol{P}$, but may not be so for $U^\dagger \boldsymbol{P} U$. Thus, from the above, we immediately see that:

i) the OE of an isolated system starting in a macroscopic state never decreases (cfr. Lemma 5 in [7]);

ii) it remains constant if and only if ρ_1 is *also* macroscopic for the *same* $\boldsymbol{P}$ as ρ_0.

Given that, the question that we want to consider now is: when does the OE *strictly* increase? In order to answer this question, we first need to provide a characterization of all macroscopic states associated with a given POVM $\boldsymbol{P} = \{P_x\}$.

Theorem 1 *Given a POVM $\boldsymbol{P} = \{P_x\}$, a state $\mathfrak{m}$ is macroscopic for $\boldsymbol{P}$ if and only if there exists a PVM $\boldsymbol{\Pi} = \{\Pi_y\}_y$, with $\boldsymbol{\Pi} \preceq \boldsymbol{P}$, together with coefficients $c_y \geq 0$, such that*

$$\mathfrak{m} = \sum_y c_y \Pi_y \ ,$$

where we write $\boldsymbol{Q} \preceq \boldsymbol{P}$ whenever there exists a conditional probability distribution $p(y|x)$ such that $Q_y = \sum_x p(y|x) P_x$, for all $y \in \mathcal{Y}$.

In particular, if $\mathfrak{m}$ is macroscopic for $\boldsymbol{P} = \{P_x\}$, then

$$[\mathfrak{m}, P_x] = 0 \ ,$$

for all $P_x \in \boldsymbol{P}$. This fact demonstrates that a restricted set of unitary operators, those that satisfy the conservation-like relation

$$[U\mathfrak{m}U^\dagger, P_x] = 0 \ , \quad \forall x \ ,$$

can preserve the observer's information about the system. Conversely, a generic evolution, such as one uniformly sampled from the entire set of unitary operators, will necessarily cause a strict increase in OE. In such cases, although the microscopic evolution is perfectly reversible, from the macroscopic observer's perspective, information is irreversibly lost.

OE increase in arbitrary states.—The next question to be considered is that of the behaviour of observational entropy when an arbitrary quantum state is taken as the initial state. The second result is that, under a coarse (macroscopic) measurement on a sufficiently large quantum system and taking unitary to Haar random, observational entropy increases with a very high probability.

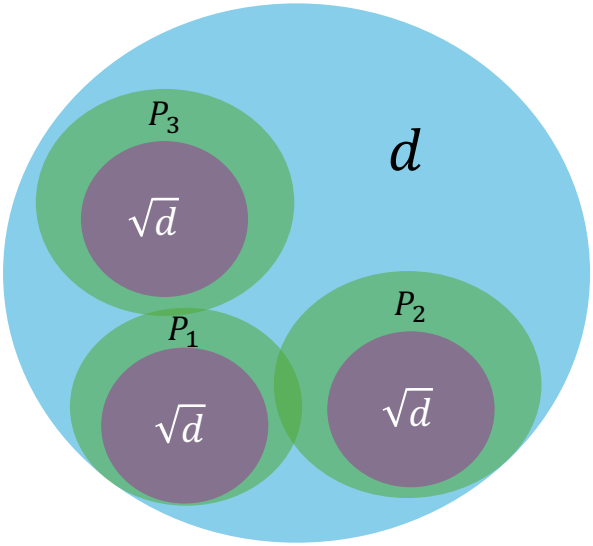


Figure 1: As the dimension of the Hilbert space, d, increases, there is a substantial amount of space between d and the square root of d, which allows for the accommodation of a multitude of POVM elements.

Theorem 2 *For quantum states ρ and POVM $\boldsymbol{P}$ on d-dimensional space,*

$$\mathbb{P}_H \left\{ S_{\boldsymbol{P}}(U\rho U^\dagger) \leq (1-\delta) \log d \right\} \leq \frac{4}{\kappa(\boldsymbol{P})} e^{-C\delta\kappa(\boldsymbol{P})^2 d \log d} \ , \tag{1}$$

where $\kappa(\boldsymbol{P}) = \min_x \mathrm{Tr}[P_x \, u]$ is an "effective coarseness" parameter and $C = \frac{1}{18\pi^3}$.

For the right-hand side of Eq. (1) to be small, it is necessary that the quantity $\kappa(\boldsymbol{P})$ plays well with the quantities C, δ, and d. This condition is analogous to the condition proposed by von Neumann on the minimum size of the phase cells in his proof of the H-theorem. In our notation, the role of the number of states in each phase cell is played by the minimum trace of P_x, denoted by $d\kappa(\boldsymbol{P})$. The number of phase cells is the number of possible outcomes, which we denote by $N(\boldsymbol{P})$. Thus, we can summarize von Neumann's condition as

$$N(\boldsymbol{P}) \ll d\kappa(\boldsymbol{P}) \ . \tag{2}$$

Consequently, von Neumann's condition is satisfied if the following condition is true:

$$\sqrt{d} \ll \min_x \mathrm{Tr}[P_x] = d\kappa(\boldsymbol{P}) \tag{3}$$

is closely related to the requirement that the right-hand side of (1) approaches zero as d approaches infinity. This relationship will be demonstrated subsequently.

Let us consider a sequence of systems and observations in the limit of the system's Hilbert space dimension, d,

which tends to infinity. We must first define precisely what it means for a sequence of observations to be asymptotically coarse.

Definition 3 *Consider a sequence of systems with increasing dimension d and, in each system, a POVM $\boldsymbol{P}^{(d)} = \{P^{(d)}_{x_d}\}_{x_d}$. For each d, define $\kappa(d) \equiv \kappa(\boldsymbol{P}^{(d)}) = \min_{x_d} \mathrm{Tr}\left[P^{(d)}_{x_d}\, u\right]$. We say that the sequence of POVMs $\{\boldsymbol{P}^{(d)}\}_{d\in\mathbb{N}}$ is* asymptotically coarse *whenever there exists $\tau > 0$ such that*

$$\kappa(d) = \Omega(d^{-\frac{1}{2}+\tau}) \,.$$

i.e., whenever $\exists M > 0$ and $\exists d_0$ such that

$$\kappa(d) \geq M \cdot d^{-\frac{1}{2}+\tau} \,, \quad \forall d > d_0 \,.$$

The preceding definition can be justified from von Neumann's condition (2) as follows. For $\kappa(d) \sim d^{\alpha}$, we obtain

$$\frac{N(d)}{d\,\kappa(d)} \leq \frac{1}{d\,\kappa(d)^2} \sim d^{-2\alpha-1} \,,$$

which goes to zero if and only if $\alpha > -1/2$, in agreement with Definition 3. Moreover, for coarse (macro) measurements on a sufficiently large quantum system, the following approximation holds:

$$\mathbb{P}_H\{S_{\boldsymbol{P}}(U\rho U^\dagger) \approx \log d\} \approx 1 \,.$$

Physical random evolutions.— The aforementioned results are also observed in a more physically feasible pseudo-random setting (approximate 2-design). Our findings indicate that the concentration of observational entropy occurs even under random unitaries generated by random polynomial-depth quantum circuits, which is often regarded as a more physically realistic model of local quantum chaotic dynamics.

Theorem 4 *For a unitary operator U sampled at random from an ε-approximate 2-design $\mathcal{E}$,*

$$\mathbb{P}_{\mathcal{E}}\left\{S_{\boldsymbol{P}}(U\rho U^\dagger) \leq (1-\delta)\log d\right\} \leq \frac{1}{\kappa(\boldsymbol{P})^3 d\log d}\frac{4(1+\varepsilon)}{\delta} \,, \tag{4}$$

for any value $\delta > 0$.

The upper bound provided in Eq. (4) is less stringent than that presented in Eq. (1). This is due to the fact that the negative exponential rate in d, which was present in Eq. (1), has been replaced by $(d\log d)^{-1}$ in the current equation. Furthermore, Eq. (4) still enables us to demonstrate an asymptotic outcome, albeit with a modified interpretation of asymptotic coarseness in accordance with Definition 3 when compared to the previous result.

In the case of 2-designs with an approximate factor of ε, it is necessary that the function $\kappa(d)$ be of the form $\Omega(d^{-\frac{1}{3}+\tau})$ for some positive value of τ. This suggests that von Neumann's condition ((2)) should be replaced with $d^{2/3} \ll \min_x \mathrm{Tr}[P_x]$. In other words, the asymptotic coarseness for ε-approximate 2-designs is less refined than the definition introduced in Definition 3, which was developed with the case of Haar-random unitaries in mind. For any sufficiently large dimension d, even in the case where U is sampled from an ε-approximate 2-design $\mathcal{E}$, it can be shown that

$$\mathbb{P}_{\mathcal{E}}\{S_{\boldsymbol{P}}(U\rho U^\dagger) \approx \log d\} \approx 1 \,.$$

Conclusions.— This research presents three methods in which observational entropy is shown to increase and reach its maximum in isolated systems undergoing a generic unitary evolution. Firstly, if the initial state is a macroscopic state, observational entropy will increase with probability 1. Secondly, if we consider unitary time evolution in Haar random for arbitrary initial states, we can show that it increases with very high probability for coarse (macroscopic) measurements on sufficiently large quantum systems. Finally, it was found that observational entropy increases not only in settings that are physically difficult to realise, such as Haar random, but also in more physically realisable pseudo-random settings (approximate 2-design).

A significant avenue for future research is to investigate the relationship between the random evolution assumption employed here and the eigenstate thermalization hypothesis. This hypothesis, when applied under additional physical assumptions, has been shown to yield results analogous to those presented here [34]. Another area of interest is to determine whether it is feasible to establish concentration inequalities for OE in the context of specific Hamiltonians.

Acknowledgments.—This work was financially supported by JST SPRING, Grant Number JPMJSP2125. T. N. would like to take this opportunity to thank the "THERS Make New Standards Program for the Next Generation Researchers." K. K. acknowledges support from JSPS Grant-in-Aid for Early-Career Scientists, No. 22K13972; from MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe," No. 22H05254. K. K, E. W. and F. B. acknowledge support from MEXT Quantum Leap Flagship Program (MEXT QLEAP) Grant No. JPMXS0120319794. F. B. also acknowledges support from MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe," No. 21H05183, and from JSPS KAKENHI Grants No. 20K03746 and No. 23K03230.

References

[1] J. von Neumann, *Mathematical foundations of quantum mechanics* (Princeton university press, 1955).

[2] D. Šafránek, J. M. Deutsch, and A. Aguirre, Phys. Rev. A **99**, 010101, 010101 (2019).

[3] D. Šafránek, J. M. Deutsch, and A. Aguirre, Phys. Rev. A **99**, 012103, 012103 (2019).

[4] D. Šafránek, A. Aguirre, J. Schindler, and J. M. Deutsch, Foundations of Physics **51**, 101, 101 (2021).

[5] F. Buscemi, J. Schindler, and D. Šafránek, New Journal of Physics **25**, 053002 (2023).

[6] G. Bai, D. Šafránek, J. Schindler, F. Buscemi, and V. Scarani, *Observational entropy with general quantum priors*, 2023.

[7] P. Strasberg and A. Winter, PRX Quantum **2**, 030202 (2021).

[8] A. Riera-Campeny, A. Sanpera, and P. Strasberg, PRX Quantum **2**, 010340 (2021).

[9] D. Šafránek, A. Aguirre, and J. M. Deutsch, Phys. Rev. E **102**, 032106, 032106 (2020).

[10] J. M. Deutsch, D. Šafránek, and A. Aguirre, **101**, 032112, 032112 (2020).

[11] D. Faiez, D. Šafránek, J. M. Deutsch, and A. Aguirre, **101**, 052101, 052101 (2020).

[12] C. Nation and D. Porras, **102**, 042115, 042115 (2020).

[13] P. Strasberg, M. G. Díaz, and A. Riera-Campeny, Phys. Rev. E **104**, L022103, L022103 (2021).

[14] R. Hamazaki, PRX Quantum **3**, 020319, 020319 (2022).

[15] R. Modak and S. Aravinda, Phys. Rev. A **106**, 062217 (2022).

[16] S. PG, R. Modak, and S. Aravinda, Phys. Rev. E **107**, 064204 (2023).

[17] J. Schindler and A. Winter, arXiv e-prints, arXiv:2302.00400, arXiv:2302.00400 (2023).

[18] D. Šafránek, D. Rosa, and F. C. Binder, Phys. Rev. Lett. **130**, 210401 (2023).

[19] D. Šafránek and D. Rosa, Phys. Rev. A **108**, 022208 (2023).

[20] D. Šafránek, arXiv e-prints, arXiv:2306.08987, arXiv:2306.08987 (2023).

[21] D. Petz, Communications in mathematical physics **105**, 123 (1986).

[22] D. Petz, The Quarterly Journal of Mathematics **39**, 97 (1988).

[23] D. Petz, Reviews in Mathematical Physics **15**, 79 (2003).

[24] A. Jenčová and D. Petz, Infinite Dimensional Analysis, Quantum Probability and Related Topics **09**, 331 (2006).

[25] M. Ledoux, *The concentration of measure phenomenon* (American Mathematical Society, 2001).

[26] P. Hayden, D. W. Leung, and A. Winter, Communications in Mathematical Physics **265**, 95 (2006).

[27] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[28] R. A. Low, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **465**, 3289 (2009).

[29] F. G. Brandão, W. Chemissany, N. Hunter-Jones, R. Kueng, and J. Preskill, PRX Quantum **2**, 10.1103/prxquantum.2.030316 (2021).

[30] A. W. Harrow and S. Mehraban, Communications in Mathematical Physics **401**, 1531 (2023).

[31] F. Buscemi, D. Fujiwara, N. Mitsui, and M. Rotondo, Physical Review A **102**, 032210 (2020).

[32] F. Buscemi and V. Scarani, Phys. Rev. E **103**, 052111 (2021).

[33] C. C. Aw, F. Buscemi, and V. Scarani, AVS Quantum Science **3**, 045601 (2021).

[34] P. Strasberg, A. Winter, J. Gemmer, and J. Wang, Phys. Rev. A **108**, 012225 (2023).

Extended abstract for: "Fundamental limits of metrology at thermal equilibrium"

Paolo Abiuso[1] * Pavel Sekatski[2] † John Calsamiglia[3] ‡ Martí Perarnau-Llobet[2] §

[1] *Institute for Quantum Optics and Quantum Information - IQOQI Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria*

[2] *Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland*

[3] *Física Teòrica: Informació i Fenòmens Quàntics, Department de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain*

Abstract. We consider the estimation of an unknown parameter through a quantum probe at fixed temperature. For a given encoding of the parameter, we derive the fundamental limits and optimal control for metrology with thermal and ground state probes, including probes at the verge of criticality, showing that: *(i)* assuming full control, quantum non-commutativity does not offer any fundamental advantage in the estimation; *(ii)* an exponential quantum advantage arises at low temperatures in gapped systems; *(iii)* the optimal sensitivity presents a Heisenberg-like N^2-scaling in terms of the number of particles of the probe, which can be reached with local measurements.

Keywords: Quantum Fisher Information, Quantum Metrology, Thermal states, Quantum Control

The complete manuscript can be found on the arXiv repository arXiv 2402.06582.

1 Introduction and overview

In typical quantum metrology problems, a parameter θ enters in the Hamiltonian of the probe system H_θ. In consequence, its state ρ_θ eventually correlates to the parameter value, which can be then estimated by measuring the probe. Through the Crámer-Rao bound [1]

$$\Delta\theta^2 \geq \frac{1}{n\mathcal{F}_\theta} \tag{1}$$

the precision of any such procedure can be related to the quantum Fisher Information (QFI) $\mathcal{F}_\theta$ of the state ρ_θ and the number of repetitions of the experiment n.

The most common setting considered in the literature is *dynamical* metrology, in which the probe is prepared in a well controlled initial state and is left to coherently evolve under the influence of the Hamiltonian H_θ for a time t. For a probe composed of N subsystems on which the Hamiltonian acts locally, the QFI of the probe's final state is bounded by the paradigmatic Heisenberg limit [2]

$$\mathcal{F}_\theta \lesssim \frac{N^2 t^2}{\hbar^2} \quad \text{(dynamical)}. \tag{2}$$

This bound follows from the geometry of quantum states, and cannot be overcome with any additional (parameter-independent) control mechanism. However, reaching the Heisenberg limit demands for specific highly-entangled initial states and a high level of precision on the interaction time and dynamics (in particular, it is in general unattainable in presence of environmental noise).

This motivates the investigation of alternative, less demanding, sensing strategies where the parameter is estimated from a steady state ρ_θ of an open quantum system. A prominent common setting is then the one of *equilibrium* (including *ground state*) metrology, where the parameter is encoded in the Gibbs (resp. ground) state of the Hamiltonian

$$\rho_\theta = \frac{e^{-\beta H_\theta}}{\mathrm{Tr}\left[e^{-\beta H_\theta}\right]}, \tag{3}$$

where $\beta = 1/k_B T$, T is the temperature of the surrounding environment. The potential of Gibbs (ground) states in quantum metrology has been long recognised in the literature, particularly close to thermal (quantum) phase transitions [3, 4]. The possibility of a measurement precision beyond the shot-noise limit ($\mathcal{F}_\theta \lesssim N$) has been reported for thermal/ground states of spin chains [5, 6, 7, 8, 9], light-matter interacting systems [10, 11, 12], and first experimental realisations are currently being developed [13, 14].

Despite this remarkable progress, the fundamental limits of equilibrium metrology remain unsettled. The establishment of such saturable upper-bounds is the main goal and result of our work [15]. For that, we consider H_θ consisting of two terms

$$H_\theta = H_\theta^{\mathrm{P}} + H^{\mathrm{C}}, \tag{4}$$

where H_θ^{P} describes the (fixed) physical mechanism imprinting θ on the probe, whereas H^{C} is under experimental control. We then optimize the QFI for thermal states (3) over all possible H^{C}, thus finding a general upper bound on it. For a N-body probe on which H_θ^{P} acts locally, our results can be summarised as follows. At *any* temperature, the QFI of the Gibbs state at best scales as

$$\mathcal{F}_\theta \lesssim N^2\beta^2 \quad \text{(thermal equilibrium)}. \tag{5}$$

Crucially, this bound can be attained without any entanglement between the N subsystem, but only through

*paolo.abiuso@oeaw.ac.at
†pavel.sekatski@gmail.com
‡john.calsamiglia@uab.cat
§marti.perarnaullobet@unige.ch

classical correlations induced by $H^{\rm C}$. At *zero* temperature this bound diverges. However, for systems with a minimal gap Δ we find that the QFI scales, in the low temperature limit, at most as

$$\mathcal{F}_\theta \lesssim \frac{N^2}{\Delta^2} \quad \text{(ground state with gap)}. \tag{6}$$

This bound can also be saturated by a proper choice of $H^{\rm C}$. In this case quantum coherence in (3) is crucial, and an exponential quantum advantage in $\beta\Delta$ appears with respect to the "classical" case $[H^{\rm C}, \partial_\theta H^{\rm P}_\theta] = 0$.

These results (5), (6) provide fundamental bounds on equilibrium metrology, analogously to Heisenberg's limit in dynamical metrology Eq. (2). Remarkably, they exhibit the same scaling of the QFI in the probe size.

2 Quantum Fisher information for thermal states and its maximization

Here we summarize the derivations and main results of our work [15]. The QFI can be generically expressed as [1]

$$\mathcal{F}_\theta := \mathrm{Tr}\left[\dot\rho_\theta \mathbb{J}^{-1}_{\mathrm{B},\rho_\theta}[\dot\rho_\theta]\right] , \tag{7}$$

where $\dot A \equiv \partial_\theta A$ identifies the variation of any operator w.r.t. θ, and $\mathbb{J}_{\mathrm{B},\rho}$ is the Bures multiplication superoperator [16]

$$\mathbb{J}_{\mathrm{B},\rho}[A] := \frac{1}{2}(\rho A + A\rho) , \tag{8}$$

which can be analytically inverted as $\mathbb{J}^{-1}_{\mathrm{B},\rho}[A] = 2\int_0^\infty \mathrm{d}s\; e^{-\rho s} A e^{-\rho s}$ on positive full rank states ρ. In order to compute the QFI (7) one can express the variation $\dot\rho_\theta$ (in our case, the Gibbs state ρ_θ (3)) via the operator exponential derivative as $\dot\rho_\theta = -\mathbb{J}_{\mathrm{L},\rho_\theta}[\beta\dot H_\theta] + \rho_\theta \mathrm{Tr}\left[\beta \dot H_\theta \rho_\theta\right]$, where we introduced the logarithmic multiplication superoperator [16]

$$\mathbb{J}_{\mathrm{L},\rho}[A] := \int_0^1 \mathrm{d}s\; \rho^s A \rho^{1-s} . \tag{9}$$

Moreover, being $\mathcal{F}_\theta$ a local function of θ, without loss of generality we can assume by relabelling that locally H_θ (10) is of the form

$$H_\theta \simeq H^{\rm C} + \theta H' . \tag{10}$$

By substituting the above expressions in Eq. (7) one obtains [15] the general expression of the QFI for perturbations of systems at thermal equilibrium, that is

$$\begin{aligned}\mathcal{F}_\theta &= \beta^2 \left(\mathrm{Tr}\left[\mathbb{J}_{\mathrm{L},\rho_0}[H']\mathbb{J}^{-1}_{\mathrm{B},\rho_0} \circ \mathbb{J}_{\mathrm{L},\rho_0}[H']\right] - \mathrm{Tr}\left[\rho_0 H'\right]^2\right) \\ &= \beta^2 \left(\mathrm{Tr}\left[H' \mathcal{J}_{\rho_0}[H']\right] - \mathrm{Tr}\left[\rho_0 H'\right]^2\right) .\end{aligned} \tag{11}$$

The expression (11) can be seen as a generalized variance of H', according to the multiplication superoperator $\mathcal{J}_\rho := \mathbb{J}_{\mathrm{L},\rho} \circ \mathbb{J}^{-1}_{\mathrm{B},\rho} \circ \mathbb{J}_{\mathrm{L},\rho}$. Notice that $\mathbb{J}_{\mathrm{B},\rho}, \mathbb{J}_{\mathrm{L},\rho}, \mathcal{J}_\rho$ can all be analytically expressed in the operator basis $|i\rangle\langle j|$ using the eigenvectors of ρ. These superoperators belong to the family of generalized quantum Petz-Fisher multiplications [17] reviewed in [16], and correspond to non-commutative versions of the multiplication times ρ. Using a formalism based on these superoperators and their properties makes our derivations natural and showcases their relevance.

Starting from the generic QFI for a system at equilibrium (11), we are able to bound (11), and find that under the assumption of full control on $H^{\rm C}$ (10) (equivalently, on ρ_0 (3)), the maximum value of $\mathcal{F}_\theta$ is obtained for diagonal states in the basis of the perturbation, meaning $[H^{\rm C}, H'] = 0$ ($[\rho_0, H'] = 0$). To see this, first we prove [15, 16] that

$$\mathrm{Tr}\left[H' \mathcal{J}_{\rho_0}[H']\right] - \mathrm{Tr}\left[\rho_0 H'\right]^2 \leq \mathrm{Var}_{\rho_0}[H'], \tag{12}$$

which is saturated for $[\rho_0, H'] = 0$. Secondly, we notice that the variance $\mathrm{Var}_{\rho_0}[H'] := \mathrm{Tr}\left[\rho_0 H'^2\right] - \mathrm{Tr}\left[\rho_0 H'\right]^2$ is upper bounded by $(\lambda_{\rm M} - \lambda_{\rm m})^2/4$, where $\lambda_{\rm M(m)}$ is the maximum(minimum) eigenvalue of H'. This bound is tight for $\rho_0 = \frac{1}{2}(|\lambda_{\rm M}\rangle\langle\lambda_{\rm M}| + |\lambda_{\rm m}\rangle\langle\lambda_{\rm m}|)$, which commutes with H' and is the Gibbs state of the Hamiltonian $H^{\rm C} = \epsilon(|\lambda_{\rm M}\rangle\langle\lambda_{\rm M}| + |\lambda_{\rm m}\rangle\langle\lambda_{\rm m}|) + H_\perp$ in the limit $\beta(H_\perp - \epsilon) \gg 1$. Connecting the two inequalities with (11) we obtain the fundamental bound

$$\mathcal{F}_\theta \leq \beta^2 \frac{(\lambda_{\rm M} - \lambda_{\rm m})^2}{4} . \tag{13}$$

This is *the ultimate upper bound to the QFI at finite temperature*, for a given encoding of θ that locally behaves as H'. Moreover, as (13) is saturated for commuting $[\rho_0, H'] = 0$ we see that *there is no fundamental quantum advantage in (thermal) equilibrium metrology.* Notice that this is valid assuming full control on $H^{\rm C}$ and finite equilibrium temperature.

A striking immediate consequence of the bound (13) can be obtained when considering the case of systems composed of N subsystems. When the parameter is encoded locally, one easily sees [15] that

$$\mathcal{F}^{\rm local}_\theta \leq \beta^2 \frac{(l_{\rm M} - l_{\rm m})^2 N^2}{4} , \tag{14}$$

$l_{\rm M,m}$ being the max/min eigenvalues of the local Hamiltonian. Hence, *at finite temperature, the QFI relative to a local parameter scales at most as N^2 in the system's size.* The quadratic N^2 scaling reminds of the well-known Heisenberg limit (2) of quantum metrology [2, 18], however our bounds are saturated for classically correlated states. In particular when H' is a local perturbation, the optimal preparation $\propto e^{-\beta H^{\rm C}}$ *does not feature entanglement*, and the measurement basis can be chosen to be local.

2.1 Low temperature limit and quantum advantage

Our main derivation and bound (13) show that at finite temperature the optimal control Hamiltonian $H^{\rm C}$ commutes with H', and can ensure a maximum sensitivity

that diverges in the limit of small temperature. However, in order to saturate (13) H^{C} needs the max/min eigenstates $\left|\lambda_{\mathrm{M/m}}\right\rangle$ of H' for (doubly degenerate) ground states. Clearly, for a given H' this in general non-trivial. We thus consider the QFI maximisation while constraining H^{C} to have a unique ground state with a minimum energy gap Δ to the first excited state.

To tackle this case we explicitly inspect the QFI (11) in the eigenbasis of H^{C}, that is $H^{\mathrm{C}}\left|i\right\rangle = E_i\left|i\right\rangle$, which diagonalises the unperturbed thermal state and separate the diagonal (classical) contribution to the QFI from the terms due to noncommutativity in general $[H^{\mathrm{C}}, H']$. In [15] we show that in the large gap/low temperature limit (large $\beta\Delta$) the classical contribution to the QFI is suppressed exponentially while only part the off-diagonal contribution is not suppressed. Concretely, in the large gap/low temperature limit the dominant contribution becomes

$$\mathcal{F}_\theta^{\text{low-T}} = \sum_{i>0} \frac{4|H'_{0i}|^2}{(E_i - E_0)^2} + \mathcal{O}(e^{-\beta\Delta}) \,. \tag{15}$$

Therefore an *exponential quantum advantage* arises in the low temperature or large gap limit, compared to classical configurations. In order to maximize (15) w.r.t. all possible Δ-gapped controls H^{C}, we then consider the following inequality

$$\sum_{i>0} \frac{|H'_{0i}|^2}{(E_i - E_0)^2} \leq \frac{\sum_{i>0}|H'_{0i}|^2}{(E_1 - E_0)^2} = \frac{\mathrm{Var}_{|0\rangle}[H']}{(E_1 - E_0)^2} \,. \tag{16}$$

Together with the gap assumption $E_1 \geq \Delta$, this lead us to the bound

$$\mathcal{F}_\theta^{\text{low-T}} \leq \frac{(\lambda_{\mathrm{M}} - \lambda_{\mathrm{m}})^2}{\Delta^2} + \mathcal{O}(e^{-\beta\Delta}) \,, \tag{17}$$

which is saturated in this case with a fully quantum strategy i.e. preparing superpositions $|0\rangle = \frac{|\lambda_{\mathrm{M}}\rangle \pm |\lambda_{\mathrm{m}}\rangle}{\sqrt{2}}$ and $|1\rangle = \frac{|\lambda_{\mathrm{M}}\rangle \mp |\lambda_{\mathrm{m}}\rangle}{\sqrt{2}}$. Eq. (17) sets the ultimate limit of estimation in low-temperature gapped systems. As a direct consequence of (17), similarly to Eq. (14), the QFI relative to a local parameter cannot scale faster than N^2, *unless the gap Δ decreases in the system size N.*

3 Comments

In our work [15] we derived fundamental bounds on equilibrium quantum metrology, where a parameter θ is estimated with a system described by the Gibbs (or ground) state $\rho_\theta \propto \exp(-\beta H_\theta)$ (3). Assuming full control on the parameter-independent part of the system's Hamiltonian, we derived the upper limit to the QFI given in Eq. (13), which depends only on β and $H' = \partial_\theta H_\theta$. This upper-bound is shown to be attained by a "classical" strategy, where the Hamiltonian satisfies $[H_\theta, H'] = 0$. In the low temperature limit the bound (13) diverges. This motivated us to strengthen it to Eq. (17), which accounts for the presence of a spectral gap $\Delta > 0$ in the Hamiltonian and remains finite in the limit $\beta \to \infty$. To saturate the low-temperature bound (17), quantum coherence is crucial and in fact an exponential gap appears in the QFI of classical ($[H_\theta, H'] = 0$) and quantum ($[H_\theta, H'] \neq 0$) strategies. When θ is encoded locally on a N-body probe, the upper bounds Eqs. (13) and (17) display a Heisenberg-like quadratic scaling QFI $\propto N^2$.

In [15] we additionally showcase our results on paradigmatic classical and quantum spin chains, in particular showing that a 1D classical spin chain probe in the strongly interacting ferromagnetic regime can approach the fundamental limit (13).

Our first main result (13) opens a clear avenue for the design of optimal thermal probes for equilibrium metrology beyond the specific case of thermometry [19, 20, 21].

Likewise, our second main result (17) is helpful to understand the limits of ground state metrology [4]. In particular, it shows that a "super-Heisensberg" scaling of the QFI $\propto N^{2+\varepsilon}$ with ground states of many body systems close to a critical point is only possible when the gap closes as $\Delta \sim N^{-\varepsilon/2}$. As discussed in [7], the natural way to reconcile this divergence with the dynamical Heisenberg limit (2) is to account for the preparation time of the ground state, which diverges as the Hamiltonian becomes gapless.

The comparison between dynamic and equilibrium approaches to metrology is indeed insightful. At a fundamental level, any strategy in equilibrium metrology should satisfy the Heisenberg limit (2) when time is accounted as a resource. Consistency between (2) and (5) then leads to the appearance of a minimal thermalization time proportional to $\tau_{\mathrm{Pl}} = \hbar/k_{\mathrm{B}}T$. This ratio is known as the Planckian time, and is conjectured to provide a model-independent fundamental thermalization timescale [22]. Our approach may provide a new avenue to investigate this property [23].

Finally, our results might provide insights to the study of Hamiltonian learning, which has been showed to saturate the Heisenberg limit in the dynamical setting with control [24, 25], and is being intensively studied in the thermal scenario [26, 27, 28].

References

[1] Matteo G. A. Paris. Quantum estimation for quantum technology. *International Journal of Quantum Information*, 07(supp01):125–137, January 2009.

[2] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Phys. Rev. Lett.*, 96:010401, Jan 2006.

[3] Paolo Zanardi, Lorenzo Campos Venuti, and Paolo Giorda. Bures metric over thermal state manifolds and quantum criticality. *Phys. Rev. A*, 76:062318, Dec 2007.

[4] Paolo Zanardi, Matteo G. A. Paris, and Lorenzo Campos Venuti. Quantum criticality as a resource for quantum estimation. *Physical Review A*, 78(4), October 2008.

[5] Carmen Invernizzi, Michael Korbman, Lorenzo Campos Venuti, and Matteo G. A. Paris. Optimal

quantum estimation in spin systems at criticality. *Physical Review A*, 78(4), October 2008.

[6] Mohammad Mehboudi, Luis A. Correa, and Anna Sanpera. Achieving sub-shot-noise sensing at finite temperatures. *Phys. Rev. A*, 94:042121, Oct 2016.

[7] Marek M. Rams, Piotr Sierant, Omyoti Dutta, Paweł Horodecki, and Jakub Zakrzewski. At the limits of criticality-based quantum metrology: Apparent super-heisenberg scaling revisited. *Phys. Rev. X*, 8:021022, Apr 2018.

[8] Victor Montenegro, Utkarsh Mishra, and Abolfazl Bayat. Global sensing and its impact for quantum many-body probes with criticality. *Phys. Rev. Lett.*, 126:200501, May 2021.

[9] Raffaele Salvia, Mohammad Mehboudi, and Martí Perarnau-Llobet. Critical quantum metrology assisted by real-time feedback control. *Phys. Rev. Lett.*, 130:240803, Jun 2023.

[10] M. Bina, I. Amelio, and M. G. A. Paris. Dicke coupling by feasible local measurements at the superradiant quantum phase transition. *Phys. Rev. E*, 93:052118, May 2016.

[11] Louis Garbe, Matteo Bina, Arne Keller, Matteo G. A. Paris, and Simone Felicetti. Critical quantum metrology with a finite-component quantum phase transition. *Phys. Rev. Lett.*, 124:120504, Mar 2020.

[12] Zu-Jian Ying, Simone Felicetti, Gang Liu, and Daniel Braak. Critical quantum metrology in the non-linear quantum rabi model. *Entropy*, 24(8):1015, July 2022.

[13] Ran Liu, Yu Chen, Min Jiang, Xiaodong Yang, Ze Wu, Yuchen Li, Haidong Yuan, Xinhua Peng, and Jiangfeng Du. Experimental critical quantum metrology with the Heisenberg scaling. *npj Quantum Information*, 7(1):170, December 2021.

[14] Dong-Sheng Ding, Zong-Kai Liu, Bao-Sen Shi, Guang-Can Guo, Klaus Mølmer, and Charles S. Adams. Enhanced metrology at the critical point of a many-body rydberg atomic system. *Nature Physics*, 18(12):1447–1452, October 2022.

[15] Paolo Abiuso, Pavel Sekatski, John Calsamiglia, and Martí Perarnau-Llobet. Fundamental limits of metrology at thermal equilibrium. *arXiv 2402.06582*, 2024.

[16] Matteo Scandi, Paolo Abiuso, Jacopo Surace, and Dario De Santis. Quantum fisher information and its dynamical nature. *arXiv 2304.14984*, 2023.

[17] Dénes Petz. Monotone metrics on matrix spaces. *Linear Algebra and its Applications*, 244:81–96, September 1996.

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

[19] Luis A. Correa, Mohammad Mehboudi, Gerardo Adesso, and Anna Sanpera. Individual quantum probes for optimal thermometry. *Phys. Rev. Lett.*, 114:220405, Jun 2015.

[20] Mohammad Mehboudi, Anna Sanpera, and Luis A Correa. Thermometry in the quantum regime: recent theoretical progress. *Journal of Physics A: Mathematical and Theoretical*, 52(30):303001, jul 2019.

[21] Paolo Abiuso, Paolo Andrea Erdman, Michael Ronen, Frank Noé, Géraldine Haack, and Martí Perarnau-Llobet. Optimal thermometers with spin networks. *Quantum Science and Technology*, 9(3):035008, apr 2024.

[22] Sean A. Hartnoll and Andrew P. Mackenzie. Colloquium: Planckian dissipation in metals. *Rev. Mod. Phys.*, 94:041002, Nov 2022.

[23] *In preparation.*

[24] Hsin-Yuan Huang, Yu Tong, Di Fang, and Yuan Su. Learning many-body hamiltonians with heisenberg-limited scaling. *Phys. Rev. Lett.*, 130:200403, May 2023.

[25] Alicja Dutkiewicz, Thomas E. O'Brien, and Thomas Schuster. The advantage of quantum control in many-body hamiltonian learning. *arXiv 2304.07172*, 2023.

[26] Anurag Anshu, Srinivasan Arunachalam, Tomotaka Kuwahara, and Mehdi Soleimanifar. Sample-efficient learning of interacting quantum systems. *Nature Physics*, 17(8):931–935, August 2021.

[27] Jeongwan Haah, Robin Kothari, and Ewin Tang. Optimal learning of quantum hamiltonians from high-temperature gibbs states. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 135–146, 2022.

[28] Ainesh Bakshi, Allen Liu, Ankur Moitra, and Ewin Tang. Learning quantum hamiltonians at any temperature in polynomial time. *arXiv 2310.02234*, 2023.

Conservation of coherence and entanglement under quantum reference frame transformations

Paweł Cieśliński,[1,*]
In collaboration with: Carlo Cepollaro,[2,3] Ali Akil,[4] Anne-Catherine de la Hamette,[2,3] and Časlav Brukner[2,3]

[1] *Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics, and Informatics, University of Gdańsk, 80-308 Gdańsk, Poland*
[2] *Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria*
[3] *Institute of Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria*
[4] *Department of Computer Science, The University of Hong Kong, Hong Kong Island, Hong Kong S.A.R. China*

Recent work on quantum reference frames (QRFs) has demonstrated that superposition and entanglement depend on the choice of QRF, such that either one can increase or decrease under a change of QRF. Given their utility in quantum information processing, it is important to understand how a mere change of perspective can produce or reduce these resources. Here we show that QRF transformations are coherence-preserving incoherent operations and find trade-offs between entanglement and subsystem coherence under these transformations. We prove an exact conservation theorem for two pairs of measures and a weaker trade-off for any possible pairs of measures. Finally, we discuss the implications of this interplay for quantum information protocols, clarifying some misconceptions about non-locality and Hilbert space factorization.

The principle of covariance, which states that physical laws remain unchanged under a reference frame transformation, forms the fundamental understanding of our physical world. However, a variety of measurable physical quantities, such as energy, or magnetic and electric fields, are frame-dependent. Similar considerations arise when investigating the behaviour of quantum systems relative to a *quantum reference frame* (QRF). For example, it may happen that a system that is well localized in space in one QRF is in a superposition of different locations in a different QRF [1]. The same applies to quantum entanglement as well, making it a frame-dependent notion in quantum theory. Since both coherence and entanglement are recognized as useful resources in quantum information science, a natural important question arises: *How can a mere change of perspective from one frame of reference to another create a useful resource?*

In our work, we give a definite answer to this question. We show that QRF transformations $S^{A\to C}$ are global coherence-preserving incoherent operations and prove that under these transformations there exists a trade-off between the measures of pure bipartite state entanglement and its subsystem coherence, in the basis associated with the symmetry group of the transformation. We show the strict conservation of the discussed resources for two pairs of measures and prove a weaker condition on their change for any coherence and entanglement measures. Furthermore, we discussed the implications of this interplay for quantum information protocols, clarifying some misconceptions about non-locality and Hilbert space factorisation to complement them.

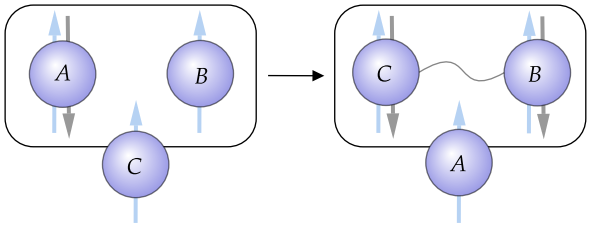


FIG. 1. Visual representation of the effects of a QRF change for a simple system of three spins. Let system A be in a uniform superposition of two basis states and let B and C be in a spin "up" state. Performing the QRF transformation for such a state one arrives at a maximally entangled state of C and B, while A points "up". This qualitatively illustrates the main premise behind our findings - the interplay between coherence and entanglement. For more discussion see the main text.

Quantum reference frames can be introduced with a simple example. Consider three spins A, B, and C and let the initial state be

$$|\psi\rangle_{AB}^{(C)} = |\uparrow\rangle_C^{(C)} \frac{1}{\sqrt{2}}(|\uparrow\rangle_A^{(C)} + |\downarrow\rangle_A^{(C)})\,|\uparrow\rangle_B^{(C)}\,.$$

We interpret this as the state of A and B with respect to C. Now, by applying the QRF transformation $S^{C\to A}$ we can infer the corresponding state $|\psi\rangle_{BC}^{(A)}$, i.e. the state of C and B with repsect to A. Doing so we find that the state relative to A is [2]:

$$|\psi\rangle_{BC}^{(A)} = |\uparrow\rangle_A^{(A)} \frac{1}{\sqrt{2}}(|\uparrow\rangle_B^{(A)}\,|\uparrow\rangle_C^{(A)} + |\downarrow\rangle_B^{(A)}\,|\downarrow\rangle_C^{(A)}).$$

In the above, one can see the basic motivation behind our work. The resulting state is maximally entangled, even

* pawel.cieslinski@phdstud.ug.edu.pl

though the initial state was product and the only operation performed was a change in perspective, see Fig. 1 for a visual representation. In general, it is possible to define a QRF change transformation $S^{C\to A}$ for any symmetry group describing the physical setting and apply it to an arbitrary state [2], but we will skip the details here.

Knowing that we outline the key results of our work that hold for any d-dimensional pure bipartite states (including the continuous variable systems) and any QRF transformation. Let $(\mathcal{E}_e, \mathcal{C}_e)$ be the entanglement entropy and subsystem entropy of coherence respectively and $(\mathcal{E}_l, \mathcal{C}_{l_2})$ be the subsystem's linear entropy and l_2-norm of coherence [3, 4]

- **Theorem 1.** The sum of entanglement and subsystem coherence $\mathcal{E} + \mathcal{C}$ is conserved under QRF transformations, for $(\mathcal{E}, \mathcal{C}) = (\mathcal{E}_e, \mathcal{C}_e)$ or $(\mathcal{E}_l, \mathcal{C}_{l^2})$.

- **Theorem 2.** For any choice of entanglement measure $\mathcal{E}$ and coherence measure $\mathcal{C}$, if there exist a QRF where the state has $\mathcal{E}^{A/C} = 0$ or $\mathcal{C}^{A/C} = 0$, under a QRF transformation it holds that $\Delta\mathcal{E}\Delta\mathcal{C} = (\mathcal{E}^A - \mathcal{E}^C)(\mathcal{C}^A - \mathcal{C}^C) \leq 0$.

In summary, quantum coherence and entanglement are fundamentally intertwined. In our work, we explore this connection in the framework of quantum reference frames, focusing on bipartite pure states. We proved that QRF transformations are coherence-preserving quantum operations and that for two pairs of measures, the sum of subsystem coherence and entanglement is conserved under QRF changes, implying that an increase of coherence under QRF change must come at the expense of a decrease in entanglement, and vice versa. Furthermore, we show that this trade-off holds for any possible pair of measures, when there exists a QRF in which either the coherence or the entanglement vanishes. These insights into the resources present in QRFs can be further explored and used in the context of quantum information. Lastly, we also discuss (not included here) why this apparent gain of entanglement or its conversion to coherence in quantum states does not affect the outcomes of quantum informational protocols. This is because every such transformation changes the Hilbert space factorization, and hence can delocalize observables, forcing an agent who would want to use the QRF-induced entanglement for any protocol to perform operations on all subsystems, defying the protocol's main purpose.

[1] F. Giacomini, E. Castro-Ruiz, and Č. Brukner, Quantum mechanics and the covariance of physical laws in quantum reference frames, Nature Communications **10**, 10.1038/s41467-018-08155-0 (2019).

[2] A.-C. de la Hamette and T. D. Galley, Quantum reference frames for general symmetry groups, Quantum **4**, 367 (2020).

[3] O. Gühne and G. Tóth, Entanglement detection, Physics Reports **474**, 1 (2009).

[4] T. Baumgratz, M. Cramer, and M. B. Plenio, Quantifying coherence, Phys. Rev. Lett. **113**, 140401 (2014).

Exploring the hierarchy of steering measurement settings of qubit-pair states via kernel-based quantum learning model

Zheng-Lin, Tsai[1] * Hong-Bin, Chen[1 2 3] †

[1] *Department of Engineering Science, National Cheng Kung University, Tainan 701401, Taiwan*
[2] *Center for Quantum Frontiers of Research & Technology, NCKU, Tainan, Taiwan*
[3] *Physics Division, National Center for Theoretical Sciences, Taipei 106319, Taiwan*

Abstract. Quantum steering has been proven to be a unique quantum correlation sandwiched between Bell nonlocality and quantum entanglement. Due to its fundamental importance, quantum steering has been studied extensively. To demonstrate the steerability, one relies on a particular resource referred to as steerable assemble on one side of a two-party system. However, it is generically unclear how to reach such steerable resource from a bipartite quantum state. For this purpose, one must optimize over all possible measurement settings, which constitute a hierarchy structure. On the other hand, in the eye of the rapid development of quantum computing technology, quantum machine learning (QML) has been an emerging field with a promising potential in demonstrating quantum advantage. Here we leverage the power of kernel-based QML models to infer the hierarchy of steering measurement setting. We design a computational protocol to generate the labeled training dataset, and encode the training data into five different features. We then apply the well-trained models to analyze random quantum states and three different types of specific quantum states. In summary, this work provides predictions of the hierarchy of steering measurement settings and the boundary between steerability and unsteerability using classical and quantum machine learning models.

Keywords: Quantum information, EPR steering, Measurement setting, Semidefinite programming, Quantum support vector machine, Quantum computing, Quantum kernel

1 Introduction

Quantum correlations play a crucial role in quantum information theory and are classified as nonlocal correlations. These correlations arise due to the peculiar characteristic of quantum mechanics, where particles can become interconnected in ways that defy classical intuition. This phenomenon was famously described in 1935 by the EPR paradox that was proposed by Einstein, Podolsky, and Rosen [1]. Until now, quantum correlations have been characterized by several phenomena, including Bell non-locality [2], quantum steering [3], and quantum entanglement [4]. Quantum steering, also known as EPR steering, involves Alice performing uncharacterized measurements on a quantum state in her possession and transmitting the results to Bob. Through her measurements, Alice steers the quantum states of Bob, even though they are spatially separated. This phenomenon cannot be explained by the local hidden state (LHS) model [5].

In the quantum steering scenario, the construction of a steerable assemblage presents a challenging problem for Alice, who must decide on an appropriate measurement setting before Bob receives his assemblage. However, we do not know the precise observables. To decide the observables, it is necessary to optimize over all possible incompatible measurements and it encompass both the number of observables and which observables need to be measured to demonstrate steerability on Bob's side.

To solve this problem, the first step involves generating a large number of datasets through the pre-filter and SDP iteration [6]. These datasets will then be screened and labeled for both random quantum states and special quantum states. An important part of the process is attempting to leverage the capabilities of the support vector machine (SVM) with potential advantage of the quantum kernel to deduce the hierarchy of steering measurement settings. Consequently, the results obtained using classical and quantum kernels will be compared to assess their differences and abilities in this context.

2 Quantum Steering

Quantum steering is a portion of quantum correlations. There exists a bipartite situation where Alice and Bob share an unknown quantum state ρ^{AB}. Subsequently, Alice performs her measurements as a black box on her system with classical input m_A and outcome o_A labeled by $x = 0, ..., m_A - 1$ and $a = 0, ..., o_A - 1$, respectively. Then, the outcomes are independent of any specific details in a one-sided device-independent scenario, Bob possesses complete control over his measurements, allowing him to perform quantum state tomography and reconstruct the set of states $\sigma_{a|x} = \mathrm{tr}_A[(M_{a|x} \otimes \mathbb{1})\rho^{AB}]$ with one-way classical communication, often known as assemblage $\{\sigma_{a|x}\}_{a,x}$, where $\sum_a M_{a|x} = \mathbb{1}$ and $M_{a|x} \geq 0 \ \forall a, x$. However, the assemblage containing both classical information of the probability $p(a|x) = \mathrm{tr}(\sigma_{a|x})$ and Bob's quantum state $\rho^B_{a|x} = \sigma_{a|x}/\mathrm{tr}[\rho^{AB}]$.

Verifying the steerability of a quantum state is a complex task. To overcome this challenge, we need to optimize over all possible measurements including the number of observables and selection of observables to be measured on a given state. This construction enables the classification of quantum states based on the minimal number n of required observables to exhibit the steer-

*n96111231@gs.ncku.edu.tw
†hongbinchen@gs.ncku.edu.tw

ability, forming a hierarchy known as the hierarchy of steering measurement settings, and we name the number of observables that can exhibit steerability from Alice to Bob as n-measurement steerable (nMS). Then, we can determine whether Bob's assemblage can be decomposed using an LHS model

$$\sigma_{a|x} = \sum_{\lambda} p(\lambda) p(a|x,\lambda) \rho'_{\lambda}, \ \forall a, x \tag{1}$$

to ascertain its steerability, where ρ'_{λ} is a set of existing quantum states, $p(\lambda)$ is a probability distribution, and $p(a|x,\lambda)$ is the post-processing of Alice under the hidden variable λ. For a given assemblage $\sigma_{a|x}$, we can determine whether it admits the LHS model by using an SDP [7]. If we can find feasible solutions from Eq. (1), the assemblage is unsteerable; otherwise, it is steerable.

3 Quantum-enhanced Machine Learning

Quantum machine learning (QML) aims to leverage quantum computers to create scalable machine learning models that could outperform classical ones. With the increasing accessibility of near-term quantum devices and the ongoing quest for fault-tolerant quantum computers, researchers are increasingly excited by investigating the potential outcomes of replacing supervised machine learning models with quantum circuits [8, 9], such as the quantum support vector machine (QSVM). In a straightforward manner, the quantum circuits encode the raw data into quantum states, This allows us to view quantum circuits as kernel functions, with their outputs then fed into the learning model.

4 Support Vector Machine

The principles of Support Vector Machines (SVM) are based on a type of learning algorithm developed in the 1990s. It is founded on results from the statistical learning theory introduced by Vapnik [11]. Support Vector Classification (SVC) is a method in SVM that can be used to solve qualitative problems. The classification task typically becomes more challenging as the number of categories increases.

In simpler terms, SVC aims to find the most effective separating boundary [11, 12], often referred to as a hyperplane which is equidistant from two distinct sets of data points. We can defined its hyperplane can be written as $\vec{w} \cdot \vec{x} + b = 0$, where $\vec{w}$ is the weight vector, $\vec{x}$ is the data points, and b is the bias. The corresponding decision functions are written as $f(x) = \text{sign}\left(\vec{w} \cdot \vec{x} + b\right)$. To find this optimal separating hyperplane, we have to maximize the distance between the two margins. The optimization becomes a quadratic programming (QP) problem, and the Lagrange multiplier method can be applied to derive its dual problem. As a result, we can write $\mathrm{F}(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1}^{n} \alpha\alpha_i yy_i \vec{x}\vec{x}_i$, where $\alpha_i (\alpha_i \geq 0)$ are the Lagrange multipliers for each data point.

If a linear classifier is not suitable, SVC has the capability to map the input vector into a feature space F of higher dimensions. SVC constructs an optimal separating hyperplane in this feature space by applying a non-linear mapping ϕ. Then the optimisation problem for non-linear classifier becomes $\mathrm{W}(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1}^{n} \alpha\alpha_i yy_i \left\langle \phi(\vec{x}) \cdot \phi(\vec{x}_i) \right\rangle$. We called kernel function K such that $K(\vec{x}, \vec{x}_i) = \left\langle \phi(\vec{x}) \cdot \phi(\vec{x}_i) \right\rangle$. Consequently, the decision function can be represented in the following form:

$$g(x) = \text{sgn}\left(f(x)\right) = \text{sgn}\left(\sum_{i=1} \alpha_i y_i K(\vec{x}, \vec{x}_i) + b\right). \tag{2}$$

5 Quantum kernel

A significant distinction between classical and quantum learning theory lies in the concept of the kernel. To surpass classical methodologies, it becomes essential to apply a mapping based on quantum circuits that are difficult to simulate classically. Currently, attention is focused on the quantum kernel, which encodes classical data into the Hilbert space of quantum states. This process is known as the quantum feature map [13].

Consider a quantum circuit $U(x)$ and let $\mathcal{X}$ be a nonempty set, where $x \in \mathcal{X}$. The operation $U(x)$ acts on the $|0\rangle$ state when the data is loaded and resulting in the transformed state $|\psi(x)\rangle = U(x)|0^n\rangle$. However, this transformed state is also commonly referred to as quantum encoding. Let $\mathcal{H}$ be a Hilbert space, called the featured space. Then, the feature map is defined as the transformation.

$$\psi : \mathcal{X} \to \mathcal{H}, \text{ and } \psi(x) = |\psi(x)\rangle\langle\psi(x)|, \tag{3}$$

and the quantum kernel can be written as $K(x, x') = |\langle\psi(x')|\psi(x)\rangle|^2$. For unitary quantum encoding, the process is uncomplicated when we are able to construct the adjoint of the data-encoding circuit, denoted as $U^{\dagger}(x)$. In this scenario, we can rewrite the quantum kernel accordingly as:

$$K(x, x') = |\langle\psi(x')|\psi(x)\rangle|^2 = |\langle 0^n|U^{\dagger}(x')U(x)|0^n\rangle|^2. \tag{4}$$

Our target is to determine the probability of observing the $|0\rangle$ state when measuring the state $|\langle 0|U^{\dagger}(x')U(x)|0\rangle|$ in the computational basis. This process is called quantum kernel estimation (QKE). To derive an estimate, we initialize the quantum system in the $|0\rangle$ state, apply $U^{\dagger}(x')U(x)$ to the input $|0\rangle$, and then estimate the probability of the 0^n output. We construct the kernel matrix from these outputs and plug it into Eq. (2).

6 Methods

For the preparation work, we first generate a number of random density matrices, then we feed them into the prefilter and SDP iteration to determine the label l of each state. After that, we obtain a total of 232,846 training

data points. The training data $\{(f, l)\}$ consists of features and labels, where $f \in \mathbb{R}^n$ and $l \in \mathbb{R}$ correspond to the ground truth (GT) associated with the feature f. Due to computational constraints, we extracted only a portion for model training purposes. Consequently, we obtained training data comprising 71,000 data points, including 1,000 Werner state instances where $\xi = \pi/4$. The composition of each class is 15,293 (2MS), 18,130 (3MS), 15,022 (4MS), 10,055 (STE), and 12,500 (UNS).

Typically, learning models are trained more efficiently when the length of the features gradually decreases. We perform feature engineering, which involves creating new features from raw data to capture more information or reduce the dimensionality of the feature space. Here we consider a type of feature named "LUTA-6" which is reduced based on the physical insights into quantum steering. Further details are present in Appendix 8.1. Then we use the **ZZFeatureMap** [13] to set up the quantum circuits for performing the quantum encoding, and we execute the quantum circuits on **AerSimulator**. In linear kernel ($K_{\text{linear}}(\vec{x}, \vec{x}_i) = \vec{x} \cdot \vec{x}_i$) and Gaussian radial basis functions (RBF) ($K_{\text{RBF}}(\vec{x}, \vec{x}_i) = \exp(-\gamma \|\vec{x} - \vec{x}_i\|^2)$), we set the regularized constant $C = 1$. Additionally, the gamma γ in RBF will depend on the training data X: $\gamma = 1/(N_{\text{features}} \times \text{variance}(X))$.

7 Results

We first illustrate the learning model's performance on random quantum states using three different kernels, as presented in Fig. (1).

To determine the generality and facilitate the visualization of the predictions, we apply these models to predict the hierarchies of two different types of quantum states generalized from the standard Werner state:

$$\begin{cases} \rho_I(p, \xi) = p|\psi_\xi\rangle\langle\psi_\xi| + (1-p)\frac{I_d}{2} \otimes \frac{I_d}{2} \\ \rho_{II}(p, \xi) = p|\psi_\xi\rangle\langle\psi_\xi| + (1-p)\rho^A \otimes \frac{I_d}{2} \end{cases}, \tag{5}$$

where $|\psi\rangle = \cos\xi|00\rangle + \sin\xi|11\rangle, 0 \le \xi \le \pi/2, p \in [0, 1]$ and $\rho^A = \text{tr}_B|\psi_\xi\rangle\langle\psi_\xi|$. We use the subscripts in ρ_I and ρ_{II} to denote the two different types of noise added to the pure entangled state and name them Werner State I and II [14, 15], respectively. Additionally, the T state [16, 17] can be expressed in the Pauli basis as $\rho_T = (I_d \otimes I_d + \sum_{i=1}^{3} t_i \sigma_i \otimes \sigma_i)/4$.

The hierarchies in these specific quantum states predicted by the learning models are shown in Fig. (2). In this figure, the solid curves represent the hierarchy determined by the SDP iteration, while the starry curves represent the prediction by the learning model. We estimate the mean absolute displacement (MAD) (Appendix 8.2) of the border of nMS states predicted by the models to quantify the performance precisely. We present the numerical results in Table (1). It is obvious that the quantum kernel always exhibits less deviation than the linear kernel. However, in the comparison between the RBF and quantum kernel, both are evenly matched, demonstrating good performance in these three states.

In conclusion, the capability of the quantum kernel surpasses that of the linear one. Furthermore, the quantum kernel and RBF are neck and neck. The investigators expect the QSVM to have a potential advantage in this era of artificial intelligence. Nowadays, there are more and more practical applications with QML [18, 19, 20].

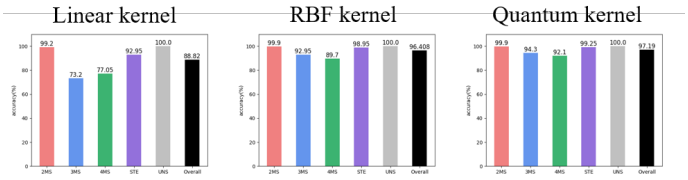


Figure 1: **The LUTA-6 model performance of random quantum states.** Although the RBF and quantum kernel are neck and neck, the quantum kernel is slightly more precise in the 3MS, 4MS, and STE classes.

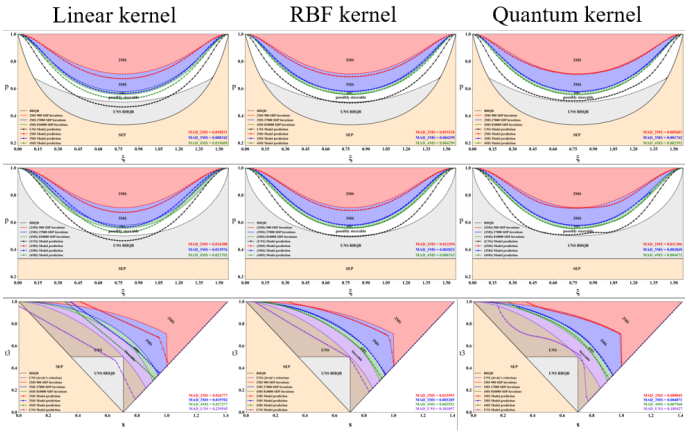


Figure 2: **The LUTA-6 model performance of specific quantum states.** The predictions of the hierarchy for Werner state I $\rho_I(p, \xi)$ (first row), Werner state II $\rho_I I(p, \xi)$ (second row), and T state (third row) by the model. The prediction performs a better agreement with the ground truth given by the quantum kernel.

Table 1: **Quantitative evaluation of the models.** This table presents the numerical results to quantify the performance of the models.

Werner I	Linear	RBF	Quantum
2MS	18.53×10^{-3}	15.12×10^{-3}	5.6×10^{-3}
3MS	8.34×10^{-3}	4.3×10^{-3}	1.74×10^{-3}
4MS	19.61×10^{-3}	4.3×10^{-3}	2.39×10^{-3}
Werner II	**Linear**	**RBF**	**Quantum**
2MS	16.39×10^{-3}	12.29×10^{-3}	11.31×10^{-3}
3MS	13.98×10^{-3}	2.82×10^{-3}	2.85×10^{-3}
4MS	21.7×10^{-3}	6.76×10^{-3}	4.67×10^{-3}
T state	**Linear**	**RBF**	**Quantum**
2MS	26.78×10^{-3}	15.59×10^{-3}	8.85×10^{-3}
3MS	19.7×10^{-3}	3.2×10^{-3}	4.07×10^{-3}
4MS	27.28×10^{-3}	3.55×10^{-3}	7.96×10^{-3}
UNS	239.55×10^{-3}	181.1×10^{-3}	189.43×10^{-3}

8 Appendix

8.1 Data Preprocessing

Performing feature engineering involves creating new features from raw data to capture more information or reduce the dimensionality of the feature space. Generally, reducing the feature length facilitates promoting efficiency during the training process by decreasing computational complexity and potentially alleviating issues related to overfitting.

From [21], we know that quantum steering can be represented by an ellipsoid. The mathematical description of Alice's ellipsoid requires a 3×3 symmetric matrix Q_A and its center $\vec{c}_A \in \mathbb{R}^3$. We can rotate the Bloch sphere such that the three semiaxes of Alice's ellipsoid align with the computational bases by applying the local unitary transformation on both sides. This operation corresponds to a diagonal Q_A, implying a rotation of Alice's ellipsoid since ellipsoids are generally skewed. This leads to the feature of length 6, denoted as LUTA-6.

8.2 Quantitative Evaluation

To quantify the gap between the two different curves more precisely, we estimate the mean absolute displacement (MAD) of the border of nMS states predicted by the models to quantify the performance. The MAD is defined as

$$\mathrm{MAD}_{\xi(s)} = \frac{\sum_{\xi(s)=0}^{\pi/2(\sqrt{2})} |p_{\xi(s)}^{\mathrm{Prediction}} - p_{\xi(s)}^{\mathrm{GT}}|}{n}, \qquad (6)$$

where n is the number of pixels on a border.

References

[1] A. Einstein. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47.10: 777, 1935.

[2] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1.3: 195, 1964.

[3] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, Cambridge University Press, pages 555-563, 1935.

[4] R. Horodecki. Quantum entanglement. *Reviews of modern physics*, 81.2: 865, 2009.

[5] H. M. Wiseman. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Physical review letters*, 98.14: 140402, 2007.

[6] H. M. Wang. Deep learning the hierarchy of steering measurement settings of qubit-pair states. *Communications Physics*, 7.1 (2024): 72, 2024.

[7] D. Cavalcanti. Quantum steering: a review with focus on semidefinite programming. *Reports on Progress in Physics*, 80.2: 024001, 2016.

[8] C. Ciliberto. Quantum machine learning: a classical perspective. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 474.2209: 20170551, 2018.

[9] V. Dunjko. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, 81.7: 074001, 2018.

[10] M. Schuld. Supervised quantum machine learning models are kernel methods. *arXiv preprint arXiv* :2101.11020, 2021.

[11] V. Vapnik. The nature of statistical learning theory. *The nature of statistical learning theory*, Springer science & business media, 2013.

[12] B. Schölkopf. *Learning with kernels: support vector machines, regularization, optimization, and beyond.* MIT press, 2002.

[13] V. Havlíček. Supervised learning with quantum-enhanced feature spaces. *Nature*, 567(7747), 209-212, 2019

[14] J. Bowles. Sufficient criterion for guaranteeing that a two-qubit state is unsteerable. *Physical Review A*, 93.2: 022121, 2016.

[15] A. C. S. Costa. Quantification of Einstein-Podolsky-Rosen steering for two-qubit states. *Physical Review A*, 93.2: 020103, 2016.

[16] R. Horodecki. Information-theoretic aspects of inseparability of mixed states. *Physical Review A*, 54.3: 1838, 1996.

[17] C. Jevtic. Einstein–Podolsky–Rosen steering and the steering ellipsoid. *JOSA B*, 32.4: A40-A49, 2015.

[18] J. Heredge. Quantum support vector machines for continuum suppression in B meson decays. *Computing and Software for Big Science*, 5.1: 27, 2021.

[19] W. Guan. Quantum machine learning in high energy physics. *Machine Learning: Science and Technology*, 3.3: 033221, 2021.

[20] S. L. Wu. Application of quantum machine learning using the quantum kernel algorithm on high energy physics analysis at the LHC. *Physical Review Research*, 2.1: 011003, 2021.

[21] S. Jevtic. Quantum steering ellipsoids. *Physical review letters*, 113.2: 020402, 2014.

Nonlocality in Networks Assisted by Neural Networks and Rigidity

Tamás Kriváchy[1] *

[1] *ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*

Abstract. The study of Bell nonlocality in networks presents a versatile framework for studying the strength of quantum correlations. However, even for small networks, such as a triangle network, there is difficulty in finding an example of a distribution that is robust to experimental noise, and in expanding nonlocality proofs beyond the currently known principle of token counting. We show how insight from variatonal numerical models such as artificial neural networks can help to focus our analytic efforts and allow us to prove nonlocality even under realistic noise (photon loss), and to expand nonlocality proofs beyond token counting.

Keywords: Bell nonlocality, networks, quantum correlations, machine learning

1 Introduction

With the advance of quantum technologies, the question of what correlations can be achieved on a network of quantum nodes has become increasingly relevant. Beyond the practical motivation, the question has become a fundamental one. For example, in standard Bell nonlocality, one can certify the quantumness of sets of measurements conducted on single systems, and indeed, many physicsists would tell you that quantum properties of measurements stem from their non-commutativity, or their lack of being jointly measureable. In contrast, recently it has been shown that in ring networks, one can achieve network nonlocality even when each party conducts the same measurement in each round, i.e. one does not require inputs as in standard Bell nonlocality and the quantum properties are not directly related to joint measurability, opening the path to a novel aspect of quantum measurements [1, 3].

Characterizing correlations on networks poses a difficult challenge, as one loses the convexity property that simplifies the study of standard Bell nonlocality [4]. Using neural networks as a variational ansatz for classical models on the network can greatly help to understand the landscape of locality, and through it, nonlocality [5]. Moreover, combined with variational models for quantum strategies help to identify regions of interest for analytic research.

The purpose of this presentation would be to display the intertwined path of human researchers and neural network-based tools, and how these insights from numerics can lead to a series of conjectures, and finally to proven analytical findings in the field of Bell nonlocality, one of the strongest frameworks for understanding and verifying the strength of quantum resources. Finally, it would also like to draw interest to a number of open questions in the field.

1.1 Nonlocality in the triangle

The triangle network without inputs is one of the workhorses of understanding quantum correlations on networks, and it is one of the simplest tripartite networks

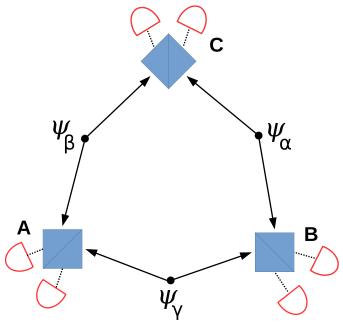


Figure 1: Topology of the triangle network, where a specific choice of measurement is depicted, a beam-splitter and two photo-detectors for each party.

that features nonlocality. Each pair of parties shares a bipartite quantum source, giving rise to distributions

$$p(a,b,c) = \mathrm{Tr}(\rho_{s_\alpha} \otimes \rho_{s_\beta} \otimes \rho_{s_\gamma} \cdot M^a \otimes M^b \otimes M^c), \quad (1)$$

where ρ_{s_y} is the state distributied by source y ($y \in \{\alpha, \beta, \gamma\}$), and $\{M^x\}_x$ is the POVM used by party $X \in \{A, B, C\}$. Notice that each party performs the same measurement in each round of the setup, contrary to standard Bell nonlocality, where they must change measurement settings from round to round. Any correlation in the triangle which can be explained with classical sources, i.e. those that have a classical decomposition of the form

$$p(a,b,c) = \sum_{\alpha,\beta,\gamma} p_A(a|\beta\gamma) p_B(b|\gamma\alpha) p_C(c|\alpha\beta) \times \quad (2)$$
$$\times\, p_{s_\alpha}(\alpha) p_{s_\beta}(\beta) p_{s_\gamma}(\gamma),$$

are termed *local*, whereas those that do not have such a decomposition are *nonlocal*, where p_{s_y} is the distribution of the random variable distributed by source s_y.

There are only a few examples of nonlocality in the triangle network without inputs. When using qubit systems, the most natural cardinality of the outputs of the parties is 4 ($a, b, c \in \{1, 2, 3, 4\}$), for which one can achieve nonlocality by morphing the standard 2-party

*tamas.krivachy@gmail.com

Bell scenario into a triangle [1, 2]. This distribution, however, requires only one of the sources to be quantum, as the other two take on the roles of the classical inputs.

The first example of genuine quantum triangle nonlocality (RGB4 distribution) was based on the concept of token counting and its rigidity [3]. Unfortunately such a proof of nonlocality is extremely sensitive to realistic noise, and thus the implementation of such a distribution in an experiment was questionable. Besides RGB4 there is another distribution which was conjectured to be genuinely triangle-nonlocal, based on the Elegant Joint Measurement [6]. This distribution is extremely symmetric, with probabilities being equal under permutation of parties and of outcome labels. There is no proof yet of nonlocality for this distribution in the literature.

1.2 Rigidity

The basic idea of rigidity is that for certain distributions, one can show that there is essentially a unique local model explaining them. For RGB4, it turns out that by coarse-graining two of the outcomes one arrives at a distribution which is rigid, hence any classical model describing the distribution must have the so-called token counting strategy [9, 10]. When fine-graining the distribution back to the original RGB4, one can show that the classical token counting model can not be adjusted to match the correlations arising from the quantum strategy, showing that RGB4 is nonlocal.

The idea of rigidity has also been used recently to prove noise-robustness for generalizations of RGB4, by showing that in the noisy distribution a part of the local model (if it exists), must have a token counting structure [11]. Unfortunately under realistic noises the method typically allows for less than 1% noise robustness of the proof of nonlocality, which falls short of experimental capabilities.

1.3 Variational tools

Local models, as described by Eq. (3), form a nonconvex set, making their analytic and numeric characterizing a challenging task, contrary to standard Bell nonlocality. In Ref. [5] (LHV-Net) we used a set of generative neural networks as a variational ansatz for local models: essentially by replacing each party with a neural network and asking them to play the game of trying to reconstruct a target distribution. Given that they are classical, any strategy constructed by them inherently leads to a local distribution, allowing us to probe the boundaries of the local set. An early success of LHV-Net was conjecturing nonlocality of the RGB4 distribution beyond the range where it was proven to be nonlocal. This conjecture has since been proven [8].

Recently, we have expanded the technique to studying variational *quantum* models, where we fix the dimension of the bipartite quantum states. Then, in order to approximate a target distribution, the parameters of the states and measurements are generated via a generative neural network, or simply optimized directly through gradient descent. This allows us to probe (a subset of) quantum distributions.

2 Towards experimental nonlocality in the triangle network

When aiming to create genuine nonlocal correlations in the triangle network, one can essentially choose to work with the RGB4 distribution (proven to be nonlocal) or with the Elegant distribution (conjectured to be nonlocal). LHV-Net was the only tool that managed to give insight into the amount of noise that these distributions could withstand while remaining nonlocal. These noise thresholds were close to what might be realizable experimentally, however, the issue of how to translate these theoretical measurements to simple enough optical setups was still an open question.

In order to find a more experimentally friendly setup, we conjectured optical setups and used LHV-Net to quickly test whether these may actually be nonlocal or not. One setup was identified as potentially nonlocal, and then proven as well [7]. In fact, by doing the proof we realized that it essentially gives an implementation of RGB4 using only single-photon sources and passive optics. Unfortunately the noise robustness of this distribution is quite on the boundary of what can be achieved experimentally, and was thus not yet implemented.

2.1 Implementing the Elegant Joint Measurement in the triangle network, and Bell inequalities

Meanwhile, colleagues from Hefei, China, have developed a way to experimentally implement the Elegant distribution [12]. The technique, however, only allows for measuring the four eigenvectors of the Elegant Joint Measurement in separate rounds, which introduces a loophole, as global postprocessing of the outcomes and measurement settings is required to reconstruct the Elegant distribution. Moreover, the experiment had to be renormalized to the events when all photons arrived, introducing yet another global postprocessing step. The global postprocessing imposes a theoretical challenge to the experiment, as with (unconstrained) global postprocessing any distribution can be constructed (e.g. all parties outputting random bits, then keeping only (0,0,0) and (1,1,1) events, leading to perfect GHZ-type correlations.

Nonetheless, the distribution realized in the experiment simulates the Elegant distribution to great accuracy. In parallel to experimental efforts in the lab, LHV-Net has been used to identify conjectures of Bell inequalities that are valid for the triangle and certify the nonlocality of the Elegant distribution [13]. These inequalities capture the trade-off between distribution being strongly correlated and being symmetric. The Elegant distribution achieves both, whereas classical distributions can not simultaneously do so. The experimental results of the Elegant distribution violate these conjectured inequalities with great confidence.

2.2 Loophole-free experimental proposals

Armed with LHV-Net, which quickly gives numeric evidence of the nonlocality of a distribution, we considered

a generalization of the previous single-photon experimental proposal (see Sec. 2). The idea was to use high-dimensional quantum states, as perhaps these could be more robust to noise. We set each source distribute the state $\psi_\alpha = \psi_\beta = \psi_\gamma = (|20\rangle + |02\rangle)/\sqrt{2}$ (in the Fock basis) and the measurements consist of a beam-splitter and photo-detectors, as shown in Fig. 1. The first numerical results of LHV-Net showed nonlocality, and in fact a decent noise robustness under a toy noise model.

Following such convincing numerics, we looked deeper at the analytics and managed to carry over many of the principles of token counting and those developed in [11], in order to prove its nonlocality. In fact these tools allowed us to prove nonlocality even under the most dominant source of noise: single photon loss. Under the noise model that each channel can lose up to one photon with probability η, we show that nonlocality is present up to $\eta^* = 18\%$. Using rigidity it is clear that noise robustness can be proven also for a full photon loss model. The derivation of the exact values are currently under way, as some changes must be made to previous rigidity-based noise robustness proofs.

Moreover, in the studied distribution, if heralding is used to create the source states, then one can circumvent the global post-selection that was required in previous experiments to make sure all photons arrived. We show how it is enough for the information heralding the creation of the source states to be sent to the parties and to be processed locally, avoiding the second loophole.

3 Nonlocality in the symmetric subspace

The importance of the symmetric subspace of distirubtion has by now become clear, presenting the only known alternative to RGB4 (or its extensions) for genuine triangle nonlocality, particularly with the given push of experimental implementation of the Elegant distribution (Sec. 2.1). Recall that symmetric distributions are those where the probabilities are symmetric under permutation of parties and outputs, leading to only three unique values, $p(1,1,1)$, $p(1,1,2)$ and $p(1,2,3)$. Equivalently one may use the sum of each of these types of events, which we call s_{111}, s_{112} and s_{123}, s.t. $s_{111} + s_{112} + s_{123} = 1$.

In a recent work, we explore the landscape of symmetric local distributions both analytically and with the neural network [13]. The analytic constructions of local models indicated that $s_{111} \leq 1/\mathbb{O}$, where $\mathbb{O}$ is the cardinality of the output variables of one party, ($\mathbb{O} = 4$ for the previous examples), The Elegant distribution has $s_{111} \approx 0.39$, well above this bound of 0.25.

Compared to the analytical constructions of local models, LHV-Net finds more correlated symmetric local distributions, up to $s_{111} \approx 0.29$ for $\mathbb{O} = 4$, outperforming the analytic constructions, hinting that the true local bound is above $1/\mathbb{O}$, but still much below the Elegant distribution's value. Indeed, this value of 0.29 is reflected in the Bell inequalities that the neural network finds in the same work. LHV-Net scans of the symmetric subspace indicate that for cardinalities $\mathbb{O} = 3, 5, 6$, the same phenomena appears: a bound slightly higher than $1/\mathbb{O}$.

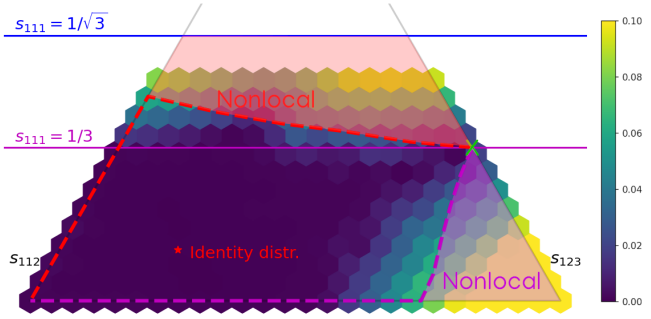


Figure 2: Nonlocality in the symmetric simplex of distributions. Color scale represents Euclidean distance from the local set, as gauged by LHV-Net (cut of at 0.1). For any quantum or classical model $s_{111} \leq 1/\sqrt{3}$ [14, 15], depicted by a blue line. From rigidity of the $s_{112} = 0$ distribution (marked with a green X), we can prove nonlocality outside the dashed lines.

In the scans of the symmetric subspace there is a peculiar point for $\mathbb{O} = 3, 4$, namely when $s_{112} = 0$, there seems to be only a single distribution that is classically realizable (with exactly $s_{111} = 1/\mathbb{O}$). Upon more detailed theoretical analysis, we managed to prove that this is indeed the case for $\mathbb{O} = 3$. In fact it turns out that not only the distribution's probability values are unique next to the $s_{112} = 0$ condition, but also the specific strategy that can be used to create it is unique. This provides a strong starting point for a rigidity-based proof of nonlocality. For $\mathbb{O} = 3$ we have managed to prove, starting from this special point, that local distributions must be contained within the dashed lines portrayed in Fig. 2, proving nonlocality for almost all of the part of the symmetric subspace where nonlocality was previously unknown. Currently, we are working on extending this to $\mathbb{O} = 4$, where we have indications that this technique could prove the nonlocality of the Elegant distribution.

Finally, we could contrast maps of the symmetric subspace with variational *quantum* methods to those of LHV-Net, allowing us to identify where quantum nonlocality could exist.

4 Conclusion

In summary, at AQIS 2024 I wish to share our journey of how neural network-based tools helped pinpoint where analytic effort would be most effective, and how this led to a variety of results, such as proving nonlocality in the symmetric subspace and to an experimentally noise-robust proposal which closes two previous loopholes. Moreover, the insights from the variational numerics lead to a number of open conjectures, including the triangle Bell inequality and further conjectures of genuine quantum nonlocality.

Hopefully the results will not just spark interest in foundational questions about the nature of quantum measurement and quantum networks, but also inspire others to more boldly use modern numerical tools in foundational and applied research.

References

[1] T. Fritz. Beyond Bell's theorem: correlation scenarios. *New Journal of Physics*, 14(10):103001, 2012.

[2] E. Polino, D. Poderini, G. Rodari, I. Agresti, A. Suprano, G. Carvacho, E. Wolfe, A. Canabarro, G. Moreno, G. Milani, R. W. Spekkens, R. Chaves, and F. Sciarrino. Experimental nonclassicality in a causal network without assuming freedom of choice. *Nature Communications*, 14(1):909, 2023.

[3] M.-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, and S. Beigi. Genuine Quantum Nonlocality in the Triangle Network. *Phys. Rev. Lett.*, 123(14):140401, 2019.

[4] A. Tavakoli, A. Pozas-Kerstjens, M.-X. Luo, and M.-O. Renou. Bell nonlocality in networks. *Reports on Progress in Physics*, 85(5):056001, 2022.

[5] T. Kriváchy, Y. Cai, D. Cavalcanti, A. Tavakoli, N. Gisin, and N. Brunner. A neural network oracle for quantum nonlocality problems in networks. *npj Quantum Information*, 6(1):1–7, 2020.

[6] N. Gisin. Entanglement 25 Years after Quantum Teleportation: Testing Joint Measurements in Quantum Networks. *Entropy*, 21(3):325, 2019.

[7] P. Abiuso, T. Kriváchy, E.-C. Boghiu, M.-O. Renou, A. Pozas-Kerstjens, and A. Acín. Single-photon nonlocality in quantum networks. *Physical Review Research*, 4(1):L012041, 2022.

[8] A. Pozas-Kerstjens, N. Gisin, and M.-O. Renou. Proofs of Network Quantum Nonlocality in Continuous Families of Distributions. *Physical Review Letters*, 130(9):090201, 2023.

[9] M.-O. Renou and S. Beigi. Nonlocality for Generic Networks. *Phys. Rev. Lett.*, 128(6):060401, 2022.

[10] M.-O. Renou and S. Beigi. Network nonlocality via rigidity of token counting and color matching. *Phys. Rev. A*, 105(2):022408, 2022.

[11] S. Boreiri, B. Ulu, N. Brunner, and P. Sekatski. Noise-robust proofs of quantum network nonlocality. arXiv:2311.02182, 2023.

[12] N.-N. Wang, C. Zhang, H. Cao, K. Xu, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, N. Gisin, T. Kriváchy, and M.-O. Renou. Experimental genuine quantum nonlocality in the triangle network. arXiv:2401.15428, 2024.

[13] E. Bäumer, V. Gitton, T. Kriváchy, N. Gisin, and R. Renner. Exploring the Local Landscape in the Triangle Network. arXiv:2405.08939, 2024.

[14] H. Finner. A Generalization of Holder's Inequality and Some Probability Inequalities. *The Annals of Probability*, 20(4):1893–1901, 1992.

[15] M.-O. Renou, Y. Wang, S. Boreiri, S. Beigi, N. Gisin, and N. Brunner. Limits on Correlations in Networks for Quantum and No-Signaling Resources. *Phys. Rev. Lett.*, 123(7):070403, 2019.

Appendices

The references contain many of the works covered in the proposed presentation [5, 7, 12, 13], however some work is still in progress. In the appendices I share drafts for these results. **Technical draft 1** regards proving nonlocality in the symmetric subspace. **Technical draft 2** regards the proposal for a noise robust experiment for genuine nonlocality in the triangle network.

.

Technical draft 1: Nonlocality in the symmetric subspace

Authors: Tamás Kriváchy, Antoine Girardin, Pavel Sekatski. *Author list not yet finalized.*

Main idea

The main idea of proving nonlocality in the symmetric subspace from rigidity is the following. First, we establish that for any distribution that is symmetric and has $s_{112} = 0$, there is a unique strategy and a unique distribution that satisfies this condition. Next, we use that for any strategy for which $s_{112} > 0$, the part that has $s_{112} = 0$ within that strategy must have the same structure, and thus the response functions of the parties must be constrained to be able to reproduce that large part. Then one can write constraints on what else the repsonse functions could consist of, if one wishes to recover a symmetric distribution with a high s_{111} value.

Symmetric subspace of the triangle network and the flag depiction

The triangle network under consideration in this work consists of three parties, Alice, Bob and Charlie, each pair connected via a commonly shared source, α, β, γ. If all three sources are classical, and thus distribute classical shared randomness to their respective two connected parties, then the distribution of outputs of the three parties has the form

$$p(a,b,c) = \sum_{\alpha,\beta,\gamma} p_A(a|\beta\gamma)p_B(b|\gamma\alpha)p_C(c|\alpha\beta)\times \quad (3)$$
$$\times\, p_{s_\alpha}(\alpha)p_{s_\beta}(\beta)p_{s_\gamma}(\gamma),$$

Any distribution $p(a,b,c)$ that has such a decomposition is deemed local, as there exists a so-called "local hidden variable" model to describe it. We are currently working with an output cardinality of three, and for the sake of visualizing the structure of events more clearly, we name the outputs with colors, s.t. $a,b,c \in \{R,G,B\}$ (for Red, Green, Blue).

Local models can be depicted in the "cube picture", since there are three independent local hidden variables (the three axes of the cube), and each response function (e.g. $p_A(a|\beta,\gamma)$ depends on two of them (three faces of the cube). Practically, one can draw a cube and draw labels on three of the sides of the cube. If the sides are normalized to 1, then the volume of (α,β,γ) triples which project to labels (a,b,c) on the three sides correspond to the probability of $p(a,b,c)$. An example of the cube picture can be seen in Fig. 3, where the three relevant faces of the cube are flattened out. These three colored faces are often referred to as flags.

In the triangle, if a distribution's outcomes are symmetric under permutation of parties and under outcome labels, then it is in the symmetric subspace. Such distributions form a simplex and can be characterized by three numbers,

$$s_{111} = \sum_{a\neq b\neq c\neq a} p(a,b,c) \quad (4)$$

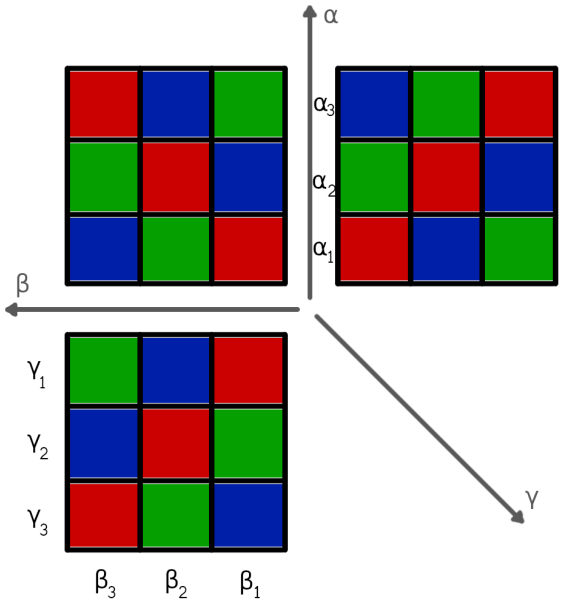


Figure 3: When drawing 3 face of the cube depiction of the local strategy, one can easily see which hidden variable triples lead to which events. Here is the strategy for 3 outcomes (Red, Green, Blue) for the distribution where 112-type events are not allowed. (Alice's "flag" in bottom left, Bob's in the top right, and Charlie's in the top left.)

such that $s_{111} + s_{112} + s_{123} = 1$. Due to the symmetry conditions, the probability of any event with a given symmetry is given by one of these numbers, e.g. $p(1,1,1) = s_{111}/3$.

No-112 condition

If we further restrict distributions such that 112 events are forbidden, which we will call condition $\mathbb{C}$, then for 3 outcomes per party it turns out that there is only a single distribution that satisfies symmetry and $\mathbb{C}$, which has $s_{111} = 1/3, s_{123} = 2/3$. Moreover, it has an essentially unique strategy that realizes it, shown in Fig. 3, where $\forall j,k:\ \beta_j = \gamma_k = 1/3$ and the condition for $\alpha_i \geq 0$ is just that $\sum_i \alpha_i = 1$. In essence, this is a rigid distribution. As an example, consider Alice's flag, where the colorings are shown in Table 1. When considering the whole cube, the 111 events come from the LHV index triples in Table 2.

Table 1: Which (β_j, γ_k) pairs contribute to colors on Alice's flag.

Color	(j,k) values of that color
R	(1,1), (2,2), (3,3)
G	(1,2), (2,3), (3,1)
B	(1,3), (2,1), (3,2)

Nonzero probability of 112 events

By definition, any distribution will have $Pr(\mathbb{C}) = 1 - s_{112}$. Let Λ be the set of triples (α,β,γ) where condition

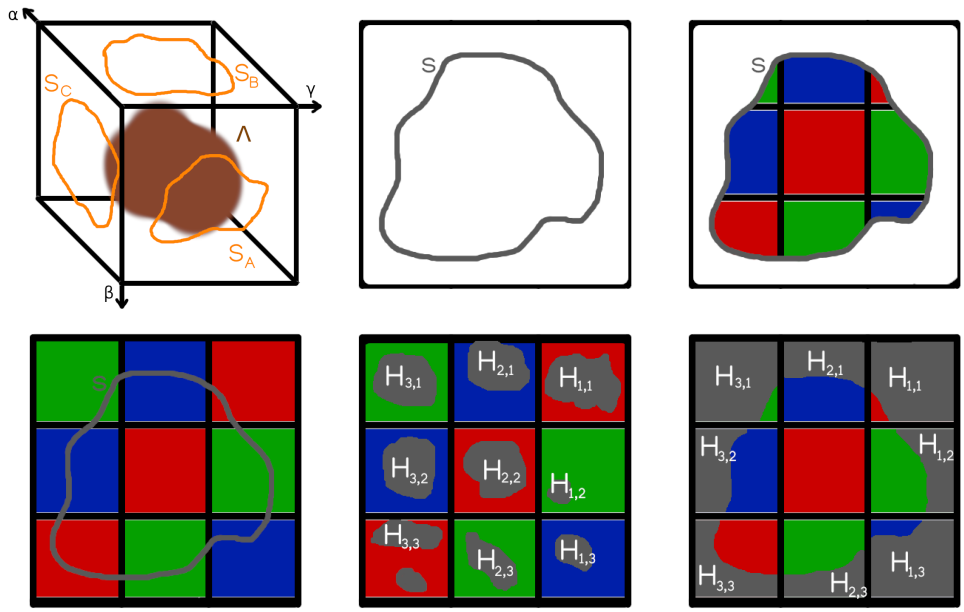


Figure 4: (a) The region Λ (brown) depicted in the cube representation of a local model. The orange contours on the faces show the projections of Λ along the three axes. (b) The projection to Alice's face, $\mathcal{S}_A$, can take any shape in Alice's flag. (c) Within $\mathcal{S}_A$, condition $\mathbb{C}$ must hold, hence there must be a grid structure with Latin-square-like coloring. (d) The extension of the Latin square coloring within $\mathcal{S}_A$ to the whole flag of A. (e) Viewed differently, for any shape of $\mathcal{S}$, one can, by rearranging β and γ LHV's, always arrive at the same flag structure as in Fig. 3, with certain holes in each of the cells (where hole $H_{j,k}$ can have size between 0 and $\beta_j \cdot \gamma_k$). In general these holes can take any shape and their internal coloring is unknown (denoted by grey here). (f) What the holes would be like for the example in panel (c).

Table 2: Which $(\alpha_i, \beta_j, \gamma_k)$ triples contribute to 111-type events.

Event	(i,j,k) values of that event
RRR	(1,1,1), (2,2,2), (3,3,3)
GGG	(3,1,2), (1,2,3), (2,3,1)
BBB	(2,1,3), (3,2,1), (1,3,2)

$\mathbb{C}$ holds. Then it is true that

$$Pr((\alpha, \beta, \gamma) \in \Lambda) = 1 - s_{112}. \tag{5}$$

Note that Λ is a subset of the whole cube, but the exact shape of Λ is unknown. However, we do know that in each face of the cube the part that is generating Λ (i.e. the projection of Λ to the face of the cube), must have the Latin square structure that the condition $\mathbb{C}$ implies, as shown in Fig. 4(c). The set Λ and its projections are illustrated in Fig. 4(a).

Once we draw the projections of Λ, we may ask: how else was the rest of the cube colored? We formalize this through several conditions that must hold. In order to do this let us extend the Latin square structures to the edges of the flags, as shown in Fig. 4(c,f), leading to

$$0 \leq \alpha_i, \beta_j, \gamma_k \quad \forall i, j, k \in \{1, 2, 3\}, \tag{6}$$

$$\sum_{k=1}^{3} \alpha_i = \sum_{j=1}^{3} \beta_j = \sum_{k=1}^{3} \gamma_k = 1. \tag{7}$$

(8)

Notice that the exact colors of the parts outside are unknown, and are thus colored grey. In reality they can be either R, G or B. Note that the holes must not have such regular shapes, as illustrated in Fig. 4(e). In summary, we can assign variables to the areas of these holes, e.g. $H^A_{j,k}$ for the size of the hole in Alice's cell (β_j, γ_k). We can alternatively divide the holes on Alice's flag based on colors, using the variables H^A_X $(X \in \{R, G, B\})$. The following constraints hold for these.

$$0 \leq H^A_{j,k} \leq \beta_j \gamma_k, \quad \forall j, k \in \{1, 2, 3\} \tag{9}$$

$$0 \leq H^A_X \leq s_{112}/3 \quad \forall X \in \{R, G, B\} \tag{10}$$

$$\sum_{j,k} H^A_{j,k} \leq s_{112} \quad \forall j, k \in \{1, 2, 3\}, \tag{11}$$

$$\sum_{j,k} H^A_{j,k} = \sum_X H^A_X, \tag{12}$$

and analogously for the other parties. The second line holds due to the fact that if any of the colors would occupy more than $s_{112}/3$ of area of the holes, then symmetry of the 112-type events could not be satisfied.

Finally, note that if the distribution is symmetric, then one can write bounds for each of the probabilities. We start by considering just one of the subcuboids (e.g. the $(\alpha_i, \beta_j, \gamma_k)$ subcuboid). Let's say according to the original strategy this contributes to a 111-type event. Then the minimum amount it can contribute to s_{111} is its size, minus the sizes that the holes take out of it (now assuming that the projections of the holes from each side don't

overlap, thus taking away as much as possible from the cuboid). Hence the minimum amount of s_{111} from this cuboid is

$$s_{111}^{(i,j,k)} \geq \alpha_i\beta_j\gamma_k - H^A_{j,k}\alpha_i - H^B_{k,i}\beta_j - H^C_{i,j}\gamma_k.$$

Adding this up for all cuboids which contribute to a specific event (e.g. to $(a,b,c) = (R,R,R)$), one gets as a constraint

$$s_{111}/3 \geq \sum_{(i,j,k)\in\mathcal{I}_{RRR}} \alpha_i\beta_j\gamma_k - H^A_{j,k}\alpha_i - H^B_{k,i}\beta_j - H^C_{i,j}\gamma_k, \tag{13}$$

where $\mathcal{I}_{RRR}$ is the set of index triples that result in an $(a,b,c) = (R,R,R)$ outcome (see Table 2). The $1/3$ factor comes from only considering the R 111-type events. Similar constraints hold for the other colors, and for the 123-type events,

$$s_{123}/6 \geq \sum_{(i,j,k)\in\mathcal{I}_{RGB}} \alpha_i\beta_j\gamma_k - H^A_{j,k}\alpha_i - H^B_{k,i}\beta_j - H^C_{i,j}\gamma_k. \tag{14}$$

These are particularly important, since the fact that s_{123} has a minimum size automatically implies an upper bound on s_{111}, since $s_{111} + s_{112} + s_{123} = 1$.

Finally, we have that these events are also upper bounded by the sums of their cuboids

$$s_{111}/6 \geq \sum_{(i,j,k)\in\mathcal{I}_{RRR}} \alpha_i\beta_j\gamma_k, \tag{15}$$

$$s_{123}/6 \geq \sum_{(i,j,k)\in\mathcal{I}_{RGB}} \alpha_i\beta_j\gamma_k, \tag{16}$$

and similarly for all other 111- and 123-type events.

Any local model with such a value of s_{112} must abide to the previously written numbered constraints. Thus, next to the constraints we may maximize either s_{111} or s_{123} using numerical software (e.g. Mathematica easily converges consistently on global optimization tasks of this size), leading to the two bounds given in Fig. 5, which we plotted on top of the LHV-Net scan of the simplex of symmetric distributions. Notice how from the simple principle of rigidity one can prove nonlocality for essentially all of the space where LHV-Net does not find any local model (i.e. where the LHV-Net distance to the local set is larger than approximately 0.02).

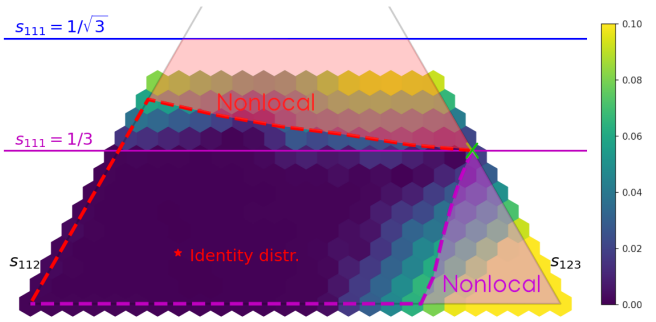


Figure 5: Nonlocality proven in the symmetric simplex of distributions. Color scale represents Euclidean distance from the local set, as gauged by LHV-Net (cut of at 0.1). For any quantum or classical model $s_{111} \leq 1/\sqrt{3}$ [14, 15], depicted by a blue line. From rigidity of the $s_{112} = 0$ distribution (marked with a green X), we can prove nonlocality outside the dashed lines. The upper dashed line (red) is obtained by maximizing s_{111} next to the constraints, while the right dashed line (magenta) is obtained by maximizing s_{123} next to the constraints.

.

Technical draft 2: Proposal for Noise-Robust Nonlocal Experiment in the Triangle Network

Authors: Martin Kerschbaumer, Tamás Kriváchy. *Author list not yet finalized.*

Network Nonlocality with NOON States

Let the sources at each party be a so-called NOON state, with N photons being sent either to the left or to the right party in equal superposition, i.e.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|N0\rangle + |0N\rangle\right),$$

We consider measurements which are experimentally friendly, relying only on passive optics and non-photon number resolving detectors ("click" or "no click" detectors). Specifically, let the two input modes be mixed on a beam splitter, followed by the detectors. The measurements have four outcomes ($a, b, c \in \{0, L, R, 2\}$) and are mathematically characterized by the POVMs

$$\begin{aligned} M_X^0 &= U^\dagger(D^\square \otimes D^\square)U, \\ M_X^R &= U^\dagger(D^\square \otimes D^\blacksquare)U, \\ M_X^L &= U^\dagger(D^\blacksquare \otimes D^\square)U, \\ M_X^2 &= U^\dagger(D^\blacksquare \otimes D^\blacksquare)U, \end{aligned}$$

where $X \in \{A, B, C\}$ represents the party label, U is the beam-splitter's unitary evolution, and $D^\blacksquare$ ($D^\square$) represents a click (no click) event,

$$\begin{aligned} D^\square &= |0\rangle\langle 0|, \\ D^\blacksquare &= \mathbb{I} - |0\rangle\langle 0|, \end{aligned}$$

and finally, and note that the outcome label 2 is used to denote that both detectors click (and not that exactly two photons arrived). See Fig. 1 for a depiction of the full experimental setup for the triangle network.

Proof of Nonlocality

Theorem: For any distribution in the triangle, $p(a, b, c)$, if

- $p(a = 0) = p(b = 0) = p(c = 0) = 1/4$, and
- $p(a = 0, b = 0) = p(b = 0, c = 0) = p(c = 0, a = 0) = 0$

then the Linear Program (LP) below (Constraints 0, 1, 2) must be satisfied if there exists a local model for the distribution.

Proof:

We will describe the main steps to construct the Linear Program. To begin, let us assume that there exists a local hidden variable model for the distribution. Then one can work in the cube picture, where each axis runs from 0 to 1 and represents a hidden variable (α, β or γ), and the faces represent the response functions, assumed to be deterministic without loss of generality.

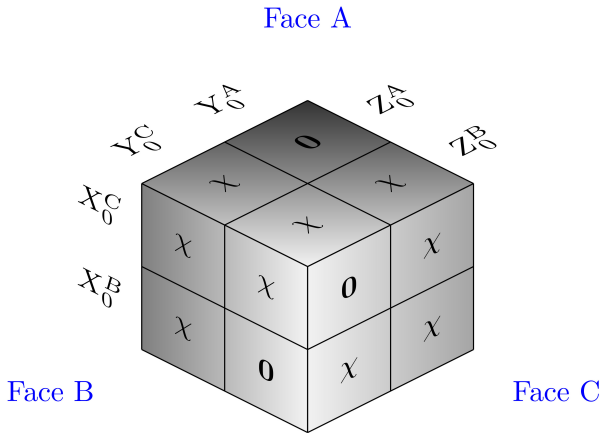


Figure 6: Any LHV model for the distribution must have this structure, where χ represents all other outcomes except 0.

We will first focus only on the 0 outcomes, as these are quite constraining. Let us draw the smallest possible square (with sides parallel to the axes) that contains *all* 0 outcomes of Alice (see Fig. 6 for an illustration). Let Y_0^A, Z_0^A be the two sides of this square. Note that the square *may* contain other outcomes as well, but at least all 0 outcomes must be contained. As such, it must be true that $Y_0^A Z_0^A \geq p(a = 0)$, as the marginal probability $p(a = 0)$ corresponds to the area on Alice's face that is labeled with 0. One can introduce the corresponding variables for Bob and Charlie, and one arrives at the conditions

$$Y_0^A Z_0^A \geq p(a = 0), \tag{17}$$
$$Z_0^B X_0^B \geq p(b = 0), \tag{18}$$
$$X_0^C Y_0^C \geq p(c = 0). \tag{19}$$

Due to the condition that two parties cannot output 0 at the same time, these volumes behind these squares cannot overlap at all, i.e. $X_0^B + X_0^C \leq 1$, $Y_0^C + Y_0^A \leq 1$, $Z_0^A + Z_0^B \leq 1$ (otherwise there would be $(0, 0)$-type outcomes). Since $p(a = 0) = p(b = 0) = p(c = 0) = 1/4$, *the only solution* to these set of inequalities is that $X_0^B = X_0^C = Y_0^C = Y_0^A = Z_0^A = Z_0^B = 1/2$. Due to the saturation of the inequalities at this value, we in fact also know that *the square does not contain any other output labels*, except 0's, as shown in Fig. 6.

Let $\mathbb{O}$ be the total number of outcomes per party, and let us label all outcomes except 0 together as χ ($\chi = \{1, 2, ..., \mathbb{O} - 1\}$). Since all 0 outcomes are contained in the squares, the rest of the cube faces are all χ outcomes, as can be seen in Figure 6. This immediately establishes the presence of two special subcubes, $S_0 := X_0^C \times Y_0^A \times Z_0^B$ and $S_1 := X_0^B \times Y_0^C \times Z_0^A$, where *all* (χ, χ, χ)-type outcomes must be located. Following the technique established in the seminal work [3] and later further developed in [7], we can write constraints for these cubes, which will be key to proof of nonlocality.

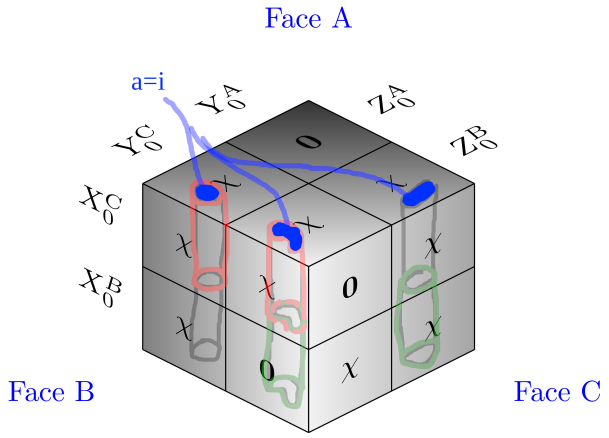


Figure 7: Visual aid for deriving Constraint 2. Areas where $a = i$ are in blue, while the volume giving $p(a = i, b = 0, c = \chi)$ is outlined in green, and $p(a = i, b = \chi, c = 0)$ in red. One can see that by switching from X_0^B to X_0^C for both green columns and vice-versa for only one of the red columns, the differences give the difference $q(i, 0) - q(i, 1)$.

In particular, we now break up the coarse-graining of χ. If a local model exists, then all (χ, χ, χ) outputs must be in $S_0 \cup S_1$, and split between S_0 and S_1. But this must be done in such a way that it is consistent with the other outcomes, i.e. with the $(\chi, 0, \chi)$-type outcomes, and with the marginal probabilities of the χ outcomes. Formally, let us define

$$q(i, j, k, s) := \tag{20}$$
$$p(a = i, b = j, c = k, (\alpha, \beta, \gamma) \in S_s | (\alpha, \beta, \gamma) \in (S_0 \cup S_1)), \tag{21}$$

where the indices i, j, k run over all non-zero indices of the outputs $(i, j, k \in \chi)$, while $s \in \{0, 1\}$.

Constraint 0. (q is a normalized probability vector.)

$$q(i, j, k, s) \geq 0 \quad \forall i, j, k, s,$$
$$\sum_{i,j,k,s} q(i, j, k, s) = 1.$$

Constraint 1. (Marginals over s, i.e., all $(a = \chi, b = \chi, c = \chi)$ outcomes must fit in S_0 and S_1)

$$\sum_s q(i, j, k, s) = 4p(i, j, k) \quad \forall i, j, k,$$

Constraint 2. (Alice is unaware of hidden variable α, so (i, χ, χ) and $(i, 0, \chi)$ are related)

$$q(i, s = 0) - q(i, s = 1) = 4\left(\sum_{k=1}^{M} p(i, 0, k) - \sum_{j=1}^{M} p(i, j, 0)\right),$$
$$q(j, s = 0) - q(j, s = 1) = 4\left(\sum_{i=1}^{M} p(i, j, 0) - \sum_{k=1}^{M} p(0, j, k)\right),$$
$$q(k, s = 0) - q(k, s = 1) = 4\left(\sum_{j=1}^{M} p(0, j, k) - \sum_{i=1}^{M} p(i, 0, k)\right),$$

for all i, j, k.

Constraints 0. follows from the definition of q.

Proof of Constraint 1.: Since each subcube has a side length of $1/2$, see Figure 6, then S_0 and S_1 both have a probability of $1/8$, so together they have a probability of $1/4$. When summing over s, we obtain $\sum_s q(i, j, k, s) = 4p(i, j, k)$ for all i, j, k. □

Proof of Constraint 2.: Constraint 2. is more contrived. To derive it, we will be examining the probability that Alice outputs some non-zero i outcome ($i \in \chi$), and one of the others outputs a 0. This can be related to S_0 and S_1, because they share the same face of Alice for the $a = i$ output, as shown in Figure 7.

$$p(a = i, b = 0, c = \chi) =$$
$$= p(a = i, X_0^B Y_0^C Z_0^B) + p(a = i, X_0^B Y_0^A Z_0^B),$$
$$p(a = i, b = \chi, c = 0) =$$
$$= p(a = i, X_0^C Y_0^C Z_0^B) + p(a = i, X_0^C Y_0^C Z_0^A).$$

Using that Alice's outcome doesn't change if the hidden variable α is changed, and $X_0^B = X_0^C$, one can swap X_0^B and X_0^C. By doing this swap for the second terms in both equations, we arrive at S_0 and S_1, respectively, which by definition give the marginal probabilities of q, namely $q(i, s = 0)$ and $q(i, s = 1)$. Finally, we do the same trick for one of the two of the first terms, such that it now matches the first term in the other equation. In total, we arrive at

$$p(a = i, b = 0, c = \chi) = p(a = i, X_0^C Y_0^C Z_0^B) + q(i, s = 0),$$
$$p(a = i, b = \chi, c = 0) = p(a = i, X_0^C Y_0^C Z_0^B) + q(i, s = 1).$$

Subtracting the two equations gives the first line in Constraint 2. The second two lines follow from the same derivation for the other two parties. □

Noise robustness under single-photon loss

Can the proof technique be used for realistic noise models? Fascinatingly, even without modification, the proof gives interesting results for the single-photon loss case (or in general max. $N - 1$ photons lost per source), if $N \geq 2$. This is because in this model we assume that the probability of the 0 outcome doesn't change.

Let us now consider $N = 2$, i.e. two photons per source. For the noise model, let us consider photon loss occurring between the sources and the parties, which is the dominant source of noise in such an optical experiment.

Mathematically, similarly to previous works [7, 11], we characterize the noise channel in the operator-sum representation with the operators

$$E_0 = |0\rangle\langle 0| + \sqrt{\eta} \sum_{n=1}^{d} |n\rangle\langle n|,$$
$$E_1 = \sqrt{1 - \eta} \sum_{n=1}^{d} |n - 1\rangle\langle n|.$$

Note that the normalization condition, $\sum_i E_i^\dagger E_i = I$, holds. The new POVM elements are

$$M^a_{X,\eta} = \sum_{i,j=1}^{2} E_i^\dagger \times \otimes E_j^\dagger M^a_X E_i \times \otimes E_j,$$

for $X \in \{A, B, C\}$, resulting in the noisy distribution

$$p_\eta(a, b, c) = \mathrm{Tr}(\rho_\alpha \rho_\beta \rho_\gamma M^a_{(A,\eta)} M^b_{(B,\eta)} M^c_{(C,\eta)}).$$

Keep in mind that this is a theoretician-friendly approximation of noise, as one would require $|n-2\rangle\langle n|$ transitions to appear as well with more or less $(1-\eta)^2$ probability (up to normalization). However, when the photon loss rate is small, such that two photon losses are rare and negligible, this model is not far from the truth.

Using this linear program, the non-number-resolving distribution can be shown to be *nonlocal up to* $13\%\pm0.1\%$ *loss*, i.e., we have nonlocality for $\eta \in [0.870, 1]$, when setting the phase to $\phi = \frac{3}{18}\pi + \frac{6}{18}M\pi$ ($M \in \mathbb{Z}$) (exact phase values inferred from numerical results). When working with the photon number-resolving distribution, we get noise tolerance *up to* $18.3\% \pm 0.1\%$ *loss*, for $\phi = \frac{\pi}{2}$, i.e., nonlocality for $\eta \in [0.817, 1]$.

Fascinatingly, the distribution with such a phase allows for proving nonlocality for an even larger range of t values than for the $N = 1$, single-photon source distribution.

Full photon loss model

For the physically most accurate full photon loss model, we characterize the noise channel in the operator-sum representation with the operators

$$\begin{aligned} E_0 &= |0\rangle\langle 0| + \sqrt{\eta}\,|1\rangle\langle 1| + \eta\,|2\rangle\langle 2|\,, \\ E_1 &= \sqrt{1-\eta}\,|0\rangle\langle 1|\,, \\ E_2 &= \sqrt{2\eta(1-\eta)}\,|1\rangle\langle 2|\,, \\ E_3 &= (1-\eta)\,|0\rangle\langle 2|\,, \end{aligned} \tag{22}$$

For such a noise model, the LP doesn't work anymore. However, using the same mentality, one can derive bounds instead of equalities in the LP. Alternatively, one can use the proofs of noise-robustness established in Ref. [11] to prove nonlocality even under the full photon loss model. There is no doubt that some noise robustness can be proven, but work is currently under way to establish exactly how much. The numerical indications of LHV-Net, seen in Fig. 8, indicate that even under the full photon loss model there is significant noise robustness of nonlocality, potentially even in the range of $\approx 40\%-80\%$, which would be well within the range of experimental feasibility.

Generation of states at the source

Typically, one could create an optical state of the form $|20\rangle + |02\rangle$ via a pump laser and an SPDC crystal, which would generate two photons simultaneously, which can be routed to a beam-splitter. If properly set up, then due to the Hong–Ou–Mandel effect, the photons bunch and exit the beam splitter in a superposition of both photons in the left mode and both in the right, effectively generating the desired state. The difficulty of this setup is that most of the time one obtains vacuum in the modes, which means most of the rounds need to be discarded via global post-selection.

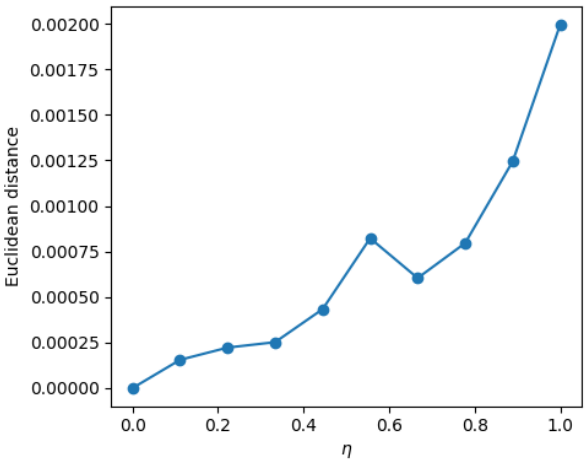


Figure 8: Distance from the local set as gauged by LHV-Net, for the distribution (using $N = 2$ NOON states as sources), for varying levels of noise $(1-\eta)$ according to the noise model in Eq. (22).

To circumvent this problem one could use 2 heralded single photon sources at each source in the triangle. Once two photons are created simultaneously at a source they can be used to generate the $|20\rangle + |02\rangle$ state. Note that naively, this also required global post-selection, which would lead to a loophole. However, for this particular distribution instead of using global post-selection, each of the the sources α, β, γ can sent the heralding information to only the respective 2 parties they are connected with, and the distribution could become a token counting one, and rigidity could still be used for the noise robustness against photon loss. This would lead to a noise-robust genuinely triangle-nonlocal distribution that does not require any global post-processing. We are currently in the process of developing the details of this proposal of sending heralding information in accordance with the causal structure of the triangle.

Magic of quantum hypergraph states

Junjie Chen, Yuxuan Yan, and You Zhou
(Dated: May 19, 2024)

This work is pre-printed at https://doi.org/10.48550/arXiv.2308.01886. The work is accepted as a talk at Quantum Resources 2023.

I. INTRODUCTION

The quantum state beyond stabilizer formalism owns nonstabilizerness called "magic" [1, 2], which enables universal fault-tolerant quantum computing [3] via the magic-state-injection approach [1, 4]. Meanwhile, magic also characterizes quantum complexity beyond entanglement [5]. However, magic is difficult to quantify for large-scale and highly entangled states, because the evaluation cost scales exponentially with the number of qubits [6].

In this work, we systemically and analytically investigate the magic of a class of states with large entanglement—quantum hypergraph states [7, 8], which are generalized from graph states [9, 10]. Quantum hypergraph states play an essential role in quantum advantage protocols [11], measurement-based quantum computing [12, 13] and topological order [14–16]. We relate the magic, measured by Stabilizer Rényi Entropy (SRE)[17], to a family of induced hypergraphs from the original one, according to the indices of all Pauli strings. This pictorial expression enables a series of analytical findings as follows. We first show a general upper bound of magic for any hypergraph state with a bounded average degree, for instance, ones whose hypergraphs are defined on lattices like Union-Jack one [16]. We further develop general theories that transform the statistical properties of magic into a series of counting problems in the binary domain. Our theories lead to the concentration result that the magic of hypergraph states is typically large and very near the maximal value, showing similar behavior to the unphysical Haar random state [17–19]. In addition, we analyze the magic of quantum hypergraph states with permutation symmetry which is detailed in [20]. Based on the symmetry simplification and pictorial derivation, we obtain exact analytical results of the stabilizer Rényi-α entropy ($\mathrm{SR}_\alpha\mathrm{E}$) for different α's, and in particular, find that $\mathrm{SR}_2\mathrm{E}$ and $\mathrm{SR}_{\frac{1}{2}}\mathrm{E}$ can be exponentially different for these states. Our findings and the developed techniques can advance further investigations of multipartite quantum magic with applications from quantum computing to quantum many-body physics, where hypergraph states can serve as an archetypal class of complex states and tractable toy models of other kinds of complex quantum systems.

II. PRELIMINARIES

The definition of quantum hypergraph states [7, 8, 21], a generalization of graph states [22], is given as follows.

Definition 1. *Given a hypergraph $G = (V, E)$ with n vertices, the corresponding quantum hypergraph state of n qubits reads*

$$|G\rangle := U(G)\,|+\rangle^{\otimes n} = \prod_{e\in E} CZ_e\,|+\rangle^{\otimes n}, \tag{1}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, the phase unitary $U(G)$ is completely determined by the hypergraph G, and $CZ_e = \bigotimes_{v_i\in e}\mathbb{I}_i - 2\bigotimes_{v_i\in e}|1\rangle_i\langle 1|$ the generalized Controlled-Z gate acting non-trivially on the support of edge e.

Quantum hypergraph states are generally not traditional stabilizer states since CZ_e are not Clifford gates as $|e| > 2$ [23]. Fortunately, one can still apply the generalized stabilizer formalism as follows.

Definition 2. *For a hypergraph state $|G\rangle$ defined in Eq. (1), it is uniquely determined by the following n independent (generalized) stabilizer generators*

$$S_i = X_i \prod_{e\in E, e\ni v_i} CZ_{e\setminus\{v_i\}}, \quad i \in [n] \tag{2}$$

such that $S_i\,|G\rangle = |G\rangle$.

Magic [1, 2] quantifies the derivation of a quantum state from the stabilizer states [24], which is an essential resource for quantum computing complexity and its fault-tolerant realization [3, 25]. Stabilizer Rényi entropy (SRE) [6, 17] is a recently introduced faithful measure of magic that is related to the probability distribution from the projection onto the Pauli operators. The $\mathrm{SR}_\alpha\mathrm{E}$ of the state $|\Psi\rangle$ is defined as follows.

$$\mathbf{M}_\alpha(|\Psi\rangle) = \frac{1}{1-\alpha}\log\sum_{P\in\mathcal{P}_n}\left(2^{-n}\operatorname{Tr}\{P|\Psi\rangle\langle\Psi|\}^2\right)^\alpha - n, \tag{3}$$

where α and $\mathcal{P}_n$ is the Pauli group $\{\mathbb{I}_i, X_i, Y_i, Z_i\}^{\otimes n}$ ignoring the phase. The offset $-n$ keeps the magic of stabilizer states to be zero. Hereafter all the log functions are base two otherwise specified.

For ease of the following discussion, we define the closely related quantity α-order *Pauli-Liouville(PL) moment* as

$$\mathbf{m}_\alpha(|\Psi\rangle) = 2^{-n}\sum_{P\in\mathcal{P}_n}\left(\operatorname{Tr}\{P|\Psi\rangle\langle\Psi|\}\right)^{2\alpha}, \tag{4}$$

and the corresponding $\mathrm{SR}_\alpha\mathrm{E}$ directly reads $\mathbf{M}_\alpha(|\Psi\rangle) = (1-\alpha)^{-1}\log\mathbf{m}_\alpha(|\Psi\rangle)$.

III. MAGIC OF A HYPERGRAPH STATE

In this section, we show a general formula of the magic for any hypergraph state by relating the PL-moment and, thus, SRE to a family of induced hypergraphs. This pictorial result enables us to find a general upper bound of magic based on the structure of the corresponding hypergraph, which constrains the magic, especially for the hypergraph states on the lattice.

First, let us define a family of induced hypergraphs $G^*_{\vec{x},\vec{z}} = (V, E^*_{\vec{x},\vec{z}})$, which are induced from the original hypergraph G. The vertex set V remains the same, and the updated edge set $E^*_{\vec{x},\vec{z}} = E^{(1)}_{\vec{z}} \cup E^{(2)}_{\vec{x}}$ is determined by two n-bit vectors $\vec{x}$ and $\vec{z}$ shown as follows. Hereafter all the additions are module 2 on the binary domain otherwise specified.

$$E^{(1)}_{\vec{z}} = \{e_1 = \{v_j\} | z_j = 1\}, \quad E^{(2)}_{\vec{x}} = \left\{ e_2 \subseteq V \middle| |e_2| \geq 2, \sum_{e\supset e_2}\prod_{i:v_i\in e\setminus e_2} x_i = 1 \right\}. \tag{5}$$

Here $E^{(1)}_{\vec{z}} \cap E^{(2)}_{\vec{x}} = \emptyset$, and $E^{(1)}_{\vec{z}}$ denotes the 1-edge set, while $E^{(2)}_{\vec{x}}$ is for the set with 2 or more cardinality edges. See Fig. 1 for an illustration of an induced hypergraph. Following the definition in Eq. (1), we denote the phase unitary encoded by this hypergraph $G^*_{\vec{x},\vec{z}}$ as $U(G^*_{\vec{x},\vec{z}})$. Then the general formula of $\mathrm{SR}_\alpha\mathrm{E}$ and its bound can be given as follows.

Theorem 1. *The $SR_\alpha E$ of a hypergraph state $|G\rangle$ shows*

$$\mathbf{M}_\alpha(|G\rangle) = \frac{1+2\alpha}{\alpha-1}n + \frac{1}{1-\alpha}\log\sum_{\vec{x},\vec{z}}\operatorname{Tr}\left\{U(G^*_{\vec{x},\vec{z}})\right\}^{2\alpha}. \tag{6}$$

where $U(G^*_{\vec{x},\vec{z}})$ is the phase unitary determined by the hypergraph $G^*_{\vec{x},\vec{z}}$ defined in Eq. (5).

Theorem 2. *For any n-qubit hypergraph state $|G\rangle$ whose corresponding graph G has average degree $\bar{\Delta}(G)$, its $SR_\alpha E$ with $\alpha \geq 2$ is upper bounded by*

$$\mathbf{M}_\alpha(|G\rangle) \leq \frac{1}{\alpha-1}\left[1 - \log\left(1 + \frac{1}{2^{(2\alpha-1)\bar{\Delta}(G)}}\right)\right]n. \tag{7}$$

IV. MAGIC OF RANDOM HYPERGRAPH STATES

In this section, we study the statistical properties magic of random hypergraph states. Here, we mainly study random c-uniform hypergraphs, which only own c-edge. A random c-uniform hypergraph ensemble can be determined by the probability p whether there is a c-edge or not among all choices of c vertices, denoted as random hypergraph state ensembles $\mathcal{E}^p_c$. The ensembles are defined formally as follows [26].

We first focus on the case $p = 1/2$ and use $\mathcal{E}_c$ to replace $\mathcal{E}^p_c$ for simplicity. Here our main focus is on the average properties of magic, especially the PL-moment, and then we show quite tight lower bounds of the average SRE. The following theorem transforms the average PL-moment into a counting problem of binary strings. We first show some related definitions of the norm and operations of an n-bit string $\vec{t} = \{t^i\}$. The 1-norm $\left\|\vec{t}\right\|_1 = \sum_i t^i$, with the addition modulo 2. The Hadamard or Schur product $\bigodot$ of some bit strings $\vec{t_k}$ is the element-wise product, i.e., $\vec{t'} = \bigodot_k \vec{t_k}$ with $t'^i = \prod_k t^i_k$.

Theorem 3. *For any integer $\alpha \geq 2 \in \mathbb{Z}$, the average α-th PL-moment of n-qubit random hypergraph state ensembles $\mathcal{E}_c$ shows $\langle \mathbf{m}_\alpha \rangle_{\mathcal{E}_c} = \frac{\mathrm{N}(c,\alpha,n)}{2^{2\alpha n}}$ where $\mathrm{N}(c,\alpha,n)$ is the number of 2-tuple $(\mathrm{T}, \vec{x})$, such that the following two constraints are satisfied.*

$$\left\| \vec{t_i} \right\|_1 = 0, \quad \forall i, \tag{8}$$

$$\sum_{q \subset e_c} \left(\prod_{v_i \in q} x_i \left\| \bigodot_{v_k \in e_c \setminus q} \vec{t_k} \right\|_1 \right) = 0, \quad \forall |e_c| = c, \tag{9}$$

where $\mathrm{T} = (\vec{t_1}, \cdots, \vec{t_i}, \cdots, \vec{t_n})$ is a $2\alpha \times n$ binary matrix, $\vec{x}$ is an n-bit vector with elements x_i, e_c labels all possible c-edges, and $q \neq \emptyset$.

Proposition 1. *For any $c \geq 3 \in \mathbb{Z}$ and $\alpha \geq 2 \in \mathbb{Z}$, with the qubit number $n \gg \alpha$ and $n \gg c$, the average PL-moment*

$$\frac{1}{2^n} \leq \langle \mathbf{m}_\alpha \rangle_{\mathcal{E}_c} \leq \frac{2^{(c+2^{2\alpha-1})}}{2^n}. \tag{10}$$

In particular, for $c = 3$ and $\alpha = 2$, more specific calculation shows $\langle \mathbf{m}_2 \rangle_{\mathcal{E}_3} = \frac{7}{2^n} - \frac{14}{4^n} + \frac{8}{8^n}$ and by utilizing Chebyshev's inequality, there is the concentration of measure effect of magic for it.

$$\Pr\{\mathbf{M}_2(|G_{n,3}\rangle) \geq n-3\} \geq 1 - \frac{60}{2^n}. \tag{11}$$

For general p in $\mathcal{E}_c^p$, we only consider $\alpha = 2$ and $c = 3$. Even though it is still hard to derive a closed form of $\langle \mathbf{M}_2 \rangle_{\mathcal{E}_3^p}$ so we numerically calculate it. To be specific, Fig. 2 shows the relation between the expected number of hyperedges $\langle n_e \rangle := p \cdot \binom{n}{3}$ and the qubit-number n, given the average magic $\langle \mathbf{m}_2 \rangle_{\mathcal{E}_3^p} = \gamma n$ for some constant γ. One can see that for a fixed proportion γ of n, $\langle n_e \rangle$ is almost linear to n for different γ's, i.e., $\langle n_e \rangle \sim \mu n$, and thus $p \sim O(n^{-2})$ far less than $1/2$ like before.

For each vertex, the expected number of edges is $\langle n_e \rangle \cdot \frac{\binom{n-1}{2}}{\binom{n}{3}} \sim 3\mu$, and thus the expected average degree $\langle \bar{\Delta}(G) \rangle$ is about a constant. This shows the consistency to Theorem 2, where the magic of a bounded-average-degree hypergraph state is also bounded. For $\gamma = 0.999$, which is very near the maximal 1, the slope $\mu \simeq 3.0$. It means that a very small p can let the average magic become a very large value.

The statistical results here may also suggest a dynamical way to generate maximal magic states efficiently. For each step, one operates a CCZ gate on any three-qubit chosen randomly from a 3-edge, and repeats this process for about $K = O(n)$ times. In particular, the numerical result implies that $K = 3n$ may be enough to let $\mathrm{SR_2E}$ reach $0.999n$. Moreover, if one parallel applies CCZ gates, a constant-depth quantum circuit could be sufficient.

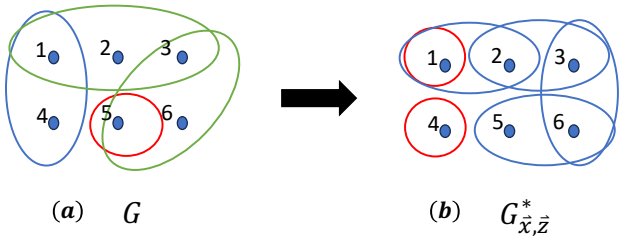


FIG. 1. It shows the induced hypergraph $G^*_{\vec{x},\vec{z}}$ according to Eq. (5). Here two 6-bit strings are chosen as $\vec{x} = \{1,0,1,0,1,0\}$ and $\vec{z} = \{1,0,0,1,0,0\}$. For example, the 2-edge $\{1,2\}$ is induced from the 3-edge $\{1,2,3\}$ of G in (a) with $x_3 = 1$, according to the edge set $E^{(2)}_{\vec{x}}$ in Eq. (5); the 1-edge $\{4\}$ is directly by $z_4 = 1$ according to $E^{(1)}_{\vec{z}}$ in Eq. (5).

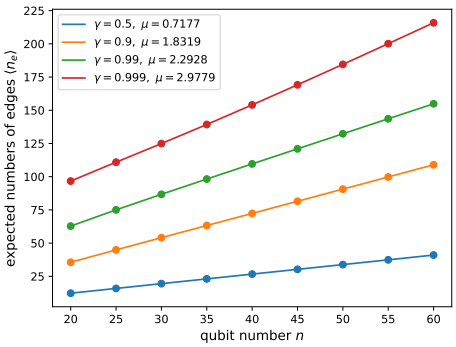


FIG. 2. Relation between qubit number n (x-axis) and expected number of hyperedges $\langle n_e \rangle = p \cdot \binom{n}{3}$ (y-axis), given the (lower bound of) expected $\mathrm{SR_2E}$ $\underline{\langle \mathbf{M}_2 \rangle_{\mathcal{E}_3^p}} = -\log \langle \mathbf{m}_2 \rangle_{\mathcal{E}_3^p} = \gamma \cdot n$ for different γ's. Different colors represent different expected magic with different slopes μ's.

[1] S. Bravyi and A. Kitaev, Universal quantum computation with ideal clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).
[2] V. Veitch, S. H. Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New Journal of Physics **16**, 013009 (2014).
[3] E. T. Campbell, B. M. Terhal, and C. Vuillot, Roads towards fault-tolerant universal quantum computation, Nature **549**, 172 (2017).
[4] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature **402**, 390 (1999).
[5] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[6] S. F. E. Oliviero, L. Leone, A. Hamma, and S. Lloyd, Measuring magic on a quantum processor, npj Quantum Information **8**, 148 (2022).
[7] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, Quantum hypergraph states, New Journal of Physics **15**, 113022 (2013).
[8] R. Qu, J. Wang, Z.-s. Li, and Y.-r. Bao, Encoding hypergraphs into quantum states, Phys. Rev. A **87**, 022311 (2013).
[9] R. Raussendorf and H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. **86**, 5188 (2001).
[10] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states, Phys. Rev. A **68**, 022312 (2003).
[11] 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).
[12] J. Miller and A. Miyake, Hierarchy of universal entanglement in 2d measurement-based quantum computation, npj Quantum Information **2**, 1 (2016).
[13] Y. Takeuchi, T. Morimae, and M. Hayashi, Quantum computational universality of hypergraph states with pauli-x and z basis measurements, Scientific Reports **9**, 13585 (2019).
[14] M. Levin and Z.-C. Gu, Braiding statistics approach to symmetry-protected topological phases, Phys. Rev. B **86**, 115109 (2012).
[15] B. Yoshida, Topological phases with generalized global symmetries, Phys. Rev. B **93**, 155131 (2016).
[16] J. Miller and A. Miyake, Latent computational complexity of symmetry-protected topological order with fractional symmetry, Phys. Rev. Lett. **120**, 170503 (2018).
[17] L. Leone, S. F. E. Oliviero, and A. Hamma, Stabilizer rényi entropy, Phys. Rev. Lett. **128**, 050402 (2022).
[18] Z.-W. Liu and A. Winter, Many-body quantum magic, PRX Quantum **3**, 020333 (2022).
[19] C. D. White and J. H. Wilson, Mana in haar-random states, arXiv preprint arXiv:2011.13937 (2020).
[20] J. Chen, Y. Yan, and Y. Zhou, Magic of quantum hypergraph states (2023), arXiv:2308.01886 [quant-ph].
[21] C. Kruszynska and B. Kraus, Local entanglability and multipartite entanglement, Phys. Rev. A **79**, 052304 (2009).
[22] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, Entanglement in Graph States and its Applications, arXiv e-prints , quant-ph/0602096 (2006), arXiv:quant-ph/0602096 [quant-ph].
[23] D. Gottesman, The heisenberg representation of quantum computers, arXiv preprint quant-ph/9807006 (1998).
[24] D. Gottesman, Stabilizer codes and quantum error correction (1997), arXiv:quant-ph/9705052 [quant-ph].
[25] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, Phys. Rev. A **70**, 052328 (2004).
[26] Y. Zhou and A. Hamma, Entanglement of random hypergraph states, Phys. Rev. A **106**, 012410 (2022).

Source-Replacement Model for Phase-Matching Quantum Key Distribution

Yizhi Huang[1] Zhenyu Du[1] Xiongfeng Ma[1] *

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

Abstract. Quantum key distribution has emerged as a promising solution for constructing secure communication networks, with its information-theoretic security rooted in quantum mechanics. One of the recent quantum key distribution protocols, the phase-matching protocol, can have a quadratic key-rate improvement. Its security was initially established using an abstract method known as symmetry-protected privacy. In this study, we reevaluate this security under the more intuitive source-replacement model, arriving at the same conclusions as the original proof. This model provides a fresh perspective on the protocol's security. As an application of this approach, we introduce a beam-splitting attack. Leveraging the source-replacement model, we derive a lower bound on the phase error rate under this attack, further underscoring the robustness of our security analysis method.

Quantum key distribution (QKD) [1, 2] is currently one of the most successful applications in quantum information science. It allows two remote communication parties, Alice and Bob, to establish a secure key by leveraging the principles of quantum mechanics. Among the various QKD protocols developed, the phase-matching scheme [3] stands out for its robustness and efficiency. The security of the phase-matching scheme was originally established using a method known as symmetry-protected privacy [4, 5]. Unlike conventional complementary-based security proofs, this method utilizes the symmetry of encoding to establish security, leveraging the parity properties of the corresponding state space to derive the phase error rate. The advantage of this method is its independence from the specifics of the source and measurements, focusing solely on encoding operations. This provides a straightforward framework for analyzing the security of QKD protocols, especially MDI QKD. However, its abstract nature limits specific security insights for varied protocols and confines analysis to encoding, hindering comprehensive assessments against potential eavesdropping attacks.

In this work, we reexamine the security of the phase-matching scheme via the source-replacement approach, which is easier to comprehend. This approach was initially introduced in [6], and its name comes from [7]. We introduce a virtual entanglement-based protocol where the users employ CNOT gates, quantum Fourier transforms, and photon number measurements to construct a pseudo-Fock state. This allows simultaneous determination of total photon number and random phase difference. Finally, we establish a correlation between photon numbers and phase errors based on the original definitions. Our alternative perspective leads to a conclusion consistent with the symmetry-protected privacy method: quantum states with odd total photon numbers yield phase errors, whereas those with even numbers do not.

Firstly, we introduce the phase-matching QKD scheme. The core idea of this scheme is that Alice and Bob encode their respective key information into the phase of individual optical pulses, with key bits 0 and 1 corresponding to phase values of 0 and π, for instance. Subsequently, they send their pulses to Charlie for single-photon interference. By analyzing the interference outcomes, they can ascertain the degree of phase matching between their encoded phases. This process, conducted through a single optical mode, establishes the connection between the key information of both parties. The central insight of the phase-matching scheme lies in the utilization of single-photon interference, allowing Alice and Bob to extract key bits from single detection.

We draw the encoding process using quantum circuit notation and attempt to transform the circuit into an entanglement-based protocol circuit by using the source-replacement approach. The corresponding quantum circuit diagram for the protocol is depicted as Figure 1. Note that the CNOT operation between systems A_0 and B_0, the quantum Fourier transformation, the photon number measurement, and the X-basis measurements on systems A_1 and B_1 are operations introduced to obtain the quantum phase error rate. These operations were not part of the original protocol and are called virtual operations. In the following sections, we will demonstrate that through these virtual operations, Alice and Bob can obtain the photon number distribution of the pulses they send and establish a connection between this distribution and the quantum phase error rates. Here, we introduce three random numbers on each side for classical control of optical encoding. The random numbers μ_a^i, μ_b^i are used to encode different intensities for decoy-state estimation [8–10]. The random bits $\kappa_a^i, \kappa_b^i \in \{0, 1\}$ are the raw key bits, and the random numbers ϕ_a^i, ϕ_b^i are used for phase randomization.

With this entanglement-based picture, we have the following observations.

Observation 1 *The number of photons emitted in the optical mode $A(B)$ can be acquired by doing a high-dimensional Z-basis measurement after the inverse quantum Fourier transformation on ancillary qudit $A_0(B_0)$, which is used to do the discrete phase randomization.*

Furthermore, in the entanglement-based picture, the users can simultaneously obtain the total photon number and the random phase difference by introducing a high-dimensional CNOT operation between systems A_0 and B_0, as shown in Figure 1, along with appropriate measurements.

*xma@tsinghua.edu.cn

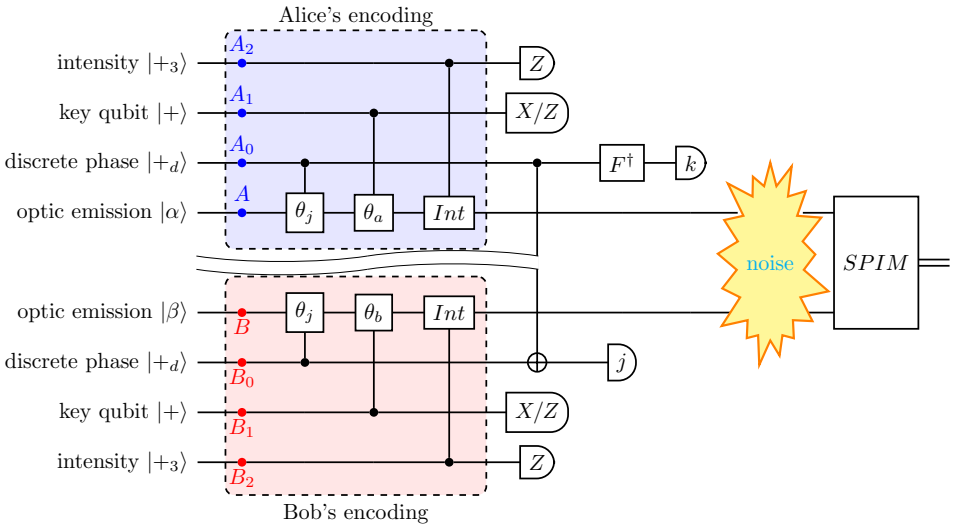


Figure 1: Encoding circuit of source-replaced PM scheme. The ancillary systems $A_0, A_1, A_2, B_0, B_1, B_2$ encode the random phases, key bits, and intensities. In this picture, the ancillary systems are measured after the encoding operations, allowing Alice and Bob to employ additional operations beyond simple Z-basis measurements to estimate parameters like photon number and phase differences. The quantum inverse Fourier transform $F^\dagger$, high-dimensional CNOT operations, and X-basis measurements depicted in the figure are virtual operations not part of the original protocol. Here, SPIM is the abbreviation for single-photon interference measurement

Observation 2 *The total number of photons emitted in two optical modes A and B and the random phase difference can be acquired simultaneously by doing a high-dimensional CNOT operation between systems A_0 and B_0 followed by an inverse quantum Fourier transformation on ancillary qudit A_0 and Z-basis measurements on A_0 and B_0.*

We now include the key-bit encoding in the scheme. As shown in Fig. 1, Alice applies another qubit ancillary system A_1. She prepares $|+\rangle$ on A_1 and employs a controlled-phase gate between A_1 and A to encode the key information. Bob applies similar operations as well. The phase error is obtained by $X \otimes X$ measurement on the key qubits A_1, B_1. Then, we can determine whether a phase error exists by the total photon number N. By calculating the post-select quantum state, we have the following results:

1. N is odd, the X-basis measurement results on qubits A_1 and B_1 are different, $|-+\rangle_{A_1B_1}$ or $|+-\rangle_{A_1B_1}$;
2. N is even, the X-basis measurement results on qubits A_1 and B_1 are the same $|++\rangle_{A_1B_1}$ or $|--\rangle_{A_1B_1}$.

In conclusion, the phase error rate is 1 if the total photon number in A and B is odd, and it is 0 if the total photon number is even. Then, the upper bound of the phase error rate is

$$\begin{aligned} e_p &\leq 1 \cdot q_{\text{even}} + 0 \cdot q_{\text{odd}} \\ &= q_{\text{even}} \\ &= 1 - \sum_k q_{2k+1}, \end{aligned} \tag{1}$$

where q_k is the detection fraction when Alice and Bob send out k-photon signals. This is consistent with the conclusion obtained by the symmetry-protected method [5]. Thus, by analyzing the fraction of odd and even states via decoy state method[11], the upper bound of phase error can be derived. Utilizing the entanglement-based source-replacement picture, we establish the relationship between the total photon number and the phase error rate in the phase-matching scheme. This provides a more concrete and physically intuitive explanation for the conclusions drawn in the symmetry-protected privacy method.

We also introduce a beam-splitting attack with unambiguous state discrimination and analyze the key rate of the phase-matching scheme under this attack. Here, we employ the source-replacement security analysis framework to analyze the attack, enabling a straightforward lower bound of the phase error rate. This underscores the efficacy of the source-replacement approach in analyzing attacks. We illustrate this attack in Figure 2, and a detailed description can be found in [12]. Here, we suppose the channel transmittance from Alice and Bob to the measurement site are both η, and the intensities of pulses are the same, $\mu_a = \mu_b = \mu$. We only consider the case of pure states for simplicity.

The core idea of this beam-splitting attack lies in that the state $|\varphi\rangle$ obtained by Eve through beam splitting is very close to the states emitted by Alice and Bob. Moreover, as the channel transmission rate decreases, these two states become even closer. With the help of quantum memory, Eve can utilize the stored states to attempt to obtain the key bits chosen by Alice and Bob, given that she knows the random phases they selected. In this scenario, Eve can maximize the utilization of all the information she can obtain without interfering with the protocol execution, thus maximizing her ability to steal the key. Whether Eve can obtain the key information depends on her ability to distinguish whether the state she holds is $|\varphi^0\rangle$ or $|\varphi^1\rangle$ through unambiguous state discrimination measurements. If she successfully distinguishes these two states, Eve will perfectly learn the key bit value. The fi-

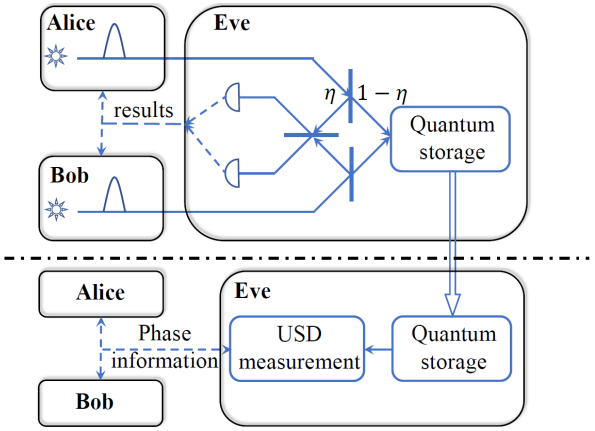


Figure 2: Illustration of beam-splitting attack. Solid arrows represent the transmission of quantum states, while dashed arrows represent the exchange of classical information. Eve splits the light pulse emitted by Alice and Bob into two parts with a ratio of $1-\eta:\eta$. The former part is stored in a quantum memory, while the latter part undergoes interference measurement, and the measurement result is publicly announced. After the measurement is completed and Alice and Bob announce the phase information ϕ_a^i and ϕ_b^i, Eve retrieves the two corresponding states from the quantum memory, performs unambiguous state discrimination measurement based on the phase information, and applies post-processing to the results.

delity between these two states gives the optimal success probability for her to distinguish these two states [13],

$$p_{usd} = 1 - |\langle\phi_0|\phi_1\rangle| = 1 - e^{-4(1-\eta)\mu}. \tag{2}$$

Given the probability for Eve to learn the key bit value perfectly, we can further estimate a lower bound on the phase error rate that Alice and Bob will encounter in the protocol. We still use the source-replacement entanglement-based picture in Figure 1, in which the states of systems A_1 and B_1 are the key states held by Alice and Bob, respectively. They will perform Z-basis measurements on their own states to obtain their raw keys. According to the definition of the phase error rate [14], if they perform X-basis measurements on these states, they will obtain the phase error rate.

When Eve successfully obtains Alice and Bob's encoded keys through unambiguous state discrimination measurements, in the entanglement-based scenario, we can consider that Eve deterministically acquired knowledge of the results of the Z-basis measurements performed on systems A_1 and B_1. In this sense, the states on these two systems have already collapsed to either $|00\rangle$ or $|11\rangle$ from Eve's point of view.

Then Alice and Bob do subsequent operations to get the raw key bits or the phase error rate. If Alice and Bob perform Z-basis measurements, the raw key bits they get will be the same as what Eve obtained. If Alice and Bob perform X-basis measurements to estimate the phase error rate, since systems A_1 and B_1 have already collapsed to either $|00\rangle$ or $|11\rangle$, the results of the X-basis measurements will be completely random, resulting in a phase error rate of $\frac{1}{2}$. This scenario here is similar to the intercept-resend attack on the BB84 protocol. Therefore, the contribution of the case where Eve successfully distinguishes the encoded states to the phase error rate is $\frac{1}{2}p_{usd}$. As for the case where Eve fails to distinguish the states, the phase error rate is lower bounded by 0 since any additional operation will only increase the phase error rate. Hence, we can conclude that the final phase error rate satisfies

$$e_p \geq \frac{1}{2}p_{usd} = \frac{1}{2} - \frac{1}{2}e^{-4(1-\eta)\mu} \equiv e_p^L. \tag{3}$$

The simulation results show that the upper bound from symmetry-protected security proof and lower bounds of the phase error rate given by the beam-splitting attack are very close, illustrated in Fig. 3. The difference becomes smaller as the intensity increases and the channel transmission decreases. Intuitively, as the intensity increases or the channel transmission rate decreases, Eve can obtain quantum states with higher intensities through beam splitting, which makes the states Eve holds closer to the ones sent by Alice and Bob. And it will finally lead to a higher success probability of unambiguous state discrimination. If the communication distance between Alice and Bob is zero, Eve cannot obtain any quantum states through beam splitting. The results imply that the attack and analysis method we proposed provides a good lower bound under the beam-splitting attack and that the entanglement-based security analysis approach can provide straightforward conclusions with simplicity when analyzing such attacks. This highlights the advantages of the entanglement-based security analysis method when dealing with these attacks.

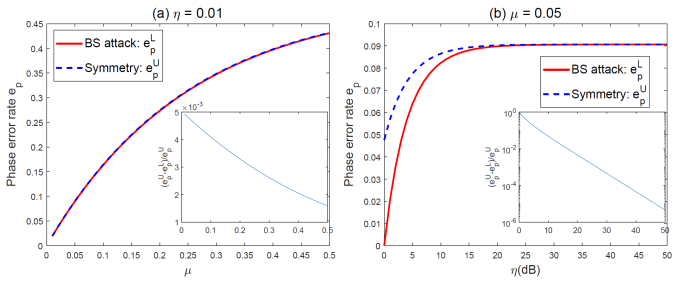


Figure 3: The difference between the phase error rate upper bounded by the symmetry-protected security proof and the beam-splitting attack under different intensities and channel transmittance.

In conclusion, the source-replacement analysis offers a fresh perspective that enriches the original security proof of the phase-matching scheme. This analysis reaffirms the protocol's security and provides valuable insights into its underlying mechanisms. In addition, we introduce a beam-splitting attack that poses a potential threat to the phase-matching scheme. We derive a lower bound for the phase error rate within the source-replacement framework. The simulation results show that the phase error rate provided by the security proof is very close to the one introduced by the beam-splitting attack. This finding indicates that the upper bound on the phase error rate and, hence, the lower bound on the key rate provided by our security analysis is already tight, leaving little room for further improvement. This analysis establishes a direct connection between the attack and the quantum phase error rate, enhancing our understanding of the security of the phase-matching scheme.

The related work is published in [12].

References

[1] 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.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991), URL http://link.aps.org/doi/10.1103/PhysRevLett.67.661.

[3] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018), URL https://link.aps.org/doi/10.1103/PhysRevX.8.031043.

[4] J. Lin and N. Lütkenhaus, Phys. Rev. A **98**, 042332 (2018), URL https://link.aps.org/doi/10.1103/PhysRevA.98.042332.

[5] P. Zeng, W. Wu, and X. Ma, Phys. Rev. Applied **13**, 064013 (2020), URL https://link.aps.org/doi/10.1103/PhysRevApplied.13.064013.

[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.441.

[7] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012), URL https://link.aps.org/doi/10.1103/PhysRevA.85.052310.

[8] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003), URL https://link.aps.org/doi/10.1103/PhysRevLett.91.057901.

[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005), URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

[10] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005), URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230503.

[11] 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.

[12] Y. Huang, Z. Du, and X. Ma, Advanced Quantum Technologies **7**, 2300275 (2024).

[13] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995), ISSN 0375-9601, URL https://www.sciencedirect.com/science/article/pii/037596019400919G.

[14] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999), URL http://science.sciencemag.org/content/283/5410/2050.

[15] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, et al., Nat. Photonics **14**, 422 (2020), ISSN 1749-4893, URL https://doi.org/10.1038/s41566-020-0599-8.

Developing and evaluating a quantum annealing simulator using QuTiP

Akimasa Saito[1] * Masashi Imai[1] †

[1] *Hirosaki University, Graduate School of Science and Technology*

Abstract. In today's research about developing quantum computers, a real machine is often used for evaluating the control circuit. However, since it involves a cost of experimentation and limits scalability for evaluation, a simulating environment for quantum processors from the control circuit perspective would be beneficial. We develop a simulating environment for the theoretical quantum annealing process by using QuTiP which is a Python library for analyzing quantum dynamics, as a first step in developing a simulator for the quantum annealing processor. Furthermore, we evaluate the scalability of this simulator and its usability by evaluating the results of quantum annealing for some NP-hard problems.

Keywords: quantum annealing, quantum simulation, QuTiP, LHZ

1 Introduction

Quantum annealing is a quantum metaheuristic that exploits the properties of quantum mechanics to solve combinatorial optimization problems and is related to quantum adiabatic computation[1]. A combinatorial optimization problem is the act of trying to find out the combination of variables that optimizes an index from among many options, and many socially important combinatorial optimization problems can be formulated as the problem of finding the ground state of the Ising model Hamiltonian. Quantum annealing machine is used to quickly find the ground state of the Ising model's Hamiltonian.

The Ising model's Hamiltonian is described by following equation.

$$H_{Ising} = -\sum_{i<j} J_{ij}\sigma_i^z\sigma_j^z - \sum_{i=1}^{N} h_i\sigma_i^z \tag{1}$$

where σ can express ± 1 and is called spin variable. N is number of spins and usually is big number. J_{ij} is interaction and h_i is external field. The goal of quantum annealing is to find the combination of spins that minimizes the energy H_{Ising} given by these coefficients.

In adiabatic quantum annealing, the system is adiabatically transitioned from a trivial initial state to a ground state of H_{Ising}. A transverse field is used to construct the trivial initial state. The following Hamiltonian formulates this condition.

$$H(t) = A(t)H_{Ising} - B(t)\sum_{i=1}^{N}\sigma_i^x \tag{2}$$

Here $A = 1$ and $B = 0$ in the initial state, and finally $A = 0$ and $B = 1$. In other words, quantum fluctuations are introduced into the quantum system in the initial state, and each spin variable will be superposed. Then, as the quantum fluctuations are reduced and at the same time the interaction and external fields are strengthened, the ground state of the Hamiltonian of the Ising model is finally reached.

*h23ms409@hirosaki-u.ac.jp

†miyabi@hirosaki-u.ac.jp

Although the Hamiltonian H_{Ising} has a long-range interaction between each spin variable, the quantum annealing machines available from D-Wave do not implement the long-range interaction directly. These machines implement it indirectly through chimera graphs [2][3]. This configuration results in an overhead in the number of qubits and also tends to introduce errors due to imperfect realization of the embedding in the real device.

The Lechner-Hauke-Zoller(LHZ) scheme has been proposed to solve the problem based on this long-range interaction[4]. In the LHZ model, the product $\sigma_i^z\sigma_j^z$ of the spin variables appearing in the above equation is replaced by a newly introduced single spin variable $\tilde{\sigma}_i^z$. This configuration requires $N_p = N_l(N_l-1)/2$ physical qubits and $N_c = N_p - N_l + 1$ constraint terms to construct the equivalent Ising model Hamiltonian formulated by N_l logical qubits. The Hamiltonian of the LHZ model is realized by a local field terms for the physical spin variables and a constraining four-body interaction terms, so there is no need to implement long-range interactions as in the Ising model. The Hamiltonian of the LHZ model is formulated as follows.

$$H_{LHZ} = -\sum_{k=1}^{N_p} J_k\tilde{\sigma}_k^z - \sum_{l=1}^{N_c} C_l\tilde{\sigma}_{l,1}^z\tilde{\sigma}_{l,2}^z\tilde{\sigma}_{l,3}^z\tilde{\sigma}_{l,4}^z \tag{3}$$

where C_l is the coupling coefficient related in the four-body interaction.

Our research group has been working on implementing a quantum annealing machine based on the LHZ model. However, at present, an actual quantum annealing machine is being utilized to evaluate the usability of its control circuit. Therefore, it would be beneficial to create a simulating environment to design and evaluate the control system.

We develop a simulator for the theoretical quantum annealing process by using QuTiP which is a Python library for analyzing quantum dynamics, as a first step in developing the simulating environment, and we evaluate the usability of the simulator. Section 2 explains the algorithm of the simulator and section 3 describes benchmarks which are used for evaluation of the simulator. Section 4 provides the results of the benchmarks and section 5 provides a discussion of the results. Finally

section 6 provides overall conclusion.

2 Quantum annealing simulator

We develop a simulator using QuTiP[5], which is a open source library for Python to analyze quantum dynamics. We can simulate quantum system by using QuTiP easily. In particular, since the reliability of the simulator is important in developing a simulator for quantum annealing, we simulate the behavior by analyzing the Schrödinger equation in adiabatic quantum computing using the "sesolve" function in QuTiP. The time dependence of the Hamiltonian evaluated in this simulator is defined as follows.

$$H(t) = (t/\tau)H_{problem} - (1 - t/\tau)\sum_{i=1}^{N}\sigma_i^x \qquad (4)$$

where τ is a finite quantum annealing time. By inserting H_{Ising} or H_{LHZ} into $H_{problem}$, we simulate the adiabatic quantum computing for each Hamiltonian. In the initial state, the quantum state is $|+ + ...+\rangle$ which is the ground state for the transverse field term.

Algorithm 1 is the adiabatic quantum computing algorithm using QuTiP for the Ising Hamiltonian.

The ground state $|\psi_0\rangle$ corresponding to the optimal solution of the combinatorial optimization problem for the constructed Ising Hamiltonian $H0$ is pre-analyzed using "groundstate" in QuTiP. The probability of success of quantum annealing can be determined by calculating the expected value of the operator $|\psi_0\rangle\langle\psi_0|$ in the final state.

3 Evaluation methods

Since this simulator directly analyzes the Schrödinger equation, the main focus is on evaluation with a small number of qubits. The following benchmarks are used.

- Vertex cover problem

  To verify that we can correctly solve the combinatorial optimization problem, we take the vertex cover problem for the small-scale graph shown in Figure 1(a). The vertex cover problem has already been formulated as an Ising model Hamiltonian [6]. The usability of this algorithm is evaluated by its ability to solve this problem.

- Traveling salesman problem

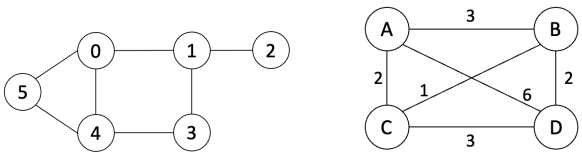
  To evaluate a relatively large Hamiltonian, we consider solving a traveling salesman problem. Here we use 16 qubits to set up a Hamiltonian based on the 4-point problem shown in Figure 1(b).

- Random spin glass

  To evaluate the scalability of the simulator, we evaluate the quantum annealing time required to obtain the optimal solution at each qubit number. Search for the ground state of the Hamiltonian, randomly set in the range [-1,1] for the local field and interaction coefficients, and [0,1] for the coupling coefficients.

Algorithm 1 Simulate quantum annealing for Ising Hamiltonian

Input: N, J, h, τ
Output: Final state
Initialisation :
$sz[i] \leftarrow$ the Pauli-z operator for i-th qubit
$sx[i] \leftarrow$ the Pauli-x operator for i-th qubit
$|\psi_{initial}\rangle \leftarrow |+ + ...+\rangle$
$H0 \leftarrow 0$ // the Ising Hamiltonian
$H1 \leftarrow 0$ // the Hamiltonian for the transverse fields
for $i = 0$ to $N - 2$ **do**
  for $j = i + 1$ to $N - 1$ **do**
    $H0 \leftarrow H0 + -J[(i, j)] * sz[i] * sz[j]$
  end for
end for
for $i = 0$ to $N - 1$ **do**
  $H0 \leftarrow H0 + -h[i] * sz[i]$
end for
for $i = 0$ to $N - 1$ **do**
  $H1 \leftarrow H1 + -sx[i]$
end for
$|\psi_0\rangle \leftarrow$ groundstate($H0$)
Evolve the system in time :
$H(t) \leftarrow (t/\tau)H0 + (1 - t/\tau)H1$
Generate *tlist* in steps of τ in the range [0, τ].
$|\psi_{final}\rangle \leftarrow$ sesolve(H,$|\psi_{initial}\rangle$,*tlist*)
Post-processing :
$prob \leftarrow |\langle\psi_{final}|\psi_0\rangle|^2$
print *prob*
return $|\psi_{final}\rangle$



(a) vertex cover problem **(b)** traveling salesman problem

Figure 1: The NP-hard graph problem

4 Evaluation results

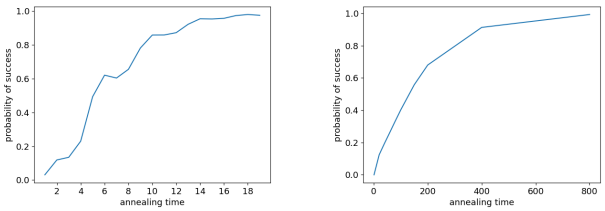
We use following environment for the evaluation.

- Apple Mac Studio
- CPU : Apple M1 Ultra
- Memory : 128GB

PyQUBO[7] is used to construct the Ising model Hamiltonian related to the NP-hard problems. The availability of this simulator is evaluated by constructing an Ising model Hamiltonian with it and simulating quantum annealing.

Vertex cover problem This problem has two optimal solutions (0,1,4) or (1,4,5). These are related to quantum states $|110010\rangle$,$|010011\rangle$.

Figure 2(a) shows how the probability of observing the above state vector changes when quantum annealing is



(a) vertex cover problem **(b)** traveling salesman problem

Figure 2: The result of the quantum annealing for graph problems

simulated for this Hamiltonian while increasing the quantum annealing time τ. The probability of obtaining the optimal solution increases with the length of τ. This confirms that quantum annealing can be simulated correctly.

Traveling salesman problem We confirmed that $|0001010000101000\rangle$,$|1000001001000001\rangle$ are ground states for the Hamiltonian related to the traveling salesman problem. Figure 2(b) shows how the probability of observing the above ground states changes when quantum annealing is simulated for this Hamiltonian while increasing the quantum annealing time τ. Although the required quantum annealing time is longer than that of the vertex cover problem, it confirms that this simulator can also solve the ground states for the relatively large Hamiltonian. The path corresponding to this ground state is shown in Figure 3.

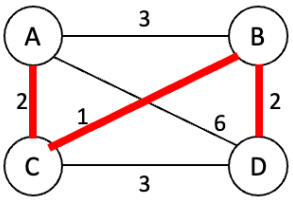


Figure 3: The optimal solution for the traveling salesman problem

Random spin glass In our evaluation environment, the analysis of the optimal solution using "groundstate" function in QuTiP is applicable up to 15 qubits. Therefore, the relationship between the number of qubits and the quantum annealing time is evaluated for a range of up to 15 qubits for the Ising model Hamiltonian and 6 logical qubits for the LHZ model Hamiltonian. Figure 4 shows the average quantum annealing time required for the probability of success to exceed 0.9 for each qubit number.

5 Discussion

In the evaluation of random spin glass, there are a few cases where the quantum annealing time requirement is extremely long. According to the adiabatic theorem, if the energy gap between the ground state and the first excited state of a system's Hamiltonian is small, it takes

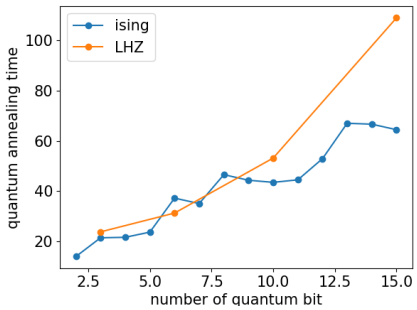


Figure 4: Average quantum annealing time required for the probability of success for each qubit number

a long time to find the optimal solution[8]. Therefore, this result can be attributed to the extremely small energy gap in the random Hamiltonian. In order to consider the relationship between quantum annealing times, these data are not used in the calculation of the average quantum annealing time required. Therefore, the results shown in Figure 4 can be used as an indicator of the amount of quantum annealing time that would be required for a typical problem.

6 Conclusion

We have applied small-scale NP-hard problems to this simulator and confirmed that for each problem, the state vector corresponding to the optimal solution appears as the end state. We have also confirmed the relationship between the number of qubits and the quantum annealing time required to obtain the optimal solution. The results will be useful for developing the simulating environment. In this study, we have simulated small-scale quantum annealing based on the analysis of the Schrödinger equation, but the number of qubits that can be handled needs to be increased for the construction of larger circuits. Therefore, more efficient algorithms such as Simulated Annealing(SA) and Simulated Quantum Annealing(SQA) need to be considered.

Our research group is developing a quantum annealing machine for the LHZ model using superconducting quantum circuits [9] and using microwaves to control the qubits. Therefore, we will build a simulating environment that considers microwave information as input/output signals.

Acknowledgements

This paper is based on results obtained from a project, JPNP16007, subsidized by the New Energy and Industrial Technology Development Organization (NEDO).

References

[1] T.Kadowaki and H.Nishimori Quantum annealing in the transverse Ising model *Physical Review E 58*, pages 5355, 1998.

[2] Choi, Vicky. Minor-embedding in adiabatic quantum computation: I. The parameter setting problem *Quantum Information Processing 7*, pages 193–209, 2008.

[3] Choi, Vicky. Minor-embedding in adiabatic quantum computation: II. Minor-universal graph design *Quantum Information Processing 10.3*, pages 343–353, 2011.

[4] Lechner, Wolfgang, Philipp Hauke, and Peter Zoller. A quantum annealing architecture with all-to-all connectivity from local interactions *Science advances 1.9*, pages e1500838, 2015.

[5] Johansson, J. Robert, Paul D. Nation, and Franco Nori. QuTiP: An open-source Python framework for the dynamics of open quantum systems *Computer Physics Communications 183.8*, pages 1760–1772, 2012.

[6] Zaman, Mashiyat, Kotaro Tanahashi, and Shu Tanaka. PyQUBO: Python Library for Mapping Combinatorial Optimization Problems to QUBO Form *IEEE Transactions on Computers 71.4*, pages 838-850, 2021.

[7] Lucas, Andrew. Ising formulations of many NP problems *Frontiers in physics 2*, pages 74887, 2014.

[8] David J. Griffiths and Darrell F. Schroeter *Introduction To Quantum Mechanics Third edition.* Cambridge University Press, 2018

[9] Yamaji, Tomohiro, Masayuki Shirane, and Tsuyoshi Yamamoto. Development of Quantum Annealer Using Josephson Parametric Oscillators. *IEICE Transactions on Electronics 105.6*, pages 283–289, 2022.

Second Law of Entanglement Manipulation with a Battery

Ray Ganardi[1 2 *] Tulja Varun Kondra[3] Nelly H.Y. Ng[2] Alexander Streltsov [4 1]

[1] *Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland*

[2] *School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore, 637371*

[3] *Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany*

[4] *Institute of Fundamental Technological Research, Polish Academy of Sciences, Pawińskiego 5B, 02-106 Warsaw, Poland*

Abstract. A central question since the beginning of quantum information science is how two distant parties can convert one entangled state into another. Answers to these questions enable us to optimize the performance of tasks such as quantum key distribution and quantum teleportation, since certain entangled states are more useful than others for these applications. It has been conjectured that entangled state transformations could be executed reversibly in an asymptotic regime, mirroring the reversible nature of Carnot cycles in classical thermodynamics. While a conclusive proof of this conjecture has been missing so far, earlier studies excluded reversible entanglement manipulation in various settings. In this work, we investigate the concept of an entanglement battery, an auxiliary quantum system that facilitates quantum state transformations without a net loss of entanglement. We establish that reversible manipulation of entangled states is achievable through local operations when augmented with an entanglement battery. In this setting, two distant parties can convert any entangled state into another of equivalent entanglement. The rate of asymptotic transformation is quantitatively expressed as a ratio of the entanglement present within the quantum states involved. Different entanglement quantifiers give rise to unique principles governing state transformations, effectively constituting diverse manifestations of a "second law" of entanglement manipulation. Our methods provide a solution to the long-standing open question regarding the reversible manipulation of entangled states and are also applicable to entangled systems involving more than two parties, and to other quantum resource theories, including quantum thermodynamics.

Keywords: entanglement, reversibility, thermodynamics, resource theory, battery

This submission is based on arXiv:2405.10599

1 Introduction

Over the past decades, striking parallels between the principles governing manipulation of entangled systems and the laws of thermodynamics [1, 2, 3, 4, 5] have been revealed. A prime illustration of this similarity is often cast with the narrative of two agents, Alice and Bob, sharing n copies of an entangled state $|\psi\rangle$ that they can also manipulate. It is known that under certain conditions, by utilizing simple operations such as local operations and classical communication [6], Alice and Bob can transform their initially shared state into n copies of another state $|\phi\rangle$. In the regime of large n, this transformation is contingent upon an important condition: a reduction in entanglement entropy [6]. This rule mirrors a fundamental concept in classical thermodynamics, where the entropy of a system uniquely determines its potential for interconversion through adiabatic processes [7]. This resemblance highlights the universality of entropy as a key concept in both domains, for understanding and describing state transformations.

The striking similarity between entanglement theory and thermodynamics naturally leads to an intriguing inquiry: Does there exist a "second law of entanglement manipulation" [1], akin to its thermodynamic counterpart, that governs all state transformations of entangled systems? This question is linked to the question of reversibility, in particular when it comes to manipulating entangled states in an asympttic setting. This enables a theoretically lossless conversion between any two entangled states in the asymptotic limit. Furthermore, this mirrors classical thermodynamics, where Carnot's theorem connects the reversibility of a heat engine cycle and its efficiency.

Despite numerous dedicated efforts [1, 2, 3, 4, 5, 8, 9], the quest for a second law of entanglement manipulation is still ongoing. Ref. [5] establishes that there is no second law of entanglement manipulation through a certain class of deterministic protocols. However, this no-go statement can still be bypassed via relaxations such as probabilistic protocols [9]. One of the main challenges in this endeavor is the existence of bound entanglement [10]. Bound entangled quantum states require entanglement for their formation, yet we cannot extract any singlets from them [10]. This paradoxical feature of entanglement poses significant theoretical and practical challenges, complicating the path towards a fully reversible framework of entangled state manipulations.

We resolve this conundrum by focusing on state transformations instead of protocols. Our framework relies on the concept of entanglement batteries [11]. An entanglement battery is an additional entangled quantum system shared between Alice and Bob. In order to prevent the embezzling of resources [12], the battery must be returned at the end of the procedure with at least

*ray.ganardi@ntu.edu.sg

the same amount of entanglement. This idea can be viewed as a generalization of catalytic state transformations [13], a topic that has garnered significant interest recently [14, 15]. An entangled catalyst, in this context, is an ancillary quantum system in an entangled state provided to Alice and Bob. They are allowed to employ this catalyst in their transformation process, with the requirement that it must be returned in its original state. Our approach extends this setup by allowing changes in the state of the ancillary system, provided that there is no reduction in its entanglement.

2 Results

We demonstrate that considering transformations aided with a battery leads to a second law of entangled state manipulation. This law asserts that Alice and Bob can transform a state ρ into another σ if and only if $E(\rho) \geq E(\sigma)$, where E represents an entanglement quantifier with certain natural properties. In the asymptotic limit, the conversion rates in this setting are characterized by the ratio $E(\rho)/E(\sigma)$, leading to the implication that asymptotic state manipulations can be executed in a reversible manner. Our results lead to a family of second laws of entanglement manipulation, contingent on the method of entanglement quantification in both the system and the battery. Moreover, we recover a variant of the second law previously conjectured in [2], achieved without resorting to the generalized quantum Stein's lemma, for which a comprehensive proof is still missing [8].

We first provide a characterization of single-copy LOCC transformations when aided with an entanglement battery.

Theorem 1 *A state ρ can be converted into another state σ via LOCC with an entanglement battery if and only if*

$$E(\rho) \geq E(\sigma). \tag{1}$$

Here, E is an additive and finite entanglement measure.

Next, we move to characterize the asymptotic rate of many-copy transformations.

Theorem 2 *The maximal conversion rate for converting ρ into σ via LOCC with an entanglement battery is given by*

$$R(\rho \to \sigma) = \frac{E(\rho)}{E(\sigma)}. \tag{2}$$

Here, E is an entanglement measure which is finite, additive and asymptotically continuous.

An immediate consequence of our work is the construction of a framework of reversible entanglement manipulation. More specifically, we establish that $R(\rho \to \sigma) \times R(\sigma \to \rho) = 1$ for any ρ and σ, implying that in the asymptotic limit, any two entangled states ρ and σ can be interconverted reversibly. Furthermore, when the ratio $E(\rho)/E(\sigma)$ is rational, reversible interconversion is feasible even with a finite number of copies. This means there exist integers m and n such that $m/n = E(\rho)/E(\sigma)$, allowing for bidirectional conversion $\rho^{\otimes n} \to \sigma^{\otimes m}$ and $\sigma^{\otimes m} \to \rho^{\otimes n}$. We further notice that the optimal conversion rate can be achieved through a protocol involving local operations alone, which interestingly obviates the need for classical communication in this task. We suspect that this arises from allowing the battery to contain any finite amount of entanglement. However, we anticipate that achieving the conversion with minimal entanglement in the battery may require some level of classical communication.

An example of an entanglement quantifier that satisfies our criteria, namely being additive and asymptotically continuous, is the squashed entanglement, defined as [16]

$$E(\rho^{AB}) = \inf\left\{\frac{1}{2}I(A;B|E) : \rho^{ABE} \text{ extension of } \rho^{AB}\right\}, \tag{3}$$

with the quantum conditional mutual information $I(A;B|E)$. We note that the squashed entanglement is not the only entanglement quantifier having these properties, another example is given in the full version.

We further note that the additivity property of entanglement measures is more fundamental than asymptotic continuity for obtaining reversible manipulations of entangled states. Specifically, any additive entanglement measure allows for the derivation of a second law for zero-error transformations, i.e., transformations that convert n copies of ρ into m copies of σ exactly. Logarithmic negativity is an example of a measure that is additive and yet not asymptotically continuous [17, 18, 5]. We demonstrate that this measure leads to a theory with bounded entanglement distillation rates, even if an error margin is allowed in the asymptotic transformations. Additionally, we illustrate a phenomenon termed *self-dilution*: the asymptotic conversion of n copies of an entangled state into $m > n$ copies of itself, with an error that can be made arbitrarily small in the asymptotic limit.

Furthermore, the findings discussed thus far are readily adaptable to multipartite scenarios. In situations involving N parties, the objective becomes transforming an N-partite state ρ into another N-partite state σ, utilizing an ancillary system that may also exhibit entanglement across all N parties. In such contexts, Theorems 1 and 2 remain applicable when the entanglement measure employed is the multipartite squashed entanglement [19], since the latter is additive and asymptotically continuous. This implies that in this framework, reversible transitions are feasible between any multipartite entangled states.

Fully quantum second law of thermodynamics. The framework described in this work has immediate implications beyond entanglement theory. The second law of thermodynamics says that state transformations in classical thermodynamics are governed by the free energy [7]. However, this statement relies on several assumptions such as the negligibility of fluctuations and energetic coherence, which might not necessarily hold in the quantum regime.

A commonly used model to study the thermodynamics of quantum systems is the framework of thermal opera-

tions, which explicitly model interactions with a thermal bath through an energy-preserving unitary [20]. For energy-incoherent states, the transformations are fully governed by a family of inequalities called the thermomajorization conditions [21]. The original form of the second law is subsequently recovered, if we consider catalytic transformations that allows correlations between the system and catalyst [22]. More precisely, it was shown that for any two energy-incoherent states ρ, σ, there exists a thermal operation that transforms ρ^S into $\sigma^{S'}$ if and only if $F(\rho^S, H^S) \geq F(\sigma^{S'}, H^{S'})$, where F is the free energy, defined as

$$F(\rho, H) = k_B T(S(\rho\|\gamma) - \log Z). \tag{4}$$

Here, T is the temperature Z is the partition function, and $\gamma = \exp(-H/k_B T)/Z$ is the thermal state associated with the system (that is characterized by H). Numerical evidences even suggest that low-dimensional catalysts already provide significance advantage [23], when it comes to the problem of simplifying the required unitary control over system and bath.

The obvious enhancement of catalysis in quantum thermodynamics even for energy-incoherent state transformations raises the following question: is it possible to extend this result to coherent states?

We answer this question by showing that the free energy determines general state transformations under thermal operations when we allow access to a thermodynamic battery. This framework includes catalysis as a special case, but relaxes the requirement of restoring the catalyst, and simply focuses on the reusability of the battery – requiring that the thermodynamic resource of the battery does not decrease.

Theorem 3 *A state $\left(\rho^S, H^S\right)$ can be converted into another state $\left(\sigma^{S'}, H^{S'}\right)$ with thermal operations and a free energy battery if and only if $F(\rho^S, H^S) \geq F(\sigma^{S'}, H^{S'})$.*

The choice of free energy F in Theorem 3 is not unique: in the quantum regime, there exists a family of generalized free energies F_α [24] that determines the allowed transformations with exact catalysis. All of these generalized free energies are additive, and therefore using them in our framework will lead to transformations that are governed by a single monotone. We can go further and relate the resource change in the battery to that in the system:

$$f(\rho^S, H^S) - f(\sigma^{S'}, H^{S'}) \geq f(\tilde{\tau}^{B'}, H^{B'}) - f(\tau^B, H^B), \tag{5}$$

which hold for any additive monotone f. However, when we allow correlations, then Eq. (5) is equivalent to the local monotonicity property studied in Ref. [25]. There, it was shown that standard free energy F is essentially the only function that is locally monotonic and continuous, up to additive and multiplicative constants. This gives a formulation of the thermodynamic second law for coherent quantum systems.

References

[1] Michał Horodecki, Jonathan Oppenheim, and Ryszard Horodecki. Are the Laws of Entanglement Theory Thermodynamical? *Phys. Rev. Lett.*, 89:240403, Nov 2002.

[2] Fernando G. S. L. Brandão and Martin B. Plenio. Entanglement theory and the second law of thermodynamics. *Nat. Phys.*, 4(11):873–877, Nov 2008.

[3] Fernando G. S. L. Brandão and Martin B. Plenio. A Generalization of Quantum Stein's Lemma. *Commun. Math. Phys.*, 295(3):791–828, May 2010.

[4] Fernando G. S. L. Brandão and Martin B. Plenio. A Reversible Theory of Entanglement and its Relation to the Second Law. *Commun. Math. Phys.*, 295(3):829–851, May 2010.

[5] Ludovico Lami and Bartosz Regula. No second law of entanglement manipulation after all. *Nat. Phys.*, 19(2):184–189, Feb 2023.

[6] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, Apr 1996.

[7] Elliott H. Lieb and Jakob Yngvason. The physics and mathematics of the second law of thermodynamics. *Phys. Rep.*, 310(1):1–96, 1999.

[8] 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, September 2023.

[9] Bartosz Regula and Ludovico Lami. Reversibility of quantum resources through probabilistic protocols. *Nat. Commun.*, 15(1):3096, Apr 2024.

[10] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature? *Phys. Rev. Lett.*, 80:5239–5242, Jun 1998.

[11] Álvaro M. Alhambra, Lluis Masanes, Jonathan Oppenheim, and Christopher Perry. Entanglement fluctuation theorems. *Phys. Rev. A*, 100:012317, Jul 2019.

[12] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Phys. Rev. A*, 67:060302, Jun 2003.

[13] Daniel Jonathan and Martin B. Plenio. Entanglement-Assisted Local Manipulation of Pure Quantum States. *Phys. Rev. Lett.*, 83:3566–3569, Oct 1999.

[14] Chandan Datta, Tulja Varun Kondra, Marek Miller, and Alexander Streltsov. Catalysis of entanglement and other quantum resources. *Rep. Prog. Phys.*, 86(11):116002, oct 2023.

[15] Patryk Lipka-Bartosik, Henrik Wilming, and Nelly Huei Ying Ng. Catalysis in Quantum Information Theory. *arXiv:2306.00798*, 2023.

[16] Matthias Christandl and Andreas Winter. "Squashed entanglement": An additive entanglement measure. *J. Math. Phys.*, 45(3):829–840, 02 2004.

[17] Karol Życzkowski, Paweł Horodecki, Anna Sanpera, and Maciej Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58:883–892, Aug 1998.

[18] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, Feb 2002.

[19] Dong Yang, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Wei Song. Squashed Entanglement for Multipartite States and Entanglement Measures Based on the Mixed Convex Roof. *IEEE Trans. Inf. Theory*, 55(7):3375–3387, 2009.

[20] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and Th. Beth. Thermodynamic Cost of Reliability and Low Temperatures: Tightening Landauer's Principle and the Second Law. *Int. J. Theor. Phys.*, 39(12):2717–2753, Dec 2000.

[21] Michał Horodecki and Jonathan Oppenheim. Fundamental limitations for quantum and nanoscale thermodynamics. *Nat. Commun.*, 4(1):2059, Jun 2013.

[22] Markus P. Müller. Correlating Thermal Machines and the Second Law at the Nanoscale. *Phys. Rev. X*, 8:041051, Dec 2018.

[23] Jeongrak Son and Nelly H Y Ng. Catalysis in action via elementary thermal operations. *New J. Phys.*, 26(3):033029, mar 2024.

[24] Fernando Brandão, Michał Horodecki, Nelly Huei Ying Ng, Jonathan Oppenheim, and Stephanie Wehner. The second laws of quantum thermodynamics. *Proc. Natl. Acad. Sci. USA*, 112(11):3275–3279, 2015.

[25] Paul Boes, Nelly H.Y. Ng, and Henrik Wilming. Variance of Relative Surprisal as Single-Shot Quantifier. *PRX Quantum*, 3:010325, Feb 2022.

Second Law of Entanglement Manipulation with Entanglement Battery

Ray Ganardi,[1,2] Tulja Varun Kondra,[3] Nelly H.Y. Ng,[2] and Alexander Streltsov[4,1]

[1]*Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland*
[2]*School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore, 637371*
[3]*Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany*
[4]*Institute of Fundamental Technological Research, Polish Academy of Sciences, Pawińskiego 5B, 02-106 Warsaw, Poland*

A central question since the beginning of quantum information science is how two distant parties can convert one entangled state into another. Answers to these questions enable us to optimize the performance of tasks such as quantum key distribution and quantum teleportation, since certain entangled states are more useful than others for these applications. It has been conjectured that entangled state transformations could be executed reversibly in an asymptotic regime, mirroring the reversible nature of Carnot cycles in classical thermodynamics. While a conclusive proof of this conjecture has been missing so far, earlier studies excluded reversible entanglement manipulation in various settings. In this work, we investigate the concept of an entanglement battery, an auxiliary quantum system that facilitates quantum state transformations without a net loss of entanglement. We establish that reversible manipulation of entangled states is achievable through local operations when augmented with an entanglement battery. In this setting, two distant parties can convert any entangled state into another of equivalent entanglement. The rate of asymptotic transformation is quantitatively expressed as a ratio of the entanglement present within the quantum states involved. Different entanglement quantifiers give rise to unique principles governing state transformations, effectively constituting diverse manifestations of a "second law" of entanglement manipulation. Our methods provide a solution to the long-standing open question regarding the reversible manipulation of entangled states and are also applicable to entangled systems involving more than two parties, and to other quantum resource theories, including quantum thermodynamics.

The industrial revolution was a transformative era spanning the 18th and 19th centuries. It was significantly driven by breakthrough discoveries in statistical physics and thermodynamics. These disciplines provided crucial insights into energy conversion, particularly in heat engines that paved the way for advancements in technology and industry. Today, we stand on the cusp of a similar threshold, this time driven by quantum technology. This field hinges on the intricate properties of quantum systems, with quantum entanglement [1] and coherence [2] playing a pivotal role.

Over the past decades, striking parallels between the principles governing manipulation of entangled systems and the laws of thermodynamics [3–7] have been revealed. A prime illustration of this similarity is often cast with the narrative of two agents, Alice and Bob, sharing n copies of an entangled state $|\psi\rangle$ that they can also manipulate. It is known that under certain conditions, by utilizing simple operations such as local operations and classical communication [8], Alice and Bob can transform their initially shared state into n copies of another state $|\phi\rangle$. In the regime of large n, this transformation is contingent upon an important condition: a reduction in entanglement entropy [8]. This rule mirrors a fundamental concept in classical thermodynamics, where the entropy of a system uniquely determines its potential for interconversion through adiabatic processes [9]. This resemblance highlights the universality of entropy as a key concept in both domains, for understanding and describing state transformations.

The striking similarity between entanglement theory and thermodynamics naturally leads to an intriguing inquiry: Does there exist a "second law of entanglement manipulation" [3], akin to its thermodynamic counterpart, that governs all state transformations of entangled systems? This question is linked to the feasibility of reversibility in quantum mechanics, in particular when it comes to manipulating entangled states in an asymptotic setting. This enables a theoretically lossless conversion between any two entangled states in the asymptotic limit. Furthermore, this mirrors classical thermodynamics, where Carnot's theorem connects the reversibility of a heat engine cycle and its efficiency.

Despite numerous dedicated efforts [3–7, 10, 11], the quest for a second law of entanglement manipulation is still ongoing. Ref. [7] establishes that there is no second law of entanglement manipulation through a certain class of deterministic protocols. However, this no-go statement can still be bypassed via relaxations such as probabilistic protocols [11]. One of the main challenges in this endeavor is the existence of bound entanglement [12]. Bound entangled quantum states, akin to black holes in the realm of astrophysics, require entanglement for their formation, yet they defy the extraction of usable entanglement in the form of singlets [12]. This paradoxical feature of entanglement poses significant theoretical and practical challenges, complicating the path towards a fully reversible framework of entangled state manipulations.

In this article, we resolve this conundrum by focusing on state transformations instead of protocols. We introduce the concept of entanglement batteries [13] into our framework. An entanglement battery is an additional entangled quantum system shared between Alice and Bob. In order to prevent the embezzling of resources [14], the battery must be returned at the end of the procedure with at least the same amount of entanglement. This idea can be viewed as a generalization of catalytic state transformations [15], a topic that has garnered significant interest recently [16, 17]. An entangled catalyst, in this context, is an ancillary quantum system in an entan-

gled state provided to Alice and Bob. They are allowed to employ this catalyst in their transformation process, with the requirement that it must be returned in its original state. Our approach extends this setup by allowing changes in the state of the ancillary system, provided that there is no reduction in its entanglement.

We demonstrate in this work that such an approach leads to a second law of entangled state manipulation. This law asserts that Alice and Bob can transform a state ρ into another σ if and only if $E(\rho) \geq E(\sigma)$, where E represents an entanglement quantifier with certain natural properties. In the asymptotic limit, the conversion rates in this setting are characterized by the ratio $E(\rho)/E(\sigma)$, leading to the implication that asymptotic state manipulations can be executed in a reversible manner. Our results lead to a family of second laws of entanglement manipulation, contingent on the method of entanglement quantification in both the system and the battery. Moreover, we recover a variant of the second law previously conjectured in [4], achieved without resorting to the generalized quantum Stein's lemma, for which a comprehensive proof is still missing [10].

ASYMPTOTIC TRANSFORMATIONS OF ENTANGLED STATES AND REVERSIBILITY

A fundamental challenge in quantum information science revolves around the interconversion of quantum states by two distant agents, Alice and Bob [1, 18]. Given a shared entangled quantum state, the question arises: What quantum states can Alice and Bob obtain, if they are restricted to local operations and classical communication (LOCC)? By LOCC, we mean local transformations within their respective laboratories and communication via classical messages. Addressing this problem is crucial for delineating the utility of specific quantum states within this framework, effectively identifying the states that offer the greatest utility for quantum information processing and communication tasks.

The problem posed above is closely connected to the important process of entanglement distillation, which involves extracting singlets $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ from a – possibly noisy – quantum state [19]. Singlets are "gold standards" of entanglement, which have a pivotal role in foundational tasks such as quantum teleportation [20] and quantum key distribution [21]. Typically, entanglement distillation is explored within an asymptotic framework, wherein Alice and Bob have access to n copies of a quantum state ρ, and their aim is to generate m singlets. A key metric of success in this endeavor is the maximum achievable ratio m/n. An error margin is permitted in the transformation, with the stipulation that the error vanishes in the limit of large n.

Provided with a large number of copies of a pure entangled state $|\psi\rangle$, Alice and Bob have the capability to transform these into singlets at a rate determined by the entanglement entropy $E(|\psi\rangle) = S(\psi^A)$ [8], where $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$ is the von Neumann entropy. Expanding upon this, Alice and Bob are also able to convert $|\psi\rangle$ into another entangled state $|\phi\rangle$ at a rate of $S(\psi^A)/S(\phi^A)$ [8]. Consequently, this framework enables a reversible, asymptotic conversion between $|\psi\rangle$ and $|\phi\rangle$, allowing for a lossless interconversion in the limit of large numbers of copies.

In general, a transformation between two entangled states ρ and σ is deemed reversible if the asymptotic transformation rates satisfy the relation $R(\rho \to \sigma) \times R(\sigma \to \rho) = 1$. However, LOCC manipulations of entangled states generally do not exhibit reversibility, meaning that there exist states with the property $R(\rho \to \sigma) \times R(\sigma \to \rho) < 1$. An extreme manifestation of such irreversibility arises from the phenomenon of bound entanglement [12]. This phenomenon is characterized by entangled states ρ from which singlets cannot be extracted, such that $R(\rho \to \psi^-) = 0$, while $R(\psi^- \to \rho) > 0$, indicating that singlets are still necessary for the state's formation [22]. This disparity signifies that the conversion between ρ and $|\psi^-\rangle$ cannot be performed in a reversible manner.

The findings presented in Ref. [4] indicate that reversibility of entangled state transformations may be achievable by expanding the set of LOCC to encompass protocols that permit the injection of a small amount of entanglement into the system, which vanishes in the asymptotic limit. Nonetheless, it is important to note that the assertions in [4] rely on the generalized quantum Stein's lemma [5]. Recent scrutiny, as discussed in [10], has raised questions about the validity of this lemma, casting uncertainty on the robustness of the conclusions drawn from its application. On the other hand, reversibility within this framework can be achieved probabilistically [11].

Recent studies have also established that reversibility cannot be achieved in settings limited to non-entangling operations, which are protocols incapable of generating entanglement from non-entangled states [7]. Furthermore, reversible manipulations of entangled states cannot be obtained by using entanglement catalysis due to the existence of bound entanglement in this setting [23, 24].

REVERSIBLE ENTANGLEMENT MANIPULATIONS WITH ENTANGLEMENT BATTERY

We demonstrate that reversible manipulations across all entangled states become feasible when an entanglement battery is incorporated. Specifically, we consider a setting where Alice and Bob can perform LOCC, and additionally are given access to a supplementary shared entangled state, which is our *entanglement battery*. This setting has been previously studied in Ref. [13], where it was shown that we can formulate a fluctuation theorem in pure state entanglement transformations with an explicit battery model. It was shown that the average change in the battery entanglement when transforming a pure state ψ^{AB} to ϕ^{AB} is bounded above by the change in entanglement $S(\psi_A) - S(\phi_A)$. In this article, we generalize this framework to allow for a general battery and we study transformations between general mixed states. We show that we obtain a reversible theory when we impose the following

Figure 1. **State transformations with an entanglement battery.** A conversion from ρ to σ is possible if $\rho \otimes \tau$ can be converted into $\sigma \otimes \tilde{\tau}$ via LOCC, and the amount of entanglement in the battery does not decrease (left part of the figure). Transformations which decrease the entanglement in the battery are not allowed (right part of the figure).

restriction on the battery: Alice and Bob must not decrease the level of entanglement within the battery throughout the process. The setup is shown in Fig. 1.

More specifically, we examine transformations of the form

$$\rho \otimes \tau \to \sigma \otimes \tilde{\tau}, \tag{1}$$

where τ represents the initial state of the battery, and $\tilde{\tau}$ denotes its final state. The requirement that the battery does not lose any entanglement then amounts to

$$E(\tilde{\tau}) \geq E(\tau), \tag{2}$$

where the choice of the entanglement quantifier E plays a pivotal role in our analysis. We show that varying the choice of entanglement quantifiers leads to the emergence of distinct "second laws" of entanglement manipulation.

The basic property of any entanglement measure E is that it should not increase under LOCC, i.e., $E(\Lambda[\rho]) \leq E(\rho)$ for any LOCC protocol Λ [25]. A particularly interesting class of entanglement measures for our analysis are quantifiers which are additive, i.e., they satisfy $E(\rho \otimes \tau) = E(\rho) + E(\tau)$ for any states ρ and τ. Additionally, we will consider entanglement quantifiers that exhibit asymptotic continuity [26]. This property implies that for two states close to each other in trace distance, the difference in the amount of entanglement can grow at most logarithmically in the Hilbert space dimension. We further require the entanglement measure to be finite for all states.

The subsequent theorem offers a comprehensive characterization of state transformations within this setup.

Theorem 1. *A state ρ can be converted into another state σ via LOCC with an entanglement battery if and only if*

$$E(\rho) \geq E(\sigma). \tag{3}$$

Here, E is an additive and finite entanglement measure.

We provide a concise outline of our proof, with comprehensive details available in the Methods section. First, we leverage the properties of additive entanglement measures to establish that under the framework of LOCC augmented with an entanglement battery, the amount of entanglement does not increase. Subsequently, we introduce a protocol that transforms the state ρ into σ for any pair of states that comply with the stipulations outlined in Eq. (3). This protocol is remarkably straightforward: the battery is initialized in the target state σ, and then local transformations are employed to interchange the states of the main system and the battery. A similar technique has been used recently in [17] in the context of correlated catalysis, see also [13].

Theorem 1 further implies that a state $\rho \otimes \mu$ can be converted into another state $\sigma \otimes \mu'$ via LOCC with entanglement battery if and only if $E(\rho) - E(\sigma) \geq E(\mu') - E(\mu)$. Here, the system in the state μ can be considered as an additional component of a battery. While $E(\rho) - E(\sigma) > 0$, i.e. the main system loses entanglement during the procedure, the battery is capable of storing entanglement to compensate for this loss.

Let us now consider the multi-copy setting, where Alice and Bob are provided with n copies of the initial quantum state ρ. The aim is to produce m copies of the target state σ. We are interested in the maximal rate of the transformation m/n, allowing for an error which vanishes in the asymptotic limit. The following theorem gives a complete characterization of the transformation rates if Alice and Bob perform an LOCC protocol with an entanglement battery.

Theorem 2. *The maximal conversion rate for converting ρ into σ via LOCC with an entanglement battery is given by*

$$R(\rho \to \sigma) = \frac{E(\rho)}{E(\sigma)}. \tag{4}$$

Here, E is an entanglement measure which is finite, additive and asymptotically continuous.

An outline of the proof is provided here, with detailed elaboration available in the Methods section. Employing the properties of additive and asymptotically continuous entanglement measures, we first demonstrate that the transformation rate is upper-bounded by $E(\rho)/E(\sigma)$. The converse is shown by introducing a protocol that accomplishes the transformation at the aforementioned rate. Echoing the approach of Theorem 1, the optimal protocol involves a battery in an entangled state,

specifically comprising copies of the target state σ. The transformation $\rho \to \sigma$ at the rate of $E(\rho)/E(\sigma)$ can be realized by permuting the main system with the battery.

An immediate consequence of our work is the construction of a framework of reversible entanglement manipulation. More specifically, we establish that $R(\rho \to \sigma) \times R(\sigma \to \rho) = 1$ for any ρ and σ, implying that in the asymptotic limit, any two entangled states ρ and σ can be interconverted reversibly. Furthermore, when the ratio $E(\rho)/E(\sigma)$ is rational, reversible interconversion is feasible even with a finite number of copies. This means there exist integers m and n such that $m/n = E(\rho)/E(\sigma)$, allowing for bidirectional conversion $\rho^{\otimes n} \to \sigma^{\otimes m}$ and $\sigma^{\otimes m} \to \rho^{\otimes n}$. We further notice that the optimal conversion rate can be achieved through a protocol involving local operations alone, which interestingly obviates the need for classical communication in this task. We suspect that this arises from allowing the battery to contain any finite amount of entanglement. However, we anticipate that achieving the conversion with minimal entanglement in the battery may require some level of classical communication.

An example of an entanglement quantifier that satisfies our criteria, namely being additive and asymptotically continuous, is the squashed entanglement, defined as [27]

$$E(\rho^{AB}) = \inf\left\{\frac{1}{2} I(A;B|E) : \rho^{ABE} \text{ extension of } \rho^{AB}\right\}, \quad (5)$$

with the quantum conditional mutual information $I(A;B|E)$. We refer to the Methods section for more details about the properties of squashed entanglement. We note that the squashed entanglement is not the only entanglement quantifier having these properties, another example is given in the Methods section.

Our findings not only affirm the existence of a second law for entangled state transformations, but also link it to the squashed entanglement present in the involved quantum states. Prior to our work, it was hypothesized [4] that should reversible manipulation of entangled states be achievable in any framework, the rates at which such reversible transformations occur would be linked to a different measure of entanglement: the regularized relative entropy of entanglement. This quantity is defined as [25]

$$E_{\mathrm{r}}^{\infty}(\rho) = \lim_{n\to\infty} \frac{1}{n} E_{\mathrm{r}}(\rho^{\otimes n}) \quad (6)$$

with the relative entropy of entanglement defined as $E_{\mathrm{r}}(\rho) = \min_{\sigma\in\mathcal{S}} S(\rho\|\sigma)$, and the quantum relative entropy $S(\rho\|\sigma) = \mathrm{Tr}(\rho \log_2 \rho) - \mathrm{Tr}(\rho \log_2 \sigma)$. Here, the minimization is done over the set of separable (i.e. non-entangled) states $\mathcal{S}$.

As we will see in the following, our methodologies extend to establish a version of the second law of entanglement manipulations predicated on the relative entropy of entanglement. This can be achieved by replacing the squashed entanglement by E_{r}^{∞} in our approach, i.e., the requirement that the regularized relative entropy of entanglement in the battery does not decrease during the procedure. It is currently unknown whether E_{r}^{∞} is additive for all states, which prevents a direct application of our results. If E_{r}^{∞} exhibits additivity, our results directly imply that $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$ is the optimal transformation rate in this setting. Nevertheless, in the Methods section we show that this configuration results in a meaningful entanglement theory with finite asymptotic distillation rates, even if E_{r}^{∞} is not additive in general. Moreover, we show that $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$ is an achievable rate for the transformation $\rho \to \sigma$ in this setting. Intriguingly, this closely resembles the second law of entanglement manipulation as delineated in [4], yet it circumvents the reliance on the generalized quantum Stein's lemma.

We further note that the additivity property of entanglement measures is more fundamental than asymptotic continuity for obtaining reversible manipulations of entangled states. Specifically, any additive entanglement measure allows for the derivation of a second law for zero-error transformations, i.e., transformations that convert n copies of ρ into m copies of σ exactly. Logarithmic negativity is an example of a measure that is additive and yet not asymptotically continuous [7, 28, 29]. We demonstrate that this measure leads to a theory with bounded entanglement distillation rates, even if an error margin is allowed in the asymptotic transformations. Additionally, we illustrate a phenomenon termed *self-dilution*: the asymptotic conversion of n copies of an entangled state into $m > n$ copies of itself, with an error that can be made arbitrarily small in the asymptotic limit. More details with concrete examples are discussed in the Methods section.

Furthermore, the findings discussed thus far are readily adaptable to multipartite scenarios. In situations involving N parties, the objective becomes transforming an N-partite state ρ into another N-partite state σ, utilizing an ancillary system that may also exhibit entanglement across all N parties. In such contexts, Theorems 1 and 2 remain applicable when the entanglement measure employed is the multipartite squashed entanglement [30], since the latter is additive and asymptotically continuous. This implies that in this framework, reversible transitions are feasible between any multipartite entangled states.

We will now discuss the difference of our methods from the approach considered in Ref. [7]. Specifically, Ref. [7] posits that reversible manipulations of entangled states are unattainable in frameworks reliant on non-entangling operations. In such frameworks, Alice and Bob, possessing many copies of a state ρ, are restricted to quantum operations that cannot generate entanglement from separable states. Under these conditions, the authors of [7] demonstrate the impossibility of reversible interconversion between certain entangled states ρ and σ, i.e., $R(\rho \to \sigma) \times R(\sigma \to \rho) < 1$. It is important to note that the methods in Ref. [7] do not cover the transformations considered in this work, because we allow the agents to further optimize on the operation in a way that depends on the system's initial and final states. This is critical in enabling reversible interconversions within our framework, and moreover is a standard feature of catalytic processes [15–17]. Additionally, it is crucial to clarify that in our setup, Alice and Bob are also precluded from creating entanglement from separable

states if the entanglement measure E is additive and vanishes solely on separable states. These conditions are satisfied, for example, by the squashed entanglement [27, 31, 32].

In the preceding discussion, we operated under the assumption that the main system and the battery return to an uncorrelated state at the procedure's conclusion. However, this requirement can be relaxed to allow for correlations between them, with the constraint that the amount of entanglement in the battery does not decrease. In this scenario, any entanglement measure E yields a reversible theory provided it satisfies four conditions: monotonicity under LOCC, continuity, additivity on product states, and general superadditivity, expressed as $E(\rho^{AA'BB'}) \geq E(\rho^{AB}) + E(\rho^{A'B'})$. This means that the amount of entanglement present in a joint state is always at least as high as the individual entanglement. Superadditivity has been shown to be a critical feature of resource monotones in general [17, 33, 34]. Notably, for pure bipartite states, transformations in this framework are entirely governed by the entanglement entropy, regardless of the entanglement measure chosen. This mirrors the uniqueness of entanglement entropy as the measure governing the transformations under standard LOCC [8, 35, 36]. For an in-depth discussion, we refer to the Supplemental Material.

As elaborated upon in the Supplemental Material, not all entanglement measures prove useful within this context. Specifically, for certain measures such as geometric entanglement, the constraint in Eq. (2) fails to impose limitations on potential transformations, permitting arbitrary amplification of entanglement within the main system. This phenomenon bears resemblance to the concept of entanglement embezzlement, as previously discussed in [14].

QUANTUM THERMODYNAMICS

The framework described in this work has immediate implications beyond entanglement theory. The second law of thermodynamics says that state transformations in classical thermodynamics are governed by the free energy [9]. However, this statement relies on several assumptions such as the negligibility of fluctuations and energetic coherence, which might not necessarily hold in the quantum regime. In particular, one commonly refers to quantum states without any coherence in the energy eigenbasis as energy-incoherent states.

A commonly used model to study the thermodynamics of quantum systems is the framework of thermal operations, which explicitly model interactions with a thermal bath through an energy-preserving unitary [37]. For energy-incoherent states, the transformations are fully governed by a family of inequalities called the thermomajorization conditions [38]. The original form of the second law is subsequently recovered, if we consider catalytic transformations that allows correlations between the system and catalyst [39]. More precisely, it was shown that for any two energy-incoherent states ρ, σ, there exists a thermal operation that transforms ρ^S into $\sigma^{S'}$ if and only if $F(\rho^S, H^S) \geq F(\sigma^{S'}, H^{S'})$, where F is the free energy, defined as

$$F(\rho, H) = k_B T (S(\rho \| \gamma) - \log Z). \tag{7}$$

Here, T is the temperature Z is the partition function, and $\gamma = \exp(-H/k_B T)/Z$ is the thermal state associated with the system (that is characterized by H). Numerical evidences even suggest that low-dimensional catalysts already provide significance advantage [40], when it comes to the problem of simplifying the required unitary control over system and bath.

The obvious enhancement of catalysis in quantum thermodynamics even for energy-incoherent state transformations raises the following question: is it possible to extend this result to coherent states? In fact, it has recently been shown that the presence of catalysts in thermodynamics fully bridge between a hierarchy of thermal processes [41] on the level of the generated set of quantum channels, i.e. including energy-coherent state transformations. Nevertheless, it is still an open question whether such catalytic power also closes the gap between thermal operations and Gibbs-preserving ones. The most recent progress on this problem is Ref. [42], which suggests that there are Gibbs-preserving operations that require infinite coherence to be implemented; however, it is unclear whether this coherence can be used *catalytically*. One of the challenges to this open problem lies again in the challenge of retaining external correlations (or similarly, coherence) in the catalyst after the process, as exemplified in [43].

We answer this question by showing that the free energy determines general state transformations under thermal operations when we allow access to a thermodynamic battery. This framework includes catalysis as a special case, but relaxes the requirement of restoring the catalyst, and simply focuses on the reusability of the battery – requiring that the thermodynamic resource of the battery does not decrease. This approach is much more flexible and avoids the problems in catalysis such as fine-tuning and embezzling. More formally, we study transformations of the form $\rho^S \otimes \tau^B \to \sigma^{S'} \otimes \tilde{\tau}^{B'}$, along with the requirement that the free energy does not decrease $F(\tilde{\tau}^{B'}, H^{B'}) \geq F(\tau^B, H^B)$. Intuitively, this allows the battery to act as a source of coherence without giving away free energy. By analogous arguments to Theorem 1, we can show that at any finite temperature $T < \infty$, the allowed set of transformations is governed by free energy, i.e. $\rho^S \to \sigma^{S'}$ if and only if $F(\rho^S, H^S) \geq F(\sigma^{S'}, H^{S'})$.

Theorem 3. *A state $\left(\rho^S, H^S\right)$ can be converted into another state $\left(\sigma^{S'}, H^{S'}\right)$ with thermal operations and a free energy battery if and only if $F(\rho^S, H^S) \geq F(\sigma^{S'}, H^{S'})$.*

We emphasize that Theorem 3 is fully general, i.e. it holds for generic states, as opposed to most results in single-shot thermodynamics that hold only for energy-incoherent states. Furthermore, we can even allow the system and battery to get correlated, similar to the entanglement case. Because free energy is a superadditive measure, it will still govern the allowed transformations. The proof of Theorem 3 relies on the key insight that thermal operations allow for the swapping of system

and battery states. To reiterate, while swapping only the state between two systems is only allowed if they have the same Hamiltonian, swapping both the state and the Hamiltonian is always allowed since it amounts to a relabelling of the systems.

Note that as we take the limit of the temperature $T \to \infty$, the free energy of any state diverges except for the Gibbs state. The condition in Theorem 3 suggests that in this limit, the set of states can be divided into two classes: the Gibbs state and everything else. However, this is not the case; if we allow the battery to have infinite free energy, then we can subtract any finite amount of free energy from the battery and satisfy the resource non-decreasing condition on the battery. This would allow us to create any state, even starting from the Gibbs state. Thus, in order to obtain meaningful conditions for state manipulations, the resource measure of the battery should be finite.

The choice of free energy F in Theorem 3 is not unique: in the quantum regime, there exists a family of generalized free energies F_α [44] that determines the allowed transformations with exact catalysis. All of these generalized free energies are additive, and therefore using them in our framework will lead to transformations that are governed by a single monotone. We can go further and relate the resource change in the battery to that in the system:

$$f(\rho^S, H^S) - f(\sigma^{S'}, H^{S'}) \geq f(\tilde{\tau}^{B'}, H^{B'}) - f(\tau^B, H^B), \qquad (8)$$

which hold for any additive monotone f. However, when we allow correlations, then Eq. (8) is equivalent to the local monotonicity property studied in Ref. [45]. There, it was shown that standard free energy F is essentially the only function that is locally monotonic and continuous, up to additive and multiplicative constants. This gives a formulation of the thermodynamic second law for coherent quantum systems.

It is worth noting that the state transformation conditions in Theorem 3 are identical to that of Gibbs-preserving operations with correlated catalysis [33]. Thus, our theorem provides an operational interpretation of catalytic Gibbs-preserving operations as thermal operations augmented with a free energy battery. In our setting, the battery can act as a reservoir of coherence that can be freely used. At the same time, we can prevent pumping free energy into the system by constraining the free energy of the battery. It would be interesting to investigate whether we can augment thermal operations in a similar way to reproduce the non-catalytic version of Gibbs-preserving operations.

CONCLUSIONS

In this article, we have explored the concept of entanglement batteries and their impact on the manipulation of entangled systems. Our findings illuminate the path toward achieving reversible entanglement manipulations across all quantum states, thereby addressing a long-standing challenge in quantum information science.

Our results lead to a family of "second laws" for entanglement manipulation, each characterized by the specific measure used to quantify entanglement of the system. Notably, we demonstrate that, for certain entanglement quantifiers, the asymptotic conversion rates for any two states ρ and σ take a particularly simple form $E(\rho)/E(\sigma)$.

This work also opens several avenues for future research, presenting intriguing questions pivotal for a deeper understanding of entangled systems. A particularly compelling area for further investigation involves identifying all entanglement quantifiers that yield conversion rates in the form of $E(\rho)/E(\sigma)$. Although it was previously speculated [4] that the regularized relative entropy of entanglement might uniquely possess this characteristic, our findings hint at the possibility that other entanglement quantifiers may also be suitable for this task.

Our techniques are not limited to the domain of entanglement but are applicable to a broad spectrum of quantum resources [46]. This can be achieved through generalizing the concept of entanglement battery to a *resource battery* – a supplementary system that participates in the transformation process without a decrease of the resource in question. Although the principle of reversibility has been confirmed in various quantum resource theories by other methods, our framework stands out as a comprehensive model. It can systematically enable the demonstration of reversibility across quantum resource theories based on a minimal set of assumptions.

METHODS

LOCC with entanglement battery

Let us start with a formal definition of the procedure considered in our article. We say that ρ^{AB} can be converted into σ^{AB} via LOCC with entanglement battery if there exists an LOCC protocol Λ and states $\tau^{A'B'}$ and $\tilde{\tau}^{A'B'}$ such that

$$\Lambda(\rho^{AB} \otimes \tau^{A'B'}) = \sigma^{AB} \otimes \tilde{\tau}^{A'B'}. \qquad (9)$$

For more details about LOCC protocols and their features we refer to Ref. [47]. In the following, we denote AB as the *main system*, and $A'B'$ comprises the entanglement battery. Moreover, we require that the final state of the battery $\tilde{\tau}$ has at least the same amount of entanglement as the initial state τ, i.e.,

$$E(\tilde{\tau}^{A'B'}) \geq E(\tau^{A'B'}). \qquad (10)$$

If E is continuous, then without loss of generality we can even assume that the entanglement of the battery is conserved, as we can always mix the final state of the battery with a separable state to decrease the final battery entanglement. A similar scenario has been introduced in [13], without the entanglement non-decreasing condition on the battery.

In the asymptotic setting, we say that ρ can be converted into σ with an achievable rate r via LOCC with entanglement

battery, if for any $\varepsilon, \delta > 0$, there are integers m, n, an LOCC protocol Λ, and a battery state τ such that

$$\Lambda\left(\rho^{\otimes n} \otimes \tau^C\right) = \mu^{S_1 \ldots S_m} \otimes \tilde{\tau}^C, \tag{11a}$$

$$\left\|\mu^{S_1 \ldots S_m} - \sigma^{\otimes m}\right\|_1 < \varepsilon, \tag{11b}$$

$$E(\tilde{\tau}^C) \geq E(\tau^C), \tag{11c}$$

$$\frac{m}{n} > r - \delta. \tag{11d}$$

Here, each system S_i denotes a copy of the bipartite system AB, and C denotes the battery system, which is also bipartite. Furthermore, entanglement in the battery is measured by a fixed measure E. The supremum over all achievable rates r is denoted by $R(\rho \to \sigma)$.

In the setting defined above, the battery is not correlated with the main system at the end of the procedure. In the Supplemental Material, we also discuss the more general setting where correlations between the main system and the battery are taken into account.

Proof of Theorems 1 and 2

In the following, we assume that E is an additive and asymptotically continuous measure [26], i.e.,

$$E^{AA'|BB'}(\rho^{AB} \otimes \sigma^{A'B'}) = E^{A|B}(\rho^{AB}) + E^{A'|B'}(\sigma^{A'B'}), \tag{12}$$

$$|E(\rho) - E(\sigma)| \leq K \|\rho - \sigma\|_1 \log_2 d + f(\|\rho - \sigma\|_1). \tag{13}$$

Here, $K > 0$ is a constant, d is the dimension of the Hilbert space, and $f(x)$ is some function which does not depend on d and vanishes in the limit $x \to 0$.

To prove Theorem 1, let us first assume that ρ^{AB} can be converted into σ^{AB} via LOCC with entanglement battery. Then, there is an LOCC protocol Λ and states $\tau^{A'B'}$ and $\tilde{\tau}^{A'B'}$ such that Eqs. (9) and (10) are fulfilled. Using the additivity of E, finiteness and its monotonicity under LOCC, we obtain

$$\begin{aligned} E(\sigma^{AB}) &= E(\sigma^{AB} \otimes \tilde{\tau}^{A'B'}) - E(\tilde{\tau}^{A'B'}) \\ &\leq E(\rho^{AB} \otimes \tau^{A'B'}) - E(\tilde{\tau}^{A'B'}) \leq E(\rho^{AB}). \end{aligned} \tag{14}$$

This shows that the amount of entanglement in the main system AB cannot increase in this procedure.

To prove the converse, let ρ and σ be two states fulfilling

$$E(\rho) \geq E(\sigma). \tag{15}$$

A conversion $\rho \to \sigma$ can be achieved in this setting by choosing

$$\tau^{A'B'} = \sigma^{A'B'}, \tag{16}$$

and the LOCC protocol consists of local permutations of A and A' on Alice's side, and correspondingly B and B' on Bob's side. Performing this protocol, the overall initial state $\rho^{AB} \otimes \sigma^{A'B'}$ is converted into $\sigma^{AB} \otimes \rho^{A'B'}$. Thus, the state of the battery at the end of the process is given by

$$\tilde{\tau}^{A'B'} = \rho^{A'B'}. \tag{17}$$

Due to Eq. (15) we have $E(\tilde{\tau}) \geq E(\tau)$ as required, and thus this protocol achieves the transformation $\rho^{AB} \to \sigma^{AB}$. This completes the proof of Theorem 1.

We will now prove Theorem 2, showing that for any entanglement measure which is additive and asymptotically continuous, the asymptotic transformation rates take the form

$$R(\rho \to \sigma) = \frac{E(\rho)}{E(\sigma)}. \tag{18}$$

For this, we will first show that the rate is upper bounded by $E(\rho)/E(\sigma)$. From Eqs. (11), additivity of E, and the fact that E is nonincreasing under LOCC, it follows that

$$\begin{aligned} E\left(\mu^{S_1 \ldots S_m}\right) + E\left(\tilde{\tau}^C\right) &= E\left(\mu^{S_1 \ldots S_m} \otimes \tilde{\tau}^C\right) \leq E\left(\rho^{\otimes n} \otimes \tau^C\right) \\ &= nE(\rho) + E(\tau), \end{aligned} \tag{19}$$

which together with Eq. (11c) implies

$$E\left(\mu^{S_1 \ldots S_m}\right) \leq nE(\rho). \tag{20}$$

Using again Eqs. (11) with asymptotic continuity of E we arrive at

$$E\left(\sigma^{\otimes m}\right) \leq E\left(\mu^{S_1 \ldots S_m}\right) + K\varepsilon m \log_2 d + f(\varepsilon), \tag{21}$$

where d is the dimension of S_i. Combining these results we obtain

$$mE(\sigma) = E\left(\sigma^{\otimes m}\right) \leq nE(\rho) + K\varepsilon m \log_2 d + f(\varepsilon), \tag{22}$$

which can also be expressed as

$$\frac{m}{n} \leq \frac{E(\rho) + \frac{f(\varepsilon)}{n}}{E(\sigma) - \varepsilon K \log_2 d}. \tag{23}$$

Assuming that

$$0 < \varepsilon < \frac{E(\sigma)}{K \log_2 d} \tag{24}$$

and using Eqs. (11), we see that any feasible rate r must fulfill

$$r < \frac{E(\rho) + \frac{f(\varepsilon)}{n}}{E(\sigma) - \varepsilon K \log_2 d} + \delta. \tag{25}$$

Recalling that we can choose arbitrary $\delta > 0$ and ε in the range (24), it follows that the asymptotic transformation rate is upper bounded by $E(\rho)/E(\sigma)$, as claimed.

We will now present a protocol achieving conversion at rate $E(\rho)/E(\sigma)$. Assume first that $E(\rho)/E(\sigma)$ is a rational number, i.e., there exist integers m and n such that

$$\frac{m}{n} = \frac{E(\rho)}{E(\sigma)}. \tag{26}$$

In this case, we can choose the initial state of the battery to be $\tau = \sigma^{\otimes m}$, and the total initial state is $\rho^{\otimes n} \otimes \sigma^{\otimes m}$ [48]. Similar to the proof of Theorem 1, Alice and Bob now apply local permutations, permuting the main system and the battery. The final state is given by $\sigma^{\otimes m} \otimes \rho^{\otimes n}$, where the battery is now in the state $\tilde{\tau} = \rho^{\otimes n}$. The final amount of entanglement of the battery is given by $E(\tilde{\tau}) = nE(\rho)$, which is equal to the initial amount of entanglement $E(\tau) = mE(\sigma)$ due to Eq. (26). This proves that for rational $E(\rho)/E(\sigma)$ a transformation with this rate is achievable.

If $E(\rho)/E(\sigma)$ is irrational, then for any $\varepsilon > 0$ there are integers m and n such that

$$\frac{E(\rho)}{E(\sigma)} - \varepsilon < \frac{m}{n} < \frac{E(\rho)}{E(\sigma)}. \tag{27}$$

Alice and Bob now use the same procedure as in the rational case. The amount of entanglement in the battery does not decrease in this procedure, since $nE(\rho) > mE(\sigma)$ due to Eq. (27). Since $\varepsilon > 0$ in Eq. (27) can be chosen arbitrarily, Alice and Bob can also achieve conversion at rate $E(\rho)/E(\sigma)$ in this case.

Proof of Theorem 3

We know that the free energy F is an additive monotone for thermal operations. Furthermore, when $0 < T < \infty$, then F is always finite. Therefore, we can repeat the arguments of Theorem 1 to obtain the only if direction.

For the if direction, we simply note that swapping the system and battery along with their Hamiltonians is allowed in thermal operations. Then, we can run the protocol in the proof of Theorem 1 to show the if direction.

Zero error conversion

We will now consider a more restricted version of the conversion problem, which we term *zero error conversion*. We say that ρ can be converted into σ with zero error via LOCC with entanglement battery if for any $\delta > 0$, there exist integers m, n, an LOCC protocol Λ, and states of the battery τ and $\tilde{\tau}$ such that

$$\Lambda\left(\rho^{\otimes n} \otimes \tau^C\right) = \sigma^{\otimes m} \otimes \tilde{\tau}^C, \tag{28a}$$

$$E(\tilde{\tau}^C) \geq E(\tau^C), \tag{28b}$$

$$\frac{m}{n} + \delta > r. \tag{28c}$$

In comparison to Eqs. (11), no error is allowed in the final state, i.e., the state at the end of the procedure should be exactly $\sigma^{\otimes m} \otimes \tilde{\tau}^C$. The supremum over all feasible rates r in this process will be called $R_{\mathrm{ze}}(\rho \to \sigma)$.

For zero-error conversion, Theorem 2 is true for any additive entanglement measure, i.e., asymptotic continuity is not required, and it holds that

$$R_{\mathrm{ze}}(\rho \to \sigma) = \frac{E(\rho)}{E(\sigma)}. \tag{29}$$

To see this, we can write

$$\begin{aligned} mE(\sigma) + E(\tilde{\tau}) = E\left(\sigma^{\otimes m} \otimes \tilde{\tau}\right) &\leq E\left(\rho^{\otimes n} \otimes \tau\right) \\ &= nE(\rho) + E(\tau), \end{aligned} \tag{30}$$

which implies that

$$\frac{m}{n} \leq \frac{E(\rho)}{E(\sigma)}. \tag{31}$$

This means that the maximal transformation rate is upper bounded by $E(\rho)/E(\sigma)$. The converse can be seen with the same protocol as in the proof of Theorem 2, see the discussion below Eq. (26).

Entanglement measures which are additive and asymptotically continuous

As mentioned in the main text, an example for an entanglement measure which is additive and asymptotically continuous is the squashed entanglement given in Eq. (5) with the quantum conditional mutual information of a state ρ^{ABE} defined as

$$I(A;B|E) = S(\rho^{AE}) + S(\rho^{BE}) - S(\rho^{ABE}) - S(\rho^{E}). \tag{32}$$

Additivity of the squashed entanglement on all states has been proven in [27], while asymptotic continuity is a direct consequence of the results presented in [32]. Moreover, squashed entanglement is zero on separable states, and is larger than zero otherwise [31].

Another example is the conditional entanglement of mutual information, defined as [49, 50]

$$E(\rho^{AB}) = \inf \frac{1}{2}\left\{I(AA' : BB') - I(A' : B')\right\}, \tag{33}$$

where the infimum is taken over all extensions $\rho^{AA'BB'}$ of the state ρ^{AB}, and $I(X : Y)$ denotes the quantum mutual information of the state ρ^{XY}:

$$I(X : Y) = S(\rho^{X}) + S(\rho^{Y}) - S(\rho^{XY}). \tag{34}$$

Additivity and asymptotic continuity of this entanglement measure has been proven in [49, 50]. Moreover, this measures is zero on separable states and larger than zero otherwise, as follows from the fact that it vanishes on separable states [49] and is lower bounded by squashed entanglement [50].

Other entanglement measures

Many entanglement measures known in the literature are not generally additive or do not satisfy asymptotic continuity.

However, we demonstrate that the presented approach can be applied to some commonly used measures, even if these properties are not fulfilled, or not known to hold. An important example is the relative entropy of entanglement [25], defined as

$$E_{\mathrm{r}}(\rho) = \min_{\sigma\in\mathcal{S}} S(\rho\|\sigma), \tag{35}$$

where $\mathcal{S}$ is the set of separable states, and $S(\rho\|\sigma) = \mathrm{Tr}(\rho\log_2\rho) - \mathrm{Tr}(\rho\log_2\sigma)$ is the quantum relative entropy. Since the relative entropy of entanglement is not additive [51], our Theorems do not directly apply in this case. Nevertheless, as we show in the Supplemental Material, quantifying the amount of entanglement in the battery by the relative entropy of entanglement leads to a theory with bounded distillation rates, in particular the asymptotic rate for converting a state ρ into $|\psi^-\rangle$ is upper bounded by $E_{\mathrm{r}}(\rho)$. Moreover, we show that $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$ is a feasible transformation rate for any two entangled states ρ and σ, where E_{r}^{∞} is the regularized relative entropy of entanglement defined in Eq. (6). The same rate is also feasible if the amount of entanglement in the battery is quantified via E_{r}^{∞}. In this setting, we also obtain a theory with bounded distillation rates. We note that for some states ρ and σ the asymptotic transformation rate might exceed $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$. We refer to the Supplemental Material for a more detailed discussion.

Another frequently used entanglement measure in the literature is the logarithmic negativity [28, 29], defined as

$$E_{\mathrm{n}}(\rho) = \log_2\left\|\rho^{T_A}\right\|_1, \tag{36}$$

where T_A denotes partial transposition. Although this measure is additive, it does not satisfy asymptotic continuity [7]. As discussed above in the Methods section, the additivity of E_{n} implies a reversible framework for zero error transformations. Additionally, in the Supplemental Material, we demonstrate that the entanglement distillation rate is bounded even when allowing for an error margin in the transformation. Specifically, the asymptotic rate for the conversion $\rho\to|\psi^-\rangle$ is given by $E_{\mathrm{n}}(\rho)$. We further note that logarithmic negativity vanishes if and only if the state has positive partial transpose (PPT), which means that this framework allows for the creation of PPT states from separable states.

We will now show that measuring entanglement with logarithmic negativity entails a curious phenomenon, where it is possible to dilute a state ρ into more copies of itself. More precisely, we demonstrate an asymptotic conversion of n copies of a quantum state ρ into a noisy state which is close to m/n copies of the initial state ρ, where $m > n$. Note that the error may vanishes only in the limit $n\to\infty$. We call this phenomenon *self-dilution*. We emphasize that this effect does not lead to embezzling of entanglement, since the entanglement distillation rates are finite for any given state.

First, recall that we can convert any state ρ into singlets at rate $E_{\mathrm{n}}(\rho)$ in this setup. As discussed above in the Methods section, this conversion can be achieved with zero error. Moreover, by using LOCC it is possible to convert singlets approximately into the state ρ at rate $1/E_{\mathrm{c}}(\rho)$, where E_{c} is the entanglement cost [52]. Thus, performing these operations in sequence will convert $\rho^{\otimes n}$ into a state which is close to $nE_{\mathrm{n}}(\rho)/E_{\mathrm{c}}(\rho)$ copies of ρ, and the error can be made arbitrarily small in the limit of large n. Self-dilution of ρ occurs whenever $E_{\mathrm{n}}(\rho)/E_{\mathrm{c}}(\rho) > 1$.

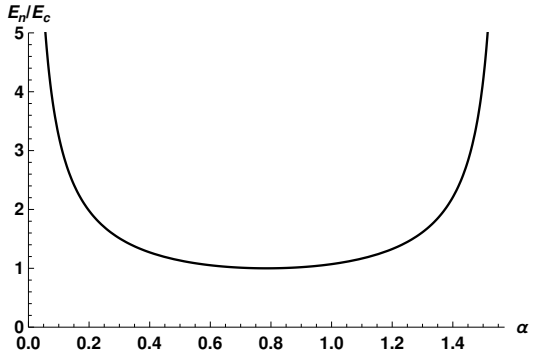


Figure 2. Self-dilution rate $E_{\mathrm{n}}(|\psi\rangle)/E_{\mathrm{c}}(|\psi\rangle)$ for $|\psi\rangle = \cos\alpha\,|00\rangle + \sin\alpha\,|11\rangle$ as a function of α.

In Fig. 2 we show the rate $E_{\mathrm{n}}(|\psi\rangle)/E_{\mathrm{c}}(|\psi\rangle)$ as a function of α for the states $|\psi\rangle = \cos\alpha\,|00\rangle + \sin\alpha\,|11\rangle$. The rate is above one as long as $|\psi\rangle$ is not maximally entangled, and diverges in the limit $\alpha\to 0$.

This phenomenon is not unique to logarithmic negativity, or even entanglement theory. By analogous arguments, we can show that self-dilution occurs in thermodynamics for incoherent states if we use $F_{\max}(\rho) = \inf\{\log\lambda\,|\,\rho\le\lambda\gamma\}$ to quantify the resources in the battery. Similarly to logarithmic negativity, $F_{\max}(\rho)$ is not asymptotically continuous and has the operational interpretation as the exact cost of preparing ρ from many copies of $|1\rangle\langle 1|$ [38]. We refer to the Supplementary Material for more details.

While counter intuitive, self-dilution does not mean that there are no cost associated with creating more copies of ρ. This is because it is not clear that we can repeat the protocol to obtain even more copies of ρ, and in fact this is forbidden since the distillation rate to the singlet state is bounded. Physically, the battery is providing the extra entanglement/work that is needed to create more copies of ρ. Therefore, this scenario is relevant when only certain types of resource in the battery are scarce [53], even in the asymptotic limit.

ACKNOWLEDGEMENTS

This work was supported by the National Science Centre Poland (Grant No. 2022/46/E/ST2/00115) and within the QuantERA II Programme (Grant No. 2021/03/Y/ST2/00178, acronym ExTRaQT) that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101017733. The work of TVK is supported by the German Federal Ministry of Ed-

ucation and Research (BMBF) within the funding program "quantum technologies – from basic research to market" in the joint project QSolid (grant number 13N16163). RG and NHYN are supported by the start-up grant for Nanyang Assistant Professorship of Nanyang Technological University, Singapore.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[2] A. Streltsov, G. Adesso, and M. B. Plenio, Colloquium: Quantum coherence as a resource, Rev. Mod. Phys. **89**, 041003 (2017).
[3] M. Horodecki, J. Oppenheim, and R. Horodecki, Are the Laws of Entanglement Theory Thermodynamical?, Phys. Rev. Lett. **89**, 240403 (2002).
[4] F. G. S. L. Brandão and M. B. Plenio, Entanglement theory and the second law of thermodynamics, Nat. Phys. **4**, 873 (2008).
[5] F. G. S. L. Brandão and M. B. Plenio, A Generalization of Quantum Stein's Lemma, Commun. Math. Phys. **295**, 791 (2010).
[6] 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).
[7] L. Lami and B. Regula, No second law of entanglement manipulation after all, Nat. Phys. **19**, 184 (2023).
[8] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).
[9] E. H. Lieb and J. Yngvason, The physics and mathematics of the second law of thermodynamics, Phys. Rep. **310**, 1 (1999).
[10] 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).
[11] B. Regula and L. Lami, Reversibility of quantum resources through probabilistic protocols, Nat. Commun. **15**, 3096 (2024).
[12] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?, Phys. Rev. Lett. **80**, 5239 (1998).
[13] Á. M. Alhambra, L. Masanes, J. Oppenheim, and C. Perry, Entanglement fluctuation theorems, Phys. Rev. A **100**, 012317 (2019).
[14] W. van Dam and P. Hayden, Universal entanglement transformations without communication, Phys. Rev. A **67**, 060302 (2003).
[15] D. Jonathan and M. B. Plenio, Entanglement-Assisted Local Manipulation of Pure Quantum States, Phys. Rev. Lett. **83**, 3566 (1999).
[16] C. Datta, T. V. Kondra, M. Miller, and A. Streltsov, Catalysis of entanglement and other quantum resources, Rep. Prog. Phys. **86**, 116002 (2023).
[17] P. Lipka-Bartosik, H. Wilming, and N. H. Y. Ng, Catalysis in Quantum Information Theory, arXiv:2306.00798 (2023).
[18] M. A. Nielsen, Conditions for a Class of Entanglement Transformations, Phys. Rev. Lett. **83**, 436 (1999).
[19] 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).
[20] 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, Phys. Rev. Lett. **70**, 1895 (1993).
[21] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[22] G. Vidal and J. I. Cirac, Irreversibility in Asymptotic Manipulations of Entanglement, Phys. Rev. Lett. **86**, 5803 (2001).
[23] L. Lami, B. Regula, and A. Streltsov, No-go theorem for entanglement distillation using catalysis, Phys. Rev. A **109**, L050401 (2024).
[24] R. Ganardi, T. V. Kondra, and A. Streltsov, Catalytic and asymptotic equivalence for quantum entanglement, arXiv:2305.03488 (2023).
[25] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying Entanglement, Phys. Rev. Lett. **78**, 2275 (1997).
[26] B. Synak-Radtke and M. Horodecki, On asymptotic continuity of functions of quantum states, J. Phys. A **39**, L423 (2006).
[27] M. Christandl and A. Winter, "Squashed entanglement": An additive entanglement measure, J. Math. Phys. **45**, 829 (2004).
[28] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Volume of the set of separable states, Phys. Rev. A **58**, 883 (1998).
[29] G. Vidal and R. F. Werner, Computable measure of entanglement, Phys. Rev. A **65**, 032314 (2002).
[30] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, Squashed Entanglement for Multipartite States and Entanglement Measures Based on the Mixed Convex Roof, IEEE Trans. Inf. Theory **55**, 3375 (2009).
[31] K. Li and A. Winter, Relative Entropy and Squashed Entanglement, Commun. Math. Phys. **326**, 63 (2014).
[32] R. Alicki and M. Fannes, Continuity of quantum conditional information, J. Phys. A **37**, L55 (2004).
[33] N. Shiraishi and T. Sagawa, Quantum Thermodynamics of Correlated-Catalytic State Conversion at Small Scale, Phys. Rev. Lett. **126**, 150502 (2021).
[34] R. Takagi and N. Shiraishi, Correlation in Catalysts Enables Arbitrary Manipulation of Quantum Coherence, Phys. Rev. Lett. **128**, 240501 (2022).
[35] M. J. Donald, M. Horodecki, and O. Rudolph, The uniqueness theorem for entanglement measures, J. Math. Phys. **43**, 4252 (2002).
[36] T. V. Kondra, C. Datta, and A. Streltsov, Catalytic Transformations of Pure Entangled States, Phys. Rev. Lett. **127**, 150503 (2021).
[37] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and T. Beth, Thermodynamic Cost of Reliability and Low Temperatures: Tightening Landauer's Principle and the Second Law, Int. J. Theor. Phys. **39**, 2717 (2000).
[38] M. Horodecki and J. Oppenheim, Fundamental limitations for quantum and nanoscale thermodynamics, Nat. Commun. **4**, 2059 (2013).
[39] M. P. Müller, Correlating Thermal Machines and the Second Law at the Nanoscale, Phys. Rev. X **8**, 041051 (2018).
[40] J. Son and N. H. Y. Ng, Catalysis in action via elementary thermal operations, New J. Phys. **26**, 033029 (2024).
[41] J. Son and N. H. Ng, A hierarchy of thermal processes collapses under catalysis, arXiv:2303.13020 (2023).
[42] H. Tajima and R. Takagi, Gibbs-preserving operations requiring infinite amount of quantum coherence, arxiv:2404.03479 (2024).
[43] S. H. Lie and N. H. Y. Ng, Catalysis always degrades external quantum correlations, Phys. Rev. A **108**, 012417 (2023).

[44] F. Brandão, M. Horodecki, N. H. Y. Ng, J. Oppenheim, and S. Wehner, The second laws of quantum thermodynamics, Proc. Natl. Acad. Sci. USA **112**, 3275 (2015).

[45] P. Boes, N. H. Ng, and H. Wilming, Variance of Relative Surprisal as Single-Shot Quantifier, PRX Quantum **3**, 010325 (2022).

[46] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[47] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask), Comm. Math. Phys. **328**, 303 (2014).

[48] If $\rho^{\otimes n}$ and $\sigma^{\otimes m}$ have different dimensions, product states are appended accordingly, making the dimensions of the main system and the battery equal.

[49] D. Yang, M. Horodecki, and Z. D. Wang, An Additive and Operational Entanglement Measure: Conditional Entanglement of Mutual Information, Phys. Rev. Lett. **101**, 140501 (2008).

[50] D. Yang, M. Horodecki, and Z. D. Wang, Conditional Entanglement, arXiv:quant-ph/0701149 (2007).

[51] K. G. H. Vollbrecht and R. F. Werner, Entanglement measures under symmetry, Phys. Rev. A **64**, 062307 (2001).

[52] M. B. Plenio and S. Virmani, An introduction to entanglement measures, Quant. Inf. Comput. **7**, 1 (2007), arXiv:quant-ph/0504163.

[53] N. H. Y. Ng, M. P. Woods, and S. Wehner, Surpassing the Carnot efficiency by extracting imperfect work, New J. Phys. **19**, 113005 (2017).

[54] G. Vidal, Entanglement of Pure States for a Single Copy, Phys. Rev. Lett. **83**, 1046 (1999).

[55] G. Gour, Infinite number of conditions for local mixed-state manipulations, Phys. Rev. A **72**, 022323 (2005).

[56] C. Datta, R. Ganardi, T. V. Kondra, and A. Streltsov, Is There a Finite Complete Set of Monotones in Any Quantum Resource Theory?, Phys. Rev. Lett. **130**, 240204 (2023).

[57] R. Takagi and B. Regula, General resource theories in quantum mechanics and beyond: Operational characterization via discrimination tasks, Phys. Rev. X **9**, 031053 (2019).

[58] R. Rubboli and M. Tomamichel, New additivity properties of the relative entropy of entanglement and its generalizations, arXiv:2211.12804 (2023).

[59] A. Winter, Tight Uniform Continuity Bounds for Quantum Entropies: Conditional Entropy, Relative Entropy Distance and Energy Constraints, Commun. Math. Phys. **347**, 291 (2016).

[60] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, Phys. Rev. A **57**, 1619 (1998).

[61] M. Christandl, *The Structure of Bipartite Quantum States - Insights from Group Theory and Cryptography*, Ph.D. thesis, University of Cambridge (2006), arXiv:quant-ph/0604183.

[62] V. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, 2003).

[63] T.-C. Wei and P. M. Goldbart, Geometric measure of entanglement and applications to bipartite and multipartite quantum states, Phys. Rev. A **68**, 042307 (2003).

[64] A. Streltsov, H. Kampermann, and D. Bruß, Linking a distance measure of entanglement to its convex roof, New J. Phys. **12**, 123004 (2010).

[65] F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Resource Theory of Quantum States Out of Thermal Equilibrium, Phys. Rev. Lett. **111**, 250404 (2013).

[66] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, SpringerBriefs in Mathematical Physics (Springer International Publishing, 2015).

SUPPLEMENTAL MATERIAL

Connection to catalysis

The notion of a resource battery is closely related to catalysis [16, 17], which is studied extensively in resource theories, entanglement being a special case thereof. Resource theories are characterized by free operations and states, that describe the abilities that an agent has unlimited access to. In entanglement theory, the standard set of free operations often correspond to LOCC while free states being separable states; in thermodynamics, thermal operations form the basic set of free operations, with Gibbs thermal states being free states.

Given any resource theory, we say that ρ can be transformed to σ with (exact) catalysis if we can find a catalyst state τ, and a free operation Λ such that

$$\Lambda\left(\rho^S \otimes \tau^C\right) = \sigma^S \otimes \tau^C. \tag{37}$$

Comparing this to our conditions on e.g. an entanglement battery Eqs. (9) and (10), we see that catalysis is a stricter condition: in catalysis, the state of the catalyst must be preserved, while Eq. (10) only requires the entanglement in the battery is preserved.

We can show that we can recover the catalytic condition if we impose additional restrictions on the battery. Taking entanglement theory as an example, let $\{E_i\}$ be a complete set of monotones for LOCC, i.e. there is an LOCC protocol transforming ρ to σ if and only if $E_i(\rho) \geq E_i(\sigma)$ for all i. Let us now impose the following condition on the battery-assisted transformations: the battery entanglement must not decrease for all of these E_i's, namely $E_i(\tilde{\tau}) \geq E_i(\tau)$ for all i. In this case, the completeness of $\{E_i\}$ implies that there exists an LOCC protocol that transform $\tilde{\tau}$ back to τ. Thus we can always post-process the battery into its initial state, and we recover the catalytic condition. This implies that by imposing only a single entanglement measure, we are ignoring all of the other types of entanglement that are present in the battery. Complete sets of monotones for entangled state transformations have been investigated in [18, 54–57], while in thermodynamics, the complete set of monotones have also been found for smaller sets of state transformations [38].

Relative entropy of entanglement

Let us discuss the consequences of constraining the amount of entanglement in the battery by the relative entropy of entanglement defined as [25]

$$E_{\mathrm{r}}(\rho) = \min_{\sigma\in\mathcal{S}} S(\rho\|\sigma) \tag{38}$$

with the quantum relative entropy

$$S(\rho\|\sigma) = \mathrm{Tr}(\rho\log_2\rho) - \mathrm{Tr}(\rho\log_2\sigma), \tag{39}$$

and $\mathcal{S}$ denotes the set of separable states. In particular, we are interested in asymptotic transformations with rates defined in Eqs. (11). This means that condition (11c) is replaced by

$$E_{\mathrm{r}}(\tilde{\tau}) \geq E_{\mathrm{r}}(\tau). \tag{40}$$

While the non-additivity of relative entropy of entanglement prevents a straightforward application of our Theorems, we can show that this framework gives rise to a nontrivial resource theory, with bounded entanglement distillation rates. For this, we recall some useful properties of the relative entropy of entanglement. In particular, E_{r} does not increase under LOCC [25] and is subadditive, i.e., for any two states ρ and τ it holds that

$$E_{\mathrm{r}}^{AA'|BB'}(\rho^{AB}\otimes\tau^{A'B'}) \leq E_{\mathrm{r}}^{A|B}(\rho^{AB}) + E_{\mathrm{r}}^{A'|B'}(\tau^{A'B'}). \tag{41}$$

In addition, the inequality becomes an equality if (at least) one of the states is pure [58].

Additionally, we will use the following continuity property which was proven implicitly in [59]. For completeness, we will provide a proof.

Proposition 4. *For any two states ρ^{AB} and σ^{AB} with $\frac{1}{2}\|\rho^{AB} - \sigma^{AB}\|_1 \leq \varepsilon$ and any $\tau^{A'B'}$, it holds*

$$\begin{aligned}&\left|E_{\mathrm{r}}^{AA'|BB'}\left(\rho^{AB}\otimes\tau^{A'B'}\right) - E_{\mathrm{r}}^{AA'|BB'}\left(\sigma^{AB}\otimes\tau^{A'B'}\right)\right| \\ &\leq \varepsilon\log_2 d_{AB} + (1+\varepsilon)h\left(\frac{\varepsilon}{1+\varepsilon}\right),\end{aligned} \tag{42}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy and d_{AB} is the dimension of AB.

Proof. The proof is implicitly contained in the proofs of Lemma 2 and Lemma 7 in Ref. [59]. Without loss of generality we can set $\|\rho^{AB} - \sigma^{AB}\|_1 = 2\varepsilon$. We now define the state

$$\Delta = \frac{1}{\varepsilon}(\rho - \sigma)_+, \tag{43}$$

where $(\rho-\sigma)_+$ denotes the positive part of $\rho - \sigma$. Using the same arguments as in the proof of Lemma 2 in Ref. [59], we find

$$\begin{aligned}\rho\otimes\tau &= \sigma\otimes\tau + (\rho-\sigma)\otimes\tau \\ &\leq \sigma\otimes\tau + \varepsilon\Delta\otimes\tau \\ &= (1+\varepsilon)\omega\otimes\tau,\end{aligned} \tag{44}$$

where we have defined the state

$$\omega = \frac{1}{1+\varepsilon}\sigma + \frac{\varepsilon}{1+\varepsilon}\Delta. \tag{45}$$

Due to Eq. (44), we can define another state

$$\Delta' = \frac{1+\varepsilon}{\varepsilon}\omega - \frac{1}{\varepsilon}\rho, \tag{46}$$

which implies that ω can also be written as

$$\omega = \frac{1}{1+\varepsilon}\rho + \frac{\varepsilon}{1+\varepsilon}\Delta'. \tag{47}$$

Using convexity of the relative entropy of entanglement [60], we find

$$E_{\mathrm{r}}(\omega\otimes\tau)\leq\frac{1}{1+\varepsilon}E_{\mathrm{r}}(\sigma\otimes\tau)+\frac{\varepsilon}{1+\varepsilon}E_{\mathrm{r}}(\Delta\otimes\tau). \tag{48}$$

Now, let $\gamma\in\mathcal{S}$ be a separable state such that $E_{\mathrm{r}}(\omega\otimes\tau)=S(\omega\otimes\tau\|\gamma)$. Recalling that the von Neumann entropy fulfills $S(\sum_i p_i\rho_i)\leq\sum_i p_i S(\rho_i)+H(p)$ with $H(p)=-\sum_i p_i\log_2 p_i$, we obtain

$$\begin{aligned}E_{\mathrm{r}}(\omega\otimes\tau)&=-S(\omega\otimes\tau)-\mathrm{Tr}(\omega\otimes\tau\log_2\gamma) \qquad (49)\\ &\geq -h\left(\frac{\varepsilon}{1+\varepsilon}\right)-\frac{1}{1+\varepsilon}S(\rho\otimes\tau)-\frac{\varepsilon}{1+\varepsilon}S(\Delta'\otimes\tau)\\ &\quad-\frac{1}{1+\varepsilon}\mathrm{Tr}(\rho\otimes\tau\log_2\gamma)-\frac{\varepsilon}{1+\varepsilon}\mathrm{Tr}(\Delta'\otimes\tau\log_2\gamma)\\ &=-h\left(\frac{\varepsilon}{1+\varepsilon}\right)+\frac{1}{1+\varepsilon}S(\rho\otimes\tau\|\gamma)+\frac{\varepsilon}{1+\varepsilon}S(\Delta'\otimes\tau\|\gamma)\\ &\geq -h\left(\frac{\varepsilon}{1+\varepsilon}\right)+\frac{1}{1+\varepsilon}E_{\mathrm{r}}(\rho\otimes\tau)+\frac{\varepsilon}{1+\varepsilon}E_{\mathrm{r}}(\Delta'\otimes\tau).\end{aligned}$$

Using Eqs. (48) and (49), we arrive at the inequality

$$\begin{aligned}E_{\mathrm{r}}(\rho\otimes\tau)-E_{\mathrm{r}}(\sigma\otimes\tau)\leq\varepsilon\left[E_{\mathrm{r}}(\Delta\otimes\tau)-E_{\mathrm{r}}(\Delta'\otimes\tau)\right]\\ +(1+\varepsilon)h\left(\frac{\varepsilon}{1+\varepsilon}\right). \qquad (50)\end{aligned}$$

Therefore, to complete the proof of the proposition, it is enough to show that

$$E_{\mathrm{r}}(\Delta\otimes\tau)-E_{\mathrm{r}}(\Delta'\otimes\tau)\leq\log_2 d_{AB}. \tag{51}$$

For this, note that

$$E_{\mathrm{r}}(\Delta\otimes\tau)\leq E_{\mathrm{r}}(\Phi_{d_{AB}}\otimes\tau)=\log_2 d_{AB}+E_{\mathrm{r}}(\tau), \tag{52}$$

where $|\Phi_{d_{AB}}\rangle=\sum_{i=0}^{d_{AB}-1}|ii\rangle/\sqrt{d_{AB}}$ is a maximally entangled state on AB. Using $E_{\mathrm{r}}(\Delta'\otimes\tau)\geq E_{\mathrm{r}}(\tau)$, we arrive at Eq. (51), and the proof is complete. □

Now, consider an asymptotic conversion $\rho\to\phi^+$ with $|\phi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$. Using Eqs. (11) together with the properties of E_{r} mentioned above, we obtain

$$\begin{aligned}m+E_{\mathrm{r}}(\tilde{\tau})&=E_{\mathrm{r}}\left(|\phi^+\rangle\langle\phi^+|^{\otimes m}\otimes\tilde{\tau}\right) \qquad (53)\\ &\leq E_{\mathrm{r}}\left(\mu^{S_1\ldots S_m}\otimes\tilde{\tau}\right)+\frac{\varepsilon}{2}m+\left[1+\frac{\varepsilon}{2}\right]h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right)\\ &\leq E_{\mathrm{r}}\left(\rho^{\otimes n}\otimes\tau\right)+\frac{\varepsilon}{2}m+\left[1+\frac{\varepsilon}{2}\right]h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right)\\ &\leq nE_{\mathrm{r}}(\rho)+E_{\mathrm{r}}(\tau)+\frac{\varepsilon}{2}m+\left[1+\frac{\varepsilon}{2}\right]h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right).\end{aligned}$$

This expression is equivalent to

$$\frac{m}{n}\leq\frac{1}{1-\frac{\varepsilon}{2}}\left[E_{\mathrm{r}}(\rho)-\frac{1}{n}\left[E_{\mathrm{r}}(\tilde{\tau})-E_{\mathrm{r}}(\tau)\right]+\frac{1}{n}\left[1+\frac{\varepsilon}{2}\right]h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right)\right]. \tag{54}$$

Using Eq. (40) we further obtain

$$\frac{m}{n}\leq\frac{1}{1-\frac{\varepsilon}{2}}\left[E_{\mathrm{r}}(\rho)+\frac{1}{n}\left[1+\frac{\varepsilon}{2}\right]h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right)\right]. \tag{55}$$

Recalling that we can choose arbitrary $\varepsilon>0$, these results imply that the asymptotic rate for converting ρ into ϕ^+ in this framework is bounded above by $E_{\mathrm{r}}(\rho)$, i.e.,

$$R(\rho\to\phi^+)\leq E_{\mathrm{r}}(\rho). \tag{56}$$

For any two entangled states ρ and σ, we will now show that $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$ is a feasible rate for the conversion $\rho\to\sigma$, where E_{r}^{∞} is the regularized relative entropy of entanglement

$$E_{\mathrm{r}}^{\infty}(\rho)=\lim_{n\to\infty}\frac{1}{n}E_{\mathrm{r}}(\rho^{\otimes n}). \tag{57}$$

For proving this, consider first two states ρ and σ such that

$$E_{\mathrm{r}}^{\infty}(\rho)>E_{\mathrm{r}}^{\infty}(\sigma). \tag{58}$$

Then, it must be that $E_{\mathrm{r}}(\rho^{\otimes n})/n>E_{\mathrm{r}}(\sigma^{\otimes n})/n$ for all large enough n, and thus also

$$E_{\mathrm{r}}(\rho^{\otimes n})>E_{\mathrm{r}}(\sigma^{\otimes n}). \tag{59}$$

It is now possible to convert $\rho^{\otimes n}$ into $\sigma^{\otimes n}$ using a similar protocol as in the proof of Theorem 2. For this, we choose the initial state of the battery to be $\tau=\sigma^{\otimes n}$, i.e., the total initial state is $\rho^{\otimes n}\otimes\sigma^{\otimes n}$. Permuting the main system and the battery (which can be achieved via local operations only), we obtain the final state $\sigma^{\otimes n}\otimes\rho^{\otimes n}$, where the battery is now in the state $\tilde{\tau}=\rho^{\otimes n}$. Due to Eq. (59), it holds that $E(\tilde{\tau})>E(\tau)$, i.e., the amount of entanglement in the battery does not decrease.

The above arguments show that for any two states fulfilling Eq. (58) the asymptotic rate for converting ρ into σ is at least one. Consider now two general states ρ and σ, not necessarily fulfilling Eq. (58). For any $\varepsilon>0$ we can find two integers k and l such that

$$1<\frac{E_{\mathrm{r}}^{\infty}(\rho^{\otimes k})}{E_{\mathrm{r}}^{\infty}(\sigma^{\otimes l})}<1+\varepsilon. \tag{60}$$

Following the same reasoning as above, it is possible to convert the state $\rho^{\otimes k}$ into $\sigma^{\otimes l}$ with rate at least one, which means that ρ can be converted into σ with rate at least l/k. Recall that E_{r}^{∞} is additive on the same state, i.e., $E_{\mathrm{r}}^{\infty}(\rho^{\otimes k})=kE_{\mathrm{r}}^{\infty}(\rho)$ and similar for σ. It follows that

$$\frac{l}{k}>\frac{E_{\mathrm{r}}^{\infty}(\rho)}{(1+\varepsilon)E_{\mathrm{r}}^{\infty}(\sigma)}, \tag{61}$$

which means that $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$ is a feasible transformation rate in this setting.

In Ref. [7], an example of a state with different distillable entanglement and entanglement cost with non-entangling operations was presented. The state is $\rho=\frac{1}{6}\sum_{i,j=1}^{3}(|ii\rangle\langle ii|-|ii\rangle\langle jj|)$, which is a maximally correlated

state, with distillable entanglement $E_d(\rho) = \log 3/2$ and entanglement cost $E_c(\rho) = 1$. Let us compare what happens if we have access to an entanglement battery, quantified by relative entropy. Since the relative entropy of entanglement is additive if one of the states is a maximally correlated state [58], the arguments above show that transformations between maximally correlated states are reversible. This means that we can reversibly convert the state ρ to a singlet at a rate $E_r(\rho) = \log 3/2$ with the help of an entanglement battery. This is in contrasts to the non-entangling operations case, where the entanglement cost is strictly higher.

Let us now analyze the transformation rates if the amount of entanglement in the battery is quantified via the regularized relative entropy of entanglement, i.e., Eq. (11c) is replaced by

$$E_{\mathrm{r}}^{\infty}(\tilde{\tau}) \geq E_{\mathrm{r}}^{\infty}(\tau). \tag{62}$$

Since it is not known if the regularized relative entropy of entanglement is fully additive, this prevents a straightforward application of our Theorems. Nevertheless, we will see in the following that we obtain a nontrivial theory of entanglement manipulations, with bounded asymptotic entanglement distillation rates. Similar to the non-regularized version, note that E_{r}^{∞} is subadditive, i.e.,

$$E_{\mathrm{r}}^{\infty}(\rho \otimes \tau) \leq E_{\mathrm{r}}^{\infty}(\rho) + E_{\mathrm{r}}^{\infty}(\tau). \tag{63}$$

Moreover, we can show that E_{r}^{∞} fulfills Proposition 4. More precisely, for any two states ρ and σ in a Hilbert space of dimension d_{AB} with $\frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon$ and any τ, we have

$$\left|E_{\mathrm{r}}^{\infty}(\rho \otimes \tau) - E_{\mathrm{r}}^{\infty}(\sigma \otimes \tau)\right| \leq \varepsilon \log_2 d_{AB} + (1+\varepsilon) h\left(\frac{\varepsilon}{1+\varepsilon}\right). \tag{64}$$

For this, we can use similar arguments as in the proof of Corollary 8 in [59]. As can be seen by inspection, the following equality holds:

$$\begin{aligned} & E_{\mathrm{r}}\left(\rho^{\otimes n} \otimes \tau^{\otimes n}\right) - E_{\mathrm{r}}\left(\sigma^{\otimes n} \otimes \tau^{\otimes n}\right) \\ &= \sum_{t=1}^{n} E_{\mathrm{r}}\left(\rho^{\otimes t} \otimes \tau^{\otimes t} \otimes \sigma^{\otimes n-t} \otimes \tau^{\otimes n-t}\right) \\ &\qquad - E_{\mathrm{r}}\left(\rho^{\otimes t-1} \otimes \tau^{\otimes t-1} \otimes \sigma^{\otimes n-t+1} \otimes \tau^{\otimes n-t+1}\right) \\ &= \sum_{t=1}^{n} E_{\mathrm{r}}(\rho \otimes \tau \otimes \Omega_t) - E_{\mathrm{r}}(\sigma \otimes \tau \otimes \Omega_t) \end{aligned} \tag{65}$$

with $\Omega_t = (\rho \otimes \tau)^{\otimes t-1} \otimes (\sigma \otimes \tau)^{\otimes n-t}$. Using triangle inequality, we obtain:

$$\begin{aligned} & \left|E_{\mathrm{r}}\left(\rho^{\otimes n} \otimes \tau^{\otimes n}\right) - E_{\mathrm{r}}\left(\sigma^{\otimes n} \otimes \tau^{\otimes n}\right)\right| \\ &\leq \sum_{t=1}^{n} \left|E_{\mathrm{r}}(\rho \otimes \tau \otimes \Omega_t) - E_{\mathrm{r}}(\sigma \otimes \tau \otimes \Omega_t)\right|. \end{aligned} \tag{66}$$

Using Proposition 4, we further obtain

$$\begin{aligned} & \left|E_{\mathrm{r}}(\rho \otimes \tau \otimes \Omega_t) - E_{\mathrm{r}}(\sigma \otimes \tau \otimes \Omega_t)\right| \\ &\leq \varepsilon \log_2 d_{AB} + (1+\varepsilon) h\left(\frac{\varepsilon}{1+\varepsilon}\right) \end{aligned} \tag{67}$$

for any t. Collecting the above results gives us

$$\begin{aligned} \left|E_{\mathrm{r}}\left(\rho^{\otimes n} \otimes \tau^{\otimes n}\right) - E_{\mathrm{r}}\left(\sigma^{\otimes n} \otimes \tau^{\otimes n}\right)\right| &\leq n\varepsilon \log_2 d_{AB} \\ &\quad + n(1+\varepsilon) h\left(\frac{\varepsilon}{1+\varepsilon}\right). \end{aligned} \tag{68}$$

From this expression we directly obtain

$$\begin{aligned} \left|\frac{1}{n} E_{\mathrm{r}}\left(\rho^{\otimes n} \otimes \tau^{\otimes n}\right) - \frac{1}{n} E_{\mathrm{r}}\left(\sigma^{\otimes n} \otimes \tau^{\otimes n}\right)\right| &\leq \varepsilon \log_2 d_{AB} \\ &\quad + (1+\varepsilon) h\left(\frac{\varepsilon}{1+\varepsilon}\right), \end{aligned} \tag{69}$$

which implies the claimed inequality (64) by taking the limit $n \to \infty$.

Now, we can obtain statements analogous to Eq. (53) for the transition $\rho \to \phi^+$:

$$\begin{aligned} m + E_{\mathrm{r}}^{\infty}(\tilde{\tau}) &= E_{\mathrm{r}}^{\infty}\left(|\phi^+\rangle\langle\phi^+|^{\otimes m} \otimes \tilde{\tau}\right) \\ &\leq E_{\mathrm{r}}^{\infty}\left(\mu^{S_1 \ldots S_m} \otimes \tilde{\tau}\right) + \frac{\varepsilon}{2} m + \left[1 + \frac{\varepsilon}{2}\right] h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right) \\ &\leq E_{\mathrm{r}}^{\infty}\left(\rho^{\otimes n} \otimes \tau\right) + \frac{\varepsilon}{2} m + \left[1 + \frac{\varepsilon}{2}\right] h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right) \\ &\leq n E_{\mathrm{r}}^{\infty}(\rho) + E_{\mathrm{r}}^{\infty}(\tau) + \frac{\varepsilon}{2} m + \left[1 + \frac{\varepsilon}{2}\right] h\left(\frac{\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}}\right). \end{aligned} \tag{70}$$

Using the same arguments as below Eq. (53), we conclude that the asymptotic entanglement distillation rate is upper bounded by $E_{\mathrm{r}}^{\infty}(\rho)$. Moreover, for any two entangled states ρ and σ a transformation at rate $E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$ can be achieved by using the protocol described below Eq. (57).

We further notice that if the regularized relative entropy of entanglement is additive, i.e., if the inequality (63) is an equality for all states ρ and τ, then by asymptotic continuity of E_{r}^{∞} [59, 61] we can apply Theorem 2. It follows that the optimal transformation rate for any pair of states in this setting is given by $R(\rho \to \sigma) = E_{\mathrm{r}}^{\infty}(\rho)/E_{\mathrm{r}}^{\infty}(\sigma)$, which interestingly coincides with the rate conjectured in [4].

Logarithmic negativity

We will now quantify entanglement using logarithmic negativity [28, 29]

$$E_{\mathrm{n}}(\rho) = \log_2 \left\|\rho^{T_A}\right\|_1, \tag{71}$$

and investigate transformations with entanglement battery, replacing condition (10) by

$$E_{\mathrm{n}}(\tilde{\tau}) \geq E_{\mathrm{n}}(\tau). \tag{72}$$

Recalling that logarithmic negativity is additive and monotonic under LOCC [29], we directly see that Theorem 1 also holds in this setting. Moreover, due to the additivity of logarithmic negativity, we immediately see that the zero-error rates are given by

$$R_{\mathrm{ze}}(\rho \to \sigma) = \frac{E_{\mathrm{n}}(\rho)}{E_{\mathrm{n}}(\sigma)}. \tag{73}$$

More details can also be found in the Methods section.

We will now consider asymptotic transformation with an error margin which vanishes in the asymptotic limit, as defined in Eqs. (11). Logarithmic negativity is not asymptotically continuous [7], which prevents a direct application of Theorem 2. However, we will show that it still leads to a nontrivial theory of entanglement manipulation, with bounded singlet distillation rates. To see this, consider the asymptotic transformation $\rho \to \phi^+$. Due to additivity, note that the final state $\mu^{S_1\ldots S_m}$ fulfills

$$E_{\mathrm{n}}\left(\mu^{S_1\ldots S_m}\right) \leq nE_{\mathrm{n}}(\rho). \tag{74}$$

Assume now that $\mu^{S_1\ldots S_m}$ is close to m Bell states, i.e.,

$$\left\|\mu^{S_1\ldots S_m} - |\phi^+\rangle\langle\phi^+|^{\otimes m}\right\|_1 < \varepsilon. \tag{75}$$

In the next step, we use the following continuity bound [62]

$$\left\|\rho^{T_A}\right\|_1 - \left\|\sigma^{T_A}\right\|_1 \leq d_A \left\|\rho - \sigma\right\|_1 . \tag{76}$$

This implies that

$$\left\|\mu^{T_A}\right\|_1 \geq \left\||\phi^+\rangle\langle\phi^+|^{T_A}\right\|_1^m - 2^m\varepsilon, \tag{77}$$

where μ^{T_A} denotes the partial transpose of the state $\mu^{S_1\ldots S_m}$.

Collecting the above results and recalling that $\| |\phi^+\rangle\langle\phi^+|^{T_A} \|_1 = 2$, we obtain

$$\begin{aligned} nE_{\mathrm{n}}(\rho) &\geq E_{\mathrm{n}}\left(\mu^{S_1\ldots S_m}\right) = \log_2\left(\left\|\mu^{T_A}\right\|_1\right) \\ &\geq \log_2\left(\left\||\phi^+\rangle\langle\phi^+|^{T_A}\right\|_1^m - 2^m\varepsilon\right) \\ &= m + \log_2(1-\varepsilon). \end{aligned} \tag{78}$$

This inequality can also be expressed as

$$\frac{m}{n} \leq E_{\mathrm{n}}(\rho) - \frac{1}{n}\log_2(1-\varepsilon). \tag{79}$$

Since we can choose arbitrary $\varepsilon > 0$, this result means that the asymptotic transformation rate for the conversion $\rho \to \phi^+$ is upper bounded by $E_{\mathrm{n}}(\rho)$. It is further clear that $E_{\mathrm{n}}(\rho)$ is a feasible rate for the transformation $\rho \to \phi^+$, as can be seen using the same techniques as in the proof of Theorem 2. This gives an operational meaning to logarithmic negativity as the optimal rate of distilling singlets in the presence of a resource battery.

Geometric entanglement

We will now show that not all entanglement quantifiers lead to a meaningful theory for entanglement manipulation. This can be demonstrated in particular for the geometric entanglement, defined as [63, 64]

$$E_{\mathrm{g}}(\rho) = 1 - \max_{\sigma\in\mathcal{S}} F(\rho,\sigma) \tag{80}$$

with fidelity $F(\rho,\sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$ and $\mathcal{S}$ is the set of separable states. We now consider asymptotic transformation rates as defined in Eq. (11), where the condition (11c) is replaced by

$$E_{\mathrm{g}}(\tilde{\tau}^C) \geq E_{\mathrm{g}}(\tau^C), \tag{81}$$

i.e., the amount of entanglement in the battery is constrained by the geometric entanglement.

As we will now show, in this setting it is possible to convert n Bell states $|\phi^+\rangle$ into rn copies of $|\phi^+\rangle$ for any r with arbitrary accuracy. For this, consider a pure state of the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2(d-1)}}\sum_{i=1}^{d-1}|ii\rangle, \tag{82}$$

where d is the local dimension of Alice and Bob. The geometric entanglement of this state is given by $E_{\mathrm{g}}(|\psi\rangle) = 1/2$, which is the same amount as in the Bell state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. At the same time, the entanglement entropy of $|\psi\rangle$ is given by

$$S(\psi^A) = 1 + \frac{1}{2}\log_2(d-1), \tag{83}$$

which is unbounded for large d. This also means that the distillable entanglement of $|\psi\rangle$ is unbounded [8].

Assume now that Alice and Bob share an initial state of the form $|\phi^+\rangle^{\otimes n} \otimes |\psi\rangle^{\otimes n}$, where the battery is in the state $|\psi\rangle^{\otimes n}$. If Alice and Bob permute the primary system and the battery, they obtain the state $|\psi\rangle^{\otimes n} \otimes |\phi^+\rangle^{\otimes n}$, where the final state of the battery is $|\phi^+\rangle^{\otimes n}$. Noting that

$$E_{\mathrm{g}}(|\phi^+\rangle^{\otimes n}) = E_{\mathrm{g}}(|\psi\rangle^{\otimes n}) = 1 - \frac{1}{2^n} \tag{84}$$

we conclude that it is possible to convert n Bell states into n copies of the state $|\psi\rangle$, while preserving the geometric entanglement of the battery. Since we can perform another LOCC protocol to distill singlets, it follows that in this setting $|\phi^+\rangle^{\otimes n}$ can be converted into $|\phi^+\rangle^{\otimes nS(\psi^A)}$ with arbitrary accuracy for large enough n. Moreover, $S(\psi^A)$ can be made arbitrarily large by appropriately choosing the local dimension d.

In summary, we have shown that choosing the geometric entanglement for the setting considered in this article leads to a trivial theory of entanglement. Note that this is distinct from the phenomenon of self-dilution observed with logarithmic negativity, since in that case, the distillation rates are still bounded. Here, the divergence of distillation rates is caused by the lack of sensitivity in geometric entanglement to distinguish $|\psi\rangle$ and $|\phi^+\rangle$.

Correlations between main system and battery

We will now consider a more general setting where the battery might become correlated with the main system. We say that a state ρ can be transformed into another state σ in this

setting if for any $\varepsilon > 0$ there exists an LOCC protocol Λ and a state of the battery τ such that

$$\Lambda\left(\rho^{AB} \otimes \tau^{A'B'}\right) = \mu^{ABA'B'}, \tag{85a}$$
$$\left\|\mu^{AB} - \sigma^{AB}\right\|_1 < \varepsilon, \tag{85b}$$
$$E(\mu^{A'B'}) \geq E(\tau^{A'B'}). \tag{85c}$$

To obtain nontrivial state transformations, we consider entanglement measures E having the following properties:

1. Monotonicity under LOCC:

$$E(\Lambda[\rho]) \leq E(\rho) \tag{86}$$

for any LOCC protocol Λ.

2. Superadditivity:

$$E^{AA'|BB'}(\rho^{AA'BB'}) \geq E(\rho^{AB}) + E(\rho^{A'B'}). \tag{87}$$

3. Additivity on product states:

$$E^{AA'|BB'}(\rho^{AB} \otimes \sigma^{A'B'}) = E(\rho^{AB}) + E(\sigma^{A'B'}). \tag{88}$$

4. Continuity.

Note that asymptotic continuity is not required in the following. Examples of entanglement measures fulfilling these properties are the squashed entanglement [27] and the conditional entanglement of mutual information [49, 50] (see main text and Methods section for the definition of these measures). To see that conditional entanglement of mutual information fulfills superadditivity (property 2), consider an extension $\tau^{AA'A''BB'B''}$ of the state $\rho^{AA'BB'}$. It holds that

$$\begin{aligned} &I(AA'A'' : BB'B'') - I(A'' : B'') \\ &= I(AA'A'' : BB'B'') - I(A'A'' : B'B'') \\ &\quad + I(A'A'' : B'B'') - I(A'' : B''), \end{aligned} \tag{89}$$

which directly implies that $E(\rho^{AA'BB'}) \geq E(\rho^{AB}) + E(\rho^{A'B'})$.

Continuity together with Eqs. (85) implies that for any $\delta > 0$, there is an LOCC protocol Λ and a state of the battery τ such that

$$\Lambda\left(\rho^{AB} \otimes \tau^{A'B'}\right) = \mu^{ABA'B'}, \tag{90a}$$
$$\left|E\left(\sigma^{AB}\right) - E\left(\mu^{AB}\right)\right| < \delta, \tag{90b}$$
$$E(\mu^{A'B'}) \geq E(\tau^{A'B'}). \tag{90c}$$

We will now show that state transformations in this setting are fully characterized by the amount of entanglement E, i.e., a state ρ^{AB} can be converted into σ^{AB} if and only if

$$E(\rho^{AB}) \geq E(\sigma^{AB}). \tag{91}$$

To prove this, we will first show that the amount of entanglement in the main system AB cannot increase in this procedure. If ρ^{AB} can be converted into σ^{AB}, then

$$\begin{aligned} E\left(\sigma^{AB}\right) &\leq E\left(\mu^{AB}\right) + \delta \leq E^{AA'|BB'}\left(\mu^{ABA'B'}\right) - E\left(\mu^{A'B'}\right) + \delta \\ &\leq E^{AA'|BB'}\left(\rho^{AB} \otimes \tau^{A'B'}\right) - E\left(\mu^{A'B'}\right) + \delta \\ &= E\left(\rho^{AB}\right) + E\left(\tau^{A'B'}\right) - E\left(\mu^{A'B'}\right) + \delta \\ &\leq E\left(\rho^{AB}\right) + \delta. \end{aligned} \tag{92}$$

Since $\delta > 0$ can be chosen arbitrarily, we obtain Eq. (91) as claimed. The converse can be shown using the same protocol as in the proof of Theorem 2, i.e., initializing the battery in the desired target state, and then permuting the state of the main system and the battery.

We will now show that for bipartite pure states $|\psi\rangle^{AB}$ and $|\phi\rangle^{AB}$, the transitions are fully characterized by the entanglement entropy, i.e., the transformation $|\psi\rangle^{AB} \to |\phi\rangle^{AB}$ is possible if and only if

$$S(\psi^A) \geq S(\phi^A). \tag{93}$$

Interestingly, this result does not depend on the entanglement measure used, as long as the measure fulfills the properties 1-4 mentioned above. Note that this generalizes the result of Ref. [13] by allowing general mixed states as a battery.

For proving this statement, recall that Eq. (93) completely characterizes transformations between pure states in a catalytic setting [36], which is a more restrictive setting than allowing for a correlated battery. In more detail, we say that ρ can be converted into σ via LOCC with correlated catalyst if for any $\varepsilon > 0$ there exists an LOCC protocol Λ and a state τ such that [23, 24, 36]

$$\Lambda\left(\rho^{AB} \otimes \tau^{A'B'}\right) = \mu^{ABA'B'}, \tag{94a}$$
$$\left\|\mu^{AB} - \sigma^{AB}\right\|_1 < \varepsilon, \tag{94b}$$
$$\mu^{A'B'} = \tau^{A'B'}. \tag{94c}$$

As follows from the results in [36], a pure state $|\psi\rangle^{AB}$ can be converted into another pure state $|\phi\rangle^{AB}$ in this setting if and only if Eq. (93) is fulfilled. Note that any entanglement measure E which fulfills conditions 1-4 mentioned above does not increase in this setting [36]. In more detail, if ρ^{AB} can be converted into σ^{AB} via LOCC with correlated catalysis, it holds that $E(\sigma^{AB}) \leq E(\rho^{AB})$.

Summarizing these arguments, any entanglement measure E which fulfills the properties 1-4 mentioned above must have the same monotonicity on pure states as the entanglement entropy:

$$E\left(|\psi\rangle^{AB}\right) \geq E\left(|\phi\rangle^{AB}\right) \iff S\left(\psi^A\right) \geq S\left(\phi^A\right). \tag{95}$$

This shows that Eq. (93) is necessary and sufficient for a transition $|\psi\rangle^{AB} \to |\phi\rangle^{AB}$ via LOCC with entanglement battery, as defined in Eqs. (85).

We will now consider asymptotic state transformations in this setting. We say that ρ can be converted into σ at rate r if

for any $\varepsilon, \delta > 0$ there exist integers m, n, an LOCC protocol Λ, and a state of the battery τ such that

$$\Lambda\left(\rho^{\otimes n} \otimes \tau^C\right) = \mu^{S_1 \ldots S_m C}, \tag{96a}$$

$$\left\|\mu^{S_1 \ldots S_m} - \sigma^{\otimes m}\right\|_1 < \varepsilon, \tag{96b}$$

$$E(\mu^C) \geq E(\tau^C), \tag{96c}$$

$$\frac{m}{n} + \delta > r. \tag{96d}$$

In the following, $R(\rho \to \sigma)$ denotes the supremum over all feasible rates r in this setting.

We will now show that for any entanglement measure satisfying the properties 1-4 mentioned above, the asymptotic rate is given by

$$R(\rho \to \sigma) = \frac{E(\rho)}{E(\sigma)}. \tag{97}$$

We will first show that the transformation rate is upper bounded as

$$R(\rho \to \sigma) \leq \frac{E(\rho)}{E(\sigma)}. \tag{98}$$

For this, we consider the following relaxation of the asymptotic transformation task (a similar technique has been used in [24]). Instead of establishing m copies of σ from n copies of ρ with a battery C, our goal is to establish a state $\mu^{S_1 \ldots S_m C}$, with each of the subsystems S_i having almost the same amount of entanglement as σ. In more detail, we require that for any $\varepsilon, \delta > 0$ there are integers m and n, an LOCC protocol Λ and a state of the battery τ^C such that for all $i \leq m$,

$$\Lambda\left(\rho^{\otimes n} \otimes \tau^C\right) = \mu^{S_1 \ldots S_m C}, \tag{99a}$$

$$\left|E(\mu^{S_i}) - E(\sigma)\right| < \varepsilon, \tag{99b}$$

$$E(\mu^C) \geq E(\tau^C), \tag{99c}$$

$$\frac{m}{n} > r - \delta. \tag{99d}$$

Here, r is a feasible transformation rate in this process, and the supremum over all feasible rates will be denoted by $R'(\rho \to \sigma)$. Recalling that E is continuous (property 4), we have

$$R'(\rho \to \sigma) \geq R(\rho \to \sigma). \tag{100}$$

Using Eqs. (99) and the properties 1-4 of E we find

$$\begin{aligned} nE(\rho) + E(\tau) = E\left(\rho^{\otimes n} \otimes \tau^C\right) &\geq E\left(\mu^{S_1 \ldots S_m C}\right) \\ &\geq \sum_{i=1}^{m} E\left(\mu^{S_i}\right) + E\left(\mu^C\right), \end{aligned} \tag{101}$$

which further implies

$$nE(\rho) \geq \sum_{i=1}^{m} E\left(\mu^{S_i}\right). \tag{102}$$

Using once again Eqs. (99) we arrive at

$$nE(\rho) > m\left[E(\sigma) - \varepsilon\right], \tag{103}$$

leading to

$$\frac{m}{n} < \frac{E(\rho)}{E(\sigma) - \varepsilon}. \tag{104}$$

Applying Eqs. (99) one more time we obtain

$$r < \frac{E(\rho)}{E(\sigma) - \varepsilon} + \delta. \tag{105}$$

Since $\varepsilon > 0$ and $\delta > 0$ can be chosen arbitrarily, we obtain

$$R'(\rho \to \sigma) \leq \frac{E(\rho)}{E(\sigma)}. \tag{106}$$

Together with Eq. (100) this completes the proof of Eq. (98).

To complete the proof of Eq. (97), we need to show the converse, i.e., a protocol achieving conversion at rate $E(\rho)/E(\sigma)$. This can be done in the same way as in the proof of Theorem 2. In summary, we have proven that the asymptotic rates are given by Eq. (97) in this setting. This applies to any entanglement quantifier E which fulfills properties 1-4 mentioned above.

Self-dilution in thermodynamics

As mentioned, self-dilution also occurs in thermodynamics if we quantify the battery using $F_{\max}$

$$F_{\max}(\rho) = \inf\{\log \lambda \,|\, \rho \leq \lambda\gamma\}. \tag{107}$$

As with entanglement, we look at the protocol where we perform a distillation with a battery and then dilute the result to get the initial state back. Let us focus on transitions between incoherent states on a single qubit. In this setting, we can perform a distillation/dilution into $|1\rangle\langle 1|$ reversibly, with a rate determined by free energy F [65]. Furthermore, since we only look at transformations between incoherent states, no additional source of coherence is needed in the dilution process.

Now, let us look at the distillation rate $R(\rho \to |1\rangle\langle 1|)$ when we use a free energy battery quantified by $F_{\max}$. Note that $F_{\max}$ is additive, so the final state μ satisfies $nF_{\max}(\rho) \geq F_{\max}(\mu)$. Furthermore, $F_{\max}$ satisfies the asymptotic equipartition property [66], so

$$\lim_{\epsilon \to 0} \lim_{m \to \infty} \inf_{\left\|\mu - |1\rangle\langle 1|^{\otimes m}\right\| \leq \epsilon} \frac{1}{m} F_{\max}(\mu) = F(|1\rangle\langle 1|). \tag{108}$$

Now, for any $\epsilon, \delta > 0$, we have m, n, μ from Eqs. (11) which satisfies

$$\frac{m}{n} \leq \frac{F_{\max}(\rho)}{F_{\max}(\mu)/m}. \tag{109}$$

Using the asymptotic equipartition property and the definition of r, we get

$$\begin{aligned} r &\leq \lim_{\epsilon \to 0} \lim_{m \to \infty} \sup_{\left\|\mu - |1\rangle\langle 1|^{\otimes m}\right\| \leq \epsilon} \frac{F_{\max}(\rho)}{F_{\max}(\mu)/m} \\ &= \frac{F_{\max}(\rho)}{F(|1\rangle\langle 1|)} + \delta. \end{aligned} \tag{110}$$

Since this holds for any $\delta > 0$, we must have $R(\rho \to |1\rangle\langle 1|) \leq F_{\max}(\rho)/F(|1\rangle\langle 1|)$, and in particular the distillation rate is bounded.

Now, consider the following process: we start with $\rho^{\otimes n}$ and we distill $|1\rangle\langle 1|^{\otimes nr}$ with the help of a battery, where $r = F_{\max}(\rho)/F_{\max}(|1\rangle\langle 1|)$. Since we are doing this with a battery, we know that this can be done without error. Then, we perform a dilution procedure $|1\rangle\langle 1|^{\otimes nr} \to \rho^{\otimes nrr'}$ *without* battery, with $r' = F(|1\rangle\langle 1|)/F(\rho)$ [65]. Then, we have

$$rr' = \frac{F_{\max}(\rho)}{F(\rho)} \frac{F(|1\rangle\langle 1|)}{F_{\max}(|1\rangle\langle 1|)}, \tag{111}$$

and we can perform the transformation $\rho^{\otimes n} \to \rho^{\otimes nrr'}$ with a battery. We finish by noting that in general we have $F_{\max}(\rho) \geq F(\rho)$, and for incoherent states on a single qubit $\rho = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|$, we have equality only when $p = 0, 1$ or when $\rho = \gamma$.

A new approach to Bayesian lower bounds for quantum state estimation

Jianchao Zhang[1] * Jun Suzuki[1] †

[1] *Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo, 182-8585 Japan*

Abstract. Quantum Bayesian estimation, a framework for interpreting the process of quantum state estimation through Bayesian principles, has recently gained prominence in quantum metrology, particularly within the finite sample regime. The lower bound for Bayes risk serves as a critical value for achieving ultimate precision in this context. Building upon the recently proposed bound in quantum point estimation, the Nagaoka-Hayashi bound, which refines the Holevo bound, we extend this bound within the framework of Bayesian methodology. As a by-product, we demonstrate that the proposed bound unifies previously established lower bounds based on logarithmic derivative-type equations.

Keywords: quantum Bayesian estimation, Holevo bound, Nagaoka-Hayashi bound

1 Introduction

Quantum estimation has gained significant importance in recent years, primarily due to advancements in the study of near-term quantum technologies, quantum communication over noisy quantum channel [1–3], quantum sensors [4–6], quantifying phase information [7, 8], quantum imaging [9–11], and quantum metrology [12,13]. Quantum Bayesian estimation, which applies the Bayesian approach to quantum estimation, is crucial in the fields of quantum sensing and quantum metrology from the perspective of practical applications of quantum estimation [14–17].

The concept of the Quantum Bayesian estimation bound was pioneered by Personick back in 1969 [18, 19]. He developed two different approaches to the quantum Bayesian lower bounds: one is the van Trees type bound and the other is based on the optimal Bayes estimator [20]. The second-type bound is now referred to as the Personick bound, and it is known that classically this yields the achievable bound. Indeed, Personick proved that his bound is attainable for estimating a single parameter encoded in quantum states. This work was much later extended to multi-parameter scenarios by Rubio and Dunningham [21], Demkowicz-Dobrzański *et al.* [22], and Sidhu and Kok [23]. Importantly, the Personick bound and its generalization is based on the symmetric logarithmic derivative (SLD) type equation [24]. A less known bound in the community is based on the right logarithmic derivative (RLD) type equation [25], which was intensively analyzed by Holevo [26–28]. In passing, various other significant contributions for bounding of Bayes risks should also be mentioned [22, 29–33].

In the area of quantum point estimation, the various types of lower bounds were known [34, 35], and extensively studied. Among them, the Holevo bound stands [27,35] as a milestone in quantum estimation theory. This is because it sets the so-called *ultimate* bound, which can be attained asymptotically [36–41]. Recently, this bound has been refined to what is now known as the NH (NH) bound [42] after the contributions of Nagaoka and Hayashi [43, 44]. A significant difference between the two bounds is that the NH bound is *always* tighter than the Holevo bound for estimating multi-copied quantum states jointly. Thereby, the NH bound is recognized as the tightest existing bound for a finite-sample theory [45, 46].

Having these historical backgrounds, a natural question arises: can the approach to the NH bound be generalized within the Bayesian framework? Furthermore, is it possible to unify the bounds based on Personick, Holevo, and others? Our findings confirm that this is the case. The Bayesian version of the NH bound has been proposed by one of the authors [47]. The key point to the second question is that these bounds employ quantum logarithmic derivative (QLD) type equations, prompting an exploration of their unification [48]. In this work, we derive the Bayesian NH bound, the Bayesian Holevo-type bound, and the Bayesian λLD-type bound, which is a one-parameter family of QLD-type bounds ($\lambda \in [-1, 1]$). The first two bounds are formulated as optimization problems, with the Bayesian NH bound representable as a semi-definite programming (SDP) problem, making it computationally efficient. The Bayesian Holevo-type bound serves as a lower bound to the former. Additionally, we introduce the Bayesian λLD-type bound, the first bound in quantum Bayesian estimation to be expressible in closed form. This family unifies the Bayesian SLD-type and the RLD-type bounds as special cases. The interplay among newly proposed bounds is explained in Fig. 1.

2 Overview of results

In this work, our proposed three bounds are based on the NH bound [42]. This bound is the known tightest as we already showed in some examples and even in specific states this bound takes the true value. Another important advantage of the NH bound is that, compared to other lower bounds, this one can be written in an SDP problem. This makes this bound efficient to compute due to the advanced improvement of current SDP solvers.

More detailed contributions of this work are summarized as follows. (Technical details are available in

* c2141016@edu.cc.uec.ac.jp
† junsuzuki@uec.ac.jp

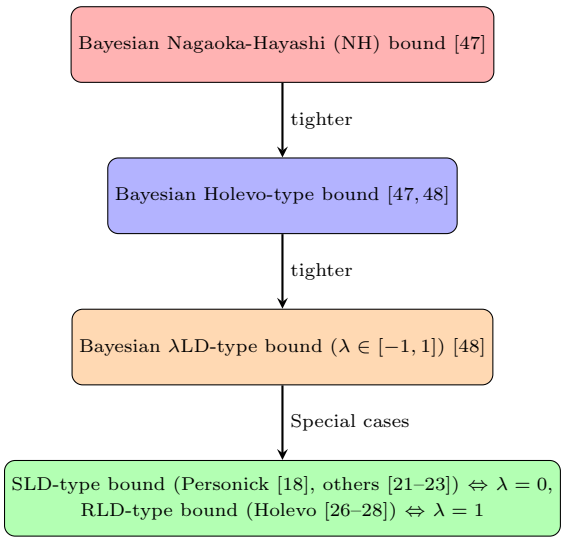


Figure 1: The interplay among newly proposed bounds and previously known bounds.

[47, 48].)

- We derive the Bayesian version of the NH bound. It keeps the good point that efficient to compute by representing it as an SDP problem. Arbitrary prior knowledge and weight matrix are compatible with this bound. (Theorem 2)
- To seek the relationship between it and the previously known Bayesian quantum estimation bound, we derive a lower bound to the Bayesian NH bound, called the Bayesian Holevo-type bound. As in point estimation, this bound is expressed as an optimization over the set of Hermitian matrices. (Theorem 3)
- After handling some inequalities, we derive a one-parameter family of the Bayesian λLD-type bounds, which is based on the QLD-type equation. Unlike the above two bounds, this is expressed in the closed form without being subject to any optimization. (Theorem 4)
- We show this bound is larger than the Personick bound [19], its generalization [21–23], and the RLD-type bound [26–28] by strict proof (Theorem 8 of [48]).

3 Background

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. A quantum parametric model is a family of density matrices on $\mathcal{H}$, $\{S_\theta \,|\, \theta \in \Theta\}$, which is parametrized by n-dimensional real parameters $\theta = (\theta_1, \theta_2, \ldots, \theta_n)$. A measurement is described by a set of positive semidefinite matrices Π_x where the index x corresponds to a measurement outcome. The set of operators corresponding to a quantum measurement is normally called a positive operator-valued measure (POVM). The measurement outcomes are labeled by an arbitrary set $\mathcal{X}$. When the measurement outcomes are labeled with a continuous set, the condition on the POVM elements is $\forall x, \Pi_x \geq 0$, $\int_{\mathcal{X}} dx\, \Pi_x = I$ with I the identity operator on $\mathcal{H}$

The conditional probability distribution is described by measurement as $p_\theta(x) = \mathrm{tr}\{S_\theta \Pi_x\}$ where $\mathrm{tr}\{\cdot\}$ denotes the trace on $\mathcal{H}$. The expectation value for a continuous random variable X is denoted by $E_\theta[X|\Pi] = \int x p_\theta(x) dx$. To infer the parameter value, we use an estimator that returns values on the set Θ: $\hat{\theta} = (\hat{\theta}_1, \hat{\theta}_2, \ldots, \hat{\theta}_n) : \mathcal{X} \to \Theta$.

To proceed further, we define the Bayes risk that is the main quantity of interest.

Definition 1 *The Bayes risk for a given prior probability distribution $\pi(\theta)$ on Θ is defined by*

$$R_{\mathrm{B}}[\Pi, \hat{\theta}] := \int_\Theta d\theta\, \pi(\theta) \mathrm{Tr}\left\{W(\theta) V_\theta[\Pi, \hat{\theta}]\right\}, \qquad (1)$$

where V_θ is the mean squared error matrix,

$$V_{\theta,jk}[\Pi, \hat{\theta}] := E_\theta\left[(\hat{\theta}_j(X) - \theta_j)(\hat{\theta}_k(X) - \theta_k)|\Pi\right]. \qquad (2)$$

$W(\theta)$ is an $n \times n$ positive semidefinie matrix as a weight matrix and $\mathrm{Tr}\{\cdot\}$ denotes the trace for matrices on the n-dimensional parameter space.

With this quantum Bayes risk, the objective is to find the best quantum estimator that minimizes the risk, i.e. the minimization problem over all possible quantum estimators $(\Pi, \hat{\theta})$. In other words, minimizing the quantum Bayes risk involves initially assigning a specific weight to each element of the mean squared error matrix. Subsequently, the weighted elements are averaged with respect to the prior distribution.

4 Results

4.1 Bayesian NH bound

We derive the NH bound in the Bayesian setting which is called the Bayesian NH bound [47]. This bound is the generalization in the Bayesian version by considering the parameter of the state as a random variable with a prior distribution.

We first introduce a new set of variables for quantum measurement and estimator by

$$\mathbb{L}_{jk}[\Pi, \hat{\theta}] = \int dx \hat{\theta}_j(x) \Pi_x \hat{\theta}_k(x) \quad (j, k = 1, 2, \ldots, n),$$
$$X_j[\Pi, \hat{\theta}] = \int dx \hat{\theta}_j(x) \Pi_x \quad (j = 1, 2, \ldots, n).$$

Briefly, these two variables encapsulate all the information of the quantum estimator, despite the lack of a one-to-one correspondence. Instead of optimizing the quantum estimator directly, our strategy involves optimizing over the variables $\mathbb{L}$ and X. Because of that, we will omit the argument $[\Pi, \hat{\theta}]$ when it is clear.

The key idea is to regard the above quantities as the operator-valued matrix and vector [42, 44]. We introduce the extended Hilbert space by $\mathbb{H} = \mathbb{C}^n \otimes \mathcal{H}$, and then

$\mathbb{L}$ is identified as a matrix on $\mathbb{H}$, whose block matrix representation is given by $[\mathbb{L}_{jk}]$. Similarly, $X = [X_j]$ is presented by the column vector of matrices.

Next, define the following quantities when combining the state with the weight matrix.

$$\mathbb{S}(\theta) := [\mathbb{S}_{ij}(\theta)] \text{ with } \mathbb{S}_{ij}(\theta) := W_{ij}(\theta) S_\theta,$$
$$D(\theta) := [D_i(\theta)] \text{ with } D_i(\theta) := \sum_{j=1}^{n} W_{ij}(\theta)\theta_j S_\theta.$$

Then directly by the lemma 1 and lemma 2 in [47] we present our main result in the following theorem.

Theorem 2 (Bayesian NH bound [47]) *For any POVM Π and estimator $\hat{\theta}$, the following lower bound holds for the Bayes risk.*

$$R_{\mathrm{B}}[\Pi, \hat{\theta}] \geq \mathcal{C}_{\mathrm{BNH}}$$
$$\mathcal{C}_{\mathrm{BNH}} := \min_{\mathbb{L}, X} \left\{ \mathrm{Tr}\left[\overline{\mathbb{S}}\mathbb{L}\right] - \mathrm{Tr}\left[\overline{D} X^{T_1}\right] - \mathrm{Tr}\left[X \overline{D}^{T_1}\right] \right\} + \overline{w},$$

where $\bar{\cdot}$ denotes the averaged operators with respect to the prior distribution, and $w(\theta) := \sum_{j,k} \theta_j W_{jk}(\theta)\theta_k$. X^{T_1} means the transpose over the parameter space and $\mathrm{Tr}[\cdot]$ is the trace over both the Hilbert space and the parameter space. Here optimization is subject to the following constraints: $\forall j, k, \mathbb{L}_{jk} = \mathbb{L}_{kj}$, $\mathbb{L}_{jk}$ is Hermitian, X_j is Hermitian, and $\mathbb{L} \geq X X^{T_1}$.

The primary advantage of this bound is that it retains the benefits of the point estimation version, specifically that the optimization problem can be formulated as an SDP problem, thereby enhancing computational efficiency [47].

As we noticed that the Bayesian NH bound involves two optimizations, it is reasonable to remove one of them to get a lower bound which is stated as the following bound.

4.2 Bayesian Holevo-type bound

This Bayesian Holevo-type bound optimization is subject to X_j, which is similar to the Holevo bound in point estimation. This is the reason we call it Holevo-type. The form is written in the following theorem.

Theorem 3 (Bayesian Holevo-type bound [48])

$$\begin{aligned} \mathcal{C}_{\mathrm{BNH}} \geq \mathcal{C}_{\mathrm{BH}} := \min_X \{ & \mathrm{Tr}\left[\mathrm{Re}\, Z(X)\right] + \mathrm{Tr}|\mathrm{Im}\, Z(X)| \\ & - \mathrm{Tr}\left[\overline{D} X^{T_1}\right] - \mathrm{Tr}\left[X \overline{D}^{T_1}\right] + \overline{w} \}, \end{aligned} \tag{3}$$

where

$$Z(X) := \frac{1}{2} \mathrm{tr}\left[\overline{\mathbb{S}} X X^{T_1} + X X^{T_1} \overline{\mathbb{S}}\right], \tag{4}$$

is an $n \times n$ complex positive semidefinite matrix, and minimization is subject to X_j: Hermitian. Here $\mathrm{Re}\,(\mathrm{Im}\,)$ *denote the element-wise real (imaginary) part of a matrix and $|A| = \sqrt{A^\dagger A}$.*

Since the form looks like the Holevo bound, we find it is able to show this bound is greater than the Personick bound with its generalization (SLD type) and the RLD-type bound by Holevo when we set the parameter independent weight matrix. This relationship automatically shows that the Bayesian NH bound is greater than all these bounds. Additionally, since the Personick bound and the RLD-type bound both are related to QLD-type equation, this gives us a hint to derive the λLD-type bound which is the unification of these two bounds.

4.3 Bayesian λLD-type bound

In the following discussion, we consider the setting in which the weight matrix is parameter-independent.

Theorem 4 (Bayesian λLD-type bound [48])

$$\mathcal{C}_{\mathrm{BH}} \geq \mathcal{C}^{(\lambda)}_{\mathrm{BLD}},$$
$$\mathcal{C}^{(\lambda)}_{\mathrm{BLD}} := -\mathrm{Tr}\left[W \mathrm{Re}\, K^{(\lambda)}\right] + \mathrm{Tr}|\sqrt{W}\, \mathrm{Im}\, K^{(\lambda)} \sqrt{W}| + \overline{w},$$

for $\lambda \in [-1, 1]$, where the $n \times n$ Hermitian matrix $K^{(\lambda)}$ is defined by

$$K^{(\lambda)}_{jk} := \mathrm{tr}[D_{\mathrm{B},k} L^{(\lambda)}_j],$$
$$D_{\mathrm{B},j} = \frac{1+\lambda}{2} S_{\mathrm{B}} L^{(\lambda)}_j + \frac{1-\lambda}{2} L^{(\lambda)}_j S_{\mathrm{B}},$$
$$S_{\mathrm{B}} = \int d\theta\, \pi(\theta) S_\theta,$$
$$D_{\mathrm{B},j} = \int d\theta\, \pi(\theta) \theta_j S_\theta.$$

This bound is derived with the λLD-type equation, which makes it in a closed form. This bound is the unification of the Personick bound [19] and its generalization ($\lambda = 0$) [21–23], and the Bayesian bound proposed by Holevo ($\lambda = 1$) [26–28]. Thereby, we also show that our bound is tighter than the Personick bound and the Bayesian bound proposed by Holevo.

5 Conclusion

In summary, we introduce three new lower bounds for the Bayes risk in quantum Bayesian estimation and present the hierarchical structure of these bounds. Furthermore, it naturally unifies previously established lower bounds; the Personick bound and its generalization, and the RLD-type bound as it contains them as special cases. Our result is based on a new approach to derive lower bounds in quantum Bayesian estimation. This provides a new methodology to analyze the Bayes risk in a finite sample theory and applications to various problems as well as comparison to previous results are awaited.

Acknowledgment

The work is partly supported by JSPS KAKENHI Grant Numbers JP21K04919, JP21K11749, and 24K14816. JZ is also supported by the research assistant scholarship at the University of Electro-Communications.

References

[1] N. Gisin and R. Thew, "Quantum communication," *Nature photonics*, vol. 1, no. 3, pp. 165–171, 2007.

[2] M. M. Wilde, *Quantum information theory*. Cambridge university press, 2013.

[3] A. S. Holevo, *Quantum systems, channels, information: a mathematical introduction*. Walter de Gruyter GmbH & Co KG, 2019.

[4] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Reviews of Modern Physics*, vol. 89, no. 3, p. 035002, 2017.

[5] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," *Nature Photonics*, vol. 12, no. 12, pp. 724–733, 2018.

[6] T. J. Proctor, P. A. Knott, and J. A. Dunningham, "Multiparameter estimation in networked quantum sensors," *Physical review letters*, vol. 120, no. 8, p. 080501, 2018.

[7] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Entanglement-enhanced lidars for simultaneous range and velocity measurements," *Physical Review A*, vol. 96, no. 4, p. 040304, 2017.

[8] M. Szczykulska, T. Baumgratz, and A. Datta, "Reaching for the quantum limits in the simultaneous estimation of phase and phase diffusion," *Quantum Science and Technology*, vol. 2, no. 4, p. 044004, 2017.

[9] M. I. Kolobov, *Quantum imaging*. Springer Science & Business Media, 2007.

[10] M. Genovese, "Real applications of quantum imaging," *Journal of Optics*, vol. 18, no. 7, p. 073002, 2016.

[11] F. Albarelli, M. Barbieri, M. G. Genoni, and I. Gianani, "A perspective on multiparameter quantum metrology: From theoretical tools to applications in quantum imaging," *Physics Letters A*, vol. 384, no. 12, p. 126311, 2020.

[12] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology," *Nature Photonics*, vol. 5, no. 4, p. 222, 2011.

[13] J. P. Dowling and K. P. Seshadreesan, "Quantum optical technologies for metrology, sensing, and imaging," *Journal of Lightwave Technology*, vol. 33, no. 12, pp. 2359–2370, 2015.

[14] M. Jarzyna and R. Demkowicz-Dobrzański, "True precision limits in quantum metrology," *New Journal of Physics*, vol. 17, no. 1, p. 013010, 2015.

[15] H. T. Dinani, D. W. Berry, R. Gonzalez, J. R. Maze, and C. Bonato, "Bayesian estimation for quantum sensing in the absence of single-shot detection," *Physical Review B*, vol. 99, no. 12, p. 125413, 2019.

[16] V. Gebhart, A. Smerzi, and L. Pezzè, "Bayesian quantum multiphase estimation algorithm," *Physical Review Applied*, vol. 16, no. 1, p. 014035, 2021.

[17] S. Nolan, A. Smerzi, and L. Pezzè, "A machine learning approach to bayesian parameter estimation," *npj Quantum Information*, vol. 7, no. 1, p. 169, 2021.

[18] S. D. Personick, *Efficient analog communication over quantum channels*. Ph.D thesis, Massachusetts Institute of Technology, 1969.

[19] S. Personick, "Application of quantum estimation theory to analog communication over quantum channels," *IEEE Transactions on Information Theory*, vol. 17, no. 3, pp. 240–246, 1971.

[20] H. L. Van Trees, *Detection, estimation, and modulation theory, part I: detection, estimation, and linear modulation theory*. John Wiley & Sons, 2004.

[21] J. Rubio and J. Dunningham, "Bayesian multiparameter quantum metrology with limited data," *Physical Review A*, vol. 101, no. 3, p. 032114, 2020.

[22] R. Demkowicz-Dobrzański, W. Górecki, and M. Guţă, "Multi-parameter estimation beyond quantum fisher information," *Journal of Physics A: Mathematical and Theoretical*, vol. 53, no. 36, p. 363001, 2020.

[23] J. S. Sidhu and P. Kok, "Geometric perspective on quantum parameter estimation," *AVS Quantum Science*, vol. 2, no. 1, 2020.

[24] C. W. Helstrom, "Minimum mean-squared error of estimates in quantum statistics," *Physics letters A*, vol. 25, no. 2, pp. 101–102, 1967.

[25] H. Yuen and M. Lax, "Multiple-parameter quantum estimation and measurement of nonselfadjoint observables," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 740–750, 1973.

[26] A. S. Holevo, "Investigations in the general theory of statistical decisions," *Trudy Matematicheskogo Instituta imeni VA Steklova*, vol. 124, pp. 3–140, 1976.

[27] ——, "Noncommutative analogues of the cramér-rao inequality in the quantum measurement theory," *Proceedings of the Third Japan — USSR Symposium on Probability Theory, Lecture Notes in Mathematics*, vol. 550, pp. 194–222, 1976.

[28] ——, "Commutation superoperator of a state and its applications to the noncommutative statistics," *Reports on mathematical physics*, vol. 12, no. 2, pp. 251–271, 1977.

[29] C. W. Helstrom, J. W. Liu, and J. P. Gordon, "Quantum-mechanical communication theory," *Proceedings of the IEEE*, vol. 58, no. 10, pp. 1578–1598, 1970.

[30] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with gaussian states," *Physics reports*, vol. 448, no. 1-4, pp. 1–111, 2007.

[31] M. Tsang, "Ziv-zakai error bounds for quantum parameter estimation," *Physical review letters*, vol. 108, no. 23, p. 230401, 2012.

[32] X.-M. Lu and M. Tsang, "Quantum weiss-weinstein bounds for quantum metrology," *Quantum Science and Technology*, vol. 1, no. 1, p. 015002, 2016.

[33] M. Tsang, "Physics-inspired forms of the bayesian cramér-rao bound," *Physical Review A*, vol. 102, no. 6, p. 062217, 2020.

[34] C. W. Helstrom, *Quantum detection and estimation theory*. Academic press, 1976.

[35] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory*. Edizioni della Normale, 2011.

[36] M. Hayashi and K. Matsumoto, "Asymptotic performance of optimal state estimation in qubit system," *Journal of Mathematical Physics*, vol. 49, no. 10, p. 102101, 2008.

[37] M. Guţă and J. Kahn, "Local asymptotic normality for qubit states," *Physical Review A*, vol. 73, no. 5, p. 052108, 2006.

[38] J. Kahn and M. Guţă, "Local asymptotic normality for finite dimensional quantum systems," *Communications in Mathematical Physics*, vol. 289, no. 2, pp. 597–652, 2009.

[39] K. Yamagata, A. Fujiwara, and R. D. Gill, "Quantum local asymptotic normality based on a new quantum likelihood ratio," *The Annals of Statistics*, vol. 41, no. 4, pp. 2197–2217, 2013.

[40] A. Fujiwara and K. Yamagata, "Noncommutative lebesgue decomposition and contiguity with applications in quantum statistics," *Bernoulli*, vol. 26, no. 3, pp. 2105–2142, 2020.

[41] ——, "Efficiency of estimators for locally asymptotically normal quantum statistical models," *The Annals of Statistics*, vol. 51, no. 3, pp. 1159–1182, 2023.

[42] L. O. Conlon, J. Suzuki, P. K. Lam, and S. M. Assad, "Efficient computation of the nagaoka–hayashi bound for multiparameter estimation with separable measurements," *npj Quantum Information*, vol. 7, no. 1, p. 110, 2021.

[43] H. Nagaoka, "A new approach to cramér-rao bounds for quantum state estimation," *IEICE Tech Report*, vol. IT 89-42, pp. 9–14, 1989, (Reprinted in [49]).

[44] M. Hayashi, "On simultaneous measurement of noncommutative observables," *Surikaisekikenkyusho (RIMS), Kyoto Univ., Kokyuroku (in japanese)*, no. 96, p. 1099, 1999.

[45] L. O. Conlon, J. Suzuki, P. K. Lam, and S. M. Assad, "The gap persistence theorem for quantum multiparameter estimation," 2022, arXiv:2208.07386.

[46] A. Das, L. O. Conlon, J. Suzuki, S. K. Yung, P. K. Lam, and S. M. Assad, "Holevo cramér-rao bound: How close can we get without entangling measurements?" 2024, arXiv:2405.09622.

[47] J. Suzuki, "Bayesian nagaoka-hayashi bound for multiparameter quantum-state estimation problem," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 107, no. 3, pp. 510–518, 2024.

[48] J. Zhang and J. Suzuki, "Bayesian logarithmic derivative type lower bounds for quantum estimation," 2024, arXiv:2405.10525.

[49] M. Hayashi, Ed., *Asymptotic theory of quantum statistical inference: selected papers*. World Scientific, 2005.

Error and Disturbance as Irreversibility with Applications: Unified Definition, Wigner–Araki–Yanase Theorem and Out-of-Time-Order Correlator

Haruki Emori[1 2 *] Hiroyasu Tajima[2 3 †]

[1] *Graduate School of Information Science and Technology, Hokkaido University, Hokkaido 060-0814, Japan*
[2] *Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo 182-8585, Japan*
[3] *JST, PRESTO, Saitama 332-0012, Japan*

Abstract. We define error and disturbance in quantum measurements as irreversibility, and characterize physical quantities beyond measurement contexts using our formulation. The full abstract is provided in the submission form. The present report is based on the preprint [H. Emori and H. Tajima, arXiv:2309.14172].

Keywords: Error, Disturbance, Irreversibility, Wigner–Araki–Yanase theorem, OTOC, Quantum comb

1 Introduction

Error and disturbance are fundamental concepts in quantum measurements. The importance of these concepts has been widely recognized since the pioneering proposal of the uncertainty principle [1]. In quantum measurements, the error and disturbance arise not as a consequence of negligence but as an intrinsic facet of measuring process, deeply rooted in the fundamental principle of quantum mechanics *per se*; so, the question of how to formulate the error and disturbance has come to be considered. As is usual with problems of quantum phenomena, there is no single answer to the question. To date, the error and disturbance have been formulated by various styles: Arthurs–Kelly–Goodman (AKG) [2–6], Ozawa [7–10], Watanabe–Sagawa–Ueda (WSU) [11, 12], Busch–Lahti–Werner (BLW) [13–15], and Lee–Tsutsui (LT) [16–18]. Although these formulations enable a multifaceted examination of the question, they pose the drawback of hindering the attainment of a unified understanding.

In this report, we provide a one answer to the question by establishing a novel formulation based on an *irreversibility*, which plays a key role in physical and information theories. We show that both of the error and disturbance can be defined as special cases of the irreversibility of quantum processes, by applying a *quantum comb* [19] to the measuring process of a target system and converting its error and disturbance into the irreversibility of an ancillary system.

Our formulation provide fruitful byproducts: First, we unify the above existing formulations of the error and disturbance as special aspects of the irreversibility. We also obtain a unified understanding of the distinction between the error and disturbance. *The error is the irreversibility when solely the classical outputs of the measurement are employed for the recovery process, and the post-measurement states are disregarded.* On the other hand, *the disturbance is the irreversibility when the classical outputs of the measurement are disregarded, and only the probabilistic mixture of post-measurement states is employed for the recovery process.* Second, we extend the Wigner–Araki–Yanase (WAY) theorem [20, 21], a universal restriction on a measurement implementation under some conservation laws, to a quantitative version for the error and disturbance of arbitrary definitions and arbitrary processes. Third, we provide a new treatment of out-of-time-order correlator (OTOC) [22], a measure of information scrambling [23] in many-body systems, as the irreversibility using the connection between disturbance and operator spreading. This treatment also give an experimental evaluation method of the OTOC, and a general bound for the OTOC when the scrambling dynamics obey a conservation law.

2 A proposed formulation

Irreversibility of quantum processes: To define the error and disturbance, we begin by introducing the irreversibility measure used in Ref.[24]. Consider a quantum process described by a completely positive trace-preserving (CPTP) map $\mathcal{L}$ from a target system S to another system S' and an arbitrary test ensemble $\Omega = \{p_k, \rho_k\}$, where $\{\rho_k\}$ is a set of quantum states in S with preparation probabilities $\{p_k\}$. Then, we define the irreversibility of $\mathcal{L}$ with respect to Ω as follows:

$$\delta(\mathcal{L}, \Omega) := \min_{\mathcal{R}: S' \to S} \sqrt{\sum_k p_k \delta_k^2}, \tag{1}$$

$$\delta_k := D_F(\rho_k, \mathcal{R} \circ \mathcal{L}(\rho_k)). \tag{2}$$

Here, the minimization is performed over CPTP maps $\mathcal{R}$ from S' to S, $D_F(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}$ is the purified distance [25], and $F(\rho, \sigma) := \mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]$ is the Uhlmann fidelity [26]. With treating a specific CPTP map $\mathcal{R}'$, the irreversibility of $\mathcal{L}$ regarding Ω is $\delta(\mathcal{L}, \mathcal{R}', \Omega) = \sqrt{\sum_k p_k \delta_k^2}$. It is important to note that $\delta(\mathcal{L}, \Omega) \leq \delta(\mathcal{L}, \mathcal{R}', \Omega)$ always holds, by definition.

Unified definition of error and disturbance: Under these settings, we design irreversibility evaluation

*emori.haruki.i8@elms.hokudai.ac.jp
†hiroyasu.tajima@uec.ac.jp

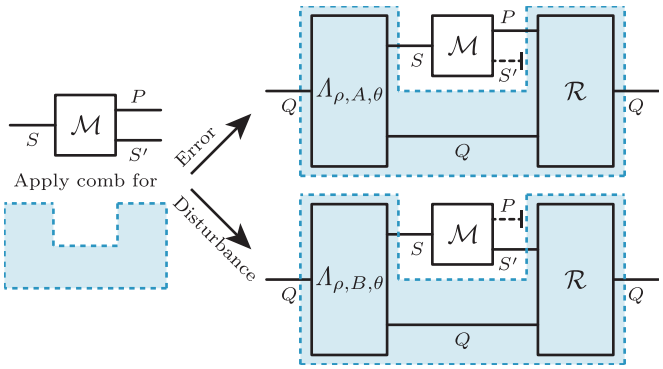


Figure 1: The irreversibility evaluation protocols for the error and disturbance.

protocols (IEPs), which translate the effect on the target system by the measurement into the effect on an ancillary system by the transformed quantum process, via inserting additional operations to and reshaping the measuring process as a *comb*. The IEPs allow us to evaluate the error and disturbance of the measurement by looking at the irreversibility (more precisely, its derivative) of these whole transformations. As a rule, the IEPs consist of two components: (P1) a loss process $\mathcal{L}$, including a weak interaction between the target system S and the qubit system Q to make the composite system have a correlation and the subsequent measurement on S; and (P2) a recovery process $\mathcal{R}$, involving an inverse map that exploits information obtained by the measurement to restore Q to its original state.

Based on the IEPs, we now state the main result: Suppose a measurement $\mathcal{M}$ of an observable A for an initial state ρ in S and its process is described by measurement operators $\{M_m\}$ mapping from S to S', where $\{m\}$ are measurement outcomes; and denote B as a disturbed observable. With these notations, we define the error ϵ and disturbance η of $\mathcal{M}$ as

$$\epsilon^2(\rho, A, \mathcal{M}) := \lim_{\theta\to 0} \frac{\delta^2(\mathcal{L}_{\rho,A,\theta,\mathcal{P}}, \Omega_{1/2,\pm})}{\theta^2}, \tag{3a}$$

$$\eta^2(\rho, B, \mathcal{M}) := \lim_{\theta\to 0} \frac{\delta^2(\mathcal{L}_{\rho,B,\theta,\mathcal{I}}, \Omega_{1/2,\pm})}{\theta^2}; \tag{3b}$$

where $\Omega_{1/2,\pm}$ is a specific test ensemble $\{(1/2, 1/2), (|+\rangle, |-\rangle)\}$, $|\pm\rangle$ are eigenvectors of the Pauli-x operator σ_x in Q, $\mathcal{L}_{\rho,A,\theta,\mathcal{P}} := \mathcal{P}_{\mathcal{M}} \circ \Lambda_{\rho,A,\theta}$ is a composite process from Q to QP with $\Lambda_{\rho,A,\theta} := \mathcal{U}_{A,\theta} \circ \mathcal{A}_\rho$, and $\mathcal{L}_{\rho,B,\theta,\mathcal{I}} := \mathcal{I}_{\mathcal{M}} \circ \Lambda_{\rho,B,\theta}$ is also from Q to QS' with $\Lambda_{\rho,B,\theta} := \mathcal{U}_{B,\theta} \circ \mathcal{A}_\rho$. P is a memory system for outcomes of $\mathcal{M}$. The loss process $\mathcal{L}_{\rho,A,\theta,\mathcal{P}}$ is implemented by (E1) an appending process $\mathcal{A}_\rho(...) := (...) \otimes \rho$ which adds the quantum state ρ on S; (E2) a unitary process $\mathcal{U}_{A,\theta}$ on SQ to make a correlation before the measurement, where $\mathcal{U}_{X,\theta}(...) := e^{-i\theta X\otimes\sigma_z}(...)e^{i\theta X\otimes\sigma_z}$ with an arbitrary observable X and the Pauli-z operator σ_z; and (E3) a measuring process $\mathcal{P}_{\mathcal{M}}(...) := \sum_m \mathrm{Tr}[M_m(...)M_m^\dagger]|m\rangle\langle m|_P$ from S to P. Similarly, the other loss process $\mathcal{L}_{\rho,B,\theta,\mathcal{I}}$ is implemented by (D1) an appending process $\mathcal{A}_\rho$; (D2) a unitary process $\mathcal{U}_{B,\theta}$; and (D3) a measuring process $\mathcal{I}_{\mathcal{M}}(...) := \sum_m M_m(...)M_m^\dagger$ from S to S'. The difference between $\mathcal{L}_{\rho,A,\theta,\mathcal{P}}$ and $\mathcal{L}_{\rho,A,\theta,\mathcal{I}}$ arises from a way of mathematical description of the measuring process, *i.e.*, what is chosen as the output, either outcomes or post-measurement states of $\mathcal{M}$. The IEPs for the error and disturbance are illustrated in Fig. 1. According to $\delta(\mathcal{L}, \mathcal{R}', \Omega)$, we also define the error and disturbance as

$$\epsilon^2(\rho, A, \mathcal{M}, \mathcal{R}') := \lim_{\theta\to 0} \frac{\delta^2(\mathcal{L}_{\rho,A,\theta,\mathcal{P}}, \mathcal{R}', \Omega_{1/2,\pm})}{\theta^2}, \tag{4a}$$

$$\eta^2(\rho, B, \mathcal{M}, \mathcal{R}') := \lim_{\theta\to 0} \frac{\delta^2(\mathcal{L}_{\rho,B,\theta,\mathcal{I}}, \mathcal{R}', \Omega_{1/2,\pm})}{\theta^2} \tag{4b}$$

for a specific recovery process $\mathcal{R}'$.

3 Applications

1. Derivation of existing formulations from ours: From the perspectives of state-dependence (or not), physical significance, and experimental accessibility, the existing formulations have been pursued through physical, mathematical, statistical, and information-theoretical approaches. However, a formulation unifying all these aspects has not been known. As solving this problem, our definition covers previously well-formulated proposal by AKG, Ozawa, WSU, BLW, and LT. Moreover, our definition not only brings these under a common umbrella but also has the capability to elucidate operational distinctions between error and disturbance, as well as the physical essence captured by each approach, using the corresponding IEP.

To derive the existing formulations, we introduce a crucial recovery process $\mathcal{R}_X$ represented by $\mathcal{R}_X := \mathcal{J}_\bullet \circ \mathcal{U}_{X,\theta}^\dagger$, where $\mathcal{J}_\bullet(...) := \sum_{j=\pm}\langle j|\mathrm{Tr}_\bullet[(...)]|j\rangle|j\rangle\langle j|_Q$ and $\bullet = P$ or S'. Applying $\mathcal{U}_{X,\theta}^\dagger$ to the composite system becomes possible to restore the relative phase of the state in Q shifted during the loss process $\mathcal{L}$. It should be noted that the bounds $\epsilon(\rho, A, \mathcal{M}) \le \epsilon(\rho, A, \mathcal{M}, \mathcal{R}_X)$ and $\eta(\rho, B, \mathcal{M}) \le \eta(\rho, B, \mathcal{M}, \mathcal{R}_{X'})$ hold for any X and X', by definition.
Example: Ozawa's error and disturbance (other errors and disturbances are in the preprint). Below, we demonstrate the derivation of Ozawa's one to facilitate intuitive understanding. Consider a set of outcomes $\{A(m)\}$ obtained from the measurement of a meter observable M in P. Then, Ozawa's error and disturbance are defined by $\epsilon_{\mathrm{O}}^2(A) := \sum_m \|M_m(A - A(m))\sqrt{\rho}\|^2$ and $\eta_{\mathrm{O}}^2(B) := \sum_m \|[M_m, B]\sqrt{\rho}\|^2$, respectively, where $S = S'$ [7, 8, 27]. If we apply the recovery processes of $\mathcal{R}_M$ from PQ to Q and $\mathcal{R}_B$ from SQ to Q, we obtain the relations: $\epsilon(\rho, A, \mathcal{M}, \mathcal{R}_M) = \epsilon_{\mathrm{O}}(A)$ and $\eta(\rho, B, \mathcal{M}, \mathcal{R}_B) = \eta_{\mathrm{O}}(B)$. Hence, $\epsilon(\rho, A, \mathcal{M}) \le \epsilon_{\mathrm{O}}(A)$ and $\eta(\rho, B, \mathcal{M}) \le \eta_{\mathrm{O}}(B)$ are obviously true.

2. WAY theorem for errors and disturbances of arbitrary definitions and processes: Our formulation also contributes to solve an open problem in the field of quantum measurements: Extensions of the WAY theorem to the errors and disturbances of arbitrary definitions and processes. The WAY theorem [24, 28–34] predicts that in the presence of an additive conservation law, the implementation of a projective measurement for

a physical quantity that does not commute with the conserved quantity is impossible. Although the quantitative WAY theorems for finite errors have been actively studied [24, 28, 29, 32], these theorems for quantum measurements have been limited to Ozawa-type error [28, 29, 32] and gate-fidelity error [24]. The quantitative WAY theorem for arbitrary error and disturbance has thus remained an open problem. By virtue of our formulation, we solve this problem, combining with the symmetry–irreversibility–quantum coherence (SIQ) trade-off relation [24].

To show our result, we introduce the SLD-quantum Fisher information for the state family $\{e^{-iX\varepsilon}\rho e^{iX\varepsilon}\}_{\varepsilon\in\mathbb{R}}$ as $\mathcal{F}_\rho(X) = 4\lim_{\varepsilon\to 0} D_F^2(e^{-iX\varepsilon}\rho e^{iX\varepsilon},\rho)/\varepsilon^2$, which is a standard measure of quantum coherence in the resource theory of asymmetry [35–43]. This quantity indicates the amount of quantum fluctuation of the observable X in the state ρ [39, 41, 43–45].

Theorem 1 *Suppose a measurement $\mathcal{M}$ of an observable A on a quantum system S in a state ρ. We realize the measuring process by $\mathcal{P}_\mathcal{M}$ for error- and $\mathcal{I}_\mathcal{M}$ for disturbance-evaluation under the conservation law of some conserved charge $X_\bullet$ ($\bullet = S, S', P$). Then, the following inequalities hold with any ρ:*

$$\epsilon(\rho,A,\mathcal{M}) \geq \frac{|\langle[Y_S,A]\rangle_\rho|}{\sqrt{\mathcal{F}^{cost}_{\mathcal{P}_\mathcal{M}}}+\Delta_F}, \tag{5a}$$

$$\eta(\rho,B,\mathcal{M}) \geq \frac{|\langle[Y'_S,B]\rangle_\rho|}{\sqrt{\mathcal{F}^{cost}_{\mathcal{I}_\mathcal{M}}}+\Delta'_F}. \tag{5b}$$

Here $\mathcal{F}^{cost}_\mathcal{N}$ is the implementation resource cost of a CPTP map $\mathcal{N}$ from α to α' under the conservation law of X and defined as $\mathcal{F}^{cost}_\mathcal{N} := \min\{\mathcal{F}_{\rho_\beta}(X_\beta)|(\rho_\beta, X_\beta, X_{\beta'}, U) \to \mathcal{N}\}$, where $(\rho_\beta, X_\beta, X_{\beta'}, U)$ runs implementations of $\mathcal{N}$ via $\mathcal{N}(...) = \mathrm{Tr}_{\beta'}[U\{(...)\otimes\rho_\beta\}U^\dagger]$ and satisfies the conservation law $U^\dagger(X_{\alpha'}+X_{\beta'})U = X_\alpha + X_\beta$. The quantities Y_S, Y'_S, Δ_F and Δ'_F are defined as $Y_S := X_S - \mathcal{P}^\dagger_\mathcal{M}(X_P)$, $Y'_S := X_S - \mathcal{I}^\dagger_\mathcal{M}(X_{S'})$, $\Delta_F := \sqrt{\mathcal{F}_\rho(X_S)} + 2\sqrt{V_{\mathcal{P}_\mathcal{M}(\rho)}(X_P)}$, and $\Delta'_F := \sqrt{\mathcal{F}_\rho(X_S)} + 2\sqrt{V_{\mathcal{I}_\mathcal{M}(\rho)}(X_{S'})}$, where $V_\sigma(Z)$ is the variance of Z in σ.

We remark that Theorem 1 does not assume the Yanase condition introduced in Ref. [28] and our contribution is not limited to the WAY theorem for measurements, but for other arbitrary processes. For arbitrary processes, there are no error-cost trade-off relations (there are counterexamples), except for unitary processes [24, 46–49] and its variants [24]. Even so, the existence of disturbance-cost trade-off relations for arbitrary processes has not been denied; and now we can obtain them as corollaries of Theorem 1 by noting that any CPTP map can be described as $\mathcal{I}_\mathcal{M}$. For measuring processes, the error-cost trade-off relation can be derived from the form of error in Theorem 1. When we assume X_P satisfies $[X_P, |m\rangle\langle m|_P] = 0$ for any m (Yanase condition) where $\{|m\rangle_P\}$ are given in the definition of $\mathcal{P}_\mathcal{M}$, we can make the form of error in Theorem 1 simpler and tighter as follows $\epsilon(\rho,A,\mathcal{M}) \geq |\langle[X_S,A]\rangle_\rho|/\sqrt{\mathcal{F}^{\mathrm{cost}}_{\mathcal{P}_\mathcal{M}}+\mathcal{F}_\rho(X_S)}$.

3. OTOC as irreversibility and its experimental evaluation method: In terms of propagating information by interactions, we find that OTOC is linked to disturbance. The OTOC $C_T(t) := -\langle[W(t),V(0)]^2\rangle_\rho$ [23] quantifies the degree of information scrambling [50–53] and is characterized by operator spreading (commutator) [54–58] in situations where a local observable W becomes correlated with a distant one V, by a global interaction in dynamical quantum systems. Besides the disturbance quantitatively express how much the observable B is affected by the measuring interaction of the measurement for the observable A [59, 60]. In these regards, it can be seen that they share the spirit of quantification for observable correlations. Take account of this aspect, we explicitly associate the OTOC with the disturbance and uniformly describe them in our formulation by providing a specific IEP.

Theorem 2 *Suppose W is a self-adjoint and unitary operator while V is a self-adjoint operator. Then, the OTOC is represented by*

$$C_T(t) = \eta^2(\rho,V,\mathcal{D},\mathcal{R}_V)\ \left(:= \lim_{\theta\to 0}\frac{\delta^2(\mathcal{L}_{\rho,V,\theta,\mathcal{D}},\Omega_{1/2,\pm},\mathcal{R}_V)}{\theta^2}\right),$$

where $\mathcal{L}_{\rho,V,\theta,\mathcal{D}} := (\mathcal{D}_W\otimes\mathbb{1}_Q)\circ\mathcal{U}_{V,\theta}\circ\mathcal{A}_\rho$ is a loss process with $\mathcal{D}_W(...) = W(t)(...)W^\dagger(t)$ and $\mathcal{R}_V := \mathcal{J}_S\circ\mathcal{U}^\dagger_{V,\theta}$ is a recovery process.

As a natural consequence, we can come by a universal lower bound as $\eta(\rho,W,\mathcal{D}) \leq C_T(t)$ and the WAY theorem for the OTOC. It is noteworthy that Theorem 2 can also be extended to the case where W is a self-adjoint operator and this IEP works as an experimental evaluation method for the OTOC. Although most of existing methods [61–71] require a number of measurements at each time point during the time evolution in whole system with several prepared measuring devices, our method only requires a single measuring device for measuring Q at the end of the process. In this regard, our method has the advantages of measuring at one point, simplifying the setup and being easy to implement.

4 Conclusions

The fact—the error and disturbance of a quantum measurement can be formulated as the irreversibility—means that we can use the accumulated knowledge about irreversibility in physics to evaluate the performance of quantum processes. Furthermore, it can be used for various physical processes and some sort of quantities in their frameworks as the irreversibility beyond the error, disturbance, and OTOC. It pave the way for applying quantum information processing tasks, and their further advancements are promising. Also, we have room to generalize the following degrees of freedom used in our formulation: the irreversibility measure $\delta(\mathcal{L},\Omega)$, the specific test ensemble $\Omega_{1/2,\pm}$, the qubit system Q, and the unitary process $\mathcal{U}_{X,\theta}$. We intend to leave these aspects for the future work.

References

[1] W. Heisenberg, Z. Phys. **43**, 172– (1927).

[2] E. Arthurs and J. L. Kelly jr, Bell Syst. Tech. J. **44**, 725 (1965).

[3] Y. Yamamoto and H. A. Haus, Rev. Mod. Phys. **58**, 1001 (1986).

[4] E. Arthurs and M. S. Goodman, Phys. Rev. Lett. **60**, 2447 (1988).

[5] S. Ishikawa, Rep. Math. Phys. **29**, 257 (1991).

[6] M. Ozawa, in *Quantum Aspects of Optical Communications*, edited by C. Bendjaballah, O. Hirota, and S. Reynaud (Springer, Heidelberg, Berlin, 1991) pp. 1–17.

[7] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).

[8] M. Ozawa, Ann. Phys. (N.Y.) **311**, 350 (2004).

[9] M. Ozawa, npj Quantum Inf. **5**, 1 (2019).

[10] M. Ozawa, arXiv:2104.11909 (2021).

[11] Y. Watanabe, T. Sagawa, and M. Ueda, Phys. Rev. A **84**, 042121 (2011).

[12] Y. Watanabe and M. Ueda, arXiv:1106.2526 (2011).

[13] P. Busch, P. Lahti, and R. F. Werner, Phys. Rev. Lett. **111**, 160405 (2013).

[14] P. Busch, P. Lahti, and R. F. Werner, Phys. Rev. A **89**, 012129 (2014).

[15] P. Busch, P. Lahti, and R. F. Werner, Rev. Mod. Phys. **86**, 1261 (2014).

[16] J. Lee and I. Tsutsui, arXiv:2002.04008 (2020).

[17] J. Lee and I. Tsutsui, Entropy **22**, 1222 (2020).

[18] J. Lee, arXiv:2204.11814 (2022).

[19] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008).

[20] E. P. Wigner, Z. Physik **133**, 101 (1952).

[21] H. Araki and M. M. Yanase, Phys. Rev. **120**, 622 (1960).

[22] A. I. Larkin and Y. N. Ovchinnikov, Sov. J. Exp. Theor. Phys. **28**, 1200 (1969).

[23] J. Maldacena, S. H. Shenker, and D. Stanford, J. High Energy Phys. **2016** (08), 106.

[24] H. Tajima, R. Takagi, and Y. Kuramochi, arXiv:2206.11086 (2022).

[25] M. Tomamichel, *A framework for non-asymptotic quantum information theory*, Phd thesis, ETH Zurich (2012), arXiv:1203.2142.

[26] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[27] M. Ozawa, J. Opt. B: Quantum Semiclass. Opt. **7**, S672 (2005).

[28] M. Ozawa, Phys. Rev. Lett. **88**, 050402 (2002).

[29] K. Korzekwa, Resource theory of asymmetry (2013).

[30] I. Marvian and R. W. Spekkens, arXiv:1212.3378 (2012).

[31] M. Ahmadi, D. Jennings, and T. Rudolph, New J. Phys. **15**, 013057 (2013).

[32] H. Tajima and H. Nagaoka, arXiv:1909.02904 (2019).

[33] Y. Kuramochi and H. Tajima, arXiv:2208.13494 (2022).

[34] M. H. Mohammady, T. Miyadera, and L. Loveridge, Quantum **7**, 1033 (2023).

[35] F. Hansen, Proc. Natl. Acad. Sci. U.S.A. **105**, 9909 (2008).

[36] I. Marvian, *Symmetry, Asymmetry and Quantum Information*, Phd thesis, University of Waterloo (2013).

[37] C. Zhang, B. Yadin, Z.-B. Hou, H. Cao, B.-H. Liu, Y.-F. Huang, R. Maity, V. Vedral, C.-F. Li, G.-C. Guo, and D. Girolami, Phys. Rev. A **96**, 042327 (2017).

[38] R. Takagi, Sci. Rep. **9**, 14562 (2019).

[39] I. Marvian, Nat. Commun. **11**, 25 (2020).

[40] K. Yamaguchi and H. Tajima, arXiv:2204.08439 (2022).

[41] I. Marvian, Phys. Rev. Lett. **129**, 190502 (2022).

[42] K. Yamaguchi and H. Tajima, Quantum **7**, 1012 (2023).

[43] D. Kudo and H. Tajima, Phys. Rev. A **107**, 062418 (2023).

[44] S. L. Luo, Theor. Math. Phys. **143**, 681– (2005).

[45] S. Yu, arXiv:1302.5311 (2013).

[46] M. Ozawa, Phys. Rev. Lett. **89**, 057902 (2002).

[47] H. Tajima, N. Shiraishi, and K. Saito, Phys. Rev. Lett. **121**, 110403 (2018).

[48] H. Tajima, N. Shiraishi, and K. Saito, Phys. Rev. Res. **2**, 043374 (2020).

[49] H. Tajima and K. Saito, arXiv:2103.01876 (2021).

[50] P. Hayden and J. Preskill, J. High Energy Phys. **2007** (09), 120.

[51] Y. Sekino and L. Susskind, J. High Energy Phys. **2008** (10), 065.

[52] S. H. Shenker and D. Stanford, J. High Energy Phys. **2014** (03), 067.

[53] S. H. Shenker and D. Stanford, J. High Energy Phys. **2015** (05), 132.

[54] I. L. Aleiner, L. Faoro, and L. B. Ioffe, Ann. Phys. (Amsterdam) **375**, 378 (2016).

[55] D. A. Roberts and B. Yoshida, J. High Energy Phys. **2017** (04), 121.

[56] C. W. von Keyserlingk, T. Rakovszky, F. Pollmann, and S. L. Sondhi, Phys. Rev. X **8**, 021013 (2018).

[57] A. Nahum, S. Vijay, and J. Haah, Phys. Rev. X **8**, 021014 (2018).

[58] T. Rakovszky, F. Pollmann, and C. W. von Keyserlingk, Phys. Rev. X **8**, 031058 (2018).

[59] M. Ozawa, Phys. Lett. A **335**, 11 (2005).

[60] M. Ozawa, Ann. Phys. (N.Y.) **321**, 744 (2006).

[61] B. Swingle, G. Bentsen, M. Schleier-Smith, and P. Hayden, Phys. Rev. A **94**, 040302(R) (2016).

[62] G. Zhu, M. Hafezi, and T. Grover, Phys. Rev. A **94**, 062329 (2016).

[63] N. Y. Yao, F. Grusdt, B. Swingle, M. D. Lukin, D. M. Stamper-Kurn, J. E. Moore, and E. A. Demler, arXiv:1607.01801 (2016).

[64] N. Yunger Halpern, Phys. Rev. A **95**, 012120 (2017).

[65] J. Dressel, J. R. González Alonso, M. Waegell, and N. Yunger Halpern, Phys. Rev. A **98**, 012132 (2018).

[66] M. Campisi and J. Goold, Phys. Rev. E **95**, 062127 (2017).

[67] R. Fan, P. Zhang, H. Shen, and H. Zhai, Sci. Bull. **62**, 707 (2017).

[68] K. X. Wei, C. Ramanathan, and P. Cappellaro, Phys. Rev. Lett. **120**, 070501 (2018).

[69] B. Yoshida and N. Y. Yao, Phys. Rev. X **9**, 011006 (2019).

[70] B. Vermersch, A. Elben, L. M. Sieberer, N. Y. Yao, and P. Zoller, Phys. Rev. X **9**, 021061 (2019).

[71] E. Lantagne-Hurtubise, S. Plugge, O. Can, and M. Franz, Phys. Rev. Res. **2**, 013254 (2020).

Hybrid squeezed cat code with universal gate set for easy implementation by optics

Shohei Kiryu[1] * Atsushi Okamoto[1] † Akihisa Tomita[1] ‡

[1] *Hokkaido University, Sapporo 060-0808, Japan*

Abstract. Currently, bosonic codes, such as the cat code and GKP code, have been extensively investigated to realize fault-tolerant photonic quantum computers, due to their resilience to loss. We propose a novel hybrid code that combines the squeezed cat code and polarization qubit. We demonstrate a straightforward construction of the universal gate set with the proposed hybrid code. Moreover, the hybrid squeezed cat code yields a higher success probability of Bell state measurement than the conventional hybrid cat code.

Keywords: bosonic code, squeezed cat code

1 introduction

Bosonic codes have recently attracted attention toward the realization of error-tolerant optical quantum computers, due to their tolerance to errors. Bosonic codes encode single-mode of light or multimode into qubits, and several codes have been proposed that use different quantum states of light, such as the cat code [1], the Gottesman-Kitaev-Preskill (GKP) code [2], the squeeze cat code [3, 4, 5] are known. The bosonic code is expected to be applied not only to quantum computation but also to quantum information technology such as quantum communication and quantum sensing.

Recently hybrid bosonic codes combining with different bosonic codes or photon states have been developed to improve performances of the codes. In particular, it has been shown that a hybrid qubit [6, 7, 8] of photon and cat state, which are known to have complementary properties, can compensate for the shortcomings of both to some extent. However, the performances of the hybrid cat code are still not enough to construct a fault-tolerant quantum computer. Moreover, it is complicate to implement a universal gate set with the hybrid cat code.

In this paper, we improve the performances of a novel hybrid code based on the squeezed cat code and the polarization qubit[9, 10] to overcome the limitations on the conventional hybrid cat code.

2 Squeezed cat code

The cat code is defined as the following superposition of the coherent states $|\alpha\rangle$ and $|-\alpha\rangle$,

$$|\mathcal{C}_\alpha^\pm\rangle = \frac{1}{\mathcal{N}_\alpha^\pm}(|\alpha\rangle \pm |-\alpha\rangle) \ , \tag{1}$$

where $\mathcal{N}_\alpha^\pm$ are the normalization constant and is given by

$$\mathcal{N}_\alpha^\pm = \sqrt{2(1 \pm e^{-2\alpha^2})} \ .$$

the cat code is tolerant of dephasing error. On the other hand, the cat code is vulnerable to a single photon loss, because it causes the phase inversion in eq.(1), which converts $|\mathcal{C}_\alpha^+\rangle$ to $|\mathcal{C}_\alpha^-\rangle$ and vice versa. This error is uncorrectable, because a state is transformed to the one in the code space.

The coherent squeezed state is obtained for the displacement operation performed after the squeezing operation to the vacuum state,

$$|\alpha, \xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)\,|0\rangle \ ,$$

where $\hat{D}(\alpha)$ is the displacement operator and $\hat{S}(\xi)$ is the squeeze operator, defined as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$$

$$\hat{S}(\xi) = e^{\frac{1}{2}(\xi^*\hat{a}^2 - \xi(\hat{a}^\dagger)^2)} \ .$$

The superposition of coherent squeezed states defines a squeezed cat code as follows

$$|\mathcal{C}_{\alpha,\xi}^\pm\rangle = \frac{1}{\mathcal{N}_{\alpha,\xi}^\pm}(|\alpha, \xi\rangle \pm |-\alpha, \xi\rangle) \ , \tag{2}$$

where $\mathcal{N}_{\alpha,\xi}^\pm$ are the normalization constants. When single photon loss described with the annihilation operator $\hat{a}$ occurs, the squeezed cat code is transformed as follows:

$$\hat{a}\,|\mathcal{C}_{\alpha,\xi}^\pm\rangle = c\,|\mathcal{C}_{\alpha,\xi}^\mp\rangle + d\,|\tilde{\mathcal{C}}_{\alpha,\xi}^\pm\rangle \ ,$$

Here c and d are constants, where $|\tilde{\mathcal{C}}_{\alpha,\xi}^\pm\rangle$ are defined as states in the space orthogonal to the code space. Therefore, the state $\hat{a}\,|\mathcal{C}_{\alpha,\xi}^\pm\rangle$ with single photon loss will span the sign space and orthogonal error space. This implies that the state $|\tilde{\mathcal{C}}_{\alpha,\xi}^\pm\rangle$ is not an eigenstate of $\hat{a}$, and complete bit flipping does not occur even with single photon loss. This indicates that the squeezed cat code is partially tolerant is the single photon loss. It has also been pointed out that the Knill-Lalamme error correction condition may be satisfied to of both dephasing error and single photon loss[4].

3 Hybrid squeezed cat code

A hybrid cat (H-cat) code, which combines a cat code and polarization state, is defined as follows

$$|0\rangle = |+\rangle\,|\mathcal{C}_\alpha^+\rangle$$

*kiryu.kiryu.u6@elms.hokudai.ac.jp
†ao@optnet.ist.hokudai.ac.jp
‡tomita@ist.hokudai.ac.jp

$$|1\rangle = |-\rangle |\mathcal{C}_\alpha^-\rangle \ ,$$

where $|\pm\rangle$ is the superposition state of polarization states $|H\rangle$ and $|V\rangle$ as

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle) \ .$$

Unlike cat codes, H-cat codes can detect single photon loss. When single photon loss occurs in the H-cat code, the state is transformed to

$$\hat{a}\,|+\rangle |\mathcal{C}_\alpha^+\rangle = |+\rangle |\mathcal{C}_\alpha^-\rangle \neq |-\rangle |\mathcal{C}_\alpha^-\rangle \ ,$$

This is because the polarization state does not change under the photon loss. Since the $|+\rangle$ and $|-\rangle$ of polarization are orthogonal to each other the error can be detected. Note that, however, the error in the cat state is detectable only if there is no loss in polarization state. Since the squeezed cat code is tolerant to the single photon loss, we propose a hybrid squeezed cat code to improve resilience against the loss.

The hybrid squeezed cat code (H-SC code) is defined as follows

$$|0_L\rangle = |+\rangle |\mathcal{C}_{\alpha,\xi}^+\rangle \tag{3}$$

$$|1_L\rangle = |-\rangle |\mathcal{C}_{\alpha,\xi}^-\rangle \tag{4}$$

In the following, we consider the practicality of the H-SC code. First we describe the gate operation of the H-SC code. The X gate can be realized by rotating the polarization by $\pi/2$ and applying $iD(i\frac{\pi}{4\xi})$ to the squeezed cat code. The Z gate can be realized by applying the transformation $|+\rangle + |-\rangle \rightarrow |+\rangle + e^{i\theta}|-\rangle$ to the polarized qubit. These can be implemented with the optical system shown in the figure1. Hadamard gate(H gate) and control-not(CNOT) gate can be implemented by gate teleportation with the entangled states $|\psi_H\rangle \propto |0_L,0_L\rangle + |0_L,1_L\rangle + |1_L,0_L\rangle - |1_L,1_L\rangle$ and $|\psi_{CNOT}\rangle \propto |0_L,0_L,0_L,0_L\rangle + |0_L,0_L,1_L,1_L\rangle + |1_L,1_L,0_L,0_L\rangle - |1_L,1_L,1_L,1_L\rangle$, respectively. The gate operations can be done by entanglement generation with these and bell measurement. The state $|0_L,0_L,0_L,0_L\rangle$ refers to $|0_L\rangle|0_L\rangle|0_L\rangle|0_L\rangle$ and so on. The Z gate can be implemented with the H-SC code much easier than with a non-hybrid squeezed cat code, where the Z gate can be implemented by the operation $e^{i\pi\hat{a}^\dagger\hat{a}}$[5]. It requires impractically large optical nonlinearity to turn the phase π by one photon.

4 Hybrid Bell measurement

Implementing the H gate and CNOT gate of the H-SC code with optics requires a circuit shown in Figure2, where Bell measurements for both the squeezed cat code and the polarized state should be performed. A gate operation is possible done by applying unitary transformations according to the results of the bell measurement of the squeezed cat code and the polarization qubit. We show that the Bell measurements on the squeezed cat code are made with a half beam splitter (HBS) and photon number detection. When the squeezed coherent

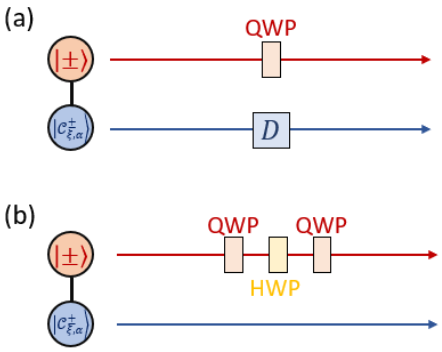


Figure 1: (a)The optical system that executes the X gate. It can be implemented by the quater waveplate(QWP) and Displacement operators. (b)The optical system that executes the Z gate. It can be implemented by QWP and half waveplate(HWP).

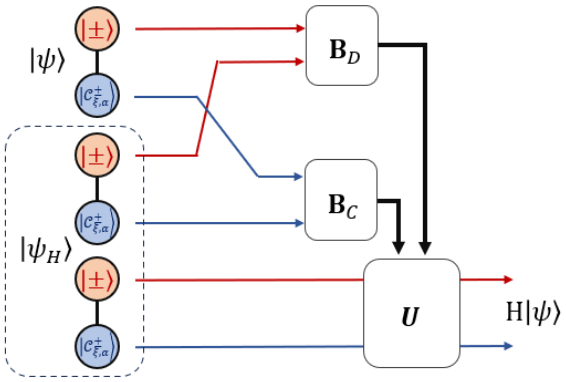


Figure 2: H gate implementation of hybrid squeezed cat code. where B_C is the bell measurement of the squeezed cat codes and B_D is the bell measurement of the polarization state.

states $|\alpha,\xi\rangle$ and $|\beta,\xi\rangle$ are inputs to the HBS, the output state is as follows:

$$\begin{aligned}&\hat{B}_{HBS}\hat{D}_1(\alpha)\hat{D}_2(\beta)\hat{S}_1(\xi)\hat{S}_2(\xi)\,|0\rangle_1\,|0\rangle_2 \\ &= |\frac{1}{\sqrt{2}}(\alpha+\beta),\xi\rangle_1\ |\frac{1}{\sqrt{2}}(-\alpha+\beta),\xi\rangle_2\end{aligned} \tag{5}$$

Using the above relation, we obtain the output states when the Bell state s in the SC code are input to the HBS.

$$\begin{aligned}|\tilde{\phi}_+\rangle &\rightarrow |even\rangle\,|0,\xi\rangle \\ |\tilde{\phi}_-\rangle &\rightarrow |odd\rangle\,|0,\xi\rangle \\ |\tilde{\psi}_+\rangle &\rightarrow |0,\xi\rangle\,|even\rangle \\ |\tilde{\psi}_-\rangle &\rightarrow |0,\xi\rangle\,|odd\rangle\end{aligned}$$

If $\xi = 0$, the Bell measurement is possible by measuring the number of photons in the output state. On the other hand, if $\xi \neq 0$, the squeezed vacuum state $|0,\xi\rangle$ is an even-photon state, thus $|\tilde{\phi}_+\rangle$ and $|\tilde{\psi}_+\rangle$ cannot be distinguished. However, since the Bell measurement of polarization state can distinguish $|\tilde{\psi}_+\rangle$ and $|\tilde{\psi}_-\rangle$, the H-SC code is near deterministic in the Bell measurement. It

is not completely deterministic, because the SC states are not orthogonal. The finite overlap of the states probabilistically results in the output states $|0\rangle |even\rangle$ or $|0\rangle |0\rangle$. In this case, $|\tilde{\phi}_+\rangle$ and $|\tilde{\phi}_-\rangle$ cannot be distinguished and the gate operation fails. The failure probability is as follows:

$$P_f = \frac{1}{2\sqrt{\cosh \xi}} \exp\left\{ \frac{-\alpha^2 + \frac{\alpha^2 \sinh \xi}{\cosh \xi}}{2} \right\}. \quad (6)$$

The success probability $1-P_f$, is shown in Figure3. Here, the success probability of Bell measurement for the H-cat code[7] is plotted in the blue dotted line for comparison, indicating that the H-SC code has a higher success probability of Bell measurement than the H-cat code. As the

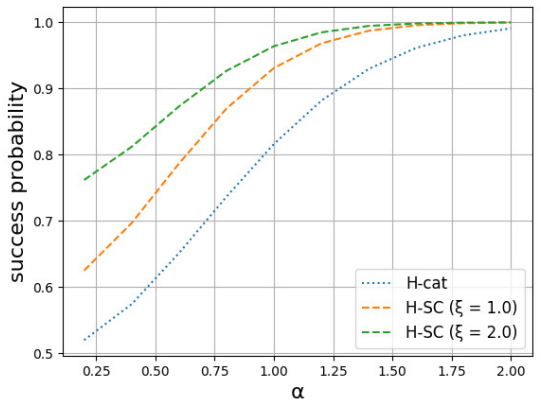


Figure 3: Success probability of Bell measurement of squeezed coherent state and hybrid cat code. This success probability is equivalent to the success probability of the H gate.

amplitude α or the squeezing parameter ξ increases, the success probability of the Bell measurement increases.

5 Conclusions

This paper proposes a hybrid squeezed cat (H-SC) code and its universal gate set construction. Furthermore, we proposed an implementation of the hybrid Bell measurement for the H-SC code, and compared its success probability with that for H-cat code, where both code require Bell measurement to implement H gate and CNOT gate. We showed that the success probability of the H-SC code is higher than that of the conventional H-cat code. This means that the H-SC code can perform these gate operations with higher probability than the H-cat code. The ability to Bell measurement with a high success probability at small amplitudes is a significant advantage because it is difficult to generate a large amplitude hybrid squeezed cat code with experimentally feasible generation method using linear optics and four photodetectors[11]. Future work will focus on determining the state generation efficiency and the logic error probability when encoded with quantum error correction codes.

6 acknowledgments

I would like to thank Kosuke Fukui for useful discussions.

References

[1] P. T. Cochrane, G. J. Milburn, and W. J. Munro. Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping. *Phys. Rev. A*, 59:2631–2634, 1999.

[2] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A*, 64:012310, 2001.

[3] David S. Schlegel, Fabrizio Minganti, and Vincenzo Savona. Quantum error correction using squeezed schrödinger cat states. *Phys. Rev. A*, 106:022431, 2022.

[4] Qian Xu, Guo Zheng, Yu-Xin Wang, Peter Zoller, Aashish A. Clerk, and Liang Jiang. Autonomous quantum error correction and fault-tolerant quantum computation with squeezed cat qubits, 2022.

[5] Suguru Endo, Keitaro Anai, Yuichiro Matsuzaki, Yuuki Tokunaga, and Yasunari Suzuki. Projective squeezing for translation symmetric bosonic codes, 2024.

[6] H. Jeong, M. S. Kim, and Jinhyoung Lee. Quantum-information processing for a coherent superposition state via a mixedentangled coherent channel. *Phys. Rev. A*, 64:052308, 2001.

[7] Seung-Woo Lee and Hyunseok Jeong. Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits. *Phys. Rev. A*, 87:022326, 2013.

[8] Jaehak Lee, Nuri Kang, Seok-Hyung Lee, Hyunseok Jeong, Liang Jiang, and Seung-Woo Lee. Fault-tolerant quantum computation by hybrid qubits with bosonic cat-code and single photons, 2023.

[9] Jennifer L. Dodd, Timothy C. Ralph, and G. J. Milburn. Experimental requirements for grover's algorithm in optical quantum computation. *Phys. Rev. A*, 68:042328, 2003.

[10] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[11] Hyukjoon Kwon and Hyunseok Jeong. Generation of hybrid entanglement between a single-photon polarization qubit and a coherent state. *Phys. Rev. A*, 91:012340, 2015.

On computational complexity and average-case hardness of shallow-depth boson sampling

Byeongseon Go[1] Changhun Oh[2] * Hyunseok Jeong[1] †

[1] *Department of Physics and Astronomy, Seoul National University, 08826 Seoul, Republic of Korea*
[2] *Department of Physics, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*

Abstract. Boson sampling is expected to be a promising approach toward quantum computational advantage. However, experimental noises render boson sampling classically simulable, revealing a susceptibility to classical simulation as noise rates increase with circuit depth. Here, we investigate the viability of achieving quantum advantage through boson sampling with shallow-depth linear optical circuits. As the average-case hardness of estimating output probabilities of boson sampling is a crucial ingredient in demonstrating its classical intractability, we make progress on establishing the average-case hardness confined to logarithmic-depth regimes. We also extend our result to Gaussian boson sampling and boson sampling subject to a lossy environment.

Keywords: Boson sampling, Quantum advantage, Quantum computation, Quantum simulation

1 Introduction

Boson sampling is a computational task that is complexity-theoretically proven to be hard to classically simulate under plausible assumptions [1–3]. Accordingly, boson sampling becomes a prominent candidate for experimentally demonstrating quantum computational advantage using near-term quantum devices. However, the experimental implementation of boson sampling with near-term devices is inevitably subject to various sources of noise [4–7], which would possibly rule out the classical intractability of boson sampling. Numerous studies [8–19] have proposed efficient classical simulation algorithms of boson sampling under physical noise models such as photon loss and partial distinguishability noise; Those results indicate that increasing noise rate eventually renders the noisy sampler classically simulable. Moreover, current implementations are expected to suffer from exponentially enlarged noise with circuit depth, which implies that circuits with polynomially increasing depth with system size would face substantial challenges to achieving quantum advantage.

A viable alternative to preclude the classical simulability due to the inevitable noise is to consider boson sampling with *shallow-depth* linear optical circuits, where the noise rate can be highly reduced. Specifically, among the shallow-depth regime, our primary focus is on investigating the simulation hardness for *logarithmic* depth circuits; the intuition behind investigating logarithmic depth circuits lies in the potential to offer a "sweet-spot" regime for the hardness of boson sampling. Namely, this depth regime may avoid significant increases in noise rates to prevent classical simulability, while still being sufficiently large to generate quantum correlations and uphold simulation hardness.

In this work, we investigate the classical simulation hardness of boson sampling in shallow linear optical circuits. Specifically, as the average-case #P-hardness of estimating output probabilities of boson sampling is a crucial ingredient to demonstrate the classical intractability of boson sampling, we make progress on establishing the average-case #P-hardness confined in shallow-depth regimes. We also extend our result to the Gaussian boson sampling scheme and noisy boson sampling subject to a lossy environment. We expect that our hardness results will provide a first step toward the full demonstration of the classical intractability of shallow-depth boson sampling.

2 Average-case hardness of shallow-depth boson sampling

In this section, we informally sketch our main results about the average-case hardness of shallow-depth boson sampling; for more details, one can check the results in [20]. To show the overall hardness results in logarithmic-depth regime, we consider a specific logarithmic-depth circuit architecture $(\mathcal{B}\mathcal{B}^*)^q$, which is a $q = O(1)$ number of iteration of $O(\log N)$ depth circuit unit $\mathcal{B}$ and $\mathcal{B}^*$ illustrated in Fig. 1.

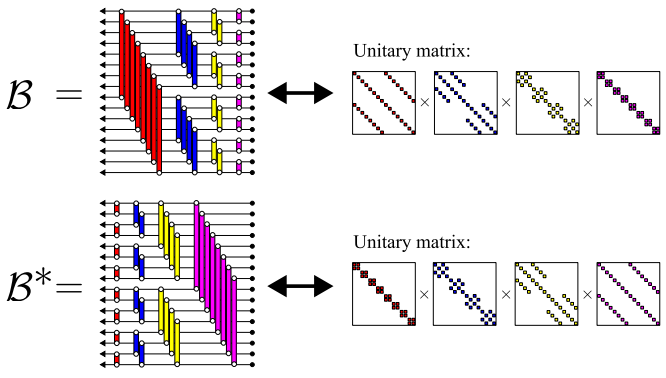


Figure 1: Schematics of the circuit architectures $\mathcal{B}$ and $\mathcal{B}^*$ and their unitary matrix form, for mode number $M = 2^4 = 16$.

Our main strategy to show the average-case hardness

*changhun0218@gmail.com
†h.jeong37@gmail.com

is (i) to show the worst-case #P-hardness and (ii) to establish worst-to-average-case reduction. Specifically, for Fock state input with photon number N and mode number $M \propto N^\gamma$ with $\gamma \geq 1$, we first show the worst-case hardness of approximating a fixed output probability of boson sampling with circuit architecture $(\mathcal{BB}^*)^q$ for $q \geq 1$ as below.

Theorem 1 (Worst-case hardness) *Approximating a fixed output probability of boson sampling to within additive error $2^{-O(N)}$ for any circuit over $(\mathcal{BB}^*)^{q\geq 1}$ is #P-hard in the worst case.*

Next, we prove the average-case hardness over *both* the randomly chosen outcome and randomly chosen circuit, by establishing a worst-to-average-case reduction. In other words, we prove that if we can well-approximate the output probability *on average* over outcomes and circuits, we can also well-approximate the worst-case output probability in Theorem 1.

Theorem 2 (Average-case hardness) *Approximating output probability of boson sampling to within additive error $2^{-O(N^{\gamma+1}(\log N)^2)}$ with high probability over randomly chosen circuits in $(\mathcal{BB}^*)^{q\geq 2}$ for high probability over randomly chosen collision-free outcomes is #P-hard under $\mathrm{BPP}^{\mathrm{NP}}$ reduction.*

Also, since our average-case hardness result considers both the random outcomes and random circuits, it is not straightforward to show the classical simulation hardness of shallow-depth boson sampling as in the original boson sampling proposal [1]. Therefore, we show how our average-case hardness result over both the randomly chosen outcomes and circuits is related to the classical simulation hardness argument. Specifically, we show that improving the allowed additive imprecision of Theorem 2 leads to the classical intractability of shallow-depth boson sampling.

Theorem 3 *If the allowed additive imprecision for the problem in Theorem 2 to be #P-hard is improved to $2^{-(\gamma-1)N\log N - O(N)}$, then the shallow-depth boson sampling in $(\mathcal{BB}^*)^{q\geq 2}$ is classically hard to simulate.*

Similarly to the above results, we also obtain hardness results for Gaussian boson sampling scheme. Specifically, we show the average-case hardness of Gaussian boson sampling, for M squeezed vacuum input and average-photon number N with $M \propto N^\gamma$ and $\gamma \geq 1$.

Theorem 4 *Approximating output probability of Gaussian boson sampling to within additive error $2^{-O(N^{\gamma+1}(\log N)^2)}$ with high probability over randomly chosen circuits in $(\mathcal{BB}^*)^{q\geq 2}$ for high probability over randomly chosen collision-free outcomes is #P-hard under $\mathrm{BPP}^{\mathrm{NP}}$ reduction.*

Lastly, we extend our average-case hardness result in Theorem 2 to noisy boson sampling case subject to photon loss channel. Specifically, we show that Theorem 2 still holds even for lossy boson sampling, with photon loss channel acts on each mode after each gate is applied in the circuit.

Corollary 5 *Suppose we have the photon loss model $\mathcal{N}$ acting on each mode after each gate, with each loss rate $\rho_i \leq \rho$ for a constant ρ. Then, approximating output probability of lossy boson sampling to within additive error $2^{-O(N^{\gamma+1}(\log N)^2)}$ with high probability over randomly chosen circuits in $(\mathcal{BB}^*)^{q\geq 2}$ for high probability over randomly chosen collision-free outcomes is #P-hard under $\mathrm{BPP}^{\mathrm{NP}}$ reduction.*

Our overall result is illustrated in Fig. 2. By successive reductions, we have shown average-case hardness of shallow-depth boson sampling for the additive imprecision level $2^{-O(N^{\gamma+1}(\log N)^2)}$. We have also shown that if the imprecision level can be improved to $2^{-(\gamma-1)N\log N - O(N)}$ then shallow-depth boson sampling is classically hard to simulate. Therefore, we can conclude that closing this imprecision gap is the only remaining problem for the fully theoretically guaranteed classical intractability of shallow-depth boson sampling.

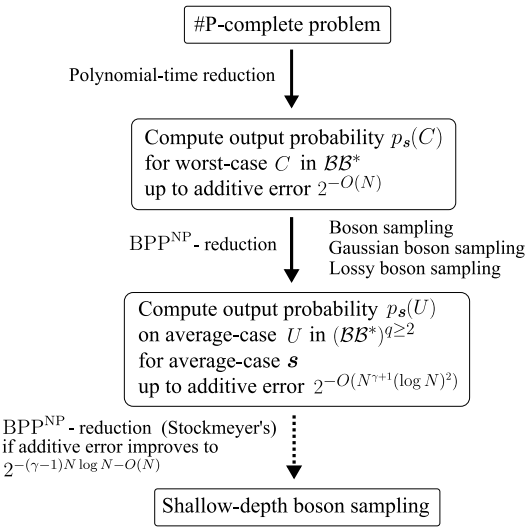


Figure 2: Outlines of our result

3 Discussions

To achieve the experimental demonstration of quantum computational advantage with boson sampling, it is crucial to reduce the noise effects, and shallow-depth circuits are a viable choice for reducing the noise effects. Accordingly, we showed the average-case #P-hardness of approximating output probabilities of shallow-depth boson sampling to within additive imprecision $2^{-O(N^{\gamma+1}(\log N)^2)}$ in a certain logarithmic-depth circuit architecture. We extended our average-case hardness result to Gaussian boson sampling scheme, and noisy boson sampling subject to photon loss channels. We showed how our average-case hardness results over both the randomly chosen outcomes and circuits is related to the classical simulation hardness argument, which implies that

improving the allowed imprecision for our hardness result is the only remaining challenge for the classical intractability of shallow-depth boson sampling.

To the best of our knowledge, the complexity-theoretical analysis on the average-case hardness of shallow-depth boson sampling has not yet been investigated. Hence, we expect that our hardness result in shallow-depth regimes will provide a first step toward a stronger hardness result and, ultimately, toward the complete demonstration of the classical intractability of shallow-depth boson sampling.

References

[1] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[2] Craig S Hamilton, Regina Kruse, Linda Sansoni, Sonja Barkhofen, Christine Silberhorn, and Igor Jex. Gaussian boson sampling. *Physical review letters*, 119(17):170501, 2017.

[3] Abhinav Deshpande, Arthur Mehta, Trevor Vincent, Nicolás Quesada, Marcel Hinsche, Marios Ioannou, Lars Madsen, Jonathan Lavoie, Haoyu Qi, Jens Eisert, et al. Quantum computational advantage via high-dimensional gaussian boson sampling. *Science advances*, 8(1):eabi7894, 2022.

[4] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[5] 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. *Physical review letters*, 127(18):180502, 2021.

[6] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[7] Yu-Hao Deng, Yi-Chao Gu, Hua-Liang Liu, Si-Qiu Gong, Hao Su, Zhi-Jiong Zhang, Hao-Yang Tang, Meng-Hao Jia, Jia-Min Xu, Ming-Cheng Chen, et al. Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage. *Physical review letters*, 131(15):150601, 2023.

[8] Jelmer Renema, Valery Shchesnovich, and Raul Garcia-Patron. Classical simulability of noisy boson sampling. *arXiv preprint arXiv:1809.01953*, 2018.

[9] Jelmer J Renema, Adrian Menssen, William R Clements, Gil Triginer, William S Kolthammer, and Ian A Walmsley. Efficient classical algorithm for boson sampling with partially distinguishable photons. *Physical review letters*, 120(22):220502, 2018.

[10] Valery S Shchesnovich. Noise in boson sampling and the threshold of efficient classical simulatability. *Physical Review A*, 100(1):012340, 2019.

[11] Alexandra E Moylett, Raúl García-Patrón, Jelmer J Renema, and Peter S Turner. Classically simulating near-term partially-distinguishable and lossy boson sampling. *Quantum Science and Technology*, 5(1):015001, 2019.

[12] Michał Oszmaniec and Daniel J Brod. Classical simulation of photonic linear optics with lost particles. *New Journal of Physics*, 20(9):092002, 2018.

[13] Raúl García-Patrón, Jelmer J Renema, and Valery Shchesnovich. Simulating boson sampling in lossy architectures. *Quantum*, 3:169, 2019.

[14] Haoyu Qi, Daniel J Brod, Nicolás Quesada, and Raúl García-Patrón. Regimes of classical simulability for noisy gaussian boson sampling. *Physical review letters*, 124(10):100502, 2020.

[15] Daniel Jost Brod and Michał Oszmaniec. Classical simulation of linear optics subject to nonuniform losses. *Quantum*, 4:267, 2020.

[16] Benjamin Villalonga, Murphy Yuezhen Niu, Li Li, Hartmut Neven, John C Platt, Vadim N Smelyanskiy, and Sergio Boixo. Efficient approximation of experimental gaussian boson sampling. *arXiv preprint arXiv:2109.11525*, 2021.

[17] Jacob FF Bulmer, Bryn A Bell, Rachel S Chadwick, Alex E Jones, Diana Moise, Alessandro Rigazzi, Jan Thorbecke, Utz-Uwe Haus, Thomas Van Vaerenbergh, Raj B Patel, et al. The boundary for quantum advantage in gaussian boson sampling. *Science advances*, 8(4):eabl9236, 2022.

[18] Changhun Oh, Liang Jiang, and Bill Fefferman. On classical simulation algorithms for noisy boson sampling. *arXiv preprint arXiv:2301.11532*, 2023.

[19] Changhun Oh, Minzhao Liu, Yuri Alexeev, Bill Fefferman, and Liang Jiang. Tensor network algorithm for simulating experimental gaussian boson sampling. *arXiv preprint arXiv:2306.03709*, 2023.

[20] Byeongseon Go, Changhun Oh, and Hyunseok Jeong. On computational complexity and average-case hardness of shallow-depth boson sampling. *arXiv preprint arXiv:2405.01786*, 2024.

On computational complexity and average-case hardness of shallow-depth boson sampling

Byeongseon Go,[1] Changhun Oh,[2,*] and Hyunseok Jeong[1,†]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Republic of Korea*
[2] *Department of Physics, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*

Boson sampling, a computational task believed to be classically hard to simulate, is expected to hold promise for demonstrating quantum computational advantage using near-term quantum devices. However, noise in experimental implementations poses a significant challenge, potentially rendering boson sampling classically simulable and compromising its classical intractability. Numerous studies have proposed classical algorithms under various noise models that can efficiently simulate boson sampling as noise rates increase with circuit depth. To address this issue particularly related to circuit depth, we explore the viability of achieving quantum computational advantage through boson sampling with shallow-depth linear optical circuits. Specifically, as the average-case hardness of estimating output probabilities of boson sampling is a crucial ingredient in demonstrating its classical intractability, we make progress on establishing the average-case hardness confined to logarithmic-depth regimes. We also obtain the average-case hardness for logarithmic-depth Fock-state boson sampling subject to lossy environments and for the logarithmic-depth Gaussian boson sampling. By providing complexity-theoretical backgrounds for the classical simulation hardness of logarithmic-depth boson sampling, we expect that our findings will mark a crucial step towards a more noise-tolerant demonstration of quantum advantage with shallow-depth boson sampling.

I. INTRODUCTION

Boson sampling is a computational task that is complexity-theoretically proven to be hard to classically simulate under plausible assumptions [1–3]. Accordingly, boson sampling has gathered significant attention, as it would possibly play a key role in the experimental demonstration of quantum computational advantage using near-term quantum devices. However, the implementation of boson sampling in experimental settings with near-term quantum devices is inevitably subject to various sources of noise [4–7]. The problem is that those noises would possibly rule out the classical intractability of boson sampling, and thus potentially hinder the experimental demonstration of quantum advantage with boson sampling. Indeed, both for finite-size near-term experiments and asymptotic limits as system size scales, numerous studies [8–19] have proposed efficient classical simulation algorithms of boson sampling under various noise models, such as photon loss, partial distinguishability, gaussian noise, etc. Their results indicate that as the noise rate of boson sampler increases, it eventually renders such a noisy sampler classically simulable. Moreover, as the noise is typically accumulated with each circuit depth, the quantum signal for classical intractability exhibits exponential decay with increasing circuit depth. Hence, circuits with polynomially increasing depth with system size would suffer from significantly enlarged noise rates, posing substantial challenges to achieving quantum advantage in such settings.

A viable alternative to preclude the classical simulability due to the inevitable noise is to consider boson sampling with *shallow-depth* linear optical circuits, where the noise rate can be highly reduced. Specifically, among the shallow-depth regime, our primary focus is on investigating the

* changhun0218@gmail.com
† h.jeong37@gmail.com

simulation hardness for *logarithmic* depth circuits; the intuition behind investigating logarithmic depth circuits lies in the potential to offer a "sweet-spot" regime for the hardness of boson sampling. Namely, this depth regime may avoid significant increases in noise rates to prevent classical simulability, while still being sufficiently large to generate quantum correlations and uphold simulation hardness. Despite such intuitive understanding, the hardness argument of boson sampling in this shallow-depth regime, particularly from a complexity-theoretical perspective, has been less studied so far and thus remains widely open. Hence, our goal is to establish the *complexity-theoretical foundations* of the classical hardness of shallow-depth boson sampling, to suppress the classical simulability by noise in a rigorous manner and obtain a more noise-tolerant demonstration of quantum advantage with boson sampling.

In this work, we investigate the classical simulation hardness of boson sampling in shallow linear optical circuits. Specifically, as the average-case #P-hardness of estimating output probabilities of boson sampling is a crucial ingredient to demonstrate the classical intractability of boson sampling, we make progress on establishing the average-case #P-hardness confined in shallow-depth regimes. Similarly, we obtain the average-case hardness result in the shallow-depth regime for the Gaussian boson sampling scheme. Finally, since noise is our main motivation for investigating shallow-depth boson sampling, we generalize our average-case hardness result to noisy boson sampling subject to a photon loss channel.

To avoid confusion, we note that the allowed imprecision level of our average-case #P-hardness result is not sufficient to fully demonstrate the classical intractability of boson sampling in shallow-depth regimes. However, to the best of our knowledge, the complexity-theoretical analysis on the average-case hardness of shallow-depth boson sampling has not yet been investigated. Hence, we believe that our hardness result in shallow-depth regimes will provide a first step toward a stronger hardness result and, ultimately, toward the full demonstration of the classical intractability of shallow-depth boson sampling.

A. Outlines: average-case hardness of shallow-depth boson sampling

We set our goal as proving the hardness of classical simulation of boson sampling in the shallow-depth regime, specifically for *approximate* simulation within total variation distance error. Two key ingredients for the current hardness proof of the approximate simulation of boson sampling are (*i*) average-case #P-hardness of output probability approximation up to sufficiently large additive imprecision ϵ, and (*ii*) hiding property. Informally, average-case hardness means that approximating the output probability of boson sampling with high probability over randomly chosen circuits (i.e., on average over circuits) is #P-hard. Here, by choosing random circuit instances that have the hiding property (i.e., symmetric over outcomes), one can reduce the average-case instances for the hardness from circuit instances to outcome instances, which is a crucial step to prove the hardness of approximate simulation within total variation distance error (See Appendix A for more details).

Most of the current theoretical foundations of the average-case hardness of boson sampling rely on global Haar random unitary circuits [1–3, 20–22], as they almost satisfy the two conditions described above. Namely, the outcome instances can be effectively hidden by global Haar random unitaries, and approximating the output probability within sufficiently large ϵ on average over global Haar random circuit instances is #P-hard under some conjectures. However, the problem is that implementing global Haar random unitary requires at least polynomial circuit depth (e.g., see [23, 24]), and thus not implementable in sub-polynomial circuit depths. Accordingly, the hardness results built upon global Haar random unitaries cannot be directly applied to the shallow-depth boson sampling we are interested in, necessitating a different approach from them.

Another problem is that there already exist efficient classical algorithms that can approximately simulate shallow-depth boson sampling in certain circumstances, which directly rule out the classical simulation hardness in shallow-depth for such cases. Although exact simulation of boson sampling is classically hard even for constant depth circuits [25], approximate simulation is easy for $1d$ local log depth circuits [26, 27] and also for more general dimension local circuits under some constraints [28, 29]. Specifically, according to their results, if we use circuits composed of only geometrically local gates, at least polynomial circuit depth is required for a sufficiently large correlation to obtain the approximate simulation hardness. Those results indicate that we cannot expect the hardness results in the most general case of shallow-depth circuits composed of local gates only.

To deal with those problems we take the following approach: first, we consider shallow linear optical circuit architectures composed of geometrically *non-local* gates. In fact, implementation of non-local gates is promising for near-term experimental settings; for example, experiments of linear optical systems based on trapped ions [30, 31] and photonic architecture [6] implemented long-range interactions. Also, since we cannot implement global Haar random unitary within shallow-depth regime, we instead employ local random circuit ensemble for random circuit instances in shallow circuit architecture, inspired by the hardness results of random circuit sampling [21, 32–35]. Here, local random distribution in this context means that each gate composing the circuit is independently chosen Haar random gate; we note that recent experimental setups of boson sampling [4–7] also follow such circuit distribution, but with geometrically local architectures.

However, local random distribution poses a subsequent challenge toward the average-case hardness of shallow-depth boson sampling, that is, the absence of the hiding property. Since the output symmetry of boson sampling over local random circuit distribution is not evident, the random outcome instances cannot be efficiently hidden by random circuit instances. This means that even if we find the average-case hardness over randomly chosen circuits for a fixed outcome, it still does not lead to the classical simulation hardness grounded in Stockmeyer's reduction from the average-case approximation over randomly chosen outcomes [1]. To address this issue, we prove the average-case hardness over *both* the randomly chosen outcome and randomly chosen circuit, by establishing a worst-to-average-case reduction for both outcome and circuit instances. Specifically, our reduction process is composed of two steps: (i) from a given fixed outcome to a randomly chosen collision-free outcome, and (ii) from a worst-case circuit to a randomly chosen circuit over local random circuit distribution.

To sum up, we show the average-case hardness over outcomes and circuit instances for shallow circuit architectures composed of non-local gates and employing the local random circuit ensemble. We informally present here our average-case hardness result of boson sampling in the logarithmic depth regime, for photon number N and mode number $M \propto N^{\gamma}$ with $\gamma \geq 1$.

Theorem 1 (Informal)**.** *There exists a $O(\log N)$-depth linear optical circuit architecture such that approximating output probability of boson sampling within additive error $2^{-O(N^{\gamma+1}(\log N)^2)}$ with high probability over randomly chosen circuits in the circuit architecture for high probability over randomly chosen collision-free outcomes is #P-hard under $\mathrm{BPP}^{\mathrm{NP}}$ reduction.*

Also, since our average-case hardness result considers both the random outcomes and random circuits due to the absence of the hiding property, it is not straightforward to show the classical simulation hardness of shallow-depth boson sampling as in the original boson sampling proposal [1]. Accordingly, we show how our average-case hardness result over both the randomly chosen outcomes and circuits leads to the classical simulation hardness argument. This implies that improving the additive imprecision for our average-case hardness result is the only remaining problem for the fully theoretically guaranteed classical intractability of shallow-depth boson sampling.

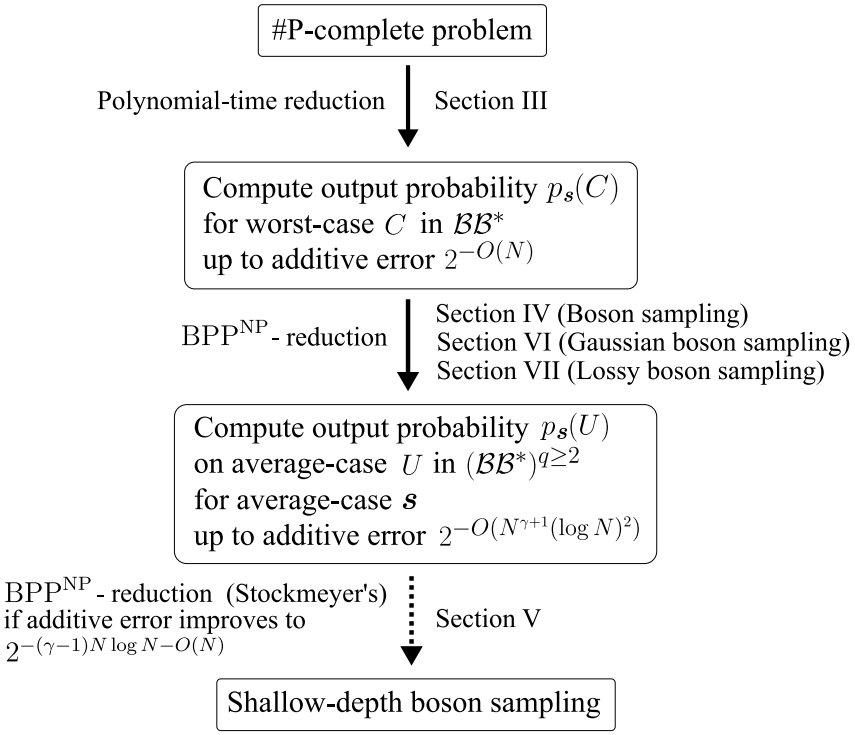


FIG. 1. Outlines of our result

Theorem 2 (Informal)**.** *If the allowed additive imprecision for the problem in Theorem 1 to be #P-hard is improved to $\epsilon = 2^{-(\gamma-1)N\log N-O(N)}$, the approximate boson sampling for the shallow-depth circuit in Theorem 1, up to constant total variation distance, is classically hard to simulate.*

Now we provide an outline of our results, which is depicted in Fig. 1. We first define in Sec. II a shallow-depth circuit architecture $(\mathcal{BB}^*)^q$ composed of non-local gates, which we will use throughout our results. Next, in Sec. III we prove the worst-case #P-hardness of approximating output probability $p_{\boldsymbol{s}}(C)$ of a fixed outcome $\boldsymbol{s}$ of boson sampling, for any circuit C in the shallow circuit architecture previously defined. In Sec. IV we prove the average-case #P-hardness of approximating output probability $p_{\boldsymbol{s}}(U)$ for randomly chosen outcome $\boldsymbol{s}$ and randomly chosen circuit U in the shallow circuit architecture, by establishing worst-to-average-case reduction. We prove in Sec. V how our average-case hardness results over both the random outcomes and random circuits lead to the classical simulation hardness. We also extend our average-case hardness result to the Gaussian boson sampling scheme in Sec. VI, and to the lossy boson sampling subject to photon loss channels in Sec. VII. In Sec. VIII, we conclude with several remarks.

II. NOTATIONS

Let us define the total mode number as M, where we set M as a power of 2 for simplicity. We set the output photon number N polynomially related to M as $M = c_0 N^\gamma$, for a constant c_0 and $\gamma \geq 1$ satisfying $M \geq 2N$. We use the notation $\boldsymbol{s}$ as an M-dimensional output configuration vector for the collision-free outcome, such that each element s_i of $\boldsymbol{s}$ denotes photon number in ith mode. Namely, $\boldsymbol{s} = (s_1, \ldots, s_M)$ where each $s_i \in \{0, 1\}$ with $\sum_{i=1}^{M} s_i = N$, so that the number of possible configurations of $\boldsymbol{s}$ is $\binom{M}{N}$. We define $p_{\boldsymbol{s}}(C)$ as an output probability of a linear optical circuit (unitary) matrix C for the outcome $\boldsymbol{s}$ from a predefined input configuration $\boldsymbol{t}$. For collision-free

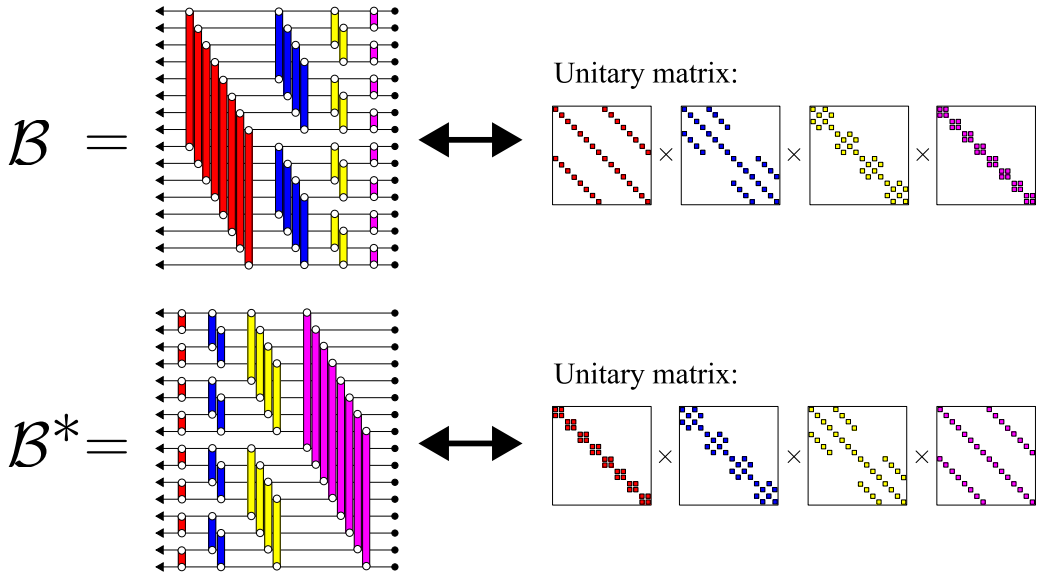


FIG. 2. Schematics of the butterfly circuit architectures in Definition 2 and their unitary matrix form, for mode number $M = 2^4 = 16$.

input and output, $p_{\boldsymbol{s}}(C)$ can be represented as [1]

$$p_{\boldsymbol{s}}(C) = |\mathrm{Per}(C_{\boldsymbol{s},\boldsymbol{t}})|^2 \tag{1}$$

where $C_{\boldsymbol{s},\boldsymbol{t}}$ is a N by N matrix obtained by taking s_i copies of the ith row and t_j copies of the jth column of the matrix C.

We note that an M-mode linear optical circuit can be represented by an M by M unitary matrix in $\mathrm{U}(M)$ which unitarily transforms M mode operators. Specifically, we can represent a single-mode gate (i.e., a phase shifter) as a $\mathrm{U}(1)$ matrix to the mode, and a two-mode gate (i.e., a beam splitter) as a $\mathrm{U}(2)$ matrix along the modes. Also, the parallel application of gates can be represented as a unitary matrix with a block matrix form, and the serial application of gates can be represented as matrix multiplication of the unitary matrices. Accordingly, throughout this work, we will interchangeably use the terminology '(linear optical) circuit' and '(unitary) matrix'.

We first define the linear optical circuit architecture, for a more rigorous analysis of the hardness proof.

Definition 1 (Linear optical circuit architecture)**.** *The linear optical circuit architecture $\mathcal{A}$ is a linear optical circuit with fixed type (i.e., single- or two-mode) and fixed location of gates, where the coefficients of each gate are not specified. If the coefficients of each gate are specified with unitary matrices (in* $\mathrm{U}(1)$ *or* $\mathrm{U}(2)$*), then the circuit and the corresponding unitary matrix are specified.*

For the shallow-depth circuit architecture, specifically in logarithmic depth, we define the shallow linear optical circuit architecture of circuit depth $D = \log M$, using the convention used in [36, 37].

Definition 2. *We define butterfly circuit architecture $\mathcal{B}$ as follows: for each layer $L = 1, 2, \ldots, D = \log M$ of the circuit architecture, allocate two-mode gate between mode number $2^L(j-1)+k$ and $2^L(j-1)+k+2^{L-1}$, for all $j = 1, 2, \ldots, 2^{D-L}$ and $k = 1, 2, \ldots, 2^{L-1}$. Also, we define inverse butterfly circuit architecture $\mathcal{B}^*$ as a butterfly circuit architecture with the inverse sequence of gate application along the depth.*

We illustrate in Fig. 2 the circuit architecture $\mathcal{B}$ and $\mathcal{B}^*$, and the form of their corresponding unitary matrix. Next, we define the Kaleidoscope circuit architecture proposed in [36], using the butterfly circuit architecture defined above.

Definition 3. *We define Kaleidoscope circuit architecture $\mathcal{B}\mathcal{B}^*$ as a serial application of $\mathcal{B}$ over $\mathcal{B}^*$. We also define q-Kaleidoscope circuit architecture $(\mathcal{B}\mathcal{B}^*)^q$ as a repeat of the Kaleidoscope circuit architecture, with repetition number $q \in \mathbb{N}$.*

Here, the circuit depth of q-Kaleidoscope architecture is $D = 2q \log M$, which is indeed a logarithmic depth in N for $q = O(1)$. Throughout this paper, we will focus on the q-Kaleidoscope circuit architecture with $q = O(1)$ to demonstrate the hardness results for shallow-depth circuits. One motivation for employing this linear optical circuit architecture is that it enjoys a useful property that is crucial for our analysis; Ref. [36] shows that for M a power of 2, any M mode permutation circuit can be implemented within $\mathcal{B}\mathcal{B}^*$.

Lemma 1 (Dao et al [36])**.** *Let $\boldsymbol{P}$ be an arbitrary $M \times M$ permutation matrix with M a power of 2. Then $\boldsymbol{P}$ can be efficiently implemented in $\mathcal{B}\mathcal{B}^*$ using two-mode permutation gates, i.e., $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.*

III. WORST-CASE HARDNESS OF OUTPUT PROBABILITY ESTIMATION

In this section, we find the worst-case #P-hardness of output probability estimation of shallow-depth linear optical circuits in $\mathcal{B}\mathcal{B}^*$, for a fixed input and output $\boldsymbol{s}$ within a certain additive imprecision. Our worst-case hardness result for the shallow circuit architecture can be represented as follows.

Theorem 3 (Worst-case hardness)**.** *For $M \geq 2N$, approximating the output probability $p_{\boldsymbol{s}}(C)$ to within additive error $2^{-O(N)}$ for any C over linear optical circuit architecture $\mathcal{B}\mathcal{B}^*$ is #P-hard in the worst case.*

We briefly sketch the proof of our worst-case hardness result for the shallow circuit architecture $\mathcal{B}\mathcal{B}^*$. The proof is based on the result by [25], which showed the simulation hardness of exact boson sampling with constant depth linear optical circuits. Specifically, there exist constant-depth linear optical circuits that can simulate an arbitrary given quantum circuit using post-selection. Also, those constant depth circuits can be embedded in our circuit architecture $\mathcal{B}\mathcal{B}^*$. Hence, additively approximating the output probability of any quantum circuit can be reduced to additively approximating the output probability of any circuit in $\mathcal{B}\mathcal{B}^*$, with imprecision blowup up to the inverse of post-selection probability. Using the fact that the additive approximation of any quantum circuit is #P-hard for certain additive imprecision [34], we can obtain the worst-case hardness of our shallow circuit architecture $\mathcal{B}\mathcal{B}^*$.

Proof of Theorem 3. See Appendix B. □

IV. AVERAGE-CASE HARDNESS OF OUTPUT PROBABILITY ESTIMATION

In this section, we prove the average-case #P-hardness of approximating output probabilities of shallow-depth boson sampling within a certain additive imprecision. We focus on q-Kaleidoscope circuit architecture $(\mathcal{B}\mathcal{B}^*)^q$ with $q = O(1)$, where the gate number m for such architecture is

$m = qM \log M$. From the result of Theorem 3, $(\mathcal{BB}^*)^q$ has the worst-case hardness of output probability approximation, for $q \geq 1$.

Our main strategy for the average-case hardness is the establishment of the worst-to-average-case reduction, using the result of Theorem 3. In other words, we prove that if we can well-approximate the output probability *on average*, we can also well-approximate the worst-case output probability in Theorem 3. Here, our average-case approximation regards both the randomly chosen outcome and the randomly chosen circuit, since we cannot rely on the hiding property that enables us to fix the outcome. For this reason, we define both the random circuit ensemble and the random outcome ensemble as follows.

Definition 4 (Random circuit ensemble)**.** *Let $\mathcal{A}$ be the circuit architecture with m number of gates. We define $\mathcal{H}_{\mathcal{A}}$ as the distribution over circuits with architecture $\mathcal{A}$, whose gates are independently distributed local Haar random matrices $\{H_i\}_{i=1}^m$.*

Definition 5 (Random collision-free outcome ensemble)**.** *We define $\mathcal{G}_{M,N}$ as the uniform distribution over $\binom{M}{N}$ collision-free outcomes of boson sampling with M modes and N photons. Each outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$ is an M-dimensional output configuration vector for the collision-free outcome, such that $\boldsymbol{s} = (s_1, \ldots, s_M)$ where each $s_i \in \{0, 1\}$ with $\sum_{i=1}^M s_i = N$.*

Using the definitions above, we first state our result on the average-case hardness over the outcome and circuit instances, for shallow-depth linear optical circuit architecture $(\mathcal{BB}^*)^{q \geq 2}$ with $q = O(1)$.

Theorem 4 (Average-case hardness)**.** *The following problem is #P-hard under a $\mathrm{BPP}^{\mathrm{NP}}$ reduction: for any constant $\delta, \eta \geq 0$ with $\delta + \eta < \frac{1}{4}$, on input a random circuit $U \sim \mathcal{H}_{\mathcal{A}}$ with $\mathcal{A} = (\mathcal{BB}^*)^{q \geq 2}$ and a random outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$, compute the output probability $p_{\boldsymbol{s}}(U)$ within additive imprecision $\epsilon = 2^{-O(N^{\gamma+1}(\log N)^2)}$, with probability at least $1 - \delta$ over the choice of U for at least $1 - \eta$ over the choice of $\boldsymbol{s}$.*

In the following, we sketch the proof of Theorem 4, by briefly describing the worst-to-average-case reduction process; we leave in Appendix C a detailed proof of Theorem 4. Since our average-case hardness regards both outcomes and circuits, we first describe how to effectively *fix* the outcome, so that the remaining problem is to establish worst-to-average-case reduction for fixed output probability over random circuit instances. To do so, our strategy is to randomly *permute* both a given worst-case circuit and a given fixed outcome. That is, we sample random M-mode permutation $\boldsymbol{P}$ and permute the worst-case circuit C_0 and the fixed outcome $\boldsymbol{s}_0$ equally with $\boldsymbol{P}$, where the permuted outcome $\boldsymbol{s} = \boldsymbol{P}\boldsymbol{s}_0$ now follows the random outcome ensemble $\mathcal{G}_{M,N}$. Then the fixed worst-case output probability $p_{\boldsymbol{s}_0}(C_0)$ is equal to $p_{\boldsymbol{s}}(\boldsymbol{P}C_0)$, and thus we can obtain the value $p_{\boldsymbol{s}_0}(C_0)$ by inferring $p_{\boldsymbol{s}}(\boldsymbol{P}C_0)$ via worst-to-average-case reduction over random circuit instances. Here, $p_{\boldsymbol{s}}(\boldsymbol{P}C_0)$ now becomes a new worst-case output probability, such that the revised worst-case circuit C is the randomly permuted circuit $\boldsymbol{P}C_0$, and the revised fixed outcome $\boldsymbol{s}$ is the randomly chosen outcome from $\mathcal{G}_{M,N}$.

To establish the worst-to-average-case reduction from the revised worst-case circuit C to the average-case circuit over $\mathcal{H}_{\mathcal{A}}$ for a fixed outcome $\boldsymbol{s}$, our strategy is to perturb the circuit from $\mathcal{H}_{\mathcal{A}}$ with the given worst-case circuit C parameterized by a constant $\theta \in [0, 1]$. That is, $\theta = 0$ corresponds to the average-case distribution $\mathcal{H}_{\mathcal{A}}$ and $\theta = 1$ corresponds to the worst-case circuit C. Specifically, we choose a perturbation method such that for small enough θ, the success probability of average-case approximation over perturbed random circuits would not have largely deviated from the ideal case ($\theta = 0$), and as θ grows, the perturbed circuit converges to the worst-case circuit C. Using such perturbation method and as long as θ values are small enough, one can obtain the

average-case approximate output probability values with high probability over perturbed circuits, parameterized by different values of θ. Also, we can expect that those average-case values contain some information about the worst-case value $p_{\boldsymbol{s}}(C)$, depending on the perturbation method and the values of θ. Assuming that worst-case value $p_{\boldsymbol{s}}(C)$ can be inferred using the average-case values with small values of θ, one can finally infer the worst-case value $p_{\boldsymbol{s}}(C)$, within a certain imprecision determined by the average-case approximation imprecision and the method for the inference.

Therefore, it is crucial to choose a proper perturbation method to establish the worst-to-average-case reduction successfully. Throughout this work, we use the Cayley path for the perturbation, which was employed in Refs. [21, 33, 34] for the hardness proposals of the random circuit sampling.

Definition 6 (Cayley transform [33])**.** *The Cayley transform of an n by n unitary matrix H parameterized by $\theta \in [0,1]$ is a unitary matrix defined as*

$$H(\theta) \coloneqq ((2-\theta)H + \theta I_n)(\theta H + (2-\theta)I_n)^{-1}, \tag{2}$$

where I_n is the n by n identity matrix. Also, for the diagonalization of the n by n unitary matrix $H = LDL^\dagger$, with unitary matrix L and diagonal matrix $D = diag(e^{i\phi_1}, \ldots, e^{i\phi_n})$, the equivalent form of the Cayley transform is

$$H(\theta) = \frac{1}{q(\theta)} L \; diag(\{p_j(\theta)\}_{j=1}^n) \, L^\dagger, \tag{3}$$

where

$$q(\theta) = \prod_{j=1}^{n} (1 + i\theta e^{i\frac{\phi_j}{2}} \sin\frac{\phi_j}{2}), \tag{4}$$

$$p_j(\theta) = e^{i\phi_j}(1 - i\theta e^{-i\frac{\phi_j}{2}} \sin\frac{\phi_j}{2}) \prod_{k\in[n]\setminus j} (1 + i\theta e^{i\frac{\phi_k}{2}} \sin\frac{\phi_k}{2}). \tag{5}$$

Using the Cayley transform defined above, we now define the perturbed random circuit distribution.

Definition 7 (Perturbed random circuit ensemble)**.** *Let $\mathcal{A}$ be the circuit architecture with m number of gates. For the given circuit C_0 in $\mathcal{A}$ with gates $\{G_i\}_{i=1}^m$, the circuit $U(\theta)$ is defined with each gate of C_0 replaced by $G_i \to H_i(\theta)G_i$, where each $H_i(\theta)$ is a Cayley transform of independently distributed local Haar random gate H_i ($i \in [m]$) parameterized by $\theta \in [0,1]$. We define $\mathcal{H}_{\mathcal{A},\theta}^{C_0}$ as the distribution for such $U(\theta)$. Here, the distribution of the $U(0)$ is $\mathcal{H}_{\mathcal{A}}$, and $U(1) = C_0$.*

Before proceeding, we should make sure that the success probability of average-case approximation over circuits is still large enough after the perturbation, to establish the reduction process successfully. This is evident in the case that the total variation distance over circuits induced by the perturbation is small enough, as the success probability over circuits perturbs by, at most, the total variation distance.

In fact, Ref. [33] proved that total variation distance between $\mathcal{H}_{\mathcal{A}}$ and $\mathcal{H}_{\mathcal{A},\theta}^{C_0}$ is small for comparably small perturbation θ.

Lemma 2 (Movassagh [33])**.** *Let $\mathcal{A}$ be the circuit architecture with m number of gates. For $\theta \ll 1$ and for any circuit C_0 in $\mathcal{A}$, total variation distance between $\mathcal{H}_{\mathcal{A},\theta}^{C_0}$ and $\mathcal{H}_{\mathcal{A}}$ is $O(m\theta)$.*

Therefore, by using small $\theta = O(m^{-1})$, one can upper-bound the total variation distance by an arbitrarily small constant, which implies that the success probability of average-case approximation over circuits also perturbs by at most a small constant.

For the worst-to-average-case reduction, we first sample a random circuit $U(\theta) \sim \mathcal{H}_{\mathcal{A},\theta}^{C_0}$ with $\mathcal{A} = (\mathcal{B}\mathcal{B}^*)^q$ and worst-case circuit C_0. Using $U(\theta)$ with the same random seed $\{H_i\}_{i=1}^m$ but with different values of θ satisfying $\theta = O(m^{-1})$, we obtain the average-case approximation of the output probability $p_{\boldsymbol{s}}(U(\theta))$ for each θ, which may enable us to infer the worst-case output probability value $p_{\boldsymbol{s}}(U(1)) = p_{\boldsymbol{s}}(C)$.

To investigate the feasibility of the inference of the worst-case value, we examine the behavior of the function $p_{\boldsymbol{s}}(U(\theta))$ characterized by the parameter θ. Using Definition 6, we find that $p_{\boldsymbol{s}}(U(\theta))$ can be represented as a low-degree rational function in θ.

Lemma 3. *Let $\mathcal{A}$ be the q-Kaleidoscope circuit architecture $(\mathcal{B}\mathcal{B}^*)^q$ with $m = qM \log M$ number of gates, and $U(\theta) \sim \mathcal{H}_{\mathcal{A},\theta}^{C_0}$ for any C_0 in $\mathcal{A}$. Then for any outcome $\boldsymbol{s}$, the output probability $p_{\boldsymbol{s}}(U(\theta))$ can be represented as a degree $(4mN, 4mN)$ rational funtion in θ.*

Proof. For given circuit unitary matrix $U(\theta) \sim \mathcal{H}_{\mathcal{A},\theta}^{C_0}$ with C_0 composed of $\{G_i\}_{i=1}^m$ gates, one can decompose $U(\theta)$ with $m = qM \log M$ product of unitary matrices, such that each matrix element of $U(\theta)$ can be represented as

$$[U(\theta)]_{j,k} = \sum_{l_1=1}^{M} \sum_{l_2=1}^{M} \cdots \sum_{l_{m-1}=1}^{M} U_{j,l_1}^{(1)} U_{l_1,l_2}^{(2)} \cdots U_{l_{m-1},k}^{(m)}, \tag{6}$$

where each $U^{(i)}$ denotes an M-dimensional unitary matrix, with a single gate unitary matrix $H_i(\theta)G_i$ applied to the modes participating in the gate and identity for the rest of the modes. For example, if the ith gate $H_i(\theta)G_i$ is a two-mode gate between the first two modes, $U^{(i)}$ is a block diagonal matrix of $H_i(\theta)G_i$ and identity matrix, namely, $U^{(i)} = H_i(\theta)G_i \bigoplus I_{M-2}$.

For circuit architecture $\mathcal{A} = (\mathcal{B}\mathcal{B}^*)^q$ which is composed of only two-mode gates, matrix elements of $U^{(i)}$ can be represented as degree $(2,2)$ rational functions in θ, where the common denominator for the elements is given by $q_i(\theta)$, defined in Eq. (4) but with index i appended for ith random gate $H_i(\theta)$. Using reduction to the common denominator for all of the m gates, $[U(\theta)]_{j,k}$ can be represented as $(2m, 2m)$ rational function in θ with the common denominator $\prod_{i=1}^m q_i(\theta)$; note that it does not change with the indices j, k.

From Eq. (1), the output probability $p_{\boldsymbol{s}}(U(\theta))$ has the form of

$$p_{\boldsymbol{s}}(U(\theta)) = \left| \sum_{\sigma \in S_N} \prod_{j=1}^{N} [U(\theta)_{\boldsymbol{s},\boldsymbol{t}}]_{\sigma_j,j} \right|^2, \tag{7}$$

where $\boldsymbol{t}$ is an input configuration vector, and S_N is N-mode permutation group. One can easily check that the common denominator for $\prod_{j=1}^N [U(\theta)_{\boldsymbol{s},\boldsymbol{t}}]_{\sigma_j,j}$ is $[\prod_{i=1}^m q_i(\theta)]^N$, and it does not change with permutation σ. Let us define $Q(\theta) = [\prod_{i=1}^m |q_i(\theta)|^2]^N$, which is a degree $4mN$ polynomial in θ. Then $Q(\theta)$ serves as the common denominator for the output probability. Hence, the output probability can be represented as $p_{\boldsymbol{s}}(U(\theta)) = \frac{P(\theta)}{Q(\theta)}$, with $P(\theta)$ also a degree $4mN$ polynomial in θ. □

We are now ready to turn to the proof of Theorem 4, i.e., the average-case hardness of the shallow-depth boson sampling. We prove that for high probability over $\boldsymbol{s} \sim \mathcal{G}_{M,N}$, well-approximating output probability $p_{\boldsymbol{s}}(U)$ with high probability over $U \sim \mathcal{H}_{\mathcal{A}}$ for the shallow-depth architecture $\mathcal{A} = (\mathcal{B}\mathcal{B}^*)^q$ is #P-hard under a $\mathrm{BPP}^{\mathrm{NP}}$ reduction.

Proof of Theorem 4. See Appendix C □

V. AVERAGE-CASE HARDNESS IMPLIES CLASSICAL SIMULATION HARDNESS

As we have previously discussed, since our average-case hardness result considers both the random outcomes and random circuits, it is not straightforward to show the classical simulation hardness of shallow-depth boson sampling as in the original boson sampling proposal [1]. Therefore, in this section, we provide a self-contained analysis of how our average-case hardness result leads to the classical simulation hardness arguments of shallow-depth boson sampling. Specifically, we show that if the allowed additive error in Theorem 4 for the hardness is improved to a certain imprecision level, an efficient classical algorithm that can approximately simulate the shallow-depth boson sampling is unlikely to exist. This emphasizes that improving the imprecision level of the average-case hardness in Theorem 4 is a crucial step for the classical intractability of shallow-depth boson sampling.

Similarly to Refs. [1, 32], we define an approximate boson sampler as follows.

Definition 8 (Approximate boson sampler)**.** *Approximate boson sampler is a classical randomized algorithm that takes input linear optical circuit C and outputs a sample from the output distribution $\mathcal{D}'_C$ such that*

$$||\mathcal{D}'_C - \mathcal{D}_C|| \leq \beta \tag{8}$$

where $\mathcal{D}_C$ is the ideal output distribution of the circuit C and $||\cdot||$ represents total variation distance.

Given the total variation distance error, the above approximate sampler can have an arbitrarily large additive error for a fixed output probability. Nevertheless, it still has a comparably small additive error for *most* of the output probabilities due to Markov's inequality. Accordingly, finding the average-case solution of the output probability of the ideal sampler over randomly chosen collision-free outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$, up to a certain additive imprecision, is in complexity class $\mathrm{BPP}^{\mathrm{NP}}$ by Stockmeyer's theorem [38].

Lemma 4 (Average-case approximation [1])**.** *If there exists an approximate boson sampler $\mathcal{S}$ with total variation distance β, then for any linear optical circuit C, the following problem is in $\mathrm{BPP}^{\mathrm{NP}^{\mathcal{S}}}$: find the average-case approximate solution $\tilde{p}_{\boldsymbol{s}}(C)$ of $p_{\boldsymbol{s}}(C)$, which satisfies*

$$\Pr_{\boldsymbol{s}\sim\mathcal{G}_{M,N}}\left[|\tilde{p}_{\boldsymbol{s}}(C) - p_{\boldsymbol{s}}(C)| \geq \frac{\kappa}{\binom{M}{N}}\right] \leq \xi, \tag{9}$$

where $\boldsymbol{s}$ is over all collision-free outcomes, and $\kappa, \xi > 0$ are the fixed error parameters satisfying $\beta = \kappa\xi/12$.

We leave the proof of Lemma 4 in Appendix D for a more self-contained analysis. The complexity $\mathrm{BPP}^{\mathrm{NP}}$ is known to be inside the finite level of PH, i.e., $\mathrm{BPP}^{\mathrm{NP}} \subseteq \mathrm{PH}$. Also, by Toda's theorem [39], PH problems can be solved given the ability to solve any #P problem, i.e., $\mathrm{BPP}^{\mathrm{NP}} \subseteq \mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$. If finding the average-case solution of output probabilities of sampler $\mathcal{S}$ is #P-hard, then $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{BPP}^{\mathrm{NP}^{\mathcal{S}}}$. Therefore, if an efficient classical algorithm exists that can simulate $\mathcal{S}$, then $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{BPP}^{\mathrm{NP}}$ which implies the collapse of PH. Consequently, under the assumption of the non-collapse of the PH, there is no efficient classical algorithm capable of simulating $\mathcal{S}$.

Based on the above arguments, we show that for the case that allowed additive imprecision of Theorem 4 for the hardness can be improved, then it is classically hard to simulate shallow-depth boson sampling within a constant total variation distance.

Theorem 5. *Suppose that the allowed additive imprecision for the problem in Theorem 4 to be #P-hard can be improved to* $\epsilon = 2^{-(\gamma-1)N\log N - O(N)}$. *Then the efficient classical simulation of approximate boson sampler* $\mathcal{S}$ *with respect to circuits from the shallow architecture* $\mathcal{A} = (\mathcal{BB}^*)^{q\geq 2}$ *implies the collapse of* PH.

Proof. We establish a reduction from the problem in Theorem 4 with allowed additive error $\epsilon = 2^{-(\gamma-1)N\log N - O(N)}$ to the problem in Lemma 4. Let $\mathcal{O}$ be an oracle that solves the problem in Lemma 4, i.e., on input a circuit C and a randomly chosen collision-free outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$, $\mathcal{O}$ outputs an estimate of output probability $p_{\boldsymbol{s}}(C)$ up to additive imprecision $\kappa\binom{M}{N}^{-1}$, with probability at least $1-\xi$ over outcomes for any circuit. For convenience, we refer to the outcomes which $\mathcal{O}$ estimates with error larger than $\kappa\binom{M}{N}^{-1}$ as bad outcomes, such that the portion of bad outcomes over possible collision-free outcomes is at most ξ for any circuit.

For the randomly chosen circuit input, bad outcomes can vary with the circuit instances, as the sampler $\mathcal{S}$ has the freedom to choose its error distribution according to the input circuit. However, no matter how the bad outcomes vary with circuit instances, $\mathcal{O}$ succeeds at least $1-\frac{\xi}{\eta}$ fraction over circuit instances for at least $1-\eta$ fraction of the outcomes, for any η satisfying $\xi < \eta < 1$. Otherwise, the failure probability over outcomes and circuits would exceed ξ, which contradicts the proposition that the success probability of $\mathcal{O}$ is at least $1-\xi$ over randomly chosen outcomes and circuits. As the above argument holds for any random circuit families, we choose the random circuit distribution as $\mathcal{H}_{\mathcal{A}}$ with the shallow architecture $\mathcal{A} = (\mathcal{BB}^*)^{q\geq 2}$.

To sum up, on input a random circuit $H \sim \mathcal{H}_{\mathcal{A}}$ and a random outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$, the oracle $\mathcal{O}$ estimates the output probability $p_{\boldsymbol{s}}(H)$ up to imprecision $\kappa\binom{M}{N}^{-1}$, with probability at least $1-\frac{\xi}{\eta}$ over the choice of H for at least $1-\eta$ over the choice of $\boldsymbol{s}$. Here, the additive imprecision can be bounded as

$$\kappa\binom{M}{N}^{-1} = \kappa\frac{N!(M-N)!}{M!} \tag{10}$$

$$= 2^{-(\gamma-1)N\log N - O(N)}, \tag{11}$$

for constant β and so as κ, where we used the relation $M = c_0 N^{\gamma}$ with a constant c_0 and $\gamma \geq 1$. By setting η and ξ small constant satisfying $\eta + \frac{\xi}{\eta} < \frac{1}{4}$, we can solve the problem in Theorem 4 up to additive imprecision $\epsilon = 2^{-(\gamma-1)N\log N - O(N)}$ using the oracle $\mathcal{O}$. Hence, assuming that the above problem is #P-hard under $\mathrm{BPP}^{\mathrm{NP}}$ reduction, we can obtain the complexity-theoretical relation $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{BPP}^{\mathrm{NP}^{\mathcal{S}}}$, which implies the collapse of PH if $\mathcal{S}$ with respect to shallow-depth circuit architecture $(\mathcal{BB}^*)^{q\geq 2}$ can be done in classical polynomial time. This completes the proof. □

VI. CLASSICAL SIMULATION HARDNESS OF SHALLOW-DEPTH GAUSSIAN BOSON SAMPLING

In this section, we show that our hardness results of the shallow-depth boson sampling can be generalized to the Gaussian boson sampling scheme [2]. Our specific setup for the Gaussian boson sampling is as follows. Let the total mode number M of the circuit be a power of 2, and now the input state is an M product of single-mode squeezed vacuum (SMSV) state $|\mathrm{SMSV}\rangle^{\otimes M}$ with equal squeezing parameter r and equal squeezing direction. Also, let us define the output mean photon number as an integer N (i.e., $N = M\sinh^2 r$) where M and N are polynomially related as $M = c_1 N^{\gamma}$ for a constant c_1 and $\gamma \geq 1$. We define $q_{\boldsymbol{s}}(C)$ as an output probability of the Gaussian boson sampling, for an N photon outcome $\boldsymbol{s}$ from an M mode linear optical circuit matrix C on

input M SMSV states. For collision-free outcome $\boldsymbol{s}$, $q_{\boldsymbol{s}}(C)$ can be expressed as [2]

$$q_{\boldsymbol{s}}(C) = \left|\langle \boldsymbol{s}|\,\hat{\mathcal{U}}(C)\,|\mathrm{SMSV}\rangle^{\otimes M}\right|^2 = \frac{\tanh^N r}{\cosh^M r}|\mathrm{Haf}((CC^T)_{\boldsymbol{s}})|^2, \tag{12}$$

where $|\boldsymbol{s}\rangle$ is an M-mode Fock state corresponding to the outcome $\boldsymbol{s}$, $\hat{\mathcal{U}}(C)$ is a unitary operator corresponding to the circuit C, and $(CC^T)_{\boldsymbol{s}}$ is an N by N matrix obtained by taking s_i copies of the ith row and column of the matrix CC^T.

Using the above settings, we first prove the worst-case hardness of Gaussian boson sampling for a fixed outcome $\boldsymbol{s}$, with the shallow-depth circuit architecture $\mathcal{BB}^*$.

Theorem 6. *Approximating the output probability $q_{\boldsymbol{s}_0}(C)$ of Gaussian boson sampling to within additive error $2^{-\frac{\gamma-1}{2}N\log N - O(N)}$ for any C over linear optical circuit architecture $\mathcal{BB}^*$ is #P-hard in the worst case.*

Proof. We establish a reduction from the worst-case hardness of boson sampling in Theorem 3 to the problem in Theorem 6. Let $p_{\boldsymbol{s}_0}(C_0)$ be the output probability of a fixed input and output $\boldsymbol{s}_0$ of boson sampling in Theorem 3, for mode number M_0, photon number N_0, and the circuit C_0 in M_0 mode circuit architecture $\mathcal{BB}^*$. In the following, we show that $p_{\boldsymbol{s}_0}(C_0)$ can be efficiently reduced to the output probability $q_{\boldsymbol{s}}(C)$ of Gaussian boson sampling, for mode number $M = 2M_0$ and mean photon number $N = 2N_0$, with output $\boldsymbol{s}$ and circuit C determined by $\boldsymbol{s}_0$ and C_0 each.

Our strategy is to employ the scheme in Ref. [40], which used M_0 product of equally squeezed two-mode squeezed vacuum (TMSV) state as an input state to perform M_0 mode boson sampling task. Specifically, a single TMSV state with squeezing parameter r can be represented as

$$|\mathrm{TMSV}\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}\tanh^n r\,|n\rangle\,|n\rangle\,, \tag{13}$$

and thus M_0 product of the TMSV state is

$$\begin{aligned}|\mathrm{TMSV}\rangle^{\otimes M_0} &= \frac{1}{\cosh^{M_0} r}\left(\sum_{n=0}^{\infty}\tanh^n r\,|n\rangle_{(1)}\,|n\rangle_{(2)}\right)^{\otimes M_0}\\ &= \frac{1}{\cosh^{M_0} r}\sum_{n=0}^{\infty}\tanh^n r\sum_{\boldsymbol{s}_n}|\boldsymbol{s}_n\rangle_{(1)}\,|\boldsymbol{s}_n\rangle_{(2)}\,,\end{aligned} \tag{14}$$

where the summation of $\boldsymbol{s}_n$ is over all possible configurations of Fock state with a total M_0 mode and n photon.

For each mode in the given M_0 mode circuit C_0, one-half of the TMSV state (i.e., subscript (2) in Eq. (14)) is input into it, and the other half of each state (i.e., subscript (1) in Eq. (14)) is sent directly to a photon counter. By setting each $|\boldsymbol{s}_{\mathrm{in}}\rangle$ and $|\boldsymbol{s}_{\mathrm{out}}\rangle$ as a total M_0 mode and total N_0 photon Fock state, the output probability can be represented as

$$\left|\langle\boldsymbol{s}_{\mathrm{in}}|_{(1)}\,\langle\boldsymbol{s}_{\mathrm{out}}|_{(2)}\,\hat{\mathcal{U}}_{(2)}(C_0)\,|\mathrm{TMSV}\rangle^{\otimes M_0}\right|^2 = \frac{\tanh^{2N_0} r}{\cosh^{2M_0} r}\left|\langle\boldsymbol{s}_{\mathrm{in}}|\,\hat{\mathcal{U}}(C_0)\,|\boldsymbol{s}_{\mathrm{out}}\rangle\right|^2, \tag{15}$$

which is the output probability of M_0 mode and N_0 photon boson sampling in circuit C_0, with an additional multiplicative factor.

Note that two M_0 mode $\mathcal{BB}^*$ architecture can be embedded in the middle of an $M = 2M_0$ mode $\mathcal{BB}^*$ architecture. Accordingly, we define a circuit C in M mode $\mathcal{BB}^*$ by embedding the given M_0 mode circuit C_0 in one side of $\mathcal{BB}^*$, setting gates located right in front of the input

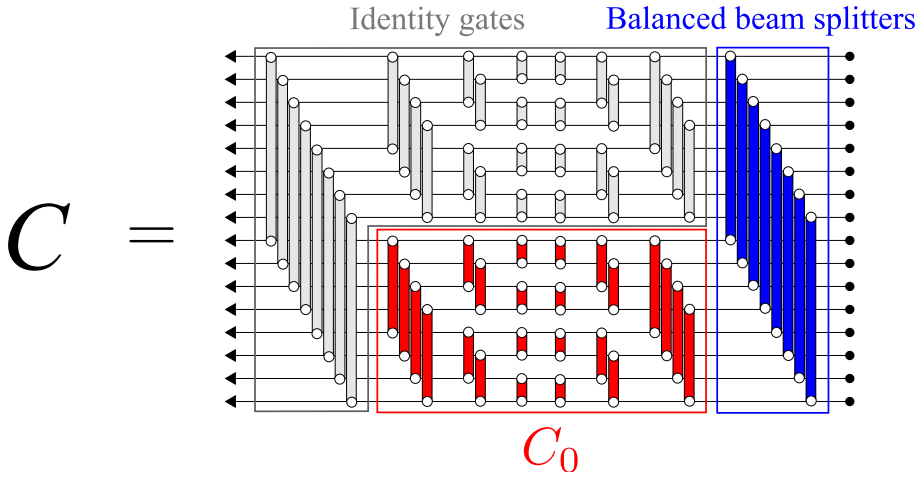


FIG. 3. Schematics of an mode number $M = 16$ circuit C in $\mathcal{BB}^*$ which contains a given $M_0 = 8$ mode circuit C_0 in $\mathcal{BB}^*$

ports as balanced beam splitters, and setting the remaining gates as identity gates; we leave in Fig. 3 an illustration of $M = 16$ mode circuit C for more clarity. Here, the input M SMSV states with squeezing parameter r combined with the balanced beam splitters at the front becomes M_0 TMSV states with squeezing parameter r. Therefore, our overall setup exactly follows the scheme in Ref. [40], such that the first M_0 mode is the photon counter sector to determine the input configuration of boson sampling, and the last M_0 mode is to simulate the boson sampling for the given circuit C_0.

We also define an M-dimensional vector $\boldsymbol{s}$ as a serial concatenation of two $\boldsymbol{s}_0$ vectors, so that $\boldsymbol{s}$ represents N photon outcome over M modes. Then the output probabilities $p_{\boldsymbol{s}_0}(C_0)$ and $q_{\boldsymbol{s}}(C)$ are related as

$$\begin{aligned} q_{\boldsymbol{s}}(C) &= \left| \langle \boldsymbol{s} | \hat{\mathcal{U}}(C) \, |\mathrm{SMSV}\rangle^{\otimes M} \right|^2 \\ &= \left| \langle \boldsymbol{s}_0 |_{(1)} \, \langle \boldsymbol{s}_0 |_{(2)} \, \hat{\mathcal{U}}_{(2)}(C_0) \, |\mathrm{TMSV}\rangle^{\otimes M_0} \right|^2 \\ &= \frac{\tanh^{2N_0} r}{\cosh^{2M_0} r} p_{\boldsymbol{s}_0}(C_0). \end{aligned} \tag{16}$$

Hence, approximating the output probability $p_{\boldsymbol{s}_0}(C_0)$ can be reduced to approximating the output probability $q_{\boldsymbol{s}}(C)$ of Gaussian boson sampling, with a blowup in the additive imprecision. The size of the additive imprecision blowup is

$$\frac{\cosh^{2M_0} r}{\tanh^{2N_0} r} = \left(\frac{M+N}{M}\right)^{M_0+N_0} \left(\frac{M}{N}\right)^{N_0} = 2^{\frac{\gamma-1}{2} N \log N + O(N)}, \tag{17}$$

using the relation $N = M \sinh r$ and $M \propto N^\gamma$. Since the allowed additive error for the worst-case hardness of $p_{\boldsymbol{s}_0}(C_0)$ is $2^{-O(N)}$, the allowed additive error for the reduction is $2^{-O(N)} 2^{-\frac{\gamma-1}{2} N \log N - O(N)}$ $= 2^{-\frac{\gamma-1}{2} N \log N - O(N)}$. This completes the proof. □

Using the results of Theorem 6 and the previous proof of the average-case hardness of boson sampling in Theorem 4, it is straightforward to find the average-case hardness of Gaussian boson sampling, for randomly chosen N photon outcomes $\boldsymbol{s} \sim \mathcal{G}_{M,N}$ and randomly chosen circuits $U \sim \mathcal{H}_{\mathcal{A}}$ in shallow-depth architecture $\mathcal{A} = (\mathcal{BB}^*)^{q \geq 2}$.

Theorem 7. *The following problem is #P-hard under a* $\mathrm{BPP}^{\mathrm{NP}}$ *reduction: for any constant* $\delta, \eta \geq 0$ *with* $\delta+\eta < \frac{1}{4}$*, on input a random circuit* $U \sim \mathcal{H}_{\mathcal{A}}$ *with* $\mathcal{A} = (\mathcal{B}\mathcal{B}^*)^{q\geq 2}$ *and a random outcome* $\boldsymbol{s} \sim \mathcal{G}_{M,N}$*, compute the output probability* $q_{\boldsymbol{s}}(U)$ *of Gaussian boson sampling within additive imprecision* $\epsilon = 2^{-O(N^{\gamma+1}(\log N)^2)}$*, with probability at least* $1-\delta$ *over the choice of* U *for at least* $1-\eta$ *over the choice of* $\boldsymbol{s}$*.*

Proof. The procedure is the same as the proof of Theorem 4, namely, establishing a worst-to-average-case reduction from the problem in Theorem 6 to the problem in Theorem 7. The only different part for the Gaussian boson sampling case is the functional form of the output probability $q_{\boldsymbol{s}}(U(\theta))$ parameterized by θ. Hence, we show that $q_{\boldsymbol{s}}(U(\theta))$ can also be represented as a degree $(4mN, 4mN)$ rational function in θ, the same degree as the boson sampling case in Lemma 3.

From Eq. (12), the output probability $q_{\boldsymbol{s}}(U(\theta))$ has the form of

$$q_{\boldsymbol{s}}(U(\theta)) = \tanh^N r \operatorname{sech}^M r \left| \sum_{\mu \in \mathrm{PMP}} \prod_{j=1}^{N/2} \left[(U(\theta)U(\theta)^T)_{\boldsymbol{s}} \right]_{\mu(2j-1),\mu(2j)} \right|^2, \tag{18}$$

where μ is along all possible perfect matching permutations over N modes. From the proof of Lemma 3, using reduction to the common denominator for all of the $m = qM \log M$ gates, $[U(\theta)]_{j,k}$ can be represented as $(2m, 2m)$ rational function in θ with the common denominator $\prod_{i=1}^m q_i(\theta)$. Using this fact, one can easily check that $\prod_{j=1}^{N/2} \left[(U(\theta)U(\theta)^T)_{\boldsymbol{s}} \right]_{\mu(2j-1),\mu(2j)}$ can be represented as $(2mN, 2mN)$ rational function in θ, with the common denominator $[\prod_{i=1}^m q_i(\theta)]^N$ which does not change with μ. Therefore, the output probability can be represented as $q_{\boldsymbol{s}}(U(\theta)) = \frac{P(\theta)}{Q(\theta)}$, with each $Q(\theta) = [\prod_{i=1}^m |q_i(\theta)|^2]^N$ and $P(\theta)$ a degree $4mN$ polynomial function in θ.

Given that $q_{\boldsymbol{s}}(U(\theta))$ can be represented as a degree $(4mN, 4mN)$ rational function with the same denominator $Q(\theta) = [\prod_{i=1}^m |q_i(\theta)|^2]^N$ from the boson sampling case in Lemma 3, we can repeat all the steps identically to the proof of Theorem 4 and obtain the same result. □

VII. EXTENSION OF HARDNESS RESULTS FOR LOSSY ENVIRONMENTS

In this section, we generalize our hardness results for *lossy* environments, namely, shallow-depth linear optical circuits suffering from photon loss channels after each gate implementation. The reason we consider such a noise channel is that photon loss is indeed a major source of error in optical systems [4–7]. Also, photon loss ruins the classical intractability of boson sampling, as there exist many efficient classical algorithms that can simulate lossy boson sampling within a constant total variation distance [12–14]. Therefore, we mainly deal with the photon loss error here; our goal is to provide evidence for the hardness of the approximate simulation of boson sampling in lossy shallow circuits within total variation distance error. For simplicity, we do not consider any photon gain error here, such as thermal radiation noise subjected to the circuits.

To proceed, we start with a brief review of the results presented by Ref. [41], which shows the hardness of simulating noisy quantum circuits. Specifically, one can simulate a noiseless circuit using a larger noisy circuit up to the desired imprecision, by establishing error-detecting code in the noisy circuit and post-selecting null syndrome measurements. Therefore, given the probability to post-select the no-error syndromes, one can approximate the output probability of the noiseless circuit from the output probability of the noisy circuit. Based on this argument, Ref. [21] demonstrates the average-case hardness of approximating output probabilities of noisy quantum circuits, under some plausible assumptions of the noise model. This result gives evidence of the approximate simulation hardness of noisy quantum circuits, within total variation distance error.

The main strategy of the above hardness results is approximating ideal output probabilities by post-selecting error-free results from noisy circuits. Here, we can directly apply their strategy to our case, i.e., lossy shallow-depth linear optical circuits. The crucial observation is that considering photon loss error on boson sampling, the error syndrome is the output photon number *itself*. Specifically, if the output photon number is the same as the input photon number, this implies that no loss occurred throughout the circuit. Therefore, by post-selecting the event that the measured output photon number is the same as the input photon number, we can infer ideal output probabilities.

For a more detailed analysis, we set the loss model as follows. Let the photon loss model $\mathcal{N}$ be local and stochastic. Specifically, $\mathcal{N}$ is a set of loss channels $\{\mathcal{N}_i\}_{i=1}^{l}$, such that after each unitary gate is applied, loss channel $\mathcal{N}_i$ acts on each mode participated in the unitary gate. Hence, the number of loss channels is $l = O(m)$ for gate number m in a given circuit architecture. We can decompose each noise channel $\mathcal{N}_i$ as follows:

$$\mathcal{N}_i = (1-\rho_i)\mathcal{I} + \rho_i \mathcal{E}_i, \tag{19}$$

where $\mathcal{I}$ is identity, $\mathcal{E}_i$ is an CPTP map representing photon loss, and ρ_i is a loss rate for each channel satisfying $\rho_i \leq \rho$ for a constant ρ. The validity of such modeling for photon loss channel is represented in [3, 12].

To simplify, we assume that we know *a priori* each error rate ρ_i for all $i \in [l]$, and the noise model $\mathcal{N}$ is fixed so that it does not change with random circuit instances. Then we can obtain the hardness of approximating output probabilities of lossy shallow circuits, from our previous hardness proposals. To do so, let $p_{\boldsymbol{s}}(C,\mathcal{N})$ be the output probability of N photon outcome $\boldsymbol{s}$ from a M mode linear optical circuit C which undergoes loss model $\mathcal{N}$ we set. By post-selecting 'no loss event', which can be accomplished by counting the output photon number, the ideal output probability $p_{\boldsymbol{s}}(C)$ can be inferred from $p_{\boldsymbol{s}}(C,\mathcal{N})$ by

$$p_{\boldsymbol{s}}(C) = \frac{p_{\boldsymbol{s}}(C,\mathcal{N})}{\Pr[\text{'no loss event'}]}. \tag{20}$$

From Eq. (19), the probability of 'no loss event' is $\prod_{i=1}^{l}(1-\rho_i)$, which can be efficiently calculated. This implies that approximating $p_{\boldsymbol{s}}(C,\mathcal{N})$ can be reduced from approximating $p_{\boldsymbol{s}}(C)$, with at most $\Pr[\text{'no loss event'}]^{-1} = \prod_{i=1}^{l}(1-\rho_i)^{-1} \leq (1-\rho)^{-l} = 2^{O(\rho m)}$ blowup in the additive imprecision.

Given Eq. (20), we can repeat the same steps from the previous hardness arguments, for the lossy shallow-depth boson sampling; the only difference is the imprecision blowup by $2^{O(\rho m)}$. For our shallow-depth architecture $(\mathcal{BB}^*)^q$, the gate number m is $qM\log M$, so the size of imprecision blowup is $2^{O(N^\gamma \log N)}$ in our case. Such imprecision blowup does not affect the allowed additive accuracy $\epsilon = 2^{-O(N^{\gamma+1}(\log N)^2)}$ for our average-case hardness result. Based on the arguments so far, the following corollary is straightforward.

Corollary 1. *Suppose we have the photon loss model $\mathcal{N}$ with each loss rate $\rho_i \leq \rho$ for a constant ρ. Then the following problem is #P-hard under a $\mathrm{BPP}^{\mathrm{NP}}$ reduction: for any constant $\delta, \eta \geq 0$ with $\delta+\eta < \frac{1}{4}$, on input a random circuit $U \sim \mathcal{H}_{\mathcal{A}}$ with $\mathcal{A} = (\mathcal{BB}^*)^{q\geq 2}$ and a random outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$, compute the lossy output probability $p_{\boldsymbol{s}}(U,\mathcal{N})$ within additive imprecision $\epsilon = 2^{-O(N^{\gamma+1}(\log N)^2)}$, with probability at least $1-\delta$ over the choice of U for at least $1-\eta$ over the choice of $\boldsymbol{s}$.*

We remark that for our noise model, the imprecision blowup grows exponentially with the gate number m. Therefore, shallow-depth circuits can be more advantageous in this perspective, since they are likely to have less gate number and thus have small imprecision blowup. For example, the current hardness results are based on M by N submatrices of M-dimensional Haar random

unitaries, and the implementation of such matrices requires gate number $m = \Omega(N^{\gamma+1})$. This arouses the imprecision blowup at least $2^{O(N^{\gamma+1})}$, which restricts the allowed additive error for the average-case hardness at most $2^{-O(N^{\gamma+1})}$.

VIII. CONCLUDING REMARKS

Here we provide a few remarks about our overall results and related open questions.

1. Our result demonstrates the average-case hardness for additive imprecision $2^{-O(N^{\gamma+1}(\log N)^2)}$. Indeed, there still remains a gap to the desired additive imprecision for the simulation hardness $2^{-(\gamma-1)N\log N-O(N)}$ in Theorem 5. Hence, closing this gap would be an ultimate challenge to the full achievement of classical intractability; more advanced proof techniques are required to reduce this gap. Here, one can take the following approach: finite-size numerical experiments suggest that the output distributions of local random circuits in the butterfly circuit architecture (Definition 2) are close enough to those of global Haar random circuits [37]. Accordingly, if one can analytically prove that the distance between those output distributions is close enough, we can directly obtain a better imprecision level $2^{-O(N\log N)}$ by results in [3, 21, 22], which employed the global Haar random circuits.

Another possible approach for reducing the imprecision gap is to perturb a random circuit matrix in a different way from the Cayley transform (Definition 6), i.e., as depicted in [22]. Specifically, instead of perturbing each random gate, one can perturb a submatrix X of our random circuit matrix U with a worst-case matrix A as $X(\theta) = (1-\theta)X + \theta A$ for $\theta \in [0,1]$. Here, a degree of polynomial $|\mathrm{Per}(X(\theta))|^2$ is $2N$, which is lower than ours derived by the Cayley transform. Therefore, if one can prove that $X(\theta)$ is distributed similarly to X for small θ, we expect that we can also obtain a better imprecision level by using the same interpolation method. However, the above approach requires one to figure out a global circuit distribution generated by the convolution of local circuit distributions. Although we believe that this problem can be resolved using techniques from random matrix theories, we have not yet developed a complete analysis. Hence, we leave it as an open question.

2. Another important challenge that should be addressed is to find the classical simulation hardness of noisy boson sampling, for general types of physical noise beyond the photon loss noise model we have dealt with so far. To do so, as described in [3, 21, 41], employing the threshold theorem would be a viable choice for this goal. Specifically, the threshold theorem for general types of noise in boson sampling setups has to be developed. This requires an efficient error detection code for general types of error using linear optical elements, for any multi-mode Fock state or Gaussian state input. However, to the best of our knowledge, such an error detection code does not exist. Hence, constructing this error detection code would be a crucial step toward the hardness of noisy boson sampling, which will contribute to a more noise-tolerant demonstration of quantum advantage with boson sampling. We leave this problem as another open question.

ACKNOWLEDGEMENT

We thank Bill Fefferman for insightful discussions. The authors acknowledge support from the National Research Foundation of Korea (NRF) grants funded by the Korean government (Grant Nos. NRF-2023R1A2C1006115, NRF-2022M3K4A1097117, and NRF-2022M3E4A1076099) via the Institute of Applied Physics at Seoul National University, the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (IITP-2021-0-01059 and IITP-20232020-0-01606). B.G. was also supported by the education and training program of the Quantum Information Research Support Center, funded

through the National Research Foundation of Korea (NRF) by the Ministry of Science and ICT (MSIT) of the Korean government (No.2021M3H3A1036573).

---

[1] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[2] Craig S Hamilton, Regina Kruse, Linda Sansoni, Sonja Barkhofen, Christine Silberhorn, and Igor Jex. Gaussian boson sampling. *Physical review letters*, 119(17):170501, 2017.

[3] Abhinav Deshpande, Arthur Mehta, Trevor Vincent, Nicolás Quesada, Marcel Hinsche, Marios Ioannou, Lars Madsen, Jonathan Lavoie, Haoyu Qi, Jens Eisert, et al. Quantum computational advantage via high-dimensional gaussian boson sampling. *Science advances*, 8(1):eabi7894, 2022.

[4] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[5] 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. *Physical review letters*, 127(18):180502, 2021.

[6] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[7] Yu-Hao Deng, Yi-Chao Gu, Hua-Liang Liu, Si-Qiu Gong, Hao Su, Zhi-Jiong Zhang, Hao-Yang Tang, Meng-Hao Jia, Jia-Min Xu, Ming-Cheng Chen, et al. Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage. *Physical review letters*, 131(15):150601, 2023.

[8] Jelmer Renema, Valery Shchesnovich, and Raul Garcia-Patron. Classical simulability of noisy boson sampling. *arXiv preprint arXiv:1809.01953*, 2018.

[9] Jelmer J Renema, Adrian Menssen, William R Clements, Gil Triginer, William S Kolthammer, and Ian A Walmsley. Efficient classical algorithm for boson sampling with partially distinguishable photons. *Physical review letters*, 120(22):220502, 2018.

[10] Valery S Shchesnovich. Noise in boson sampling and the threshold of efficient classical simulatability. *Physical Review A*, 100(1):012340, 2019.

[11] Alexandra E Moylett, Raúl García-Patrón, Jelmer J Renema, and Peter S Turner. Classically simulating near-term partially-distinguishable and lossy boson sampling. *Quantum Science and Technology*, 5(1):015001, 2019.

[12] Michał Oszmaniec and Daniel J Brod. Classical simulation of photonic linear optics with lost particles. *New Journal of Physics*, 20(9):092002, 2018.

[13] Raúl García-Patrón, Jelmer J Renema, and Valery Shchesnovich. Simulating boson sampling in lossy architectures. *Quantum*, 3:169, 2019.

[14] Haoyu Qi, Daniel J Brod, Nicolás Quesada, and Raúl García-Patrón. Regimes of classical simulability for noisy gaussian boson sampling. *Physical review letters*, 124(10):100502, 2020.

[15] Daniel Jost Brod and Michał Oszmaniec. Classical simulation of linear optics subject to nonuniform losses. *Quantum*, 4:267, 2020.

[16] Benjamin Villalonga, Murphy Yuezhen Niu, Li Li, Hartmut Neven, John C Platt, Vadim N Smelyanskiy, and Sergio Boixo. Efficient approximation of experimental gaussian boson sampling. *arXiv preprint arXiv:2109.11525*, 2021.

[17] Jacob FF Bulmer, Bryn A Bell, Rachel S Chadwick, Alex E Jones, Diana Moise, Alessandro Rigazzi, Jan Thorbecke, Utz-Uwe Haus, Thomas Van Vaerenbergh, Raj B Patel, et al. The boundary for quantum advantage in gaussian boson sampling. *Science advances*, 8(4):eabl9236, 2022.

[18] Changhun Oh, Liang Jiang, and Bill Fefferman. On classical simulation algorithms for noisy boson sampling. *arXiv preprint arXiv:2301.11532*, 2023.

[19] Changhun Oh, Minzhao Liu, Yuri Alexeev, Bill Fefferman, and Liang Jiang. Tensor network algorithm for simulating experimental gaussian boson sampling. *arXiv preprint arXiv:2306.03709*, 2023.

[20] 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, 2022.
[21] Adam Bouland, Bill Fefferman, Zeph Landau, and Yunchao Liu. Noise and the frontier of quantum supremacy. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1308–1317. IEEE, 2022.
[22] 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 preprint arXiv:2312.00286*, 2023.
[23] Karol Zyczkowski and Marek Kus. Random unitary matrices. *Journal of Physics A: Mathematical and General*, 27(12):4235, 1994.
[24] Nicholas J Russell, Levon Chakhmakhchyan, Jeremy L O'Brien, and Anthony Laing. Direct dialling of haar random unitary matrices. *New journal of physics*, 19(3):033007, 2017.
[25] Daniel J Brod. Complexity of simulating constant-depth bosonsampling. *Physical Review A*, 91(4):042316, 2015.
[26] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Physical review letters*, 91(14):147902, 2003.
[27] Haoyu Qi, Diego Cifuentes, Kamil Brádler, Robert Israel, Timjan Kalajdzievski, and Nicolás Quesada. Efficient sampling from shallow gaussian quantum-optical circuits with local interactions. *Physical Review A*, 105(5):052412, 2022.
[28] Abhinav Deshpande, Bill Fefferman, Minh C Tran, Michael Foss-Feig, and Alexey V Gorshkov. Dynamical phase transitions in sampling complexity. *Physical review letters*, 121(3):030501, 2018.
[29] Changhun Oh, Youngrong Lim, Bill Fefferman, and Liang Jiang. Classical simulation of boson sampling based on graph structure. *Physical Review Letters*, 128(19):190501, 2022.
[30] Chao Shen, Zhen Zhang, and L-M Duan. Scalable implementation of boson sampling with trapped ions. *Physical review letters*, 112(5):050504, 2014.
[31] Wentao Chen, Yao Lu, Shuaining Zhang, Kuan Zhang, Guanhao Huang, Mu Qiao, Xiaolu Su, Jialiang Zhang, Jing-Ning Zhang, Leonardo Banchi, et al. Scalable and programmable phononic network with trapped ions. *Nature Physics*, pages 1–7, 2023.
[32] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019.
[33] Ramis Movassagh. The hardness of random quantum circuits. *Nature Physics*, pages 1–6, 2023.
[34] Yasuhiro Kondo, Ryuhei Mori, and Ramis Movassagh. Quantum supremacy and hardness of estimating output probabilities of quantum circuits. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1296–1307. IEEE, 2022.
[35] Hari Krovi. Average-case hardness of estimating probabilities of random quantum circuits with a linear scaling in the error exponent. *arXiv preprint arXiv:2206.05642*, 2022.
[36] Tri Dao, Nimit S Sohoni, Albert Gu, Matthew Eichhorn, Amit Blonder, Megan Leszczynski, Atri Rudra, and Christopher Ré. Kaleidoscope: An efficient, learnable representation for all structured linear maps. *arXiv preprint arXiv:2012.14966*, 2020.
[37] Byeongseon Go, Changhun Oh, Liang Jiang, and Hyunseok Jeong. Exploring shallow-depth boson sampling: Towards scalable quantum supremacy. *arXiv preprint arXiv:2306.10671*, 2023.
[38] Larry Stockmeyer. On approximation algorithms for# p. *SIAM Journal on Computing*, 14(4):849–861, 1985.
[39] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.
[40] Austin P Lund, Anthony Laing, Saleh Rahimi-Keshari, Terry Rudolph, Jeremy L O'Brien, and Timothy C Ralph. Boson sampling from a gaussian state. *Physical review letters*, 113(10):100502, 2014.
[41] Keisuke Fujii. Noise threshold of quantum supremacy. *arXiv preprint arXiv:1610.03632*, 2016.
[42] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical review letters*, 86(22):5188, 2001.
[43] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526. IEEE, 2009.
[44] Andrew M Childs, Debbie W Leung, and Michael A Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Physical Review A*, 71(3):032318, 2005.

[45] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816):46–52, 2001.
[46] Emanuel Knill. Quantum gates using linear optics and postselection. *Physical Review A*, 66(5):052306, 2002.

Appendix A: Previous foundations: Average-case hardness of boson sampling

In this appendix, we argue the existing proof technique employed for the simulation hardness of boson sampling, specifically in the context of the approximate simulation within total variation distance error [1]. The current state-of-the-art proof technique for the hardness of sampling problems like boson sampling essentially builds upon Stockmeyer's algorithm about approximate counting [38]. Specifically, given a classical sampler that outputs a sample from a given output distribution, Stockmeyer's algorithm enables one to multiplicatively estimate a fixed output probability of the sampler, within complexity class $\mathrm{BPP}^{\mathrm{NP}}$.

Now suppose there exists an approximate classical sampler capable of simulating ideal boson sampling up to total variation distance error, as in Definition 8. This approximate sampler can have a large additive error for a fixed output probability, but have a comparably small additive error for *most* of the output probabilities due to Markov's inequality. Then, Stockmeyer's algorithm, combined with the approximate sampler, can well approximate the ideal output probability of boson sampling within a certain additive error, with a high probability over randomly chosen outcomes (See Lemma 4 for more details). For convenience, let us refer to this computational task as an *average-case approximation* problem of boson sampling. If the complexity of the average-case approximation problem is outside the Polynomial Hierarchy (PH), it implies the collapse of PH, since the complexity of Stockmeyer's algorithm is indeed inside the finite level of PH.

Here, *average-case hardness* comes into the proof of the classical simulation hardness argument, which means that approximating the ideal output probability of boson sampling with high probability over randomly chosen outcomes is #P-hard. More precisely, if the average-case hardness holds up to the imprecision level of the average-case approximation problem, this comes down to the classical simulation hardness of the approximate sampling unless PH collapses, by the complexity-theoretical foundation $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$ [39].

Moreover, by choosing random circuit instances that have symmetry over the outcomes, one can reduce the average-case instances for the hardness from *outcome* instances to *circuit* instances, which is called the *hiding* property. For the boson sampling case, global Haar random unitary (i.e., unitary matrix drawn from Haar measure on U(M), for mode number M) satisfies this condition. In detail, instead of randomly choosing the outcome, we can fix the outcome by applying a random permutation to the global Haar random unitary distribution, which is still Haar distributed from its symmetric property. This hiding property plays an important role in the current proofs of the average-case hardness, as it enables one to establish worst-to-average-case reduction. Specifically, as the output probability of boson sampling can be written as a low-degree polynomial of input circuit (matrix) values, it allows one to infer the value of a worst-case instance from the output probability of many average-case circuit instances. Hence, the average-case hardness argument for boson sampling is typically used in this context, i.e., average-case hardness over random circuit instances, for a fixed outcome [1, 3, 21].

Accordingly, the crucial step for the classical simulation hardness of approximate sampling is to prove the average-case hardness for the desired imprecision level. While there have been many impressive results about the average-case hardness of boson sampling [1, 3, 21, 22], the average-case hardness for the desired imprecision level is not yet fully demonstrated. Still, there exists a gap between the imprecision level of average-case hardness in the strongest existing results and the imprecision level of average-case approximation problem. Hence, closing this imprecision gap

remains the ultimate challenge for the fully theoretically guaranteed computational advantage of approximate boson sampling.

Appendix B: Proof of Theorem 3

The proof of Theorem 3 can be greatly simplified by introducing the following two Lemmas.

Lemma 5 (Brod [25], revised)**.** *For an arbitrary given poly-sized n-qubit quantum circuit Q, there exists a constant depth linear optical circuit C such that for $M \geq 2N$ and $N = poly(n)$,*

$$|\langle I|\hat{\mathcal{U}}(C)|I\rangle|^2 = c_Q|\langle 0|^{\otimes n} Q |0\rangle^{\otimes n}|^2, \tag{B1}$$

where c_Q is a Q dependent constant which can be efficiently computed, $\hat{\mathcal{U}}(C)$ is a unitary operator corresponding to the circuit C, and $|I\rangle$ is an M-mode Fock state composed of N single photon states and vacuum states for the rest modes.

Proof. We revise the results by [25], for a more rigorous analysis of the allowed additive imprecision level for the worst-case hardness of shallow-depth boson sampling. Ref. [25] proposed that certain 4-depth linear-optical circuits with post-selection can simulate universal quantum computing. Specifically, to simulate any poly-sized quantum circuit Q on n qubits, there exists a measurement-based quantum computation (MBQC) scheme using constant depth brickwork graph state of maximally poly(n) qubits [42–44]. The corresponding scheme can also be implemented in a linear optical system via KLM scheme [45] with post-selection, using $N = \text{poly}(n)$ number of single photon states over $M \geq 2N$ modes (requirements for the dual-rail encoding), which can simulate the quantum circuit composed of $O(N)$ number of gates.

Therefore, given the circuit in [25] and an appropriate dual-rail encoded state $|I\rangle$, the output probability of any quantum circuit Q can be represented as Eq. (B1), where c_Q denotes the product of post-selection probabilities for gate implementations. To compute c_Q, we need to figure out the required number of gates to implement the circuit Q and their probabilities to be post-selected. More precisely, from [25], post-selection occurs for two cases: (i) for the CZ gate to implement the brickwork graph state, and (ii) for the gate set {CX, T, H} (i.e., universal set of gates) which can be implemented by measurement of the graph state.

Hence, c_Q can be expressed as

$$c_Q = \prod_{k\in\{\text{CZ, CX, T, H}\}} p_k^{\Gamma_k}, \tag{B2}$$

where p_k denotes post-selection probability of k gate (e.g., p_{CZ} is 2/27 in [46]), and Γ_k denotes the number of k gate to implement the circuit Q. By counting the number of each gate to implement the circuit Q, c_Q can be computed efficiently. □

Lemma 6 (Kondo et al [34])**.** *It is #P-hard to compute $|\langle 0|^{\otimes n} Q |0\rangle^{\otimes n}|^2$ for an arbitrary given quantum circuit Q within the additive error less than 2^{-2n}.*

Combining the above results, now we prove the worst-case hardness of output probability approximation of boson sampling in the shallow-depth circuit architecture $\mathcal{BB}^*$, for fixed input and output corresponding to the $|I\rangle$ in Lemma 5. By Lemma 6, approximating output probabilities of worst-case n-qubit BQP circuits within additive error 2^{-2n} is #P-hard. Also, one can easily check that the constant depth linear-optical circuit proposed by [25] can be efficiently embedded in the architecture $\mathcal{BB}^*$. Hence, by Lemma 5, approximating $p_{\boldsymbol{s}}(C)$ of any C over $\mathcal{BB}^*$, for both input

and output $\boldsymbol{s}$ corresponding to the $|I\rangle$, can be reduced from approximating output probabilities of any BQP circuits, with c_Q^{-1} blowup in the additive imprecision. Since the post-selection occurs $O(N)$ times to implement n-qubit BQP circuit by Lemma 5, c_Q has its amplitude $c_Q = 2^{-O(N)}$, and thus the allowed additive error for the reduction is $2^{-(2n+O(N))} = 2^{-O(N)}$.

Appendix C: Proof of Theorem 4

In this proof, we establish the worst-to-average-case reduction, from the problem in Theorem 3 to the problem in Theorem 4. Let $\mathcal{O}$ be an oracle that solves the problem in Theorem 4, i.e., on input $\boldsymbol{s} \sim \mathcal{G}_{M,N}$ and $U \sim \mathcal{H}_{\mathcal{A}}$ with $\mathcal{A} = (\mathcal{BB}^*)^q$ for fixed $q \geq 2$, the oracle outputs $p_{\boldsymbol{s}}(U)$ within additive error ϵ for high constant probability over U and $\boldsymbol{s}$. Let C_0 be the worst-case circuit in $(\mathcal{BB}^*)^{q_0}$ with $q_0 \geq 1$, and $\boldsymbol{s}_0$ the fixed collision-free output given in Theorem 3. In the following, we show that approximating $p_{\boldsymbol{s}_0}(C_0)$ to within additive error $2^{-O(N)}$ (i.e., Theorem 3) is in $\mathrm{BPP}^{\mathrm{NP}^{\mathcal{O}}}$, which implies that the average-case approximation of $p_{\boldsymbol{s}}(U)$ to within ϵ is #P-hard under $\mathrm{BPP}^{\mathrm{NP}}$ reduction.

Our main idea for the reduction from the fixed outcome $\boldsymbol{s}_0$ to the randomly chosen outcome $\boldsymbol{s} \sim \mathcal{G}_{M,N}$ is to *permute* the worst-case circuit in correspondence with the random outcome $\boldsymbol{s}$. Specifically, we first sample permutation matrix $\boldsymbol{P}$ uniformly over all possible M mode permutation, where the sampled $\boldsymbol{P}$ can be efficiently implemented in the circuit architecture $\mathcal{BB}^*$ from Lemma 1. Let $\boldsymbol{s}_{\boldsymbol{P}}$ be the permuted outcome $\boldsymbol{P}\boldsymbol{s}_0$ by the sampled permutation $\boldsymbol{P}$, where one can easily check that $\boldsymbol{s}_{\boldsymbol{P}} \sim \mathcal{G}_{M,N}$. Also, let $C_{\boldsymbol{P}}$ be the permuted circuit $\boldsymbol{P}C_0$, where now the circuit $C_{\boldsymbol{P}}$ is in $(\mathcal{BB}^*)^{q_0+1}$. In this case, from Eq. (1), the output probability of the permuted outcome from the permuted circuit is identical to the worst-case output probability, i.e., $p_{\boldsymbol{s}_{\boldsymbol{P}}}(C_{\boldsymbol{P}}) = p_{\boldsymbol{s}_0}(C_0)$. From now on, we set $p_{\boldsymbol{s}_{\boldsymbol{P}}}(C_{\boldsymbol{P}})$ as a worst-case output probability, and our new goal is to estimate $p_{\boldsymbol{s}_{\boldsymbol{P}}}(C_{\boldsymbol{P}})$ given access to the oracle $\mathcal{O}$.

For the reduction from the worst-case circuit $C_{\boldsymbol{P}}$ to the average-case circuits, we sample random circuit $U(\theta)$ in $(\mathcal{BB}^*)^q$ with $q = q_0 + 1$, by sampling independently distributed local Haar random gate $\{H_i\}_{i=1}^m$ for gate number $m = qM \log M$, perturbing them by the Cayley transform parameterized by θ and multiplying the worst-case circuit gates from $C_{\boldsymbol{P}}$ as in Definition 7. Then, $U(\theta)$ follows the distribution $\mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}$, with $\mathcal{A} = (\mathcal{BB}^*)^q$, and $U(1) = C_{\boldsymbol{P}}$.

Given randomly chosen outcome $\boldsymbol{s}_{\boldsymbol{P}} \sim \mathcal{G}_{M,N}$ and circuit $U(\theta) \sim \mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}$, we input them in the oracle $\mathcal{O}$. For at least $1-\eta$ over $\boldsymbol{s}_{\boldsymbol{P}}$, the failure probability of $\mathcal{O}$ is at most

$$\Pr_{U(\theta)\sim\mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}}[|\mathcal{O}(\boldsymbol{s}_{\boldsymbol{P}}, U(\theta)) - p_{\boldsymbol{s}_{\boldsymbol{P}}}(U(\theta))| > \epsilon] < \delta + D_{\mathrm{TV}}(\mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}, \mathcal{H}_{\mathcal{A}}), \tag{C1}$$

where D_{TV} denotes total variation distance. This is evident as we can interpret the total variation distance as the supremum over events of the difference in probabilities of those events (Viz., circuits corresponding to the failure) [32]. By Lemma 2, $D_{\mathrm{TV}}(\mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}, \mathcal{H}_{\mathcal{A}})$ is $O(m\theta)$. By setting $0 \leq \theta \leq \Delta$ with $\Delta = O(m^{-1})$, we can upper bound $D_{\mathrm{TV}}(\mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}, \mathcal{H}_{\mathcal{A}})$ by an arbitrarily small constant.

By Lemma 3, $p_{\boldsymbol{s}_{\boldsymbol{P}}}(U(\theta))$ is a $(4mN, 4mN)$ degree rational function $\frac{P(\theta)}{Q(\theta)}$, where the denominator is given as $Q(\theta) = \left[\prod_{i=1}^m |q_i(\theta)|^2\right]^N$. We note that $Q(\theta)$ can be computed in $\Theta(m)$ time, as it only depends on the constant number of eigenvalues of local gate matrices (i.e., ϕ_j values in Eq. (4)) for each local gate matrix H_i). Also, given that $\theta \leq \Delta = O(m^{-1})$, $Q(\theta)$ is very close to the unity, as

$Q(\theta) \geq 1$ and

$$\begin{aligned} Q(\theta) &= \left[\prod_{i=1}^{m} |q_i(\theta)|^2\right]^N \\ &= \left[\prod_{i=1}^{m}\prod_{j=1}^{2} |(1 + i\theta e^{i\frac{\phi_{i,j}}{2}} \sin\frac{\phi_{i,j}}{2})|^2\right]^N \\ &\leq \left[\prod_{i=1}^{m}\prod_{j=1}^{2} (1+\theta^2)\right]^N \\ &\leq (1 + O(m^{-2}))^{2mN} \\ &= 1 + O(Nm^{-1}), \end{aligned} \tag{C2}$$

where $\phi_{i,j}$ denotes the phase of the jth eigenvalue of the ith gate.

Therefore, $p_{\boldsymbol{s_P}}(U(\theta))$ is very close to the degree $d = 4mN$ polynomial $P(\theta)$ in $\theta \in [0, \Delta]$, which allows us to use polynomial interpolation technique for $P(\theta)$. Specifically, we obtain estimations of $P(\theta)$ for different values of $\theta \in [0, \Delta]$ by querying the oracle $\mathcal{O}$, use polynomial interpolation for given $P(\theta)$ values to estimate $P(1)$, and infer the value $p_{\boldsymbol{s_P}}(U(1)) = p_{\boldsymbol{s_P}}(C_{\boldsymbol{P}})$ by multiplying $Q(1)^{-1}$. However, $Q(1)^{-1}$ becomes arbitrarily large for the case that even a single $\phi_{i,j}$ in Eq. (C2) is near $\pm\pi$, which will arbitrarily enlarge the imprecision of the approximation of $p_{\boldsymbol{s_P}}(U(1))$. To avoid this issue, we employ the strategy from Ref. [21], which only considers the case that all $\phi_{i,j}$ values of randomly chosen gates $\{H_i\}_{i=1}^m$ are in $[-\pi+\zeta, \pi-\zeta]$, and regards the other case as failure. This happens with probability at least $1 - O(m\zeta)$ over the random circuit instances. By setting $\zeta = O(m^{-1})$, we can make $O(m\zeta)$ arbitrarily small constant, and as a result, we can upper bound $Q(1)^{-1}$ (see Eq. (C6) below) with high probability over random circuit instances.

Now the problem reduces to approximating degree $d = 4mN$ polynomial $P(\theta)$ with the value $\mathcal{O}(\boldsymbol{s_P}, U(\theta))Q(\theta)$ in $\theta \in [0, \Delta]$ within additive error smaller than $\epsilon(1 + O(Nm^{-1})) \approx \epsilon$; such approximations will later be used for the estimation of the value $P(1)$ via polynomial interpolation technique. The failure of $\mathcal{O}$ depends on the outcome $\boldsymbol{s_P} \sim \mathcal{G}_{M,N}$ whose failure probability is at most η, and the circuit $U(\theta) \sim \mathcal{H}_{\mathcal{A},\theta}^{C_{\boldsymbol{P}}}$ whose failure probability is at most $\delta + O(m\Delta)$ from Eq. (C1). Also, the probability that at least one $\phi_{i,j}$ of randomly chosen gates $\{H_i\}_{i=1}^m$ is outside of the regime $[-\pi+\zeta, \pi-\zeta]$ is at most $O(m\zeta)$. Putting everything together and applying a simple union bound, the total failure probability of the approximation of $P(\theta)$ is at most

$$\begin{aligned} \Pr[|\mathcal{O}(\boldsymbol{s_P}, U(\theta))Q(\theta) - P(\theta)| > \epsilon] &< \eta + \delta + O(m\Delta) + O(m\zeta) \\ &\leq \delta', \end{aligned} \tag{C3}$$

where δ' is an upper bound of $\eta + \delta + O(m\Delta) + O(m\zeta)$, and given $\eta + \delta < \frac{1}{4}$, we can make $\delta' < \frac{1}{4}$ by setting $O(m\Delta)$ and $O(m\zeta)$ arbitrary small constants.

Let $\{\theta_i\}_{i=1}^{O(d^2)}$ be the set of equally spaced points in the interval $[0, \Delta]$. For each θ_i, we obtain the unitary matrix $U(\theta_i)$ using the same random gate $\{H_i\}_{i=1}^m$ and worst-case circuit $C_{\boldsymbol{P}}$. Let $y_i = \mathcal{O}(\boldsymbol{s_P}, U(\theta_i))Q(\theta_i)$. By Eq. (C3), each set of points (θ_i, y_i) satisfies

$$\Pr[|y_i - P(\theta_i)| > \epsilon] \leq \delta' < \frac{1}{4}. \tag{C4}$$

By using the interpolation algorithm introduced in Theorem 8, we can obtain the additive approximation of $P(1)$ as $\tilde{p}$ with an access to NP oracle, such that

$$\Pr\left[|\tilde{p} - P(1)| > \epsilon'\right] < \frac{1}{3}, \tag{C5}$$

where $\epsilon' = \epsilon e^{-d\log\Delta} = \epsilon 2^{O(N^{\gamma+1}(\log N)^2)}$ using $d = 4mN$ and $m = qM\log M$. Note that the failure probability in Eq. (C5) can be arbitrarily reduced by taking a polynomial number of trials, and thus we can obtain the estimated value $P(1)$ within additive error ϵ' with arbitrarily high probability.

From the estimated value $P(1)$, we can infer the worst-case output probability value $p_{\boldsymbol{sP}}(U(1)) = P(1)/Q(1)$. As the value of $Q(1)$ depends on the values $\phi_{i,j}$ in Eq. (C2), the $\phi_{i,j}$ independent lower bound of $Q(1)$ is required to set an upper bound of the additive imprecision of $p_{\boldsymbol{sP}}(U(1))$. Since we only consider the case that all of $\phi_{i,j}$ values are in $[-\pi+\zeta, \pi-\zeta]$ with $\zeta = O(m^{-1})$ for all randomly chosen gates $\{H_i\}_{i=1}^m$, we have

$$\begin{aligned} Q(1) &= \left[\prod_{i=1}^{m}\prod_{j=1}^{2} |(1+ie^{i\frac{\phi_{i,j}}{2}}\sin\frac{\phi_{i,j}}{2})|^2\right]^N \\ &= \left[\prod_{i=1}^{m}\prod_{j=1}^{2}\left(1-\sin^2\frac{\phi_{i,j}}{2}\right)\right]^N \\ &\geq \left[\prod_{i=1}^{m}\prod_{j=1}^{2}\left(1-\sin^2\frac{\pi-\zeta}{2}\right)\right]^N \\ &= \left(O(m^{-2})\right)^{2mN} \\ &= 2^{2mN\log O(m^{-2})}. \end{aligned} \tag{C6}$$

Therefore, the total additive error for estimating $p_{\boldsymbol{sP}}(U(1))$ is bounded by $\epsilon' 2^{-2mN\log O(m^{-2})} = \epsilon 2^{O(N^{\gamma+1}(\log N)^2)}$. By setting $\epsilon = 2^{-O(N^{\gamma+1}(\log N)^2)}2^{-O(N)} = 2^{-O(N^{\gamma+1}(\log N)^2)}$, we can estimate the worst-case output probability value $p_{\boldsymbol{sP}}(U(1)) = p_{\boldsymbol{sP}}(C_{\boldsymbol{P}}) = p_{\boldsymbol{s}_0}(C_0)$ within additive error $2^{-O(N)}$, and the whole reduction process is in $\mathrm{BPP}^{\mathrm{NP}}$. This completes the proof.

For the polynomial interpolation, we employ the Robust Berlekamp-Welch algorithm recently proposed in Ref. [21].

Theorem 8 (Robust Berlekamp-Welch [21])**.** *Let $P(x)$ be a degree d polynomial in x. Suppose there is a set of points $D = \{(x_i, y_i)\}$ such that $|D| = O(d^2)$ and $\{x_i\}$ is equally spaced in the interval $[0, \Delta]$. Suppose also that each points (x_i, y_i) satisfies*

$$\Pr[|y_i - P(x_i)| \geq \epsilon] \leq \delta, \tag{C7}$$

with $\delta < \frac{1}{4}$. Then there exists a P^{NP} algorithm that takes input D and outputs $\tilde{p}$ such that

$$|\tilde{p} - P(1)| \leq \epsilon e^{-d\log\Delta}, \tag{C8}$$

with success probability at least $\frac{2}{3}$.

Appendix D: Proof of Lemma 4

Let $\bar{p}_{\boldsymbol{s}}(C)$ be the output probability distribution from the approximate sampler $\mathcal{S}$ with the given linear optical circuit C. Also, let $\mathcal{C}_{M,N}$ be the set of collision-free outcomes of boson sampling, for mode number M and photon number N. Then $\bar{p}_{\boldsymbol{s}}(C)$ satisfies

$$\mathop{\mathbb{E}}_{\boldsymbol{s}\sim\mathcal{G}_{M,N}}[|\bar{p}_{\boldsymbol{s}}(C) - p_{\boldsymbol{s}}(C)|] = \frac{1}{\binom{M}{N}}\sum_{\boldsymbol{s}\in\mathcal{C}_{M,N}}|\bar{p}_{\boldsymbol{s}}(C) - p_{\boldsymbol{s}}(C)| \leq \frac{2\beta}{\binom{M}{N}}. \tag{D1}$$

Using Eq. (D1) and Markov's inequality, $\bar{p}_{\boldsymbol{s}}(C)$ satisfies

$$\Pr_{\boldsymbol{s}\sim\mathcal{G}_{M,N}}\left[|\bar{p}_{\boldsymbol{s}}(C)-p_{\boldsymbol{s}}(C)|\geq\frac{\beta k}{\binom{M}{N}}\right]\leq\frac{2}{k} \tag{D2}$$

for all $k>2$. Also, using Stockmeyer's algorithm [38] whose complexity is in $\mathrm{BPP}^{\mathrm{NP}}$, obtaining the estimate $\tilde{p}_{\boldsymbol{s}}(C)$ of $\bar{p}_{\boldsymbol{s}}(C)$ satisfying

$$\Pr\left[|\tilde{p}_{\boldsymbol{s}}(C)-\bar{p}_{\boldsymbol{s}}(C)|\geq\alpha\bar{p}_{\boldsymbol{s}}(C)\right]\leq\frac{1}{2^N}, \tag{D3}$$

in polynomial time in N and α^{-1} is in $\mathrm{BPP}^{\mathrm{NP}^{\mathcal{S}}}$. Using $\mathbb{E}_{\boldsymbol{s}\sim\mathcal{G}_{M,N}}[\bar{p}_{\boldsymbol{s}}(C)]=\binom{M}{N}^{-1}\sum_{\boldsymbol{s}\in\mathcal{C}_{M,N}}\bar{p}_{\boldsymbol{s}}(C)\leq\binom{M}{N}^{-1}$,

$$\Pr\left[|\tilde{p}_{\boldsymbol{s}}(C)-\bar{p}_{\boldsymbol{s}}(C)|\geq\frac{\alpha l}{\binom{M}{N}}\right]\leq\Pr\left[\bar{p}_{\boldsymbol{s}}(C)\geq\frac{l}{\binom{M}{N}}\right]+\Pr\left[|\tilde{p}_{\boldsymbol{s}}(C)-\bar{p}_{\boldsymbol{s}}(C)|\geq\alpha\bar{p}_{\boldsymbol{s}}(C)\right] \tag{D4}$$

$$\leq\frac{1}{l}+\frac{1}{2^N}, \tag{D5}$$

for all $l>1$. Putting all together, by applying a triangular inequality, finding an average-case approximation $\tilde{p}_{\boldsymbol{s}}(C)$ of $p_{\boldsymbol{s}}(C)$ satisfying

$$\Pr\left[|\tilde{p}_{\boldsymbol{s}}(C)-p_{\boldsymbol{s}}(C)|\geq\frac{\beta k+\alpha l}{\binom{M}{N}}\right]\leq\frac{2}{k}+\frac{1}{l}+\frac{1}{2^N} \tag{D6}$$

is in $\mathrm{BPP}^{\mathrm{NP}^{\mathcal{S}}}$. Let κ and ξ be fixed error parameters such that $k/2=l=3/\xi$ and $\beta=\kappa\xi/12=\alpha/2$. As $\beta k+\alpha l=\kappa$ and $\frac{2}{k}+\frac{1}{l}+\frac{1}{2^N}=\frac{2}{3}\xi+\frac{1}{2^N}\leq\xi$, we finally obtain the Eq. (9).

Estimating the non-Markovianity with kernel-based quantum machine learning model

Chuan-chi, Huang[1] * Hong-Bin, Chen[1 2 3] †

[1] *Department of Engineering Science, National Cheng Kung University, Tainan 701401, Taiwan*
[2] *Center for Quantum Frontiers of Research & Technology, NCKU, Tainan 701401, Taiwan*
[3] *Physics Division, National Center for Theoretical Sciences, Taipei 106319, Taiwan*

Abstract.
Characterization and quantification of the non-Markovian behaviors of dynamical processes have attracted long-lasting research interest in the field of open quantum system dynamics. Many different measures of non-Markovianity have been proposed based on the temporal variation of certain quantities of interest. Therefore, their experimental realizations would require vast raw data with sufficient time resolution along time axis. Here we propose to harness the power of kernel-based quantum machine learning models to estimate the non-Markovianity according to spare temporal data. To demonstrate our approach, we generate the training data according to the spin-boson model. We also compare the quantum model with two classical ones. We find that the quantum model is capable of reliably predicting the non-Markovianity even if the raw data is temporally spare, and the quantum model performs better than some types of classical learning models. Therefore, our approach would be promising in reducing the experimental efforts for estimating the non-Markovianity.

Keywords: open quantum system, non-Markovianity, spin-boson model, quantum kernel, quantum machine learning

1 Introduction

Due to the inevitable interactions to the surrounding environments, any quantum systems behave incoherently [1]. During their time evolutions, the past memory would have significant impacts on the time evolutions in the future, leading to non-Markovian characteristics [2, 3, 4]. Over the past decades, there have been many efforts devoted to the characterization and quantification of the non-Markovianity [2, 3]. In these quantitative measures of non-Markovianity, one typically focuses on the temporal variation of certain quantities of interest, the degree of non-Markovianity can be estimated accordingly. Additionally, the experimental realizations have been implemented [5, 6, 7].

Among these experimental realizations, It is necessary to gather a huge amount of raw data with sufficient time resolution to guarantee the accuracy of the estimation of the non-Markovianity. This would require extensive experimental efforts in repeating the experimental protocol for gathering the raw data. Therefore, we are spurred to seek for an efficient approach to estimate the non-Markovianity with merely spare data.

On the other hand, along with the rapid development of quantum computing technology [8, 9, 10], the idea of accelerating machine learning (ML) algorithms with quantum computers has been proposed. Particularly, the support vector machine (SVM) [11], one of the most well-studied and widely applied ML, has been demonstrated on quantum computers [12, 13]. The SVM model can handle two types of problems, namely, classification (e.g. Ref [14]) and regression problems [15] . When do a classification problem, The model will find a boundary to separate the data. Relatively, when model deal with the regression problem, it will find a curve to fit the data.

Here we proposed to employ the kernel-based quantum machine learning approach to estimate the non-Markovianity from spare data. It is a creative method that leveraging the principles of quantum computing to enhance classical algorithms. We have verified that this method is feasible, and the error of the quantum enhanced algorithm is much smaller than that of some classical algorithms. This lays an important foundation for further research in the future.

2 Measure of non-Markovianity

Non-Markovianity refers to the property of a quantum system's evolution where the memory effects of the system's past interactions with its environment play a significant role. It indicates deviations from the standard Markovian dynamics, where the future state of the system depends only on its current state and is independent of its past history.

A variety of techniques have been developed to quantify the non-Markovianity of quantum systems. In our study, we utilise the trace distance, which is based on the concept of information flow, and the BLP measure, which is derived from the same concept. Both measures are capable of quantifying the degree to which information flows back from the environment to the system during its evolution. This can be achieved by measuring the backflow of distinguishability, a quantity which indicates the extent to which the distinguishability of initially indistinguishable states increases due to the system-environment interaction.

*N96124365@gs.ncku.edu.tw
†hongbinchen@gs.ncku.edu.tw

3 Learning non-Markovianity with kernel based support vector machine

The incorporation of machine learning techniques into efficient measurement processes can be greatly beneficial. To achieve this, it's essential to prepare a robust dataset for model training. In our research, we leverage the spin boson model [16, 5] within the limits of our experimental equipment to generate the requisite data. During the data generation process, it became evident that there was a notable imbalance in the dataset. Our analysis revealed that the majority of the time evolution data exhibited a Markovian pattern, whereas instances demonstrating a substantial non-Markovian behavior were notably scarce. To address this imbalance, we adopt a strategic approach. We divide the entire dataset into several distinct pieces, each representing a segment of the data. Subsequently, we employed a random selection process within each piece. The objective of this method was to rectify the imbalance within the dataset, thereby ensuring a more representative and balanced training set for our machine learning models. This step is crucial in optimizing the performance and accuracy of our machine learning algorithms, as it facilitates a more comprehensive understanding of both Markovian and non-Markovian dynamics within the dataset. Ultimately, by mitigating imbalance, we enhance the effectiveness of our measurement processes and pave the way for more insightful analyses in our research endeavors.

Once a well-prepared and balanced dataset has been assembled, the subsequent crucial step is to train a machine learning (ML) model. As previously noted, support vector machines (SVMs) are particularly adept at handling both classification and regression tasks. Given that the non-Markovianity value falls within the real number spectrum, ranging from 0 to 1, it is more closely aligned with a regression problem. Consequently, during the training phase, not only are quantum feature maps applied to the data, but their efficacy is also explored in conjunction with other kernel functions that are commonly utilised in support vector machines, including the Radial Basis Function (RBF) and the linear kernels. The objective of this comparative analysis is to elucidate the impact of quantum feature mapping in contrast to classical kernel methods.

The training of an SVM model involves the identification of the optimal hyperplane that best separates the data points of different classes in the feature space. The selection of a kernel function is of paramount importance, as it determines the mapping of data into higher-dimensional spaces where the separation becomes linear. In contrast to quantum feature mapping, traditional SVMs employ classical kernel functions such as the RBF and linear kernels, which have been extensively studied and applied in a multitude of domains.

Nevertheless, with the advent of quantum computing [17] and the promise it holds for enhancing machine learning tasks, researchers have begun exploring the integration of quantum computing principles into SVMs. The use of quantum feature maps represents a novel approach to feature mapping, whereby nonlinear transformations on the input data are performed by leveraging quantum circuits. These mappings enable the SVM to operate in a higher-dimensional Hilbert space, which may result in improved performance in capturing complex relationships within the data.

In the training procedure, experiments are conducted using both quantum feature maps and classical kernel functions to assess their respective performances. The objective of this study is to compare the results obtained from the different approaches in order to discern any advantages or disadvantages inherent in employing quantum feature mapping in SVMs.

This comparative analysis contributes to the growing body of research investigating the potential of quantum computing techniques in enhancing machine learning algorithms. By elucidating the relative strengths and weaknesses of quantum feature mapping in comparison to classical kernel methods, we aim to provide valuable insights that can inform future developments in quantum-enhanced machine learning techniques.

4 Quantum feature mapping

Quantum feature mapping [12] represents a departure from the conventional methods of mapping data into feature spaces, particularly in the domain of quantum machine learning. It introduces a novel approach where classical data is encoded into quantum states, thereby enabling quantum-enhanced processing. Among the key techniques employed in this encoding process is the ZZ feature map, which plays a pivotal role in preparing the quantum state.

4.1 The encoding of classical data into quantum states

The initial step in quantum feature mapping entails the encoding of classical data into quantum states. This process is of pivotal importance, as it transforms classical information into a quantum representation suitable for processing on quantum computers. The ZZ feature map serves as a mechanism to facilitate this transformation.

4.2 Utilising the ZZ feature map

The ZZ feature map is a specific quantum feature map commonly employed for encoding classical data into quantum states. It operates by inducing entanglement between qubits through the ZZ interaction term in a quantum circuit. By leveraging this entanglement, the ZZ feature map effectively prepares the quantum state, capturing essential characteristics of the classical data.

4.3 Computing inner products

Once the classical data is encoded into quantum states using the ZZ feature map, the next step involves computing the inner product between these quantum states. This inner product essentially measures the similarity or dissimilarity between the quantum states, serving as a kernel function in classical machine learning algorithms.

5 Classical kernel

In the context of Support Vector Machines (SVM), kernels play a pivotal role in transforming the input data into a higher-dimensional space, where it may be more straightforward to identify a linear separation between classes. Two of the most commonly employed kernels in SVM are the radial basis function (RBF) kernel and the linear kernel.

5.1 Radial basis function (RBF) kernel

The RBF kernel is a popular choice due to its capacity to handle non-linear decision boundaries. The input data is mapped into a higher-dimensional space through the use of a Gaussian function. Mathematically, the RBF kernel is defined as:

$$K(x_i, x_j) = exp(-\frac{\|x_i - x_j\|^2}{2\sigma^2})$$

The symbol $\|x_i - x_j\|$ represents the Euclidean distance between the feature vectors x_i and x_j. The parameter σ determines the spread of the kernel. The RBF kernel incorporates a centre parameter, γ, which is inversely proportional to σ. A small value of γ leads to a smoother decision boundary, while a large value results in a more complex decision boundary, which may potentially lead to overfitting. It is of paramount importance to optimise the γ parameter in order to achieve optimal performance with the RBF kernel. In conclusion, while the linear kernel is effective for linearly separable data, the RBF kernel is more flexible and can effectively handle non-linear decision boundaries. Nevertheless, it is essential to exercise caution and perform meticulous parameter tuning in order to prevent overfitting.

5.2 Linear kernel

The linear kernel is the simplest kernel function, in that it is the only kernel function that does not require any additional parameters to be specified. The inner product of the feature vectors in the original space represents this kernel. Mathematically, it is defined as follows:

$$K(x_i, x_j) = x_i^T \cdot x_j$$

In this context, x_i and x_j represent two feature vectors. The effectiveness of this kernel is contingent upon the data being linearly separable, which implies that classes can be separated by a straight line or hyperplane in the original feature space. Its efficacy is enhanced when the number of features is significantly larger than the number of samples. However, in instances where classes are not linearly separable, the linear kernel may not perform optimally. In such cases, the Radial Basis Function (RBF) kernel can be leveraged to enhance the classification accuracy.

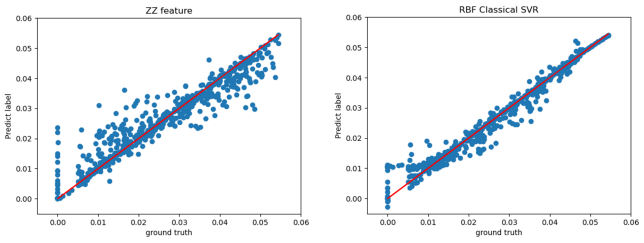
6 Conclusions

After training the models using the three different methods mentioned, the next critical step is to evaluate their predictive performance. The results of this testing phase are typically visualized to provide insight into how well the models predict compared to the ground truth. In this situation, the comparison could be illustrated using scatter plots where correctly predicted points lie on a reference line. Observing the distribution of the blue dots relative to the reference line provides important insight into the performance of each model. For example, in the case of the RBF kernel model, the blue dots tend to cluster more closely around the reference line compared to the ZZ feature model. Conversely, the linear kernel model shows the poorest performance, as evidenced by the scattered distribution of the blue dots. Additionally, it's worth noting that all three models perform suboptimally when predicting numerical values that are small. This observation underscores the importance of understanding the limitations and biases inherent in the models' predictions, especially in scenarios where the input data falls within a certain range. A common indicator used to quantitatively assess model performance is the mean squared error rate (MSE). it is defined as follows:

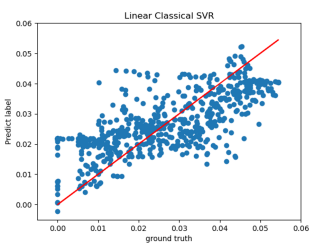
$$\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y_i})^2$$

The MSE measures the average squared difference between the predicted values and the actual ground truth values. A lower MSE indicates better predictive accuracy, while a higher MSE indicates a greater discrepancy between the predicted and actual values. By calculating and comparing the MSE for each model, users can objectively evaluate their relative performance and make informed decisions about model selection and refinement. Because the MSE is a rate of error, the smaller is better. In the table below, you can see that RBF has the lowest MSE, followed by ZZ feature map and finally linear kernel.

Method	Quantum	RBF	Linear
MSE	2.28e-05	1.62e-05	0.000114



(a) Quantum kernel (b) RBF kernel



(c) Linear kernel

Figure 1: Target versus predicted values graph

References

[1] Heinz-Peter Breuer and Francesco Petruccione. *The theory of open quantum systems*. OUP Oxford, 2002.

[2] Ángel Rivas, Susana F Huelga, and Martin B Plenio. Quantum non-markovianity: characterization, quantification and detection. *Reports on Progress in Physics*, 77(9):094001, 2014.

[3] Heinz-Peter Breuer, Elsi-Mari Laine, Jyrki Piilo, and Bassano Vacchini. Colloquium: Non-markovian dynamics in open quantum systems. *Reviews of Modern Physics*, 88(2):021002, 2016.

[4] Inés De Vega and Daniel Alonso. Dynamics of non-markovian open quantum systems. *Reviews of Modern Physics*, 89(1):015001, 2017.

[5] Bi-Heng Liu, Li Li, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Elsi-Mari Laine, Heinz-Peter Breuer, and Jyrki Piilo. Experimental control of the transition from markovian to non-markovian dynamics of open quantum systems. *Nature Physics*, 7(12):931–934, 2011.

[6] Bi-Heng Liu, Dong-Yang Cao, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Elsi-Mari Laine, Heinz-Peter Breuer, and Jyrki Piilo. Photonic realization of nonlocal memory effects and non-markovian quantum probes. *Scientific reports*, 3(1):1781, 2013.

[7] Felipe F Fanchini, Goktug Karpat, Baris Çakmak, LK Castelano, GH Aguilar, O Jiménez Farías, SP Walborn, PH Souto Ribeiro, and MC De Oliveira. Non-markovianity through accessible information. *Physical Review Letters*, 112(21):210402, 2014.

[8] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[9] Petar Jurcevic, Ali Javadi-Abhari, Lev S Bishop, Isaac Lauer, Daniela F Bogorin, Markus Brink, Lauren Capelluto, Oktay Günlük, Toshinari Itoko, Naoki Kanazawa, et al. Demonstration of quantum volume 64 on a superconducting quantum computing system. *Quantum Science and Technology*, 6(2):025020, 2021.

[10] Youngseok Kim, Andrew Eddins, Sajant Anand, Ken Xuan Wei, Ewout Van Den Berg, Sami Rosenblatt, Hasan Nayfeh, Yantao Wu, Michael Zaletel, Kristan Temme, et al. Evidence for the utility of quantum computing before fault tolerance. *Nature*, 618(7965):500–505, 2023.

[11] Corinna Cortes and Vladimir Vapnik. Support-vector networks. *Machine learning*, 20:273–297, 1995.

[12] Vojtěch Havlíček, Antonio D Córcoles, Kristan Temme, Aram W Harrow, Abhinav Kandala, Jerry M Chow, and Jay M Gambetta. Supervised learning with quantum-enhanced feature spaces. *Nature*, 567(7747):209–212, 2019.

[13] 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.

[14] Edward Farhi and Hartmut Neven. Classification with quantum neural networks on near term processors. *arXiv preprint arXiv:1802.06002*, 2018.

[15] Diego Tancara, Hossein T. Dinani, Ariel Norambuena, Felipe F. Fanchini, and Raúl Coto. Kernel-based quantum regressor models learning non-markovianity. *Physical Review A*, 107(2), 2023.

[16] Hong-Bin Chen and Yueh-Nan Chen. Canonical hamiltonian ensemble representation of dephasing dynamics and the impact of thermal fluctuations on quantum-to-classical transition. *Scientific reports*, 11(1):10046, 2021.

[17] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[18] Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, and Vincent Dubourg. Scikit-learn: Machine learning in python. *the Journal of machine Learning research*, 12:2825–2830, 2011.

Appendix A Support Vector Regression

The objective of Support Vector Regression (SVR) is to identify a function that approximates the mapping from input variables to continuous output variables. In contrast to traditional approaches that seek to separate classes by identifying a hyperplane, SVR aims to fit as many data points as possible within a specified margin around the predicted values.

A.1 SVR formulation

Given a training dataset comprising n samples (x_i, y_i), where x_i represents the feature vector and y_i represents the target value, Support Vector Regression (SVR) aims to identify a function $f(x)$ that approximates the mapping $x \to y$ with minimal error. The optimization problem can be formulated as follows:

$$min \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}(\xi_i + \xi_i^*)$$

$$subject\ to \begin{cases} y_i - w \cdot x_i - b \leq \epsilon + \xi_i \\ w \cdot x_i + b - y_i \leq \epsilon + \xi_i^* \\ \xi_i, \xi_i^* \geq 0 \end{cases}$$

Here, w represents the weights, b represents the bias term, and ξ_i and ξ_i^* represent slack variables that permit the incorporation of residual errors beyond the margin threshold. C represents a regularization parameter that serves to regulate the trade-off between the minimization of error and the maximization of the margin.

A.2 Kernel trick

We use the scikit-learn [18] module to built the SVM model. It is a Python library that provides straightforward and effective tools for data mining and data analysis. It is constructed upon the foundations of NumPy, SciPy, and matplotlib, and it provides a plethora of machine learning algorithms for the execution of tasks such as classification, regression, clustering, dimensionality reduction, and more. Its user-friendly interface and extensive documentation have made it a popular choice for both novice and experienced users of machine learning.

Appendix B Formulations of measurement of non-Markovianity

Total Hamiltonian of open quantum system :$\hat{H_T} = \hat{H_S} + \hat{H_E} + \hat{H_I}$

Unitary time-evolution operator in the interaction picture:$\hat{U^I}(t) = \exp[i\psi(t)]\exp[\frac{\sigma_z}{\hbar}\hat{H_I}]$

Time evolution of total system:$\rho_T^I(t) = [\hat{U^I}(t)](\rho_S(0) \bigotimes \rho_E(0))[\hat{U^I}(t)]^\dagger$

Time evolution of reduced system:$\rho_S^I(t) = Tr_E[\rho_T^I(t)] = \begin{bmatrix} \rho_{11} & \rho_{1-1}\phi(t) \\ \rho_{-11}\phi(t) & \rho_{-1-1} \end{bmatrix}$

Trace Distance:$D(\rho_1, \rho_2) = \frac{\|\rho_1 - \rho_2\|_1}{2} = Tr\sqrt{(\rho_1 - \rho_2)^\dagger(\rho_1 - \rho_2)}/2$

Non-Markovianity: $N = \max_{\rho_1,\rho_2} \int_{\frac{dD}{dt}>0} \frac{dD(\rho_1(t),\rho_2(t))}{dt} dt$

According to our derivation, the trace distance of the system would equal to ϕ in reduced system through the time evoluted. This happens to be the dephasing factor of the system, so we choose the Spin boson model to make the dataset. The following is the formula of the model.

Appendix C Formulations of Spin boson model

C.1 Spin boson model with family of super-Ohmic spectral density(s>1)

$$\begin{aligned} \phi(t) &= e^{-\Phi^{(s)}(t)} \\ \Phi(t) &= -2\eta\Gamma(s-1)[2 - \frac{(1-i\omega_c t)^{s-1} + (1+i\omega_c t)^{s-1}}{(1+\omega_c^2 t^2)^{s-1}}] \\ +4\eta\Gamma(s-1)(\frac{k_B T}{\hbar\omega_c})^{s-1}&[2\zeta(s-1, \frac{k_B T}{\hbar\omega_c}) - \zeta(s-1, \frac{k_B T}{\hbar\omega_c}(1+i\omega_c t)) - \zeta(s-1, \frac{k_B T}{\hbar\omega_c}(1-i\omega_c t))] \end{aligned} \tag{1}$$

Gamma function: $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}dt, Re(Z) > 0$

Hurwitz zeta function: $\zeta(s,q) = \sum_{n=0}^{\infty}(q+n)^{-s}$

C.2 Bias spin boson model with the family of super-Ohmic spectral density(s>1)

$$\phi(t) = e^{-i\vartheta^{(s)}(t)-\Phi^{(s)}(t)}$$

$$\vartheta^{(s)}(t) = sign(t)\sin\varphi\eta\Gamma(s-1)[2-\frac{(1-i\omega_c t)^{s-1}+(1+i\omega_c t)^{s-1}}{(1+\omega_c^2 t^2)^{s-1}}]$$

$$\begin{aligned}\Phi(t) = -(1-\cos\varphi)\eta\Gamma(s-1)[2-\frac{(1-i\omega_c t)^{s-1}+(1+i\omega_c t)^{s-1}}{(1+\omega_c^2 t^2)^{s-1}}] \\ +2(1-\cos\varphi)\eta\Gamma(s-1)(\frac{k_B T}{\hbar\omega_c})^{s-1}[2\zeta(s-1,\frac{k_B T}{\hbar\omega_c})-\zeta(s-1,\frac{k_B T}{\hbar\omega_c}(1+i\omega_c t))-\zeta(s-1,\frac{k_B T}{\hbar\omega_c}(1-i\omega_c t))]\end{aligned} \tag{2}$$

Basically, These two Models simulated how the environment effect the boson, with several environmental parameter such as the temperature T, Ohmicity s and Bias angle φ.

Exact and local compression of quantum bipartite states

Kohtaro Kato[1] *

[1] *Department of Mathematical Informatics, Nagoya University, Furo-cho Chikusa-ku, Nagoya 464-8601, Japan*

Abstract. We study exact local compression of a quantum bipartite state, a task that applies local quantum operations to reduce Hilbert space dimensions while preserving correlations. We provide a formula for the minimal achievable dimensions, obtained by minimizing the Schmidt rank of a constructed pure state. Additionally, we obtain numerically tractable upper and lower bounds for the dimension. As an application, we consider exact compression of quantum channels, analyzing a post-processing step that reduces output dimensions while preserving the original channel's output information. The detailds are presented in [arXiv:arXiv:2309.07434].

Keywords: quantum data-compression, one-shot information theory, data-processing inequality, quantum sufficiency

1 Introduction

Quantum data compression is one of the most fundamental quantum information processing. Its concept is analogous to Shannon's classical data compression and aims to reduce the dimensions of the storage of quantum states while minimizing information loss. Various approaches to quantum compression, primarily focusing on achieving asymptotically or approximately accurate representations of quantum states, have been proposed [1–5]. These protocols have yielded valuable insights into the trade-offs between compression efficiency, fidelity, and additional resources.

In this submission, we introduce and analyze a task that we call local and exact compressions of bipartite quantum states, that is, a task in which one apply a quantum operation to one of the subsystems to reduce the dimension of the Hilbert space while perfectly preserving the bipartite correlation. This type of data compression is an exact and noiseless one-shot quantum data compression of general mixed state sources without side information or entanglement assistance.

An asymptotic scenario of local compressions is investigated in Ref. [5], and the optimal rate is given by the entropy of the state restricted on the subalgebra defined via the Koashi-Imoto decomposition [14]. Similarly, one can check that the minimal dimension of exact local compression is also given by a subspace defined via the Koashi-Imoto decomposition. However, the explicit calculation of the Koashi-Imoto decomposition is highly complicated, and thus, no closed formula for the optimal rate has been obtained so far.

To obtain the main result, we employ the theory of quantum sufficiency. State transformations without losing any information has been gaining interest in information theory and the condition is known as the sufficiency of statistics [6, 7]. Classical statistics are *sufficient* concerning a given statistical model if they are as informative as the original model. It is well known that the minimal random variable for describing a statistical model (a family of probability distributions) is given as the minimal sufficient statistics associated with it [8]. The concept of sufficiency has been extended to quantum systems [9,10], where the concept of sufficient statistics is replaced by that of sufficient subalgebras. The Koashi-Imoto decomposition can be viewed as a particular application of the sufficiency [11].

As a result, we show a closed formula to calculate the minimal dimension of the output Hilbert spaces. The formula is obtained by minimizing the Schmidt rank (i.e., the rank of the reduced matrix) over unitarily related states. As a corollary, we provide additional tractable lower and upper bounds for the minimal dimensions. Our result is based on the recent development of quantum sufficiency [11] and operator algebra quantum error correction [12, 13].

2 Exact and local compression

We are interested in the quantum bipartite state ρ_{AB} in the finite-dimensional Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. We assume without loss of generality that $\rho_A, \rho_B > 0$ (by restricting each Hilbert space to the support of the reduced state).

Definition 1. *We say a CPTP-map $\mathcal{E}_{B\to\tilde{B}} : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_{\tilde{B}})$ is an exact local compression of ρ_{AB} on B, if there exists another CPTP-map $\mathcal{R}_{\tilde{B}\to B}$ satisfying*

$$\mathcal{R}_{\tilde{B}\to B} \circ \mathcal{E}_{B\to\tilde{B}}(\rho_{AB}) = \rho_{AB}. \tag{1}$$

This study aims to calculate the minimal dimensions $d_{\tilde{B}}$ of the exact local compressions. It is sufficient to consider only the compressions on B (or A) because of the symmetry of the problem.

2.1 Koashi-Imoto decomposition

In Ref. [14], Koashi and Imoto analyzed the structure of quantum operations that remains a set of classically labeled quantum states $\{\rho_B^x\}_{x\in\chi}$ unchanged. This idea was generalized to a fully quantum setup in Ref. [15]. Consider a direct sum decomposition

$$\mathcal{H}_B \cong \bigoplus_i \mathcal{H}_{B_i^L} \otimes \mathcal{H}_{B_i^R} \tag{2}$$

$$\rho_{AB} = \bigoplus_i p_i \rho_{AB_i^L} \otimes \omega_{B_i^R}, \tag{3}$$

*kokato@i.nagoya-u.ac.jp

where $\{p_i\}$ is a probability distribution and $\rho_{AB_i^L}$ and $\omega_{B_i^R}$ are the states of $\mathcal{H}_A \otimes \mathcal{H}_{B_i^L}$ and $\mathcal{H}_{B_i^R}$, respectively.

Definition 2. *A decomposition in Eqs.* (2)-(3) *is said to be the Koashi-Imoto decomposition if for any CPTP-map* Λ_B *satisfying*

$$\Lambda_B(\rho_{AB}) = \rho_{AB}\,,$$

any Λ*'s Stinespring dilation isometry* $V_{B\to BE}$ *defined by*

$$\Lambda_B(\cdot) = \mathrm{tr}_E\left(V_{B\to BE}\cdot(V_{B\to BE})^\dagger\right)$$

is decomposed into

$$V_{B\to BE} = \bigoplus_i I_{B_i^L}\otimes V_{B_i^R\to B_i^R E} \tag{4}$$

satisfying

$$\mathrm{tr}_E\left(V_{B_i^R\to B_i^R E}\,\omega_{B_i^R}(V_{B_i^R\to B_i^R E})^\dagger\right) = \omega_{B_i^R}\quad \forall i.$$

The factorization theorem [16,17] further demonstrates that the minimal dimension of the exact compression for ρ_{AB} is then given by

$$d_{\bar{B}} := \sum_i d_{B_i^L}\,. \tag{5}$$

3 Summary of results

To state the main theorem, the following notations are introduced: for a given ρ_{AB}, we define a unital CP map as

$$\Omega^\dagger_{A\to B}(X_A) := \mathrm{tr}_A\left(J_{AB}(X_A^{T_A}\otimes I_B)\right), \tag{6}$$

where J_{AB} is a Choi-Jamilkowski operator, defined as follows:

$$J_{AB} := \rho_B^{-\frac{1}{2}}\rho_{AB}\rho_B^{-\frac{1}{2}} \geq 0\,. \tag{7}$$

We denote the nonzero eigenvalues of J_{AB} as ω_i. Subsequently, the Kraus operators $\{K_i^\dagger\}$ of $\Omega^\dagger_{A\to B}(\cdot) = \sum_i K_i^\dagger\cdot K_i$ satisfy $\mathrm{tr}(K_i^\dagger K_j) = \omega_i\delta_{ij}$. We then define a deformed CP-map $\tilde{\Omega}^\dagger_{A\to B}$ as

$$\tilde{\Omega}^\dagger_{A\to B}(\cdot) = \sum_{i=1}^{\mathrm{rank}(\rho_{AB})}\omega_i^{-\frac{1}{2}}K_i^\dagger\cdot K_i\,. \tag{8}$$

$\tilde{\Omega}^\dagger_{A\to B}$ is no longer unital but CP. The Choi operator of $\tilde{\Omega}^\dagger_{A\to B}$ is given by $\sqrt{J_{AB}}$,

Let $\mathcal{H}_{B_1}\cong\mathcal{H}_B$ and consider the two operators

$$E_{\mathcal{T}} = \sum_{a,b=1}^{d_A}\tilde{\Omega}^\dagger_{A\to B}(|a\rangle\langle b|)\otimes\overline{\tilde{\Omega}^\dagger_{A\to B_1}(|a\rangle\langle b|)} \tag{9}$$

$$RL_B := I_B\otimes\log\rho_{B_1}^{T_{B_1}} - \log\rho_B\otimes I_{B_1}\,, \tag{10}$$

where $\{|a\rangle\}$ is an orthonormal basis of $\mathcal{H}_A$. The spectral decompositions of these operators are as follows.

$$E_{\mathcal{T}} = \bigoplus_\lambda \lambda P_\lambda \tag{11}$$

$$RL_B = \bigoplus_\eta \eta Q_\eta\,, \tag{12}$$

where P_λ and Q_η are orthogonal projections to the eigensubspaces of $E_{\mathcal{T}}$ and RL_B, respectively. Denote the set of eigenvalues of A by $\mathrm{spec}(A)$ and define P_V as the projector onto the subspace

$$V := \bigoplus_{\eta\in\mathrm{spec}(RL)}(\mathrm{supp}(Q_\eta)\cap\mathrm{supp}(P_1))\,.$$

Using the formula given in [18],

$$P_V = 2\bigoplus_{\eta\in\mathrm{spec}(RL)}Q_\eta(Q_\eta+P_1)^{-1}P_1\,,$$

where $^{-1}$ is the Moore-Penrose inverse, P_V is the superoperator of a unital CPTP-map on B which we denote as $\mathbb{E}_B$. Consider systems $\mathcal{H}_{\bar{B}}\cong\mathcal{H}_{\bar{B}_1}\cong\mathcal{H}_B$ and define $|\mathcal{I}\rangle\!\rangle_{BB_1} := \sum_i |ii\rangle_{BB_1}$ in the transposition in Eq. (9) and (10). The normalized Choi state C_{BB_1} of $\mathbb{E}_B$ is defined as follows:

$$C_{BB_1} := \frac{1}{d_B}(\mathrm{id}_B\otimes\mathbb{E}_{B_1})\left(|\mathcal{I}\rangle\!\rangle\langle\!\langle\mathcal{I}|_{BB_1}\right). \tag{13}$$

C_{BB_1} and P_V are related via the reshuffling map:

$$C_{BB_1} = \frac{1}{d_B}\sum_{i,j=1}^{d_B}(I_B\otimes|i\rangle\langle j|_{B_1})P_V(|i\rangle\langle j|_B\otimes I_{B_1}).$$

Consider the canonical purification of C_{BB_1}, which is the purification in an eigenbasis of C_{BB_1}, denoted as $|C\rangle_{BB_1\bar{B}\bar{B}_1}$. We then optimize all possible unitary to minimize the entanglement entropy $S(\rho) := -\mathrm{tr}\rho\log\rho$ between $B\bar{B}$ and $B_1\bar{B}_1$:

$$\rho_{B\bar{B}} := \mathrm{tr}_{B_1\bar{B}_1}U_{\bar{B}\bar{B}_1}|C\rangle\langle C|U^\dagger_{\bar{B}\bar{B}_1} \tag{14}$$

$$\tilde{U}_{\bar{B}\bar{B}_1} := \mathrm{argmin}_U\, S(\rho_{B\bar{B}})\,, \tag{15}$$

The optimization can be performed by using e.g., a gradient algorithm [19].

3.1 Main theorem

The main theorem of this work is showing that the minimal dimension of exact local compression is given by the Schmidt rank of $\tilde{U}_{\bar{B}\bar{B}_1}|C\rangle_{BB_1\bar{B}\bar{B}_1}$ (see the technical version for the proof).

Theorem 1. *For any* ρ_{AB} *such that* $\rho_B > 0$*, an isomorphism* $\mathcal{H}_B\cong\oplus_i\mathcal{H}_{B_i^L}\otimes\mathcal{H}_{B_i^R}$ *exists such that*

$$d_{\bar{B}} = \sum_i d_{B_i^L} = \mathrm{SchR}\left(BB_1\bar{B}_1:\bar{B}\right)_{|\tilde{C}\rangle}\,, \tag{16}$$

is the minimal dimension of any exact local compression, where

$$|\tilde{C}\rangle_{BB_1\bar{B}\bar{B}_1} := \tilde{U}_{\bar{B}\bar{B}_1}|C\rangle_{BB_1\bar{B}\bar{B}_1}\,. \tag{17}$$

It also holds that

$$d_{B^R} := \sum_i d_{B_i^R} = \mathrm{SchR}\left(BB_1:\bar{B}\bar{B}_1\right)_{|\tilde{C}\rangle}\,. \tag{18}$$

From the definition of C_{BB_1} in (13), the following holds:

Corollary 1.

$$\mathrm{rank}(C_{BB_1}) = \sum_i d_{B_i^L}^2 \tag{19}$$

and

$$\sqrt{\mathrm{rank}(C_{BB_1})}\leq d_{\bar{B}}\leq\mathrm{rank}(C_{BB_1})\,. \tag{20}$$

Unlike Eq. (16), calculating Eq. (1) does not require any optimization.

3.2 Exact compression of quantum channels

For a given CPTP-map $\mathcal{E}_{A\to B}$, $\mathcal{F}_{B\to\tilde{B}}$ is an exact compression if a post-processing CPTP-map $\mathcal{R}_{\tilde{B}\to B}$ that satisfies

$$\mathcal{E}_{A\to B} = \mathcal{R}_{\tilde{B}\to B} \circ \mathcal{F}_{B\to\tilde{B}} \circ \mathcal{E}_{A\to B}\,. \tag{21}$$

Via the Choi-Jamilkowski isomorphism, this task is equivalent to the exact local compression of the normalized Choi state

$$\rho_{AB} = (\mathrm{id}_A \otimes \mathcal{E}_{\bar{A}\to B})(|\Psi\rangle\!\rangle\langle\!\langle\Psi|_{A\bar{A}})\,, \tag{22}$$

where $|\Psi\rangle\!\rangle = \frac{1}{\sqrt{d_A}} \sum_{i=1}^{d_A} |ii\rangle_{A\bar{A}}$.

4 Conclusion

We studied exact and local compression of arbitrary quantum bipartite states. We have provided a closed formula for the minimum achievable dimension in terms of the Schmidt rank of a relevant purified Choi state constructed from the bipartite state. This is in contrast to the asymptotic result [5] given in terms of the Koashi-Imoto decomposition which is much harder to calculate. The exactly same formula is applicable for reducing the output dimension of quantum channels.

References

[1] B. Schumacher. Quantum coding. *Phys. Rev. A*, pages 2738–2747, 1995.

[2] R. Jain, J. Radhakrishnan, and P. Sen. Prior entanglement, message compression and privacy in quantum communication. *In Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 285–296, 2005.

[3] N. Datta, J. M. Renes, R. Renner and M. M. Wilde. One-shot lossy quantum data compression. *IEEE Trans. Inf. Theory* 59, 12, 8057-8076, 2013

[4] Z. B. Khanian and A. Winter. Entanglement-Assisted Quantum Data Compression. *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1147-1151, 2019.

[5] Z. B. Khanian and A. Winter. General mixed state quantum data compression with and without entanglement assistance. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1852–1857, 2020.

[6] R. A. Fisher. On the mathematical foundations of theoretical statistics. *Philos. Trans.Roy. Soc. London A*, pages 309–368, 1922.

[7] T. N. Cover and J. A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[8] E. L. Lehmann and H. Scheffé. Completeness, similar regions, and unbiased estimation: Part i. *Sankhyā: The Indian Journal of Statistics (1933-1960)*, 10(4):305–340, 1950.

[9] D. Petz. Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. *Commun. Math. Phys.*, 105(1):123–131, 1986.

[10] D. Petz. Sufficiency of channels over von Neumann algebras. *Q. J. Math.*, 39(1):97–108, 1988.

[11] A. Jenčová. Reversibility conditions for quantum operations. *Rev. Math. Phys.*, 24(07):1250016, 2012.

[12] A. Kempf C. Bény and D. W. Kribs. Generalization of quantum error correction via the Heisenberg picture. *Phys. Rev. Lett.*, 98(10):100502, 2007.

[13] A. Kempf C. Bény and D. W. Kribs. Quantum error correction of observables. *Phys. Rev. A*, 76(4):042303, 2007.

[14] M. Koashi and N. Imoto. Operations that do not disturb partially known quantum states. *Phys. Rev. A*, 66(2):022318, 2002.

[15] P. Hayden, R. Jozsa and A. Winter. Structure of States Which Satisfy Strong Subadditivity of Quantum Entropy with Equality. *Commun. Math. Phys.*, 246(2):359–374, 2004.

[16] M. Mosonyi and D. Petz. Structure of Sufficient Quantum Coarse-Grainings. *Lett. Math. Phys.*, 68(1):19–30, 2004.

[17] A. Jenčová and D. Petz. Sufficiency in Quantum Statistical Inference. *Commun. Math. Phys.*, 263(1):259–276, 2006.

[18] W.N Anderson and R.J Duffin. Series and parallel addition of matrices. *J. Math. Anal. Appl.*, 26(3):576–594, 1969.

[19] Y. Zou, K. Siva, T. Soejima, R. S. K. Mong and M. P. Zaletel. Universal tripartite entanglement in one-dimensional many-body systems. *Phys. Rev. Lett.*, 126:120501, 2021.

Estimating the nonclassicality of the free induction decay of NV centers with kernel-based quantum machine learning model

Nien-Ting Ko[1] * Hong-Bin Chen[1 2 3] †

[1] *Department of Engineering Science, National Cheng Kung University, Tainan 701401, Taiwan*
[2] *Center for Quantum Frontiers of Research & Technology, NCKU, Tainan 701401, Taiwan*
[3] *Physics Division, National Center for Theoretical Sciences, Taipei 106319, Taiwan*

Abstract. Characterization of nonclassical traits of dynamical processes has long been a study interest in the field of open quantum system theory. Recently, an approach based on the canonical Hamiltonian ensemble representation (CHER) had been proposed for the characterization and the quantification of the nonclassicality of dynamical processes; meanwhile, it had been exemplified with the free induction decay of NV centers. However, for an experimental realization of the CHER theory, it would require extensive experimental efforts to gather the raw data for the implementation of the quantum process tomography with sufficient time resolution. Here we propose to harness the power of a kernel-based quantum machine learning model to estimate the nonclassicality from temporally spare data. We demonstrate our approach with the free induction decay of NV centers. We also compare the quantum model with two classical ones. We find that the quantum model is capable of predicting the nonclassicality with high accuracy even if the raw data is temporally spare, and the quantum model performs better than some types of classical learning models.

Keywords: nonclassicality, CHER, free induction decay, nuclear spin polarization, quantum machine learning

1 Introduction

The ambiguous boundary between the quantum and the classical worlds has attracted extensive interest [1, 2, 3, 4]. In the field of quantum information science, one of the mostly employed ideas to demonstrate the genuine quantumness focuses on the failure of a classical strategy attempting to explain an experimental outcome. For example, the renowned example of the experimental violation [5, 6] of Bell's inequality [7] accentuates the breakdown of the EPR paradox [8] formulated on the tenets of realism and locality. This specific kind of nonclassical correlation resulting in the violation of Bell's inequality is termed Bell nonlocality [9].

In line with this idea, the concept of dynamical process nonclassicality has been formulated in terms of the approach of the canonical Hamiltonian ensemble representation (CHER) [10, 11, 12]. Moreover, this concept had been exemplified with the free induction decay (FID) of NV centers in the presence of nuclear spin bath polarization [13], as well as simulated on quantum computers [14]. However, on the eye of these experimental proposals, an experimental realization of the CHER theory to characterize the dynamical process nonclassicality requires extensive efforts to gather the raw data for the implementation of the quantum process tomography with sufficient time resolution. Therefore, we are spurred to seek for an efficient approach to estimate the nonclassicality from merely spare data.

Along with the rapid development of quantum computing technology [15, 16, 17], the idea of implementing kernel-based support vector machine on quantum computers had been discussed and implemented [18, 19]. In this work, we propose to adopt the kernel-base quantum model to estimate the nonclassicality from spare data. In conclusion, our quantum model is capable of predicting the nonclassicality of the FID in the presence of nuclear spin polarization with sufficient accuracy. Moreover, we have also demonstrated the advantage of our quantum model over some classical counterparts in such complicated regression problem.

2 Canonical Hamiltonian Ensemble Representation

CHER is a method for describing the evolution of quantum systems. This representation is crucial in quantum computing because it provides a mathematical framework to describe the dynamic behavior of quantum states under the control of a Hamiltonian. In reality, most quantum systems are open, meaning they interact with their external environment [10, 11]. This interaction leads to phenomena such as decoherence and relaxation. Therefore, the dynamics of open quantum systems are often described using superoperators, rather than just unitary operators. In the CHER framework, the dynamic behavior of the system can be described by the following equation:

$$\mathcal{E}_t\{\rho(0)\} = \int p_\lambda \hat{U}_\lambda(t)\rho(0)\hat{U}_\lambda^\dagger(t)d\lambda \tag{1}$$

This equation describes the dynamic evolution of the entire quantum system. This representation is typically used in the theory of open quantum systems, where the evolution of the system is influenced not only by its own Hamiltonian but also by interactions with the environment. Further details are shown in **Appendix** 7 (Dynamics of CHER).

Drawing a conclusion, the motivation for applying quantum machine learning to NV centers is driven by

*angelko0304@gmail.com
†hongbinchen@gs.ncku.edu.tw

the immense potential it holds for enhancing computational efficiency and solving problems intractable for classical computers. The distinctive quantum properties of NV centers open up unprecedented opportunities to accelerate learning algorithms and enable more accurate data analysis. The promise of quantum-enhanced sensing, communication, and computation is particularly compelling for scientists and researchers aiming to harness the power of NV centers in diamond for practical, real-world applications. Ultimately, the continuous development and optimization of quantum machine learning models on emerging quantum platforms, such as IBM, are crucial steps toward unlocking the vast potential of quantum technologies and their transformative impact on diverse sectors.

3 NV Centers

NV center is a defect structure embedded in the diamond lattice, where a nitrogen atom replaces a carbon atom and forms an adjacent vacancy. Its electronic structure can form different spin states, which have long coherence times (T_2^*), allowing them to be used as qubits in quantum computing. The long coherence time of NV centers provides an advantage in this aspect. In quantum computing, NV centers are used as fundamental logic units to perform quantum state operations and calculations by implementing quantum logic gates [13]. The dynamics of the spin states are primarily described by the Hamiltonian, given here as the total Hamiltonian $\hat{H}_T$:

$$\hat{H}_T = D\hat{S}_z^2 + \gamma_e B_z \hat{S}_z + \sum_k \gamma_c B_z \hat{J}_z^{(k)} + \hat{S}_z \sum_k A_z^{(k)} \hat{J}^{(k)} \quad (2)$$

Each term in the equation represents different physical phenomena: $D\hat{S}_z^2$ denotes the spin-spin interaction; $\gamma_e B_z \hat{S}_z$ represents the interaction between the electron spin and the external magnetic field; $\sum_k \gamma_c B_z \hat{J}_z^{(k)}$ and $\hat{S}_z \sum_k A_z^{(k)} \hat{J}^{(k)}$ indicate interactions with surrounding nuclear spins and hyperfine interactions, respectively. These interactions determine the coherence time and quantum state control capability of NV centers, which are crucial for quantum computing.

4 Quantum Machine Learning

Developing algorithms and statistical models that enable computer systems to perform tasks based on patterns and reasoning without requiring precise instructions from humans is known as machine learning (ML). ML can be divided into three major categories: supervised learning, unsupervised learning, and reinforcement learning. Here, this research focus on support vector machines (SVM) in supervised learning, which is based on provided input-output pairs with the goal of understanding the mapping function from input to output. Computer systems utilize ML algorithms to process vast amounts of data and identify patterns within it, allowing computers to make more accurate predictions based on input data sets.

The focus of this article is on quantum machine learning (QML), which involves the development of quantum algorithms, while there are numerous remarkable QML algorithms awaiting discovery and development by humans, this research will concentrate on one of its branches: quantum support vector machines (QSVM). QSVMs classify objects in n-dimensional space (where 'n' denotes the number of features) by identifying a hyperplane that separates data points. While classical machine learning algorithms can perform these tasks, the increasing volume of data will inevitably lead to significant time and resource costs. Quantum support vector machines (QSVM) become crucial when handling high-dimensional data.

In essence, classical machine learning algorithms pose considerable computational challenges for classical computers when processing high-dimensional data. Quantum algorithms offer a significant advantage in such scenarios by leveraging powerful principles like superposition and entanglement, leading to more efficient computations with exponential growth potential. Through research conducted by quantum specialists, classical algorithms can be translated into a language comprehensible and operable by quantum computers, facilitating efficient operations on quantum circuits.

However, it's worth noting that the current state of open-source quantum algorithm packages is not as advanced as their classical counterparts, and optimizing time control remains a challenge. Nevertheless, by fully utilizing local computer CPU and memory resources and fine-tuning model parameters, satisfactory calculation results can be achieved, even outperforming certain classical machine learning models [19].

5 Experimental Proposal

Our primary goal in this experiment is to ensure that our model learns all types of data and delivers precise outputs. Initially, this research used entirely random spin orientations, with these coordinates normalized and set within an external magnetic field range of 0 to 200. First, we generate a time-varying physical function, $\phi(t)$, using a series of random values. Further details for the calculation of $\phi(t)$ are shown in **Appendix** 7 (decoherence equation: $\phi(t)$). This function is defined over a time range from 1 to 10 seconds, thus we obtain values from $\phi(1)$ to $\phi(10)$ within this interval. For each time point, we calculate both the real and imaginary parts of the $\phi(t)$ function, resulting in a total of 20 features: the real and imaginary parts for $\phi(1)$ through $\phi(10)$.

Next, we employ numerical integration techniques to calculate the area of the absolute difference between each pair of real and imaginary parts. This step is based on the interactions between the real and imaginary components and ultimately produces a numerical value. In the machine learning model, these 20 values of real and imaginary parts serve as the "features" of the model, while the area computed through numerical integration acts as the "label." These labels are fundamental for the model's learning and prediction processes and are used to assess the characteristics of new data. Through this approach, we effectively transform a physically meaningful dynamic

system into a data format that can be processed by a machine learning model.

6 Results and Conclusions

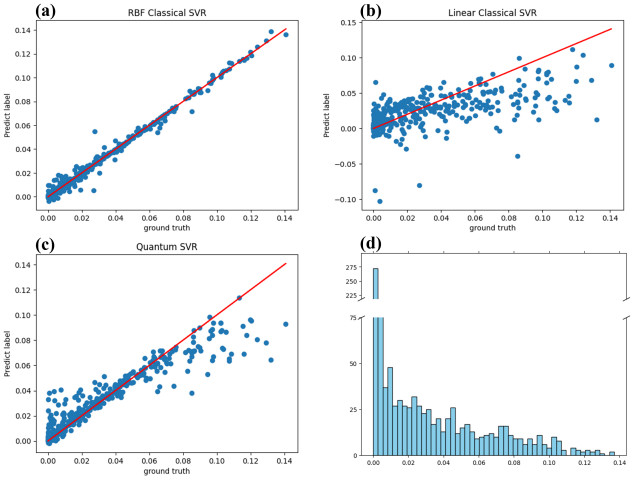


Figure 1: Put the specially adjusted data into three models for training. (a) and (b) are showing the commonly used models of classic machine learning, RBF Kernel Classical SVR and Linear Kernel Classical SVR respectively. (c) is Non-classical model from an open source information framework for quantum computing on the IBM platform, to perform some quantum machine learning tasks. (d) shows the distribution of labels for the training data. The use of a broken axis highlights the distribution of values in the range above 0.03.

As the amount of generated data increases, studies have observed that label values cluster around zero, which hinders the model from learning features far from this region, resulting in inaccurate predictions for data near zero and sometimes leading to significant errors. Therefore, this study intentionally adjusted the parameters in a random range, and by observing the non-classical properties of the quantum state, it was found that adjusting the spin bath to stronger spin polarization and higher external magnetic field resulted in label values far away from zero, ranging from 0.03 to between 0.12, as shown in Figure 1 **(d)**.

This research tested specially adjusted data on three different models. These models include two classical machine learning models: the Radial Basis Fnction (RBF) Kernel Classical Support Vector Regression (SVR) [20, 21] and the Linear Kernel Classical SVR, and a quantum machine learning model implemented using Qiskit, an open-source quantum computing framework on the IBM platform, as shown in Figure 1 from **(a)** to **(c)**. Notably, this research used the **ZZFeatureMap** [22] from Qiskit, a quantum feature mapping method that employs second-order **Pauli-Z**, details are shown in Appendix 7 (Pauli-z). rotations to encode feature data into quantum states.

The ZZFeatureMap is designed for nonlinear transformations of data via quantum circuits, thereby enhancing the model's capability to handle high-dimensional data and complex patterns, making it particularly suitable for exploration in the field of quantum machine learning. We have a total of 20 qubits, and the concept of quantum circuit structure is similar to what is shown are shown in **Appendix** 7 (Quantum circuit), the example in the Figure demonstrates the interaction of three qubits.

When comparing the training performances of these classical and quantum models, it is essential to understand the characteristics of classical machine learning models first. The RBF kernel, with its nonlinear properties, excels in nonlinear classification tasks, while the linear kernel, due to its simplicity, performs efficiently in linear problem scenarios. Moreover, the parameters of both kernels are relatively easy to adjust, providing flexible options for model optimization.

The experimental results from Figure 1 show that among the three models, the RBF kernel performed the best, followed by the quantum kernel, with the linear kernel coming in last. In this experimental setup, this research pushed the data capacity to the limits allowed by the system, with 100 precentage usage of the local computer, processing a total of 1400 data points. Of these, 1000 datas were used for training and 400 datas for testing. The results indicated that although the performance of the quantum kernel did not surpass that of the RBF kernel, it did exceed that of the classical linear kernel. Next, this research calculated the Mean Square Error (MSE) for these three models, and the results supported our observations:

Model TYPE	**MSE**
RBF Classical SVR	0.11×10^{-4}
Linear Classical SVR	7.16×10^{-4}
Quantum SVR	1.34×10^{-4}

Table1. MSE comparison of different models

This finding is particularly worth discussing. In today's society, where classical machine learning techniques have reached a high level of maturity, surpassing traditional methods requires significant effort and innovation. However, in this experiment, the performance of the quantum kernel model surpassed that of the linear kernel. This is a major development, demonstrating the potential of non-classical machine learning technologies for future advancements.

Compared to traditional machine learning methods, quantum machine learning leverages quantum properties such as superposition and entanglement, leading to significant improvements in computational efficiency and accuracy. These non-classical characteristics not only show theoretical advantages but have also been preliminarily validated in experiments. The results of this experiment clearly indicate that quantum machine learning is not merely an idealistic concept for the future but a revolutionary technology with practical application potential. As quantum technology continues to advance, quantum machine learning will become a core driver pushing the fields of artificial intelligence and data science forward.

7 Appendix

Decoherence Equation: $\phi(t)$

The pure dephasing dynamics of electron spin are characterized by the dephasing factor $\phi(t)$. This factor expresses the dephasing process of electron spin over time t, and its formula is given by:

$$\phi(t) = \langle 0|\rho_{\mathrm{NV}}(t)|1\rangle = e^{i(D+\gamma_e B_z)t} \prod_k \mathrm{Tr}\left[\hat{U}_1^{(k)}(t)\hat{U}_0^{(k)}(t)\rho^{(k)}\right] \quad (3)$$

where

$$\hat{U}_0^{(k)}(t) = \exp[-i(\vec{\Omega}_0 \cdot \hat{\sigma}^{(k)})t/2]$$
$$\hat{U}_1^{(k)}(t) = \exp[-i(\vec{\Omega}_1^{(k)} \cdot \hat{\sigma}^{(k)})t/2]$$

These formulas represent the nuclear spin precession caused by the interaction between electron spin and nuclear spin, leading to electron spin dephasing.

Dynamics of CHER

Performance of CHER as shown in Figure 2, the state of the electron spin is influenced by its polarization direction and the external magnetic field. These results correspond to the CHER depicted in the figure. Over time, electron spins exhibit distinct non-classical behaviors under different polarization directions. Furthermore, we set the external magnetic field to 150G, which significantly impacts the dynamic behavior of the electron spin. This demonstrates that the external magnetic field plays a crucial role in modifying the quantum dynamics of electron spins.

Pauli-z

Pauli matrices are fundamental tools in quantum mechanics for describing spin states and quantum bit operations. These matrices are three 2x2 Hermitian matrices, represented as σ_x, σ_y, and σ_z (i.e., Pauli-X, Pauli-Y, and Pauli-Z matrices). They are widely used in spin physics and quantum computing. Below are the specific formulas for Pauli-Z matrices and some related explanations. The formulas for the Pauli matrices are as follows:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Pauli-Z (σ_z) matrix specifically describes the component of spin along the z-axis.

Quantum circuit

We have a total of 20 qubits, and their quantum circuit structure is similar to what is shown in the Figure 3. Each pair of qubits interacts through CNOT gates, and this interaction continues until all pairs of the 20 qubits have been paired. The example in the diagram demonstrates the interaction of three qubits, and the interactions of the other qubits can be inferred similarly.

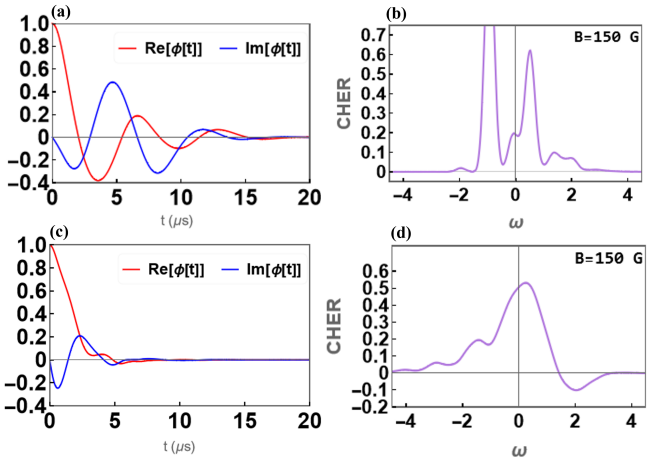


Figure 2: Dynamics and CHER of the electron spin for a polarized nuclear spin bath. **(a)** and **(b)** are showing the z-polarized dynamical behavior and the corresponding CHER for the case of polarization toward the z-axis at magnitudes = 1.0. **(c)** and **(d)** are showing the x-polarized dynamical behavior and the corresponding CHER for the case of polarization toward the x-axis at magnitudes = 1.0. The dynamical behavior shows a different response to the presence of x-polarization and z-polarization in same external magnetic field. Additionally, the most exotic property is the emergence of negative values as shown in **(d)**, which is appear when the x-polarized. This is the crucial indicator of the non-classical trait of the electron spin dynamics caused by the nuclear spin precession dynamics.

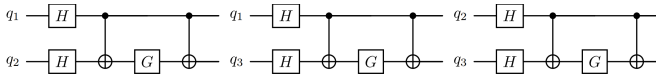


Figure 3: This diagram illustrates a quantum circuit involving three qubits q_1, q_2, and q_3, where each pair of qubits interacts through CNOT gates. Specifically, the circuit shown includes Hadamard gates H and quantum gate G.

References

[1] L. E. Ballentine. The statistical interpretation of quantum mechanics. *Reviews of Modern Physics*, 42:358, 1970.

[2] W. H. Zurek. Decoherence, einselection, and the quantum origins of the classical. *Reviews of Modern Physics*, 75:715, 2003.

[3] M. Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern Physics*, 76:1267, 2005.

[4] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Reviews of Modern Physics*, 84:1655, 2012.

[5] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, 47:460, 1981.

[6] B. Hensen et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682, 2015.

[7] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

[8] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777, 1935.

[9] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86:419, 2014.

[10] H.-B. Chen, C. Gneiting, P.-Y. Lo, Y.-N. Chen, and F. Nori. Simulating open quantum systems with Hamiltonian ensembles and the nonclassicality of the dynamics. *Physical Review Letters*, 120(3):030403, 2018.

[11] H.-B. Chen, P.-Y. Lo, C. Gneiting, J. Bae, Y.-N. Chen, and F. Nori. Quantifying the nonclassicality of pure dephasing. *Nature Communications*, 10(1):3794, 2019.

[12] H.-B. Chen and Y.-N. Chen. Canonical Hamiltonian ensemble representation of dephasing dynamics and the impact of thermal fluctuations on quantum-to-classical transition. *Scientific Reports*, 11(1):10046, 2021.

[13] M.-C. Lin, P.-Y. Lo, F. Nori, and H.-B. Chen. Precession-induced nonclassicality of the free induction decay of NV centers by a dynamical polarized nuclear spin bath. *Journal of Physics: Condensed Matter*, 34(50):505701, 2022.

[14] Y.-H. Kuo and H.-B. Chen. Adaptively partitioned analog quantum simulation on near-term quantum computers: The nonclassical free-induction decay of NV centers in diamond. *Physical Review Research*, 5(4):043139, 2023.

[15] F. Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505, 2019.

[16] P. Jurcevic et al. Demonstration of quantum volume 64 on a superconducting quantum computing system. *Quantum Science and Technology*, 6:025020, 2021.

[17] Y. Kim et al. Evidence for the utility of quantum computing before fault tolerance. *Nature*, 618:500, 2023.

[18] V. Havlicek et al. Supervised learning with quantum-enhanced feature spaces. *Nature*, 567:209, 2019.

[19] Y. Liu, S. Arunachalam, and K. Temme. A rigorous and robust quantum speed-up in supervised machine learning. *Nature Physics*, 17:1013, 2021.

[20] E. López-Rubio, M. A. Molina-Cabello, and K. Najarian. Radial basis function kernel optimization for support vector machine classifiers. *arXiv preprint arXiv:2007.08233*, 2020.

[21] F. Colombo, K. Diki, and I. Sabadini. An approach to the Gaussian RBF kernels via Fock spaces. *Journal of Mathematical Physics*, 63(11), 2022.

[22] 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(7747):209–212, 2019.

Direct and loss tolerant GHZ states generation protocol for quantum networks

Wojciech Roga[1] * Hikaru Shimizu[1] † David Elkouss[2 3] ‡ Masahiro Takeoka[1] §

[1] *Department of Electronics and Electrical Engineering, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa, 223-8522 Japan*

[2] *Networked Quantum Devices Unit, Okinawa Institute of Science and Technology Graduate University, Okinawa,Japan*

[3] *QuTech, Delft University of Technology,Lorentzweg 1, 2628 CJ Delft,The Netherlands*

Abstract. We present a novel practical approach to distribute multipartite entangled states (GHZ states) in a quantum network. The distribution rate shows quadratically improved scaling with respect to the present state-of-the-art experiments with no repeaters. Among advantages of our method are: directness – no pre-shared bi-partite entanglement; and feasibility, as our protocol only requires standard quantum optical experimental setup, including sources, linear interferometers, and photodetectors. Our solution can impact quantum networks applications such as conference cryptographic key generation or distributing sensing. Apart from that, directness of our method implies simplification of surface codes in error correction for distributed quantum computing.

Keywords: Quantum Networks, Quantum Communication, Quantum Repeater

This submission is based on arXiv:2404.19458 [1].

1 Context and motivation

Our research emerges in the context of quantum networks or quantum Internet [2, 3, 4]. Quantum network is a multifunctional platform necessary for a diverse range of applications in a network of users. These include, for example, distributed sensing [5, 6, 7, 8, 9, 10], clock synchronization [11], informational security [12, 13, 14, 15, 16, 17], as well as distributed computing [18, 19]. Many of the applications rely on the Greenberger-Horne-Zeilinger (GHZ) states:

$$|\mathrm{GHZ}\rangle_N = \frac{1}{\sqrt{2}}(|000...0\rangle + |111...1\rangle), \qquad (1)$$

where N is the number of subsystems; which makes this quantum state a strategically important resource.

Quantum networks require sharing quantum entangled states between its nodes which typically happens by means of photons transmitted through optical wires. However, photons transmitted in this way undergo unavoidable loss at the rate of 0.2 dB/km in current telecom standard.

In the present research we investigate the star network with a central node that can play the role of a router and N users in the end nodes. We assume the same length channels with power transmittance η linking the central node with the users. The basic reference idea, Fig. 1 (a), realized experimentally in [17], is to generate entangled states in the central node and distribute them via photons to the end nodes. We call this scenario "direct transmittance". In this scenario N photons are used and all N must survive the loss induced by the channels to generate a single copy of GHZ state. Therefore the success rate in generating multipartite entangled states, GHZ states, scales as η^N [23, 24].

The protection against losses would be offered by functioning quantum repeaters which could use quantum memory. This approach would ideally achieve loss rate reduction and success rate scaling as η [25, 26, 27], Fig. 1 (b). This motivates extensive research and development of the technology [28, 29, 30, 31, 32], which, however, is still in the early stage of development. Moreover, such strategy relies on generating bi-partite entanglement states from which, after rounds of state purification a multipartite entangled states can be distilled, which increases complexity of the approach.

In the present research we propose an approach that competes with the direct transmittance, offering success rate that scales as $\eta^{N/2}$, and with the quantum repeaters approach offering simpler, nowadays technology solution without mediation of bi-partite entanglement generation, purification, and distillation.

2 Protocol

Let us first discuss generation of 4 part GHZ state, then we generalize it to arbitrary N. Let us consider the setup as in Fig. 2. Each user locally prepares a photonic entangled state

$$|\psi\rangle_{X_i X_i'} = a|00\rangle_{X_i X_i'} + b|11\rangle_{X_i X_i'}, \qquad (2)$$

where $|a|^2 + |b|^2 = 1$, sends subsystem X_i' to the central node, and retains X_i at the node. Here, appropriately designed interferometer, Fig. 2, removes the information where a photon came from [33], such that when an appropriate set of detectors [1] signalizes photodetections, the state in subsystems X_i is projected, up to imperfections, to state

$$|\mathrm{GHZ}\rangle_4 = \frac{1}{\sqrt{2}}(|1010\rangle_{\mathrm{X_1X_2X_3X_4}} + |0101\rangle_{\mathrm{X_1X_2X_3X_4}}), \quad (3)$$

*wojciech.roga@keio.jp
†shimihika2357@keio.jp
‡david.elkouss@oist.jp
§takeoka@elec.keio.ac.jp

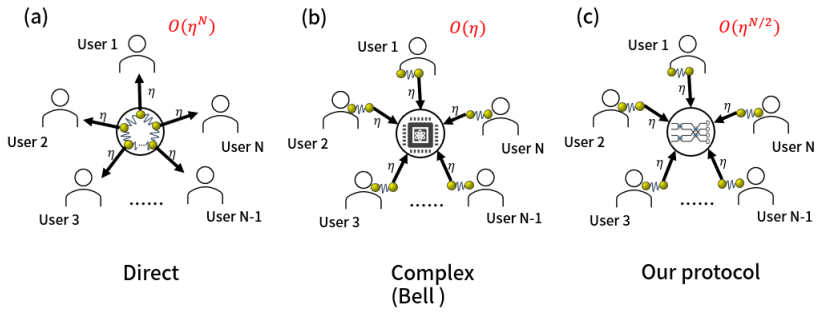


Figure 1: Multipartite entangled state generation in a star network in different scenarios. (a) Direct transmission protocol characterized by success rate scaling of η^N, were η is one channel transmittance. (b) Strategy with quantum memory-based repeaters. It is characterized by good rate scaling, but is technically demanding and requires pre-shared Bell states. (c) Proposed protocol in which interference and appropriate measurement in the central node generate desired states in subsystems hold by users.

which is up to local unitary transformations equivalent to $|GHZ\rangle_4$ from (1). As only two photons need to survive the lossy channels the success rate scales as η^2 achieving quadratic improvement with respect to the direct transmittance. In the next section we discuss the rate and fidelity of such generated state in realistic experimental conditions with nowadays quantum optics technology.

The idea presented above can be generalized, however not trivially, to generation GHZ states in the star network with arbitrary number of users. The extension utilizes the four mode scheme from Fig. 2 as a building block. The users 1 and 4, are however removed and replaced by a link with single photon entangled state connecting two neighboring building blocks, Fig. 3. In [1] we derive formulas for the rate

$$R = 3^{\frac{N}{2}-1}\left(\frac{1}{2}\right)^{N-6}\eta^{\frac{N}{2}}b^N[a^2+b^2(1-\eta)]^{\frac{N}{2}}, \quad (4)$$

and fidelity as functions of the channel loss rate η and other parameters of the setup. In Fig. 4 we show the rate for different number of users and compare it to the direct transmittance generation rate.

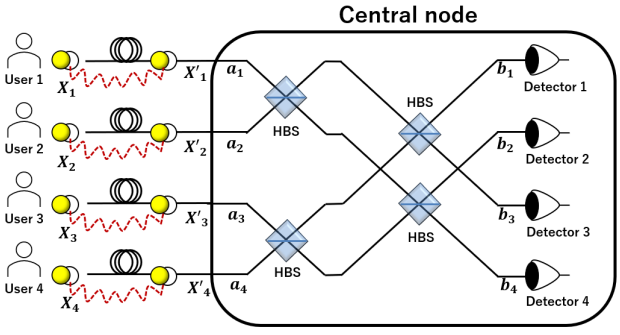


Figure 2: Scheme of GHZ states generation in modes $X_1 ... X_4$. HBS denotes the 50 : 50 (half) beam splitter. Appropriate pairs of detectors [1] herald success of the the protocol.

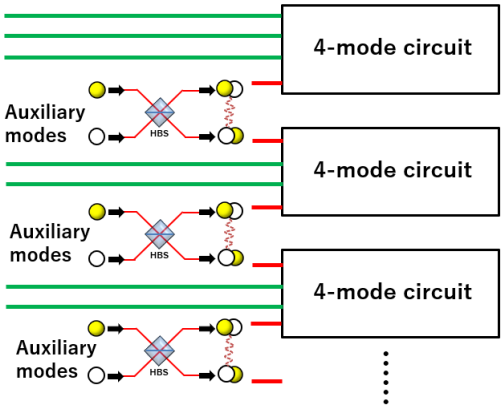


Figure 3: Scheme of generation of arbitrary size GHZ states. The 4-mode circuits as in Fig. 1 are interconnected by means of single photon entangled states.

3 Feasibility

We performed the analysis of the success rate and fidelity simulating quantum optics setup with standard elements. As a source of the users' input entangled states, two mode squeezed vacuum generated in the spontaneous parametric down conversion process is assumed. We assume photodetectors of efficiency of 80% and dark count rate 10^{-6} per second.

The rate and fidelity for different levels of squeezing are shown in Fig. 5. As the reference we show the performance of the direct transmission. We conclude that despite the experimental imperfections the advantage of our protocol still prevails.

4 Error correction application

The advantageous scaling we observe in our protocol can impact many quantum network protocols including conference key agreement and distributed sensing. Moreover, the fact that our protocol does not rely on pre-shared bi-partite entanglement provides another advantage that can lead to significant simplification of error correction codes for distributed computing. In our paper

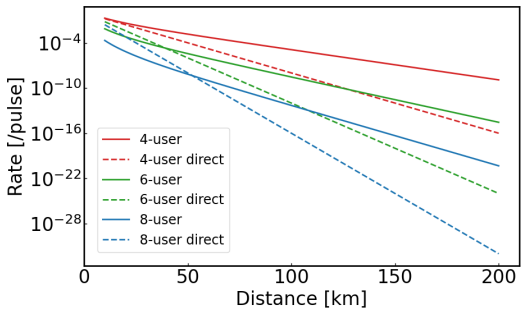


Figure 4: Rate of generation GHZ states with fixed fidelity 0.9 vs distance for different numbers of users. The solid lines indicate our protocol, the dashed lines – the direct transmission.

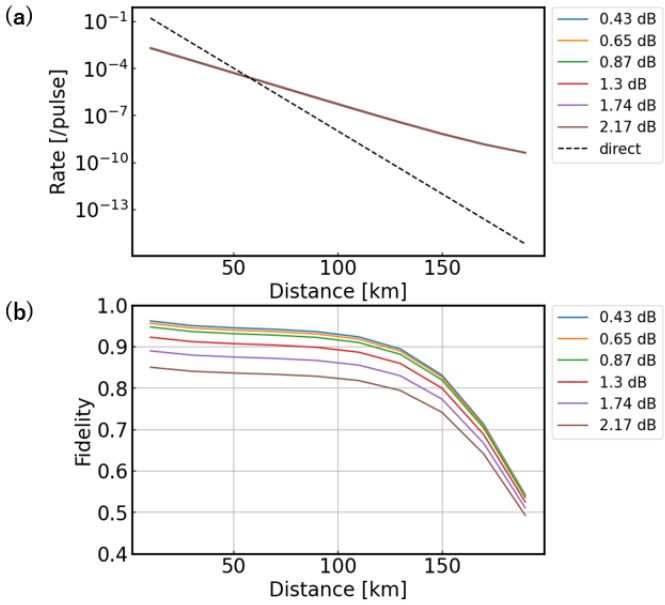


Figure 5: Rate of generation (a) and fidelity (b) of GHZ states vs distance for different squeezing levels. The solid lines indicate the proposed protocol, the dashed line – direct transmission.

[1] we report this simplification for the first time.

In Ref. [34], a distributed architecture was proposed for topological quantum computing, with noisy network channels, where many simple processor cells (consisting of small number of qubits) are networked via noisy links forming a 2D grid. This architecture was extended by combining an efficient photonic linking protocol, called "extreme photon loss (EPL)" protocol [35], to form a robust architecture under very lossy and noisy network links [36]. In this solution, instead of extra qubits for the stabilizer measurements, 4-partite GHZ states are distributed to neighbouring four cells in the grid to perform the stabilizer measurement among them.

In the original proposal, each pair of cells first share the Bell states and purify them by the EPL protocol. Then these states are further distilled to make the GHZ states. In Ref. [35], a simple purification protocol was shown where two copies of successfully generated states interacted through the controlled-NOT (CNOT) operations inside each cell and then qubits of one of the copies were locally measured in the Z basis. Provided that both measurement outcomes were 1, the remaining state turned out to be a purified Bell state. In Ref. [36], it was shown that employing the EPL protocol into their distributed surface code architecture, one can drastically increase the threshold of the networking error for fault tolerance [37].

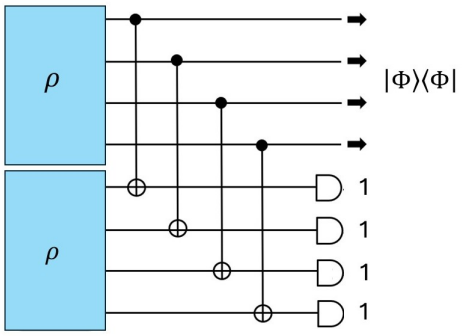


Figure 6: GHZ-state purification scheme.

The distributed state in our protocol

$$\rho = \alpha|GHZ\rangle\langle GHZ| + \sum \beta_i|\phi_i\rangle\langle\phi_i|, \qquad (5)$$

is not an ideal pure GHZ state. It contains undesired contribution $|\phi_i\rangle$ that can be recognized [1]. Let us consider that we have two copies of ρ and perform purification, just like the Bell-state purification in the EPL protocol, Fig. 6. Each cell locally applies the CNOT operation to the part of ρ and measures the target qubit in the Z bases. We can show that if $|1111\rangle$ is detected we eliminate the unwanted terms purifying the GHZ state.

Note that our protocol allows a direct generation of the GHZ state among the four neibouring cells which is possibly advantageous for efficient stabilizer measurements. This already simplifies the entire protocol. We also show that a modification of the EPL protocol to purify the GHZ states (see Fig. 6) is possible, and thus there is no critical obstacle to apply our protocol into the distributed surface code architecture.

References

[1] H. Shimizu, W. Roga, D. Elkouss, M. Takeoka, Simple loss-tolerant protocol for GHZ-state distribution in a quantum network, arXiv:2404.19458 (2024).

[2] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. Science **362**, 6412 (2018).

[3] H. J. Kimble. The quantum internet. Nature **453**, 1023 (2008).

[4] N. Gisin and R. Thew. Quantum communication. Nature Photonics **1**, 165-171 (2007).

[5] Z. Eldredge, M. Foss-Feig, J. Gross, S. Rolston, and A. Gorshkov, Optimal and secure measurement pro-

tocols for quantum sensor networks, Phys. Rev. A **97**, 042337 (2018).

[6] W. Ge, K. Jacobs, Z. Eldredge, A. Gorshkov, and M. Foss-Feig, Distributed Quantum Metrology with Linear Networks and Separable Inputs, Phys. Rev. Lett. **121**, 043604 (2018).

[7] K. Qian, Z. Eldredge, W. Ge, G. Pagano, M. Foss-Feig, C. Monroe, J. Porto, and A. Gorshkov, Heisenberg-Scaling Measurement Protocol for Analytic Functions with Quantum Sensor Networks, Phys. Rev. A **100**, 042304 (2019).

[8] T. Qian, J. Bringewatt, I. Boettcher, P. Bienias, and A. Gorshkov, Optimal Measurement of Field Properties with Quantum Sensor Networks, Phys. Rev. A **103**, L030601 (2021).

[9] D. Gottesman, T. Jennewein, and S. Croke. Longer-baseline telescopes using quantum repeaters. Phys. Rev. Lett. **109**, 070503 (2012).

[10] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin. Quantum-assisted telescope arrays. Phys. Rev. A **100**, 022316 (2019).

[11] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. A quantum network of clocks. Nature Physics **10**, 582-587 (2014).

[12] K. Chen, H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states. Quantum Inf. Comput. **7**, 689–715 (2007).

[13] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science **560**, 7-11 (2014).

[14] A. K. Ekert. Quantum cryptography based on bell's theorem. Phys. Rev. Lett. **67**, 661 (1991).

[15] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptofraphy without bell's theorem. Phys. Rev. Lett. **68**, 557 (1992).

[16] G. Carrara, G. Murta, and F. Grasselli. Overcoming fundamental bounds on quantum conference key agreement. Phys. Rev. Applied **19**, 064017 (2023).

[17] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi. Experimental quantum conference key agreement. Sci. Adv., **7**, 23 (2021).

[18] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi. Quantum internet: Networking challenges in distributed quantum computing. IEEE Network **34**, 137-143 (2020).

[19] R. Van Meter and S. J. Devitt. The path to scalable distributed quantum computing. Computer **49**, 31-42 (2016).

[20] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993).

[21] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß. Multi-partite entanglement can speed up quantum key distribution in networks. New J. Phys. **19**, 093012 (2017).

[22] H. Yamasaki, A. Pirker, M. Murao, W. Dür, and B. Kraus. Multipartite entanglement outperforming bipartite entanglement under limited quantum system sizes. Phys. Rev. A **98**, 052313 (2018).

[23] M. Takeoka, S. Guha, and M. M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. Nature Communications **5**, 5235 (2014).

[24] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. Nature Communications **8**, 15043 (2017).

[25] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics, Nature **414** (6862), 4 (2001).

[26] N. Sangouard, C. Simon, H. D. Riedmatten, and N. Gisin. Rev. Mod. Phys. **83**, 33 (2011).

[27] K. Azuma, S. B auml, T. Coopmans, D. Elkouss, and B. Li, Tools for quantum network design, AVS Quantum Science **3** (1), 014101 (2021).

[28] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto. Inside quantum repeaters. IEEE Journal of Selected Topics in Quantum Electronics, **21**, 3 (2015).

[29] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. Phys. Rev. Lett., **81**, 5932 (1998).

[30] Y. Hasegawa, R. Ikuta, N. Matsuda, K. Tamaki, H. K. Lo, T. Yamamoto, K. Azuma, and N. Imoto. Experimental time-reversed adaptive bell measurement towards all-photonic quantum repeaters. Nature Communications **10**, 378 (2019).

[31] V. Krutyanskiy, M. Canteri, M. Meraner, J. Bate, V. Krcmarsky, J. Schupp, N. Sangouard, and B. P. Lanyon. Telecom-Wavelength Quantum Repeater Node Based on a Trapped-Ion Processor. Phys. Rev. Lett. **130**,213601 (2023).

[32] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H. -K. Lo, and I. Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. Rev. Mod. Phys. **95**, 045006 (2023).

[33] W. Roga, R. Ikuta, T. Horikiri, and M. Takeoka. Efficient Dicke state generation in a network of lossy channels. Phys. Rev. A **108**, 012612 (2023).

[34] N. Nickerson, Y. Li, and S. Benjamin. Topological quantum computing with a very noisy network and local error rates approaching one percent. Nat. Communications **4**, 1756 (2013).

[35] E. T. Campbell, and S. C. Benjamin. Measurement-Based Entanglement under Conditions of Extreme Photon Loss. Phys. Rev. Lett. **101**, 130502 (2008).

[36] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin. Freely Scalable Quantum Technologies Using Cells of 5-to-50 Qubits with Very Lossy and Noisy Photonic Links. Phys. Rev. X **4**, 041041 (2014).

[37] S. de Bone, P. Möller, C. Bradley, T. Taminiau, and D. Elkouss. Thresholds for the distributed surface code in the presence of memory decoherence. arXiv preprint arXiv:2401.10770 (2024)

Broadband sensitivity enhancement for gravitational-wave detection via quantum teleportation

Yohei Nishino[1 2 3 *]

[1] *Department of Astronomy, University of Tokyo, Bunkyo, Tokyo 113-0033, Japan,*
[2] *Gravitational Wave Science Project, National Astronomical Observatory of Japan (NAOJ), Mitaka City, Tokyo 181-8588, Japan,*
[3] *Department of Gravitational Waves and Fundamental Physics, Maastricht University, 6200 MD, Maastricht, The Netherlands,*

Abstract. We propose an innovative scheme for frequency-dependent squeezing in gravitational wave detectors based on the principle of quantum teleportation [1]. This approach eliminates the need for kilometer-scale filtering cavities, which pose significant infrastructural costs for future detectors. We apply this scheme to the low-frequency detector of the Einstein Telescope and demonstrate that it maintains sensitivity without the need for filter cavities or modifications to the core optics of the interferometer.

Keywords: Gravitational wave, Quantum sensor, Quantum communication, Quantum teleportation

1 Introduction

Since the Laser Interferometric Gravitational-Wave Observatory (LIGO)[2] made history by detecting the first-ever gravitational wave from a binary black hole (BBH) merger[3] in 2015, the collaborative efforts of LIGO, Virgo, and KAGRA [4, 5] have led to the identification of over 90 gravitational wave events [6, 7, 8, 9]. The future-generation gravitational-wave detectors (GWDs), *i.e.* the Cosmic Explorer [10] and the Einstein Telescope [11], striving for tenfold greater sensitivity, will empower the exploration of gravitational wave signals from the events spanning the entire history of the universe [12, 13].

Frequency-dependent squeezing is a well-established technique for reducing quantum noise in GWDs [14, 15, 16, 17]. As will be demonstrated in the next section, reducing both sensing noise (shot noise) and measurement back-action noise (quantum radiation pressure noise) requires filtering the input quantum state to the interferometer. This filtering can be accomplished using a dispersive optical cavity. Given the observation frequency requirements (approximately 100 Hz) and the feasible optical losses in mirror substrates and coatings, the length of the filter cavity is on the order of a few hundred meters for current detectors and will extend to kilometer scales for future detectors.

To mitigate infrastructure-induced costs, several approaches have been proposed. The most advanced among these is EPR (or *conditional*) squeezing [18]. This method utilizes the principle of EPR steering to prepare a single effective filter cavity.

Our proposal in this paper is an extension of EPR squeezing. While EPR squeezing restricts the number of participating modes to two, resulting in a single equivalent filter cavity, our scheme employs Bell measurement and forms tripartite entanglement, allowing the number to increase to three. This process uses continuous variable teleportation based on the Braunstein–Kimble scheme [19, 20].

Fig. 1 illustrates the implementation of phase rotations. Victor is the initial state, and Alice and Bob are the sources of teleportation, entangled with each other. By applying physical operations to each of the beams—Victor, Alice, and Bob—the teleported Victor's state is also manipulated. Given the initial state $|\psi\rangle$, and operations $\mathbb{U}_{v,a,b}$ on each beam, the teleported state becomes $\mathbb{U}_b\mathbb{U}_a\mathbb{U}_v\,|\psi\rangle$. When $\mathbb{U}_b$ represents the response of the GWD and $\mathbb{U}_{v,a}$ represent filtering, the output state achieves the desired quantum noise suppression.

2 Frequency-dependent squeezing

A basic configuration of gravitational-wave detectors entails a Michelson interferometer, depicted in the Fig. 2. A bright-coherent light is injected into the beam splitter (BS) from the minus-x side (bright port), capturing information on the displacement of the end mirrors induced by gravitational waves (GW) tidal forces. These forces act differentially on the mirrors. The displacement information is encoded in the phase of the light, with only differential phase fluctuations emerging at the minus-y (dark) port due to destructive interference at the BS. Additionally, alongside the Michelson interferometer, two cavities are implemented[1]. Firstly, Fabry-P'erot cavities (FPCs) are installed in each Michelson arm. Secondly, there is the so-called signal extraction cavity (SEC), formed by the input mirror of the FPCs and the signal extraction mirror (SEC).

The FPCs circulate the laser light inside to effectively increase the length of the arms, thereby enhancing the interaction between the mirror motion caused by the gravitational wave (GW) and the laser light. On the other hand, the SEC recycles the GW sidebands to the main interferometer and adjusts the extraction rate of the signal beam. This recycling broadens the bandwidth of the

*yohei.nishino@grad.nao.ac.jp

[1] We do not discuss a power recycling cavity in this paper, although it is standard in current detectors.

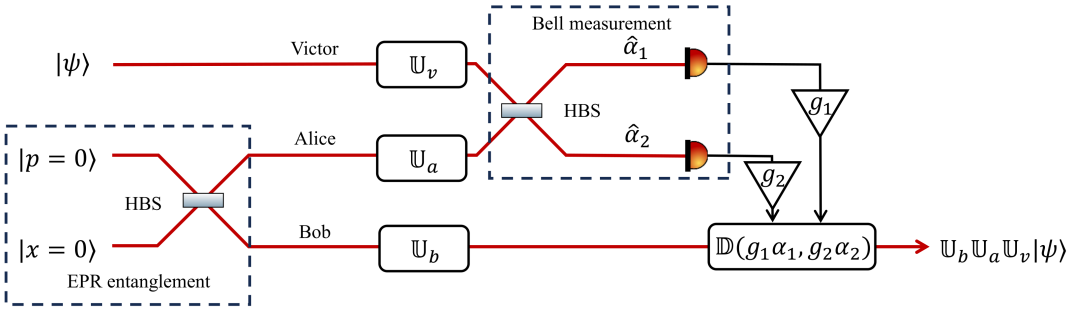


Figure 1: Schematics of continous-variable teleportation

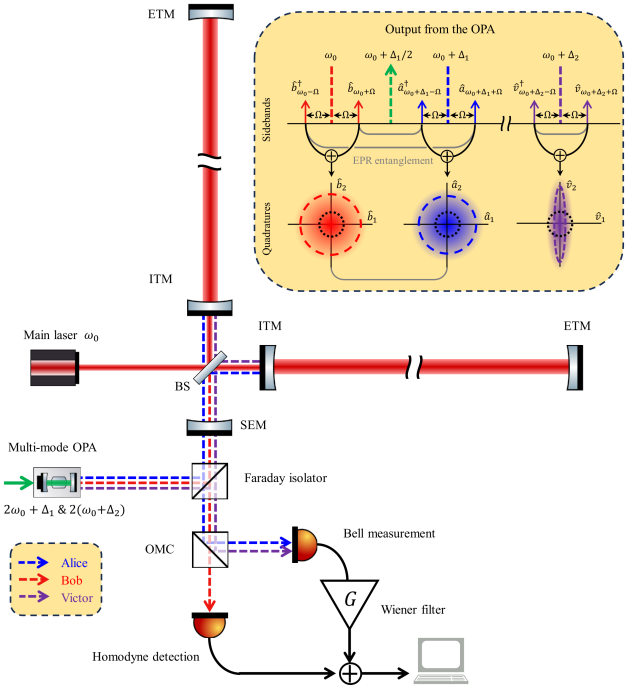


Figure 2: QT Squeezing Configuration from [1]: In the anti-symmetric port, the OPA is pumped at two frequencies, $2\omega_0 + \Delta_a$ for a two-mode EPR entanglement between Alice and Bob, and $2(\omega_0 + \Delta_v)$ for a squeezed Victor state, generating symmetrical entanglement at the sideband frequencies. These three beams are injected through a Faraday isolator. The core part is a signal-recycled Fabry-Pérot Michelson Interferometer, featuring a beam splitter (BS), input test mass (ITM), end test mass (ETM), and signal extraction mirror (SEM). This interferometer is pumped at the frequency ω_0, aligning with Bob's frequency. The output is then spectrally separated by an output mode cleaner (OMC). At the detection stage, Bob's beam undergoes homodyne detection, whereas Victor and Alice are processed through a Bell measurement. The outputs are then optimally combined using filter gains, (g_1 g_2), to achieve quantum-noise suppression.

detector effectively, enabling the detection of signals at higher frequencies.

Furthermore, by detuning the round-trip phase in the SEC, one can create a dip via the optical spring effect, potentially allowing us to surpass the standard quantum limit of free masses [21]. The input-output relation of the vacuun field entering from the dark port can be written as follows:

$$\hat{B}_2 = \Gamma e^{i\beta_b}(\hat{b}_1 \cos\theta_b - \hat{b}_2 \sin\theta_b). \tag{1}$$

Here, Γ represents the so-called frequency-dependent gain, as defined in [22]. It equals unity in the absence of optomechanical coupling but deviates from unity when such coupling is present. This coupling is also referred to as ponderomotive squeezing. θ_b denotes the frequency-dependent quadrature rotation, while β_b represents an irrelevant phase shift acquired during propagation in the interferometer. The red curve in Fig.3 represents θ_b for the ETLF. In this specific scenario, phase rotations occur at two distinct frequencies, approximately 8 Hz and 20 Hz, highlighting the requirement for two filter cavities to achieve broad-band noise suppression (for more details, see the supplementary materials in [1]).

3 Broadband noise reduction through teleportation

3.1 State preparation

Three beams participate in the teleportation process: Alice, Bob, and Victor. The quadrature-phase amplitudes for these three beams are represented as $\hat{\boldsymbol{a}} = \{\hat{a}_1, \hat{a}_2\}^{\mathrm{T}}, \hat{\boldsymbol{b}} = \{\hat{b}_1, \hat{b}_2\}^{\mathrm{T}}, \hat{\boldsymbol{v}} = \{\hat{v}_1, \hat{v}_2\}^{\mathrm{T}}$, where Ω denotes the audio-sideband frequency around the central frequency of each beam.

Alice and Bob form a two-mode squeezed state, resulting in the noise spectrum:

$$S_{(\hat{a}_1 \pm \hat{b}_1)/\sqrt{2}} = e^{\pm 2r}, \quad S_{(\hat{a}_2 \pm \hat{b}_2)/\sqrt{2}} = e^{\mp 2r} \tag{2}$$

where r represents the squeezing factor.

When the quadrature $\hat{a}_{-\theta} = \hat{a}_1 \cos\theta - \hat{a}_2 \sin\theta$ is measured, the quadrature $\hat{b}_\theta = \hat{b}_1 \cos\theta + \hat{b}_2 \sin\theta$ is conditionally squeezed, and vice versa. The spectral density of the conditionally squeezed field is given by:

$$S^{\hat{a}_{-\theta}}_{\hat{b}_\theta \hat{b}_\theta} = 1/\cosh(2r)\,, \quad S^{\hat{a}_{-\theta}}_{\hat{b}_{\pi/2+\theta}\hat{b}_{\pi/2+\theta}} = \cosh(2r)\,. \tag{3}$$

The amplitude (phase) quadrature of Victor is (anti-)squeezed as:

$$S_{\hat{v}_1\hat{v}_1} = e^{-2r}, \quad S_{\hat{v}_2\hat{v}_2} = e^{2r}. \tag{4}$$

3.2 Teleportation and Noise Suppression

To teleport Victor's state, Bell measurement between Victor and Alice's state is required, involving observables defined as:

$$\hat{\boldsymbol{\alpha}} = \begin{pmatrix} \hat{\alpha}_1 \\ \hat{\alpha}_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \hat{V}_1 - \hat{A}_1 \\ \hat{V}_2 + \hat{A}_2 \end{pmatrix}, \tag{5}$$

where $\hat{A}_1 = e^{i\beta_a}(\hat{a}_1 \cos\theta_a - \hat{a}_2 \sin\theta_a)$, $\hat{A}_2 = e^{i\beta_a}(\hat{a}_1 \sin\theta_a + \hat{a}_2 \cos\theta_a)$ and $\hat{V}_1 = e^{i\beta_v}(\hat{v}_1 \cos\theta_v - \hat{v}_2 \sin\theta_v)$, $\hat{V}_2 = e^{i\beta_v}(\hat{v}_1 \sin\theta_v + \hat{v}_2 \cos\theta_v)$ represent the quadratures of the Alice and Victor's beams after passing through the interferometer. Note that $\theta_{a,v}$ and $\beta_{a,v}$ are characterized in the same way as Eq. (1), and $\Gamma_{a,v}$ is unity since the interferometer is not pumped at Victor and Alice's frequency.

Next, we aim to determine the optimal filter to minimize the noise spectrum density of the operator:

$$\hat{B}_2^{\rm tel} = \hat{B}_2 - g_1\hat{\alpha}_1 - g_2\hat{\alpha}_2, \tag{6}$$

where $g_{1,2}$ are the filter gains. The shape of these filters can be calculated as follows:

$$g_1 = \frac{S_{\hat{B}_2\hat{\alpha}_1} S_{\hat{\alpha}_2\hat{\alpha}_2} - S_{\hat{\alpha}_2\hat{\alpha}_1} S_{\hat{B}_2\hat{\alpha}_2}}{S_{\hat{\alpha}_1\hat{\alpha}_1} S_{\hat{\alpha}_2\hat{\alpha}_2} - |S_{\hat{\alpha}_1\hat{\alpha}_2}|^2}, \tag{7}$$

$$g_2 = \frac{S_{\hat{B}_2\hat{\alpha}_2} S_{\hat{\alpha}_1\hat{\alpha}_1} - S_{\hat{\alpha}_1\hat{\alpha}_2} S_{\hat{B}_2\hat{\alpha}_1}}{S_{\hat{\alpha}_1\hat{\alpha}_1} S_{\hat{\alpha}_2\hat{\alpha}_2} - |S_{\hat{\alpha}_1\hat{\alpha}_2}|^2}, \tag{8}$$

(see more details in the Supplementary Material of [1]). Finally, the one-sided noise (power) spectrum density of $\hat{B}_2^{\rm tel}$ becomes:

$$S^{\rm tel}_{\hat{B}_2\hat{B}_2} = |\Gamma|^2 \frac{1 + e^{-2r}\cosh 2r}{e^{-2r} + \cosh 2r} \xrightarrow{r\gg 1} |\Gamma|^2 \frac{3}{e^{2r}}. \tag{9}$$

3.3 Comparison with the Conventional Scheme

We applied the teleportation scheme to the ETLF as an example (see the left panel of Fig. 4). Detailed parameters can be found in [1], therefore we show only the sensitivity curves in this article. Comparing the QT squeezing (QTS) with -17 dB of squeezing with the conventional filter-cavity scheme with -10 dB ("baseline" scheme), one can realize that QTS is inferior to the baseline at frequencies between 10 - 20 Hz and below 6 Hz (above 20 Hz it is covered by the high-frequency part of ET). This is because of the threefold noise contribution from the input and readout losses and 4.8 dB penalty for employing tripartite entanglement. However, the sensitivity around 8 Hz is better than the baseline scheme. This is one of the benefits of utilizing 10-km long, ultra-stable, and low-loss arm cavities as filter cavities. Since around this dip frequency, made by the optical spring, the optimal quadrature angle is rapidly rotated via ponderomotive squeezing, losses, and length fluctuation of the filter cavity contribute to worsening the sensitivity more than at other frequencies. This superiority at 8 Hz is the case even if one increases the squeezing level of the baseline scheme to the same level, -17 dB. One can conclude that the QT squeezing increases the upper limit of squeezing.

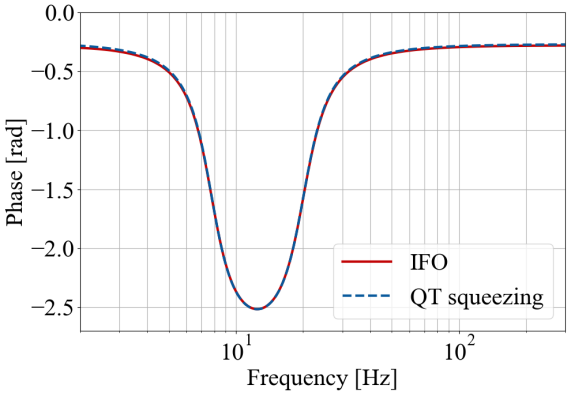


Figure 3: Phase rotation of the ETLF (red solid) and the QT squeezing (blue dashed).

The right panel of Fig. 4 shows the detection horizon of non-spinning equal-mass compact binary coalescence. The noise spectra integrate the quantum noise of ETLF with the classical noise budget of ETLF and the entire noise of ETHF. Due to the sensitivity improvement at 8 Hz, the maximum horizon stretches above $z = 80$.

4 Impact

Our scheme eliminates the need for two filter cavities in ETLF, while retaining its sensitivity. This reduction in infrastructure requirements, such as kilometer-scale vacuum chambers, tunnels, suspension systems, and caverns, significantly lowers the associated costs. By iteratively applying the teleportation process, one can extend the number of effective filter cavities from 2 to an arbitrary number. This approach can be applied to future detectors, including those in space, which may be larger and more complex, necessitating multiple filter cavities.

5 Conclusion

We have presented a method for enhancing the sensitivity of gravitational-wave detectors across a broad frequency range by leveraging the principles of quantum teleportation. Key components include the entangled source and Bell measurement, both of which are experimentally feasible. We applied this scheme to the low-frequency detector of the Einstein Telescope, revealing both benefits and drawbacks. The benefit is an enhancement around the frequency of the optical spring, approximately 8 Hz in our specific case. Drawbacks include a threefold noise contribution from input and output losses and a 4.8 dB reduction in squeezing level. From a technical standpoint, our approach eliminates the need for infrastructure associated with filter cavities, which are projected to be kilometer-scale for future large detectors.

References

[1] Yohei Nishino, Stefan Danilishin, Yutaro Enomoto, and Teng Zhang. Frequency-dependent squeezing for

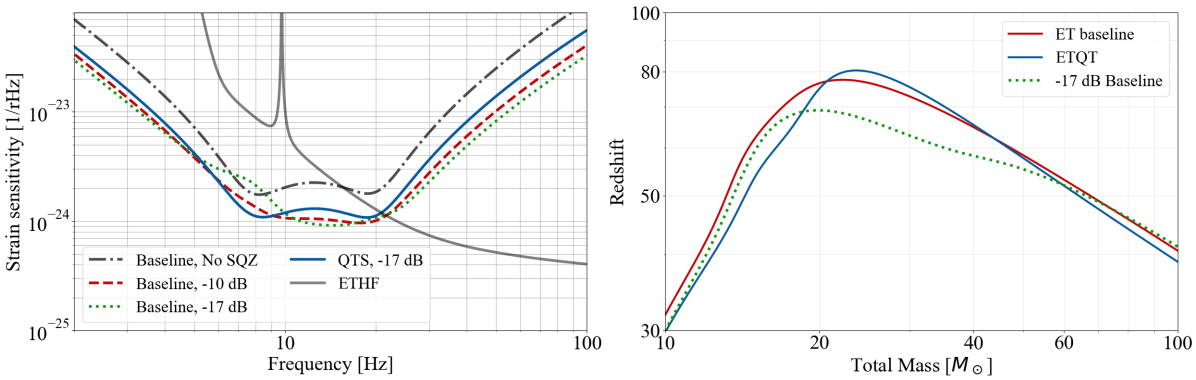


Figure 4: Left: Sensitivity curves with various configurations. The blue solid curve represents the ETLF with -17 dB QT squeezing, the red dashed curve represents the current design with -10 dB squeezing, the green dotted curve represents the current design with -17 dB squeezing, the grey dash-dotted curve represents the current design without squeezing, and the grey solid curve represents the high-frequency part of ET. Right: Detection horizon of equal-mass non-spin compact binary mergers. The horizontal axis represents the total mass of the binary, and the vertical axis represents the redshift of the detectable distance.

gravitational-wave detection through quantum teleportation. arXiv:2401.04295, 2024.

[2] LIGO Scientific Collaboration et al. Advanced ligo. *Classical and Quantum Gravity*, 32(7):074001, mar 2015.

[3] LIGO Scientific Collaboration, Virgo Collaboration, et al. Observation of gravitational waves from a binary black hole merger. *Phys. Rev. Lett.*, 116:061102, Feb 2016.

[4] F Acernese et al. Advanced virgo: a second-generation interferometric gravitational wave detector. *Classical and Quantum Gravity*, 32(2):024001, dec 2014.

[5] KAGRA Collaboration and others. KAGRA: 2.5 generation interferometric gravitational wave detector. *Nature Astronomy*, 3(1):35–40, jan 2019.

[6] LIGO Scientific Collaboration, Virgo Collaboration, et al. GWTC-1: A gravitational-wave transient catalog of compact binary mergers observed by ligo and virgo during the first and second observing runs. *Phys. Rev. X*, 9:031040, Sep 2019.

[7] LIGO Scientific Collaboration, Virgo Collaboration, et al. Gwtc-2: Compact binary coalescences observed by ligo and virgo during the first half of the third observing run. *Phys. Rev. X*, 11:021053, Jun 2021.

[8] LIGO Scientific Collaboration, Virgo Collaboration, et al. Gwtc-3: Compact binary coalescences observed by ligo and virgo during the second part of the third observing run, 2021.

[9] Tejaswi Venumadhav, Barak Zackay, Javier Roulet, Liang Dai, and Matias Zaldarriaga. New binary black hole mergers in the second observing run of advanced ligo and advanced virgo. *Phys. Rev. D*, 101:083030, Apr 2020.

[10] B P Abbott et al. Exploring the sensitivity of next generation gravitational wave detectors. *Classical and Quantum Gravity*, 34(4):044001, jan 2017.

[11] S Hild et al. Sensitivity studies for third-generation gravitational wave observatories. *Classical and Quantum Gravity*, 28(9):094013, apr 2011.

[12] Mauro Pieroni, Angelo Ricciardone, and Enrico Barausse. Detectability and parameter estimation of stellar origin black hole binaries with next generation gravitational wave detectors. *Scientific Reports*, 12(1), oct 2022.

[13] Michele Maggiore et al. Science case for the einstein telescope. *Journal of Cosmology and Astroparticle Physics*, 2020(03):050, mar 2020.

[14] H. J. Kimble, Yuri Levin, Andrey B. Matsko, Kip S. Thorne, and Sergey P. Vyatchanin. Conversion of conventional gravitational-wave interferometers into quantum nondemolition interferometers by modifying their input and/or output optics. *Phys. Rev. D*, 65:022002, Dec 2001.

[15] Carlton M. Caves. Quantum-mechanical noise in an interferometer. *Phys. Rev. D*, 23:1693–1708, Apr 1981.

[16] Yuhang Zhao, Naoki Aritomi, Eleonora Capocasa, Matteo Leonardi, Marc Eisenmann, Yuefan Guo, Eleonora Polini, Akihiro Tomura, Koji Arai, Yoichi Aso, Yao-Chin Huang, Ray-Kuang Lee, Harald Lück, Osamu Miyakawa, Pierre Prat, Ayaka Shoda, Matteo Tacca, Ryutaro Takahashi, Henning Vahlbruch, Marco Vardaro, Chien-Ming Wu, Matteo Barsuglia, and Raffaele Flaminio. Frequency-dependent squeezed vacuum source for broadband quantum noise reduction in advanced gravitational-wave detectors. *Phys. Rev. Lett.*, 124:171101, Apr 2020.

[17] L. McCuller, C. Whittle, D. Ganapathy, K. Komori, M. Tse, A. Fernandez-Galiana, L. Barsotti, P. Fritschel, M. MacInnis, F. Matichard, K. Mason, N. Mavalvala, R. Mittleman, Haocun Yu, M. E. Zucker, and M. Evans. Frequency-dependent squeezing for advanced ligo. *Phys. Rev. Lett.*, 124:171102, Apr 2020.

[18] Yiqiu Ma, Haixing Miao, Belinda Heyun Pang, Matthew Evans, Chunnong Zhao, Jan Harms, Roman Schnabel, and Yanbei Chen. Proposal for gravitational-wave detection beyond the standard quantum limit through EPR entanglement. *Nature Physics*, 13(8):776–780, may 2017.

[19] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998.

[20] Samuel L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. *Phys. Rev. Lett.*, 80:869–872, Jan 1998.

[21] Alessandra Buonanno and Yanbei Chen. Signal recycled laser-interferometer gravitational-wave detectors as optical springs. *Phys. Rev. D*, 65:042001, Jan 2002.

[22] L. McCuller et al. LIGO's quantum response to squeezed states. *Phys. Rev. D*, 104:062006, Sep 2021.

Constructing the joint quasi-distribution representations for quantum states with deep generate models

Yu-Chen Lee[1] * Kuan-Lun Lai[1] Chi-Hua Yu[1] Hong-Bin Chen[1 2 3]

[1] *Department of Engineering Science, National Cheng Kung University, Tainan 701401, Taiwan*
[2] *Center for Quantum Frontiers of Research & Technology, NCKU, Tainan 701401, Taiwan*
[3] *Physics Division, National Center for Theoretical Sciences, Taipei 10617, Taiwan*

Abstract. Our research introduces an innovative approach in quantum physics using Deep Generative Models (DGMs) to create complex joint quasi-distribution functions with minimal experimental data. By breaking down the construction of bivariate joint quasi-distribution functions into three simpler marginals, DGMs significantly cuts down on the need for human resources, funding, and time. This method enables faster and more accurate results.

Keywords: Wigner function, Machine learning, Deep Generative Models, Quantum computing

1 Introduction

The Wigner function is a useful tool in quantum mechanics for representing quantum states in phase space, allowing us to visualize quantum phenomena and connect the quantum world to classical mechanics. It reveals details about quantum interference and superposition, and its ability to show negative values highlights the non-classical nature of quantum systems, deepening our understanding of how quantum mechanics differs from classical physics. The Wigner function is also crucial in practical applications like quantum computing, quantum optics, and quantum information theory, as it helps in reconstructing and analyzing quantum states. We introduce three specific states—squeezed states, coherent states, and cat states—because their simple mathematical forms make them easier to work with.

Squeezed states reduce uncertainty in certain measurements by decreasing the quantum noise in one variable while increasing it in the conjugate variable, adhering to Heisenberg's uncertainty principle. This feature is particularly beneficial for precision measurements in areas like gravitational wave detection, where reducing noise can significantly enhance detection capabilities. Squeezed states are also crucial for quantum cryptography, teleportation, and quantum computing due to their unique quantum correlations, known as entanglement. Their Wigner function has a distinctive elongated shape along one axis, reflecting the reduced uncertainty in that direction. For detailed formulas and further discussion, please refer to Appendix2.

Coherent states have minimal uncertainty in both position and momentum, making them the closest quantum states to classical harmonic oscillators. These states are eigenstates of the annihilation operator, which means they maintain their form over time, only changing by a phase factor. Coherent states are fundamental in quantum optics and are the basis for understanding laser light, which can be described as a coherent state of the electromagnetic field. Their Wigner function is a Gaussian distribution centered in phase space, representing the minimum uncertainty and classical-like behavior of these states. The marginals of coherent states in three axes are well-defined and easy to interpret.For detailed formulas and further discussion, please refer to Appendix3

Cat states, or Schrödinger's cat states, are superpositions of two or more coherent states. They are named after the famous thought experiment by Schrödinger, which illustrates the paradox of superposition in quantum mechanics. Cat states demonstrate the principle of quantum superposition on a macroscopic scale and exhibit unique quantum features like interference patterns in their Wigner functions. These patterns alternate between positive and negative regions, showcasing the non-classical properties of cat states. They are valuable in quantum computing and communication because they can represent qubits in superposition, potentially leading to more powerful quantum algorithms and secure communication protocols.For detailed formulas and further discussion, please refer to Appendix4

We chose these states because their simple mathematical expressions make them easier to analyze, allowing for precise calculations and predictions essential for both theoretical studies and practical applications. Their well-defined Wigner functions enable detailed simulations and provide deeper insights into quantum phenomena. Traditional methods for studying quantum processes, such as quantum process tomography, are complex and require extensive experiments, often involving point-by-point scanning of the Wigner function in phase space. To simplify this, we use DGMs to construct the Wigner function from just a few marginal distributions, efficiently generating the bivariate joint quasidistribution and significantly reducing the experimental effort needed. This approach only requires three marginal distributions—probabilities in real or momentum space—to create the Wigner function, thereby reduce experimental resources.

2 Wigner functions

To train our Deep Generative Models (DGMs), we first create a labeled dataset of Wigner functions, focusing on

*N96111176@gs.ncku.edu.tw

three key marginals: $W(x)$, $W(p)$, and $W(u)$. These marginals represent spatial, momentum, and a combined axis, respectively, and can be calculated even with thermal noise. Wigner function is a crucial tool in quantum physics for visualizing quantum states, especially due to its ability to exhibit negativity, which indicates genuine quantum characteristics. However, constructing the Wigner function can be challenging. In contrast, marginals are standard probability distributions, making them easier to construct from experimental data. Our goal is to use these marginals to construct joint quasi-distribution functions that permit negativity. By leveraging artificial intelligence techniques, our trained DGMs can efficiently create these functions from the marginals. The motional state of a quantum system can be described by the density matrix ρ or the Wigner function. More information in Appendix1. This real-valued quasi-distribution function allows for negativity, indicating quantum essence. The Wigner function's unique property is that its marginals are standard probability distributions, making them easier to measure experimentally.

3 Quantum states and their marginals

We select specific quantum states, including coherent, cat, and squeezed states, and generate three distinct projections (marginals) for each along three axes. This approach allows us to examine each state's attributes and explore their characteristics in detail. Initial parameters for the spatial and momentum grid's range and resolution are established to accurately depict the environment where these quantum states manifest. Random variables such as position, momentum, squeezing parameters, and phase angles are introduced to reflect real-world conditions and enhance the DGMs' ability to generalize.Consider a quantum harmonic oscillator in coherent, cat, or squeezed states exposed to a thermal bath. The marginals $W(x)$ and $W(p)$ have clear physical interpretations as probability distributions in real and momentum space. Additionally, the third marginal $W(u)$ over the oblique variable u = (x+p)/$\sqrt{2}$ is accessible in real space after a $\pi/4$ rotation of the quantum states. This comprehensive approach allows us to deeply analyze and understand the properties of these quantum states.

4 Data generation and preparation

We prepare a labeled training dataset. The training data can be generated efficiently, with each datum consisting of three marginals $W(x)$, $W(p)$, and $W(u)$ derived analytically even in the presence of thermal noise. Each marginal is numerically sampled into 721 pixels as the raw data, more information in Appendix5. The formulas for quantum states and marginals from previous sections are used as inputs for model training. Them we create a function to ensure no information is lost while managing and preparing data from various quantum states. This function merges the data into a unified dataset formatted to match our machine learning models' input requirements. The dataset is then split into training and testing sets and shuffled to prevent biases, ensuring effective support for the model's learning process.

Additionally, the synthetic datasets are informed by physical principles, making them adaptable. By tweaking relevant parameters, they can be optimized to sufficiently reflect the target marginals of a specific quantum dynamics model. This optimization aids in enhancing the proficiency and precision of our DGMs. Armed with this knowledge, we can fine-tune the parameters during the synthetic data generation. This ensures that our synthetic marginals align closely with the nuances of the quantum model to be solved.

5 Training the ResNet-based deep generative models

We use a ResNet architecture with a mean squared error loss function and Adam optimizer. The model undergoes training in multiple cycles (epochs) using batches of data. A validation set is used to check the model's ability to generalize. Throughout training, the model is saved along with graphs showing training progress to help monitor and adjust the training parameters. Our DGMs are structured into six stages, each constructed by repeatedly stacking two core building blocks: the identity and deconvolution blocks. Aiming to produce three images from input marginals, the main stream of both blocks utilizes three deconvolutional layers. These layers extract key patterns from the input marginals and expand them to produce the output images of a quasi-distribution. However, for the model to handle this intricate task, it requires more depth and additional deconvolutional layers, which intensifies the vanishing gradient problem and significantly impedes our model's training.

To solve this, we added shortcuts to each block, known as the ResNet structure. These skip connections help keep information from earlier layers, reducing the vanishing gradient problem. This allows us to make the model deeper and more powerful.

6 Model evaluation and analysis

After training, the model is evaluated using a test dataset. We compare the model's predictions with actual data through visual and numerical analyses to ensure the experiment's reliability and accuracy. Detailed evaluation methods and results will be discussed in next section. By following this structured process, we ensure that the DGMs is effectively trained to understand and work with Wigner functions.

7 Results

Our model successfully predicted Wigner functions with high accuracy. We verified the decoder model's performance by visually comparing its predictions against actual test data. The discrepancies were quantified using the sum of squared differences (L2 norm) to measure accuracy and the sum of absolute differences (L1 norm) to evaluate marginal distributions. The model was fed

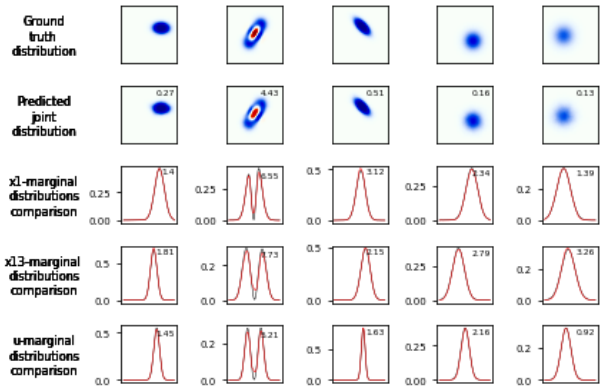


Figure 1: **Verifying the DGMs's performance**. The decoder model's performance is evaluated using two distinct test datasets. The first row shows the ground truth joint distributions for both test cases, serving as a benchmark. The second row displays the model's predicted joint distributions, with the pixel-averaged L2 norm in the upper right corner of each sub-image, indicating overall prediction accuracy. Rows three to five provide detailed analysis by comparing the marginals along the x axis, p axis, and u axis, with the pixel-averaged L1 norm in the upper right corner of each sub-image, highlighting the model's accuracy in specific aspects. This demonstrates the model's precision and areas needing refinement in predicting complex joint distributions.

inputs derived from three marginal distributions along distinct axes, discretized into 721 points each, totaling 2163 points. These points were aligned sequentially to form the feature set for the raw data. Target labels were structured in a 256x256 grid, consistent with the analysis of pure dephasing phenomena. This setup ensured a comprehensive understanding of the quantum state's characteristics.

During training, the decoder model learned to decipher complex patterns between input data and output Wigner functions, enabling accurate and fast predictions, thereby addressing time complexity challenges. By focusing on marginals, the measurement process was streamlined, significantly reducing the time and resources needed for reconstructing Wigner functions. The efficacy of our approach is demonstrated in Fig 1, showcasing the model's precision in predicting Wigner functions. This success validates our method and highlights the potential of the decoder model to transform Wigner function measurement, opening new avenues for investigating quantum systems requiring large-scale or high-resolution analysis. This innovation promises enhanced efficiency and accuracy in exploring the complexities of quantum dynamics, even under thermal noise.

8 Conclusion

Our DGMs represents a significant advancement in quantum physics analysis by simplifying the construction and understanding of Wigner functions. By focusing on the creation of bivariate joint quasi-distribution functions from three simpler marginals, our DGMs offers a more intuitive and manageable approach to analyzing complex quantum phenomena. This method enhances precision and efficiency while broadening applicability across various quantum systems. The flexibility of our approach, which allows for marginals to be derived from both experimental data and theoretical models, is a significant advantage. It ensures that the DGMs accurately captures the intricacies of quantum mechanics, providing a robust tool for understanding phenomena such as superposition and entanglement. Moreover, integrating advanced machine learning techniques addresses critical challenges in measuring quantum states in phase space. Our model's ability to process and analyze high-dimensional quantum systems efficiently, while minimizing noise and computational limitations, opens up new opportunities for quantum mechanics research. The success of our DGMs in predicting Wigner functions validates its effectiveness and potential to transform the measurement and analysis of quantum systems, paving the way for more accessible, accurate, and efficient exploration of the quantum realm.

9 Future Works

Our method addresses traditional limitations by employing neural networks, such as ResNet, to introduce a novel computational framework in quantum physics. However, there are still challenges to address, including improving the quality of training data, managing computational complexity, and enhancing model interpretability. Future research should aim to improve data collection methods, optimize neural networks, and incorporate explainable AI. Collaboration between quantum physicists and AI experts is essential to refine these models and stay updated with advancements in quantum research. Our research demonstrates significant potential for further innovations in quantum computing, simulation, and information processing. Key areas of focus include enhancing the training and scalability of DGMs and exploring new quantum phenomena. As quantum technology progresses, advanced computational models will unlock new capabilities and drive innovation. Interdisciplinary collaboration is crucial for achieving groundbreaking discoveries in quantum science.

References

[1] S. Ahmed, C. S. Muñoz, F. Nori, and A. F. Kockum. Quantum state tomography with conditional generative adversarial networks. *Physical Review Letters*, 127(14):140502, 2021. Physical Review Letters.

[2] S. Ahmed, C. S. Muñoz, F. Nori, and A. F. Kockum. Classification and reconstruction of optical quantum states with deep neural networks. *Physical Review Research*, 3(3):033278, 2021. Physical Review Research.

[3] E. Y. Zhu, S. Johri, D. Bacon, M. Esencan, J. Kim, M. Muir, N. Murgai, J. Nguyen, N. Pisenti,

A. Schouela, and others. Generative quantum learning of joint probability distribution functions. *Physical Review Research*, 4(4):043092, 2022. Physical Review Research.

[4] S. Chen, O. Savchuk, S. Zheng, B. Chen, H. Stoecker, L. Wang, and K. Zhou. Fourier-flow model generating Feynman paths. *Physical Review D*, 107(5):056001, 2023. Physical Review D.

[5] J. Weinbub and D. K. Ferry. Recent advances in Wigner function approaches. *Applied Physics Reviews*, 5(4), 2018. Applied Physics Reviews.

A Appendix 1

The Wigner function defined as

$$W(x,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{\infty} \langle x+y|\rho|x-y\rangle\, e^{-i2py/\hbar}dy, \tag{1}$$

For pure state as

$$W(x,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{\infty} \Psi^*(x+y)\Psi(x-y)e^{-i2py/\hbar}dy, \tag{2}$$

$$W_n(x,p) = \frac{(-1)^n}{\pi}e^{-(x^2+p^2)}L_n(2(x^2+p^2)), \tag{3}$$

$$\begin{cases} |\psi_n(x)|^2 = \frac{1}{\sqrt{\pi}2^n n!}e^{-x^2}H_n^2(x) \\ |\psi_n(p)|^2 = \frac{1}{\sqrt{\pi}2^n n!}e^{-p^2}H_n^2(p) \\ |\psi_n(u)|^2 = \frac{1}{\sqrt{\pi}2^n n!}e^{-u^2}H_n^2(u) \end{cases} \tag{4}$$

B Appendix 2

The Wigner function of the squeezed state is

$$\begin{aligned} W_{\alpha,\varphi,r}(x,p) = \frac{2}{\pi}exp\Big[& -2\cosh 2r(x-\Re[\alpha])^2 \\ & + (p-\Im[\alpha])^2 + 2\sinh 2r[\cos\varphi(\frac{1}{2}x^2+p^2) \\ & - \frac{1}{2}x\Re[\alpha] - p\Im[\alpha] + \Re[\alpha]^2 - \Im[\alpha]^2 \\ & - \sin\varphi\big(xp - \frac{1}{2}p\Re[\alpha] + x\Im[\alpha] \\ & + 2\Re[\alpha]\Im[\alpha]\big)\Big] \end{aligned} \tag{5}$$

To simplify this, I've transformed the original Wigner function into a more manageable Gaussian form, represented as bivariate Gaussian distribution

$$\begin{aligned} W(x,p) = & \frac{1}{2\pi\sigma_x\sigma_p\sqrt{1-\rho^2}} \\ & \times e^{\left(\frac{-1}{2(1-\rho^2)}\left[\left(\frac{x-\mu_x}{\sigma_x}\right)^2 - 2\rho\left(\frac{x-\mu_x}{\sigma_x}\right)\left(\frac{p-\mu_p}{\sigma_p}\right) + \left(\frac{p-\mu_p}{\sigma_p}\right)^2\right]\right)}, \end{aligned} \tag{6}$$

with the marginal in three axes:

$$\begin{cases} \mathrm{W(x)} = \frac{1}{\sqrt{2\pi}\sigma_x}e^{-\frac{(x-\mu_x)^2}{2\sigma_x^2}}, \\ \mathrm{W(p)} = \frac{1}{\sqrt{2\pi}\sigma_p}e^{-\frac{(p-\mu_p)^2}{2\sigma_p^2}}, \\ \mathrm{W(u)} = \frac{1}{\sqrt{\pi}\sqrt{\sigma_x^2+2\rho\sigma_x\sigma_p+\sigma_p^2}}e^{-\frac{(u-\sqrt{2}\Re[\alpha e^{-i\pi/4}])^2}{\sigma_x^2+2\rho\sigma_x\sigma_p+\sigma_p^2}}, \end{cases} \tag{7}$$

which is much simpler to compute

where $u = \frac{x+iy}{\sqrt{2}}$, and in the process of my analysis, I deduced several key coefficients, which are

$$\mu_x = \sqrt{2}\Re[\alpha] \tag{8}$$

$$\mu_p = \sqrt{2}\Im[\alpha] \tag{9}$$

$$\rho^2 = \frac{\sinh^2(2r)\sin^2\varphi}{\cosh^2(2r) - \sinh^2(2r)\cos^2\varphi} \tag{10}$$

$$\rho = -\frac{\sinh(2r)\sin\varphi}{\sqrt{\cosh^2(2r) - \sinh^2(2r)\cos^2\varphi}} \tag{11}$$

$$1-\rho^2 = \frac{1}{\cosh^2(2r) - \sinh^2(2r)\cos^2\varphi} \tag{12}$$

$$\begin{aligned} \sigma_x^2 &= \frac{\cosh(2r) + \sinh(2r)\cos\varphi}{2\left[\cosh^2(2r) - \sinh^2(2r)\cos^2\varphi - \sinh^2(2r)\sin^2\varphi\right]} \\ &= \frac{1}{2}\left[\cosh(2r) + \sinh(2r)\cos\varphi\right] \end{aligned} \tag{13}$$

$$\begin{aligned} \sigma_p^2 &= \frac{\cosh(2r) - \sinh(2r)\cos\varphi}{2\left[\cosh^2(2r) - \sinh^2(2r)\cos^2\varphi - \sinh^2(2r)\sin^2\varphi\right]} \\ &= \frac{1}{2}\left[\cosh(2r) - \sinh(2r)\cos\varphi\right] \end{aligned} \tag{14}$$

By reducing the original Wigner function to this form, I've made it much easier to calculate and analyze, especially for practical applications where a simplified model is sufficient to capture the essential features of the quantum state."

Finally, incorporating these parameters into our formulas, I arrived at the desired results:

$$\begin{aligned} W_{\alpha,r,\varphi}(x,p) = \frac{1}{\pi}exp\Bigg[& \left(\frac{-\cosh^2(2r) + \sinh^2(2r)\cos^2\varphi}{2}\right) \\ & \times \Bigg[\left(\frac{\sqrt{2}(x-\sqrt{2}\Re[\alpha])}{\sqrt{\cosh(2r)+\sinh(2r)\cos\varphi}}\right)^2 \\ & + \frac{4\sinh(2r)\sin\varphi(x-\sqrt{2}\Re[\alpha])(p-\sqrt{2}\Im[\alpha])}{\cosh^2(2r) - \sinh^2(2r)\cos^2\varphi} \\ & + \left(\frac{\sqrt{2}(p-\sqrt{2}\Im[\alpha])}{\sqrt{\cosh(2r)-\sinh(2r)\cos\varphi}}\right)^2\Bigg]\Bigg] \end{aligned} \tag{15}$$

and the marginals in three axes:

$$\begin{cases} |\ W_{\alpha,r,\varphi}(x)\ |^2 &= \frac{1}{\sqrt{\pi}\sqrt{\cosh(2r)+\sinh(2r)\cos\varphi}} \\ &\quad \times e^{-\frac{(x-2\Re[\alpha])^2}{\cosh 2r+\sinh(2r)\cos\varphi}}, \\ |\ W_{\alpha,r,\varphi}(p)\ |^2 &= \frac{1}{\sqrt{\pi}\sqrt{\cosh(2r)-\sinh(2r)\cos\varphi}} \\ &\quad \times e^{-\frac{(p-2\Im[\alpha])^2}{\cosh 2r-\sinh(2r)\cos\varphi}}, \\ |\ W_{\alpha,r,\varphi}(u)\ |^2 &= \frac{1}{\sqrt{\pi}\sqrt{\cosh(2r)-\sinh(2r)\sin\varphi}} \\ &\quad \times e^{-\frac{(u-2\Re[\alpha e^{-i\pi/4}])^2}{\cosh(2r)-\sinh(2r)}}. \end{cases} \tag{16}$$

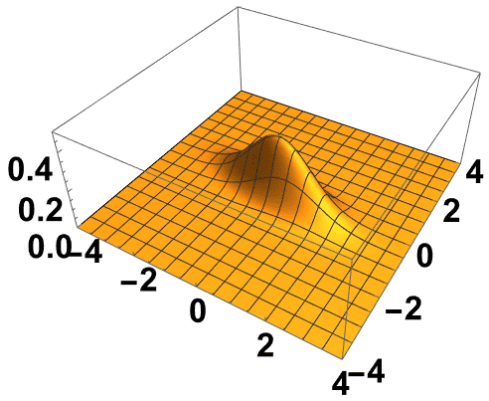


Figure 2: Cat state

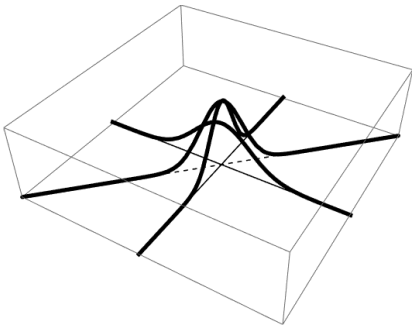


Figure 3: Cat state Marginals

C Appendix 3

Coherent states in the natural unit m = 1, $\omega = 1$, $\hbar = 1$

$$W_\alpha(x,p) = \frac{1}{\pi} e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2}, \qquad (17)$$

with the marginals in three axes:

$$\begin{cases} |\psi_\alpha(x)|^2 &= \frac{1}{\sqrt{\pi}} e^{-(x-\sqrt{2}\Re[\alpha])^2}, \\ |\psi_\alpha(p)|^2 &= \frac{1}{\sqrt{\pi}} e^{-(p-\sqrt{2}\Im[\alpha])^2}, \\ |\psi_\alpha(u)|^2 &= \frac{1}{\sqrt{\pi}} e^{-(u-\sqrt{2}\Re[\alpha e^{-i\pi/4}])^2} \end{cases} \qquad (18)$$

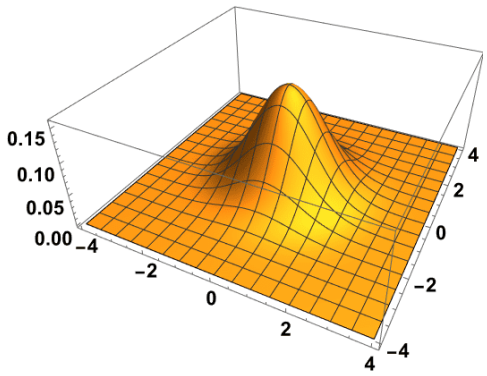


Figure 4: Coherent state

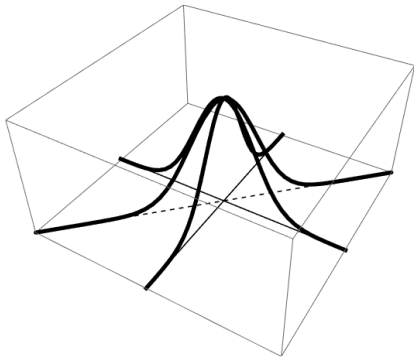


Figure 5: Coherent state marginals

D Appendix 4

Cat state is

$$\begin{aligned} W_{\alpha,\theta}(x,p) = {} & \frac{1}{\pi}\frac{1}{2+2\cos\theta e^{-2|\alpha|^2}} \\ & \times \Big[e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & \quad + e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \Big] \\ & + \frac{1}{\pi}\frac{1}{1+\cos\theta e^{-2|\alpha|^2}} e^{(-x^2-p^2)} \\ & \times \cos\Big(2x\sqrt{2}\Im[\alpha] - 2p\sqrt{2}\Re[\alpha] - \theta \Big) \end{aligned} \qquad (19)$$

with the marginals in three axes:

$$\begin{cases} |\psi_{\alpha,\theta}(x)|^2 & = \frac{1}{\sqrt{\pi}} \frac{1}{2+2\cos\theta e^{-2|\alpha|^2}} \\ & \times \Big[e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & + e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & + 2\cos\big(2x\sqrt{2}\Im[\alpha]-\theta\big) e^{-x^2-2\Re[\alpha]^2} \Big], \\ |\psi_{\alpha,\theta}(p)|^2 & = \frac{1}{\sqrt{\pi}} \frac{1}{2+2\cos\theta e^{-2|\alpha|^2}} \\ & \times \Big[e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & + e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & + 2\cos\big(2p\sqrt{2}\Re[\alpha]+\theta\big) e^{-p^2-2\Im[\alpha]^2} \Big], \\ |\psi_{\alpha,\theta}(u)|^2 & = \frac{1}{\sqrt{\pi}} \frac{1}{2+2\cos\theta e^{-2|\alpha|^2}} \\ & \times \Big[e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & + e^{-(x-\sqrt{2}\Re[\alpha])^2-(p-\sqrt{2}\Im[\alpha])^2} \\ & + 2\cos\big(2x\sqrt{2}\Im[\alpha e^{-i\pi/4}]-\theta\big) \\ & e^{-x^2-2\Re[\alpha e^{-i\pi/4}]^2} \Big], \end{cases} \tag{20}$$

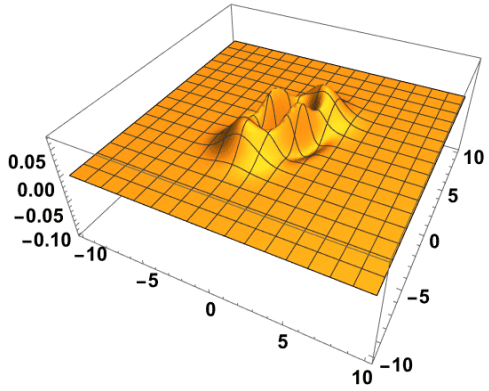


Figure 6: Cat state

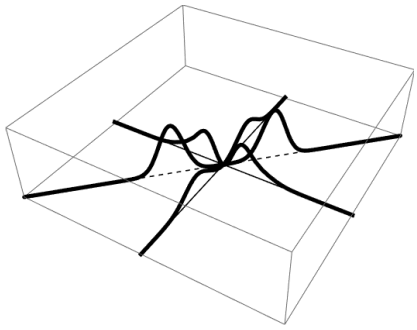


Figure 7: Cat state marginals

E Appendix 5

In our dataset, we have 16,000 coherent states, 18,000 cat states, and 20,000 squeezed states. The amplitude parameter α ranges from -1.5 to 1.5 for squeezed states and from -2 to 2 for both coherent and cat states. The squeezing parameter r ranges from 0.2 to 0.6 for squeezed states and 0.5 to 1 for coherent and cat states. The squeezing angle ϕ for squeezed states ranges from 0 to 2π. The phase θ for cat states also ranges from 0 to 2π. The average photon number $\bar{n}$ for coherent and cat states is set between 0 to 2, with photon number variance v following the formula $(1-|r|^2)\bar{n}$.

Experimental Device-independent Certification of GHZ States

Mariana M. E. Schmid[1] Michael Antesberger[1]
Huan Cao[1] * Wen-hao Zhang [2] Borivoje Dakič [1] Lee A. Rozema [1] Philip Walther [1 3]

[1] *University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), Austria.*
[2] *School of Physics and Optoelectronics Engineering, Anhui University, Hefei 230601, China.*
[3] *Christian Doppler Laboratory for Photonic Quantum Computer, University of Vienna, Austria.*

Abstract. Validation of specific states has often been a prerequisite before executing quantum tasks. The primitives of quantum state verification experiments, although offering rather efficient strategies, fall short in counteracting adversarial scenarios. Additionally, the sequence of generated states is consumed completely during the procedure. In our experimental demonstration, we address these obstacles by employing active switches and a novel procedure, defined as device-independent certification, by measuring segments of copies to justify the validity of the remaining one in black-box scenarios. With high-performance bipartite and tripartite entangled states, device-independent conclusions of high fidelity lower-bound can be made up to 99% confidence within a few hundred consumed copies.

Keywords: Quantum state certification, device independent, self-testing

Authentication of quantum resources is a crucial premise in various quantum application. There exist several approaches to characterize entanglement sources, among those the entanglement witness and quantum state tomography (QST) have been widely used. However, to make reliable evaluations, these two well-known methods require many detection events to extract the expectation value of observables. It is particularly demanding for users to characterize the quantum devices in a sample-efficient way, especially for large-scale quantum systems in the noisy intermedia-scale quantum (NISQ) era. This leads to the discovery of entanglement verification answering whether it contains genuine multipartite entanglement [1], and state verification technique that reveals more in-depth information about the specific state [2]. Furthermore, going beyond the device-dependent treatment, consideration of the black-box scenarios endows more reliability and broader applications for future quantum infrastructures. Nevertheless, reliable and efficient validation of specific quantum states remains a considerable challenge. To tackle this problem, we adopt the sample-efficient device-independent strategy that originates from the self-testing [3], and experimentally demonstrate the device-independent verification and certification of multiphoton GHZ state in few-copies regime.

The scheme of the protocol is illustrated in figure 1. A quantum source produces a sequence of independent state $S = \{\sigma_1, \sigma_2, ..., \sigma_N\}$ which is ϵ-close to the target state $|\Psi\rangle$ up to an error ϵ. We randomly distribute the generated copies between two agents. One of the agents is called 'Verifier', who is supposed to perform a state verification measurement. The other one is called 'User', who receives the remaining unmeasured copies being certified by the verifier. In this context, we only measure a fragment of produced copies and warrant the rest close to the desired state.

The DI quantum state certification protocol as developed by Gočanin et al. [3] suggests performing the non-

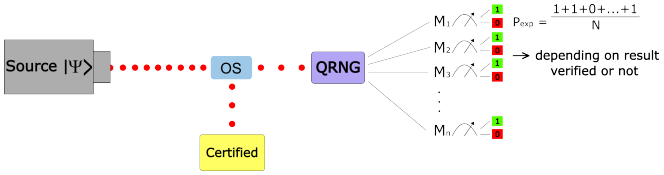


Figure 1: Scheme of the protocol. A segment of samples is sent to the verifier, where we play a nonlocal game and the copies are measured in one of ℓ settings (M_1, M_2, ..., M_ℓ) randomly chosen by a quantum random number generator (QRNG). Each outcome is either a success (1) or a failure (0). In the end, the final score P_{exp} is calculated by the sum of all outcomes divided by the number of the received copies.

local game stemmed from self-testing. In this black-box scenario, each copy of n-qubit state distributed to verifier side is queried by a global question, which termed nonlocal game is an uncharacterized measurement, depending on the classical input $\vec{i} = (i_1, i_2, \cdots, i_n)$. The possible outputs $\vec{o} = (o_1, o_2, \cdots, o_n)$ returned by the box are classified into correct output, of which the achieved score in the round is $p_j = 1$, and failed output $p_j = 0$ otherwise. A typical example of nonlocal game originates from Mermin inequality for self-testing tripartite GHZ state [4]

$$\sum_{o_1,o_2,o_3} (-1)^{o_1+o_2+o_3}[p(o_1,o_2,o_3|0,0,1) + p(o_1,o_2,o_3|0,1,0) + p(o_1,o_2,o_3|1,0,0) + p(o_1,o_2,o_3|1,1,1)] \leq 2 \quad (1)$$

$p(o_1, o_2, \cdots, o_n|i_1, i_2, \cdots, i_n) = \mathrm{Tr}\left[\bigotimes_{j=1}^{n} M_{o_j|i_j}\sigma\right]$ is the correlation regarding the physical state σ at disposal with associated local measurement $M_{o_j|i_j}$ through the Born rule. We can therefore translate the self-testing into the nonlocal game by classifying the possible outputs $\vec{o} = (o_1, o_2, \cdots, o_n)$ returned by the box into two

*huan.cao@univie.ac.at

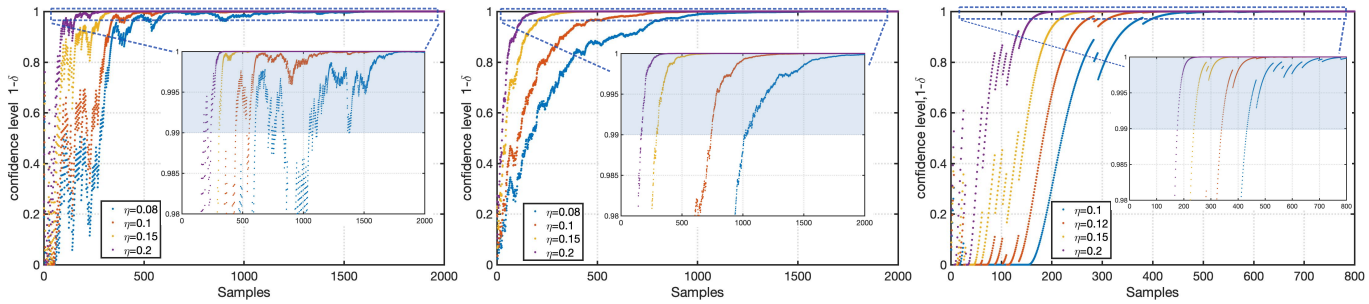


Figure 2: **Growth of confidence level with the number of consuming copies for bell state and GHZ state.** (a) results of bell state. (b) averaged results of bell state (c) results of GHZ state. The zoom-in around 99% confidence level is provided in the insets, with the zone above 99% marked by blue.

classes. One is the correct output, of which the achieved score in the round is $p_j = 1$, and failed output $p_j = 0$ otherwise. In each round, we ask one of the global questions, that corresponds to one of the input sets (0,0,1), (0,1,0), (1,0,0) or (1,1,1). We characterize the nonlocal games with the probability of success, which is defined as $P = \sum_{j=0}^{N} \frac{p_j}{N}$. Providing the averaged extractability lower bound $1-\eta$ of a sequence of independent state copies S, the maximal achievable averaged success probability is bounded by $\bar{p} = p_{QM} - c\eta$, where the p_{QM} dictates the success probability of the target state. The nonlocal game is said to pass once the experimentally observed success probability P_{exp} is higher than $\bar{p}$. The verifier can conclude that the averaged extractability (equivalent to fidelity up to local isometry) of the user's copies is at least $1-\eta$, with a confidence level $1-\delta$ of the conclusion

$$\delta \equiv \max p\left[P_{exp}|\bar{p} \leq p_{QM} - c\eta\right] \leq e^{-D(P_{exp}\|\bar{p})N} \qquad (2)$$

where $D(x \parallel y) = x\log(x/y) + (1-x)\log\left[(1-x)/(1-y)\right]$ denotes the Kullback-Leibler (KL) divergence.

We demonstrate the device-independent quantum state certification with a table-top photonic system for bipartite Bell and tripartite GHZ states. By setting a certain infidelity aimed to certify in advance, Fig. 2 illustrates the exponential growth of confidence level with the number of consumed samples for given infidelities. The failed event $p_j = 0$ would pull down the confidence level, but the effects become more and more negligible with increasing sampling number. To specify the efficiency of the strategy, we can identify the minimal sample number necessarily leading to the certification by more than 99% confidence level. From the inset, we identify that we can certify various fidelities within a few hundred consumed copies for both bipartite and tripartite cases.

There is a crucial distinction of certification tasks between the bipartite and tripartite quantum systems. The bipartite certification procedure is based on CHSH inequality, of which the algebraic maximal violation can only be reached by Popescu-Rohrlich box correlation. The optimal violation allowed by quantum mechanics corresponds to a success probability of $p_{QM}^{Bell} = (2+\sqrt{2})/4 \approx 0.85$. In contrast, in the case of the tripartite scenario, the quantum bound of the Mermin inequality is equivalent to the algebraic bound, leading to the optimal success probability $p_{QM}^{GHZ} = 1$. As discussed above, the discrepancy renders the different scaling of verifiable infidelity as the increasing samples. To demonstrate the scaling, we alternatively set the confidence level $1-\delta$ to be 99% and evaluate how the verified averaged infidelity evolves with the samples. In this stage, we perform the verification tasks for the verifier. Meanwhile, various characterizations on the user side are also taken to confirm the validity of the verifier's claim. Fig. 3 shows the estimated η (blue dots), predicted by the verifier, descends with the increasing sampling number. Since the certification procedure is translated from self-testing, the device-independent infidelity asymptotically approaches the given value by the self-testing result (yellow dashed lines). Additionally, we reveal the realistic fidelity of the user side by performing quantum state tomography for bipartite case, and witness for tripartite case, which are all well above the certified lower bound. The scalings of estimated fidelity are evaluated by running several repetitions in a specific range of samples and taking the averages, as shown in the insets of Fig. 3. A linear fitting is applied to the averaged infidelity plotted in logarithmic coordinates, which yields $\eta \propto N^{-0.5416}$ for bipartite case and $\eta \propto N^{-0.7913}$ for tripartite case. As a comparison, we also plot the scaling for the ideal target state (yellow plots in the inset). In the tripartite case, the deviation is mainly due to the imperfection in state preparation. To account for this reason, we select the specific range $N \in [10, 100]$ from the verifier's plot (the blue dots in inset of Fig. 3(b)), where all the samples pass the nonlocal game, and fit the result, which gives $\eta \propto N^{-0.9058}$ (red dots in inset), close enough to the scaling by ideal GHZ state $\eta \propto N^{-0.9349}$(yellow lines in inset). The scaling, in principle, is $\eta \propto N^{-0.5}$ for the bell state and $\eta \propto N^{-1}$ for GHZ state [3]. But it is present conditioned at (1) ideal state, and (2) asymptotic behavior of large samples, which prevents the practical experiment from exhibiting the same scaling.

References

[1] Saggio, V. et al. "Experimental few-copy multipartite entanglement detection", Nature Physics 15, 935–940 (2019).

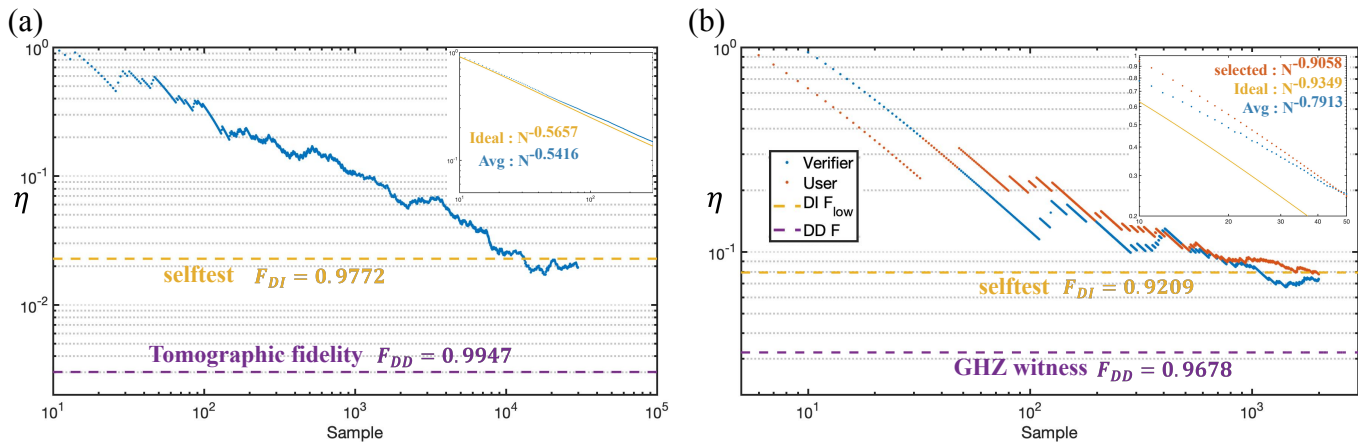


Figure 3: **Quantum state certification results when setting** $\delta = 0.01$**.** The estimated infidelities η asymptotically approach the predicted infidelity given by self-testing for (a) Bell state and (b) tripartite GHZ state. The jump is due to failed events of nonlocal games. Averaged results are taken to get smooth evolutions to estimate the scaling better. Avg: averaged results of scaling. Ideal: scaling given by ideal target state. selected: scaling calculated by the selected range. DI F_{low}: device-independent fidelity lower bound. DD F: device-dependent fidelity.

[2] Zhang, W. H. et al. "Experimental Optimal Verification of Entangled States Using Local Measurements", Phys. Rev. Lett. 125, 030506 (2020).

[3] Gočanin, A., Šupić, I. and Dakić, B. "Sample-Efficient Device-Independent Quantum State Verification and Certification", PRX Quantum 3, 010317 (2022).

[4] Kaniewski, J. "Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities", Phys. Rev. Lett. 117, 070402 (2016).

IFT-UAM/CSIC-24-59

Optimal Bell inequalities for qubit-qudit systems

Alexander Bernal , J. Alberto Casas and Jesús M. Moreno

Instituto de Física Teórica, IFT-UAM/CSIC,
Universidad Autónoma de Madrid, Cantoblanco, 28049 Madrid, Spain

Abstract

We evaluate the maximal Bell violation for a generic qubit-qudit system, obtaining easily computable expressions in arbitrary qudit dimension. This work generalizes the well-known Horodeckis's result for a qubit-qubit system. We also give simple lower and upper bounds on that violation and study the possibility of improving the amount of Bell-violation by embedding the qudit Hilbert space in one of larger dimension. The results are illustrated with a family of density matrices in the context of a qubit-qutrit system.

alexander.bernal@csic.es
j.alberto.casas@gmail.com

Contents

1 Introduction

Violation of Bell-like inequalities represents a crucial test of the character of the fundamental laws of nature, as it is incompatible with local-realism and in particular with local hidden-variables theories. The most popular variant of these inequalities is the CHSH version [1]. Given a two-qubit system, where Alice (Bob) can measure two observables, A, A' (B, B') which can take values $\{+1, -1\}$, the distribution of measurements are compatible with local realism if and only if $|\langle \mathcal{O}_{\rm Bell}\rangle| \leq 2$ with $\mathcal{O}_{\rm Bell} = AB + AB' + A'B - A'B'$. As it is well known, quantum mechanics can violate this CHSH inequality for certain entangled states. More precisely, if the state is pure there is always a choice of A, A', B, B' which violates CHSH [2]. If it is a mixture, that is not guaranteed [3].

Of course, given a quantum state, the amount of potential Bell violation depends on the choice of the four A, A', B, B' observables. It was shown in ref. [3] that for a generic qubit-qubit state, ρ, expressed as

$$\rho = \frac{1}{4}\left(\mathbb{1}_2 \otimes \mathbb{1}_2 + \sum_i (B_i^+ \sigma_i \otimes \mathbb{1}_2 + B_i^- \mathbb{1}_2 \otimes \sigma_i) + \sum_{ij} C_{ij} \sigma_i \otimes \sigma_j\right) \tag{1}$$

(with $B_i^{\pm}, C_{ij}$ real coefficients), the maximum value of $|\langle \mathcal{O}_{\rm Bell}\rangle|$ is given by

$$\max_{A,A',B,B'} |\langle \mathcal{O}_{\rm Bell}\rangle| = \max_{A,A',B,B'} \left|\langle AB\rangle + \langle AB'\rangle + \langle A'B\rangle - \langle A'B'\rangle\right| = 2\sqrt{\kappa_1 + \kappa_2}\ , \tag{2}$$

where κ_1, κ_2 are the largest eigenvalues of $C^T C$. The authors provided also the explicit choice of A, A', B, B' leading to this maximum value. In this way one can easily check whether a (qubit-qubit) state generates probability distributions incompatible with local realism.

Beyond the qubit-qubit case things get much more involved. As a matter of fact, there is not even a general description of the region (polytope) of probability distribution of A, A', B, B' which is compatible with local realism. The celebrated CGLMP inequalities [4] represent some facets of such polytope, but in general they do not provide a complete description of it. On the other hand, for qubit-qudit states it was shown by Pironio [5] that all the facets defining the "classical" polytope are given by CHSH-type inequalities. Nevertheless, this does not solve the problem of determining the maximum Bell violation for a given ρ, and thus whether the probabilities of physical observables of the system can be described by a classical (local-realistic) theory. In particular, Eq.(2) cannot be extrapolated to higher dimension. Then, in principle one should explore all possibilities for the A, A', B, B' observables, a very expensive computational task, as it involves a large number of parameters, which grows rapidly as the dimension of the qudit increases. On the other hand, $\mathcal{H}_2 \otimes \mathcal{H}_d$ states are of high physical interest. E.g. in the context of high-energy physics, it would be interesting to show that systems like top $-$ W boson, produced at the LHC, can exhibit the same Bell non-locality as systems of two spin-1/2 particles (like top pairs). In other context, qubit-qudit systems also play an important role in quantum information processing [6–9].

In this paper we address the task of evaluating the maximal Bell violation for a generic qubit-qudit system, obtaining easily computable expressions. This also allows us to examine other issues, for example the possibility of enhancing the Bell violation by embedding the qudit Hilbert space in one of larger dimension.

In section 2 we present our approach to the problem and the general result for maximal Bell-violation in qubit-qudit systems. In section 3 we give simple lower and upper bounds on $\langle \mathcal{O}_{\text{Bell}} \rangle_{\max}$, which respectively represent sufficient and necessary conditions for violation of local realism. In section 4 we examine the possibility of improving the amount of Bell-violation by embedding Bob's Hilbert space in one of larger dimension and thus choosing new (higher dimensional) observables. In section 5 we illustrate our results by studying a family of density matrices in a qubit-qutrit system. Finally, in section 6 we summarize our results and conclusions.

2 The general qubit-qudit case

Let us consider a qubit-qudit system, with Hilbert space $\mathcal{H}_2 \otimes \mathcal{H}_d$. Any $2d \times 2d$ density matrix in this space can be unambiguously expressed as

$$\rho = \frac{1}{2} \left[\mathbb{1}_2 \otimes \beta_0 + \sigma_1 \otimes \beta_1 + \sigma_2 \otimes \beta_2 + \sigma_3 \otimes \beta_3 \right], \tag{3}$$

where σ_i are the standard Pauli matrices and $\{\beta_0, \beta_i\}$ are $d \times d$ Hermitian matrices. In particular, the β_0 matrix coincides with Bob's reduced density matrix, $\rho_B = \text{Tr}_A\, \rho = \beta_0$, and therefore verifies $\text{Tr}\, \beta_0 = 1$.[1] Besides, the $\beta-$matrices must lead to a positive semidefinite ρ matrix; other than that they are arbitrary. The previous expression is a kind of Schmidt decomposition of the $\mathcal{H}_2 \otimes \mathcal{H}_d$ density matrix.

Following the result obtained by Pironio [5], we know that all the facets defining the polytope of Local Hidden Variables (LHV) are given by CHSH-type inequalities over the probability distributions of the system. In other words, all the "tight" Bell-like inequalities (those whose violation is a sufficient

[1] The rest of the β matrices are easily obtained by $\beta_i = \text{Tr}_A \left(\rho \left(\sigma_i \otimes \mathbb{1}_d \right) \right)$.

and necessary condition to violate local realism), involving two observables for both Alice and Bob, can be written as CHSH-type inequalities, $|\langle O_{\rm Bell}\rangle| \leq 2$, with

$$\mathcal{O}_{\rm Bell} = A \otimes (B + B') + A' \otimes (B - B') \ . \tag{4}$$

Here A and A' (B and B') are 2×2 ($d \times d$) linear Hermitian observables with eigenvalues $\{+1, -1\}$ ($\{+1, -1\}$ with some degeneracy). Its expectation value is given by

$$\langle \mathcal{O}_{\rm Bell}\rangle = {\rm Tr}\,(\rho \mathcal{O}_{\rm Bell}) = \frac{1}{2}\sum_{i=1}^{3} \left\{ {\rm Tr}(\sigma_i A)\ {\rm Tr}\left(\beta_i (B + B')\right) \ + \ {\rm Tr}\big(\sigma_i A'\big)\ {\rm Tr}\left(\beta_i (B - B')\right)\right\} . \tag{5}$$

As it is well known, for local realistic theories $\langle \mathcal{O}_{\rm Bell}\rangle \leq 2$, while in quantum theories it can reach $2\sqrt{2}$. Our goal is to find its maximal value:

$$\langle \mathcal{O}_{\rm Bell}\rangle_{\rm max} = \max_{A,A',B,B'} \langle \mathcal{O}_{\rm Bell}\rangle \ . \tag{6}$$

For the qubit-qubit case, the cross-terms $\sigma_i \otimes \beta_i$ in (3) can be expressed as $\frac{1}{2} C_{ij} \sigma_i \otimes \sigma_j$, where C_{ij} is a real matrix. Then, it was shown in [3] that the maximum value of $\langle \mathcal{O}_{\rm Bell}\rangle$ is given by $2\sqrt{\kappa_1 + \kappa_2}$, where κ_1, κ_2 are the largest eigenvalues of the $C^T C$ matrix. Such nice result cannot be extrapolated to the qubit-qudit case for various reasons. First, for $d > 2$ the $d \times d$ $\beta-$matrices do not obey the friendy algebra of the Pauli matrices, which makes the analysis far more involved. Second, the freedom for the choice of the B, B' observables is dramatically greater, as they live in the space of $d \times d$ Hermitian matrices. Finally, for $d > 2$ there is an increasing number of CHSH inequalities to be examined, corresponding to the distribution of $+1$s and -1s of the B and B' eigenvalues.

For this analysis it is convenient to define $\vec{r}_A$, $\vec{r}_{A'}$ and $\vec{r}_B$, $\vec{r}_{B'}$ vectors as

$$\begin{aligned} \vec{r}_A &= ({\rm Tr}(\sigma_1 A), {\rm Tr}(\sigma_2 A), {\rm Tr}(\sigma_3 A)) \, , \\ \vec{r}_B &= ({\rm Tr}(\beta_1 B), {\rm Tr}(\beta_2 B), {\rm Tr}(\beta_3 B)) \end{aligned} \tag{7}$$

and similar expressions for $\vec{r}_{A'}$ and $\vec{r}_{B'}$. Note that these are real vectors from the Hermiticity of the involved matrices. Then Eq.(5) reads

$$\langle \mathcal{O}_{\rm Bell}\rangle = \frac{1}{2}\vec{r}_A(\vec{r}_B + \vec{r}_{B'}) + \frac{1}{2}\vec{r}_{A'}(\vec{r}_B - \vec{r}_{B'}) \ . \tag{8}$$

Incidentally, this expression is explicitly invariant under simultaneous rotations in the 3-spaces of the σ_i, β_i matrices, which is in turn a consequence of the invariance of ρ, Eq.(3), under that operation. Now notice that $\frac{1}{2}\vec{r}_A$, $\frac{1}{2}\vec{r}_{A'}$ are unit vectors. This comes from A, A' having eigenvalues $\{+1, -1\}$ and thus vanishing trace[2], so they can be expressed as

$$A = \sum \frac{1}{2}\,{\rm Tr}(\sigma_i A)\sigma_i = \frac{1}{2}\vec{r}_A \vec{\sigma} \tag{9}$$

and similarly for A'. Now, since ${\rm Tr}\, A^2 = {\rm Tr}\, A'^2 = {\rm Tr}\, \mathbb{1}_2 = 2$, we get $\|\vec{r}_A\|^2 = \|\vec{r}_{A'}\|^2 = 4$. Apart from that, the $\vec{r}_A, \vec{r}_{A'}$ vectors are arbitrary since, for any choice of them, the corresponding A, A'

[2]We do not consider the case of A or A' proportional to the identity, which leads to no Bell-violation [10].

observables are given by (9). Therefore, for a given pair (B, B'), the optimal choice of (A, A') is $\vec{r}_A \parallel (\vec{r}_B + \vec{r}_{B'})$ and $\vec{r}_{A'} \parallel (\vec{r}_B - \vec{r}_{B'})$, so that

$$\langle \mathcal{O}_{\rm Bell} \rangle_{\max} = \max_{B,B'} \Big\{ \|\vec{r}_B + \vec{r}_{B'}\| + \|\vec{r}_B - \vec{r}_{B'}\| \Big\}. \tag{10}$$

As expected, this expression is also invariant under 3-rotations. Unfortunately, the $\beta-$matrices do not follow the Pauli algebra, so a similar argument cannot be done for the $\vec{r}_B, \vec{r}_{B'}$ vectors, in particular they do not have a fixed normalization. As already mentioned, this is part of the extra intricacy of the qubit-qudit case compared to the qubit-qubit one. In order to solve (10) it is useful the following lemma:

- Lemma I

  Let $\vec{v}, \vec{w}$ be two arbitrary vectors in a plane. Consider a simultaneous rotation of angle φ of both vectors and call the new vectors $\vec{v}(\varphi), \vec{w}(\varphi)$, so that $\vec{v} = \vec{v}(0)$, $\vec{w} = \vec{w}(0)$. Then the following identity takes place:

  $$\Big(\|\vec{v} + \vec{w}\| + \|\vec{v} - \vec{w}\| \Big)^2 = 4 \max_{\varphi} \Big\{ v_1(\varphi)^2 + w_2(\varphi)^2 \Big\}, \tag{11}$$

  where the subscripts 1, 2 denote the components of the vectors. This equation can be easily checked by choosing an initial reference frame for which the longest vector, say $\vec{v}$, has $v_2 = 0$. Then the expression within curl brackets reads $v_1^2 \cos^2\varphi + (w_1 \sin\varphi + w_2 \cos\varphi)^2$, which is maximal at

  $$\varphi = \frac{1}{2} \arctan \frac{2 w_1 w_2}{v_1^2 + w_2^2 - w_1^2} \tag{12}$$

  and the value at the maximum coincides with the l.h.s. of (11). Clearly, the lemma holds when we allow for rotations in 3-space, $\vec{v}, \vec{w} \to \mathcal{R}\vec{v}, \mathcal{R}\vec{w}$, *i.e.*

  $$\Big(\|\vec{v} + \vec{w}\| + \|\vec{v} - \vec{w}\| \Big)^2 = 4 \max_{\mathcal{R}} \Big\{ (\mathcal{R}\vec{v})_1^2 + (\mathcal{R}\vec{w})_2^2 \Big\} \tag{13}$$

  where $\mathcal{R}$ is an arbitrary rotation in 3D, characterized by the three Euler angles. This becomes obvious by taking into account that the r.h.s. of this equation reaches its maximum when the two vectors have vanishing third component, $(\mathcal{R}\vec{v})_3 = (\mathcal{R}\vec{w})_3 = 0$, so that the problem reduces to the above rotation in the plane.

Applying the previous lemma, Eq.(13), to the Bell expectation value, Eq.(10) we get

$$\langle \mathcal{O}_{\rm Bell} \rangle_{\max} = 2 \max_{B,B',\mathcal{R}} \sqrt{ |(\mathcal{R}\vec{r}_B)_1|^2 + |(\mathcal{R}\vec{r}_{B'})_2|^2 } \, . \tag{14}$$

From the definition of $\vec{r}_B$, Eq.(7), $(\mathcal{R}\vec{r}_B)_i = {\rm Tr}\Big[(\mathcal{R}\vec{\beta})_i \cdot B \Big]$, and an analogous expression for $(\mathcal{R}\vec{r}_{B'})_i$. Hence

$$\langle \mathcal{O}_{\rm Bell} \rangle_{\max} = 2 \max_{B,B',\mathcal{R}} \sqrt{ \Big| {\rm Tr}\Big[(\mathcal{R}\vec{\beta})_1 \cdot B \Big] \Big|^2 + \Big| {\rm Tr}\Big[(\mathcal{R}\vec{\beta})_2 \cdot B' \Big] \Big|^2 } \, . \tag{15}$$

Now we take into account the following: for a generic Hermitian matrix, M, with eigenvalues λ_i, and an arbitrary Hermitian, involutory matrix B (i.e. $B^2 = \mathbb{1}_d$), it happens that $\max_B {\rm Tr}[M \cdot B] =$

$\sum_i |\lambda_i|$. [3] This maximum is achieved when B is aligned with M, i.e. they are diagonalized by the same unitary matrix, and the signs of the B eigenvalues (1 or -1) are chosen equal to the signs of the corresponding λ_i. This is precisely our case, since B, B' are Hermitian involutory matrices, but other than that arbitrary. Here we allow B, B' to be $\pm \mathbb{1}_d$, which is the optimal choice when all λ_i have the same sign (we comment below on the meaning of this case). Consequently, the maximum value of $\langle \mathcal{O}_{\text{Bell}} \rangle$ is given by

$$\boxed{\begin{aligned} \langle \mathcal{O}_{\text{Bell}} \rangle_{\max} &= 2 \max_{\mathcal{R}} \sqrt{\|(\mathcal{R}\vec{\beta})_1\|_1^2 + \|(\mathcal{R}\vec{\beta})_2\|_1^2} \\ &= \max_{\mathcal{R}} \left[\left(\sum_{i=1}^{d} |\lambda_i^{(1)}(\mathcal{R})| \right)^2 + \left(\sum_{i=1}^{d} |\lambda_i^{(2)}(\mathcal{R})| \right)^2 \right]^{1/2} \end{aligned}} \tag{16}$$

where $\lambda_i^{(1,2)}(\mathcal{R})$ stand for the eigenvalues of the $SO(3)$-rotated β matrices, $(\mathcal{R}\vec{\beta})_1, (\mathcal{R}\vec{\beta})_2$. This is the main result of our paper. Let us briefly comment on some aspects of it.

- Note that in principle one should consider all the possibilities for the distribution of 1s and -1s of B and B' eigenvalues. Each possibility corresponds to a different CHSH inequality, which represents $\sim d^2$ CHSH inequalities. However the above result automatically selects the optimal choice for the $1s$ and $-1s$ of the B, B' observables; in other words, the CHSH inequality which gives the maximal violation of the given density matrix.

- When all the $\lambda_i^{(1)}(\mathcal{R})$ and/or $\lambda_i^{(2)}(\mathcal{R})$ at the maximum of Eq.(16) have the same sign, this entails setting either $B = \pm \mathbb{1}_d$ and/or $B' = \pm \mathbb{1}_d$, which is known to give no violation for CHSH-type inequalities [10].

- To see the computational advantage of the above expression, note the following. In this procedure, given a ρ matrix, once it is expressed in the form (3), we have to perform a (usually numerical) maximization of Eq.(16). This implies to scan the three Euler angles of the $\mathcal{R}$ rotation, which is a very cheap computation. It should be compared with the $4 + 2d(d-1)$ parameters for each CHSH inequality in the initial expression (6). Even in the simplest qubit-qutrit case this represents 16 parameters.

- The A, A', B, B' observables that realize the maximum Bell-violation are straightforward to obtain. Once we have determined the matrices $(\mathcal{R}\vec{\beta})_1$, $(\mathcal{R}\vec{\beta})_2$ that maximize (16) we simply set

$$B = U_1 D_1 U_1^\dagger, \quad B' = U_2 D_2 U_2^\dagger, \tag{17}$$

  where $U_{1,2}$ are the diagonalizing unitary matrices, i.e. $U_a (\mathcal{R}\vec{\beta})_a U_a^\dagger = \text{diag}\,(\lambda_i^{(a)})$, and $D_a = \text{diag}(\text{sign}\,[\lambda_i^{(a)}])$. The corresponding A, A' observables are given by Eq.(9), with $\vec{r_A}$, $\vec{r_{A'}}$ the unit vectors aligned along $(\vec{r}_B + \vec{r}_{B'})$, $(\vec{r}_B - \vec{r}_{B'})$ (see discussion after Eq.(9)), and

$$\vec{r}_B = \left(\text{Tr}\left[(\mathcal{R}\vec{\beta})_1 B \right], \text{Tr}\left[(\mathcal{R}\vec{\beta})_2 B \right], \text{Tr}\left[(\mathcal{R}\vec{\beta})_3 B \right] \right) \tag{18}$$

[3] This is called the trace-norm or 1-norm of a matrix, $\|M\|_1 = \text{Tr}\sqrt{M^\dagger M} = \sum_i |\lambda_i|$, in analogy to the 1-norm of vectors.

and similarly for B'.

- Let us finally see that expression (16) is consistent with the qubit-qubit result (2) obtained in ref. [3].

  In such scenario, comparing expressions (1) and (3) for ρ, the β matrices read $\beta_0 = \frac{1}{2}(\mathbb{1}_2 + \sum_i B_i^- \sigma_i)$ and $\beta_i = \frac{1}{2}(B_i^+ \mathbb{1}_2 + \sum_j C_{ij}\sigma_j)$. On the other hand, assuming that the state violates a CHSH inequality, the corresponding observables A, A', B, B' must have eigenvalues $\{+1, -1\}$. (The other inequivalent possibility, namely one or more observables proportional to the identity, leads to no CHSH-violation [10].) In that case, the terms involving $B_i^{\pm}$ are irrelevant as they cancel in $\mathrm{Tr}\{\rho \mathcal{O}_{\mathrm{Bell}}\}$, Eq. (5). Now, the (real) matrix C can be diagonalized by two orthogonal transformations, $\mathcal{R}_A, \mathcal{R}_B \in O(3)$:

$$C = \mathcal{R}_A \Sigma \mathcal{R}_B^T, \quad \Sigma = \mathrm{diag}\{\mu_1, \mu_2, \mu_3\}, \tag{19}$$

  ordered as $\mu_1 \geq \mu_2 \geq \mu_3 \geq 0$. This is equivalent to perform appropriate changes of basis in the Alice and Bob Hilbert spaces. Hence, in this new basis

$$\rho = \frac{1}{2}\left(\mathbb{1}_2 \otimes \mathbb{1}_2 + \sum_i \sigma_i \otimes \beta_i \ + \ \cdots \right) , \tag{20}$$

  where the dots denote terms which are irrelevant for the previous reasons, and $\beta_i = \frac{1}{2}\mu_i \sigma_i$ up to a sign[4]. Now, from Eq.(16) we have to maximize $\|(\mathcal{R}\vec{\beta})_1\|_1^2 + \|(\mathcal{R}\vec{\beta})_2\|_1^2$ where $\mathcal{R}$ is an arbitrary $SO(3)$ rotation. Using the fact that the eigenvalues of $\vec{v}\cdot\vec{\sigma}$ are $\pm\|\vec{v}\|$ we get

$$\|(\mathcal{R}\vec{\beta})_i\|_1^2 = \sum_j \mu_j^2 |\mathcal{R}_{ij}|^2 , \tag{21}$$

  so the maximum value of $\|(\mathcal{R}\vec{\beta})_1\|_1^2 + \|(\mathcal{R}\vec{\beta})_2\|_1^2$ occurs for $\mathcal{R}_{13} = \mathcal{R}_{23} = 0$. Then

$$\max_{\mathcal{R}} \{\|(\mathcal{R}\vec{\beta})_1\|_1^2 + \|(\mathcal{R}\vec{\beta})_2\|_1^2\} = \sum_{i=1,2} \sum_j \mu_j^2 |\mathcal{R}_{ij}|^2 = \mu_1^2 + \mu_2^2 \tag{22}$$

  (independent of $\mathcal{R}_{ij}$). Plugging this result in (16) we recover Eq.(2).

3 Necessary and sufficient conditions for Bell violation

From the general expression for the maximal Bell violation, Eq.(16), we can easily extract simple lower and upper bounds on $\langle \mathcal{O}_{\mathrm{Bell}} \rangle_{\max}$, which respectively represent sufficient and necessary conditions for violation of local realism.

The lower bound comes from simply taking $\mathcal{R} = \mathbb{1}_3$. In other words, once the density matrix has been expressed as in Eq.(3), we can assure that

$$\langle \mathcal{O}_{\mathrm{Bell}} \rangle_{\max} \ \geq \ 2\sqrt{\|\beta_1\|_1^2 + \|\beta_2\|_1^2} \ = \ 2\left[\left(\sum_{i=1}^d |\lambda_i^{(1)}| \right)^2 + \left(\sum_{i=1}^d |\lambda_i^{(2)}| \right)^2 \right]^{1/2} , \tag{23}$$

[4]The presence of a negative sign depends on whether or not $\mathcal{R}_A, \mathcal{R}_B \in SO(3)$. Nevertheless, this sign is irrelevant for the rest of the reasoning.

where in this case $\lambda_i^{(1,2)}$ stand for the eigenvalues of the initial β_1, β_2 matrices (no rotation applied). More precisely, β_1, β_2 correspond to the beta matrices with larger trace-norm.

In order to get an upper bound on $\langle \mathcal{O}_{\rm Bell}\rangle_{\rm max}$ from Eq.(16), we use the inequality $\|\cdot\|_1^2 \leq d\,\|\cdot\|_2^2$ involving the 1 and 2-norm over $d\times d$ matrices [5], so that

$$\sum_{a=1}^{2}\|(\mathcal{R}\vec{\beta})_a\|_1^2 \leq \sum_{a=1}^{3}\|(\mathcal{R}\vec{\beta})_a\|_1^2 \leq d\sum_{a=1}^{3}\|(\mathcal{R}\vec{\beta})_a\|_2^2 = d\sum_{a=1}^{3}\|\beta_a\|_2^2. \tag{24}$$

The equality comes from the fact that the last expression is invariant under $O(3)$ rotations, so we can take the initial β-matrices to evaluate the upper bound. Hence,

$$\langle \mathcal{O}_{\rm Bell}\rangle_{\rm max} \leq 2\sqrt{d}\left[\sum_{a=1}^{3}\left(\sum_{i=1}^{d}|\lambda_i^{(a)}|^2\right)\right]^{1/2}. \tag{25}$$

In summary,

$$2\left[\sum_{a=1}^{2}\left(\sum_{i=1}^{d}|\lambda_i^{(a)}|\right)^2\right]^{1/2} \leq \langle \mathcal{O}_{\rm Bell}\rangle_{\rm max} \leq 2\sqrt{d}\left[\sum_{a=1}^{3}\left(\sum_{i=1}^{d}|\lambda_i^{(a)}|^2\right)\right]^{1/2} \tag{26}$$

where, in all the equations of this section, (23)-(26), $\lambda_i^{(a)}$ stand for the eigenvalues of the unrotated β_a matrices in Eq.(3).

4 Embeddings

Having a recipe for the optimal Bell-violation for $2\times d$ systems allows us to address the following question: if we embed Bob's Hilbert space in one of larger dimension, is it possible to improve the amount of Bell-violation by a suitable choice of the new (higher dimensional) $\tilde{B}, \tilde{B}'$ observables? One may even think of the possibility of starting with an (entangled) state which does not violate Bell inequalities, but it does it in the extended Hilbert space. As we are about to see, the answer is negative for both questions.

Let us start with a generic state in a $\mathcal{H}_2\otimes\mathcal{H}_{d_1}$ Hilbert space, characterized by a density matrix

$$\rho = \frac{1}{2}\left[\mathbb{1}_2\otimes\beta_0 + \sigma_1\otimes\beta_1 + \sigma_2\otimes\beta_2 + \sigma_3\otimes\beta_3\right], \tag{27}$$

where $\{\beta_0, \beta_i\}$ are $d_1\times d_1$ matrices. Now let us consider Bob's Hilbert space as part of a higher dimensional one, $\mathcal{H}_{d_1}\subset\mathcal{H}_{d_2}$ with $d_2 > d_1$. Thus we embed the above state in the new Hilbert space by considering the $\{\beta_0, \beta_i\}$ matrices as the upper-left block of a block diagonal $d_2\times d_2$ matrix:

$$\beta_0 \to \tilde{\beta}_0 = \begin{pmatrix} \beta_0 & \mathbb{0}_{d_1\times(d_2-d_1)} \\ \mathbb{0}_{(d_2-d_1)\times d_1} & \mathbb{0}_{(d_2-d_1)\times(d_2-d_1)} \end{pmatrix}, \quad \beta_i \to \tilde{\beta}_i = \begin{pmatrix} \beta_i & \mathbb{0}_{d_1\times(d_2-d_1)} \\ \mathbb{0}_{(d_2-d_1)\times d_1} & \mathbb{0}_{(d_2-d_1)\times(d_2-d_1)} \end{pmatrix}, \tag{28}$$

where the $\mathbb{0}$ matrices have all entries vanishing. In terms of the higher-dimension observables and $\beta-$matrices, Eq.(15) reads:

$$\langle \mathcal{O}_{\rm Bell}\rangle_{\rm max} = 2\max_{\tilde{B},\tilde{B}',\mathcal{R}}\sqrt{\left|{\rm Tr}\left[(\mathcal{R}\vec{\tilde{\beta}})_1\cdot\tilde{B}\right]\right|^2 + \left|{\rm Tr}\left[(\mathcal{R}\vec{\tilde{\beta}})_2\cdot\tilde{B}'\right]\right|^2}. \tag{29}$$

[5] The 2-norm of a squared matrix is defined by $\|M\|_2^2 = {\rm Tr}\left(MM^\dagger\right) = \sum_i|\lambda_i|^2$, in analogy to the 2-norm of vectors.

Note that the $\mathcal{R}\vec{\tilde{\beta}}$ matrices are block-diagonal, with the same texture of zeroes as matrices (28). Hence, they have the same d_1 eigenvalues as $\mathcal{R}\vec{\beta}$ plus $d_2 - d_1$ zeroes. Therefore, for a given rotation $\mathcal{R}$, the *optimal* choice for $\tilde{B}, \tilde{B}'$ in Eq.(29) yields the same result as the optimal choice in the $\mathcal{H}_2 \otimes \mathcal{H}_{d_1}$ system, namely

$$\mathrm{Tr}\left[(\mathcal{R}\vec{\tilde{\beta}})_1 \cdot \tilde{B}\right] = \sum_{i=1}^{d_1} |\lambda_i^{(1)}(\mathcal{R})| \ , \quad \mathrm{Tr}\left[(\mathcal{R}\vec{\tilde{\beta}})_2 \cdot \tilde{B}'\right] = \sum_{i=1}^{d_1} |\lambda_i^{(2)}(\mathcal{R})| \ , \tag{30}$$

where $\lambda_i^{(1,2)}(\mathcal{R})$ stand for the eigenvalues of the $(\mathcal{R}\vec{\beta})_1, (\mathcal{R}\vec{\beta})_2$ matrices. Hence we recover the same result as for the initial system, Eq.(16). Note that in this case there are many choices of $\tilde{B}, \tilde{B}'$ which yield the same result (30).

5 A qubit-qutrit case study

To illustrate the use of the general result on the maximal Bell-violation (16) let us consider an example in the context of the qubit-qutrit system. As it is well known, for mixed states entanglement does not necessarily leads to violation of quantum realism (i.e. Bell-violation). A popular example of this fact in the qubit-qubit case are the Werner states, $\rho = \frac{1}{4}(\mathbb{1}_2 \otimes \mathbb{1}_2 - \eta \sum_i \sigma_i \otimes \sigma_i)$, which for $1/3 < \eta \leq 1/\sqrt{2}$ are entangled but do not violate any CHSH inequality. For a qubit-qutrit system we can perform a similar analysis, using both our result (16) and the fact that in this case the Peres-Horodecki [11, 12] criterion, i.e. the existence of some negative eigenvalue of the partially transposed matrix ρ^{T_2}, provides a necessary and sufficient condition for entanglement. For the sake of concreteness, let us consider the qubit-qutrit state

$$\rho = x|\psi_1\rangle\langle\psi_1| + y|\psi_2\rangle\langle\psi_2| + z|\psi_3\rangle\langle\psi_3|, \tag{31}$$

where $0 \leq (x, y, z) \leq 1$ with $x + y + z = 1$, and (in an obvious notation)

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |12\rangle\right), \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|02\rangle + |10\rangle\right). \tag{32}$$

Explicitly,

$$\rho = \frac{1}{2}\begin{pmatrix} x & 0 & 0 & 0 & x & 0 \\ 0 & y & 0 & 0 & 0 & y \\ 0 & 0 & 1-x-y & 1-x-y & 0 & 0 \\ 0 & 0 & 1-x-y & 1-x-y & 0 & 0 \\ x & 0 & 0 & 0 & x & 0 \\ 0 & y & 0 & 0 & 0 & y \end{pmatrix}. \tag{33}$$

The physical region, where ρ is positive definite, corresponds to $x + y \leq 1$ (triangle in Fig.1). Using the Peres-Horodecki criterion, it is easy to check that ρ is entangled for any value of x, y, except for $x = y = 1/3$. Fig.1, left panel, shows the value of the logarithmic negativity $E = \log_2\left(\|\rho^{T_2}\|_1\right)$ in the $x - y$ plane. The logarithmic negativity, which provides a sound measurement of entanglement [13], is greater than 0 in the whole physical region except at that particular point.

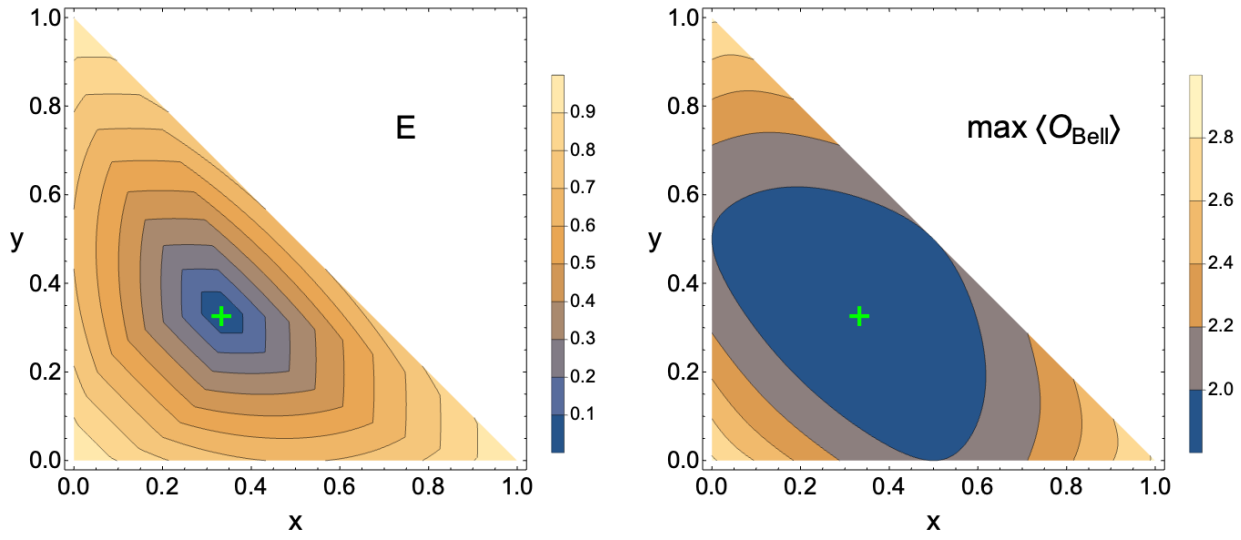


Figure 1: Values of the logarithmic negativity. $E = \log_2\left(\|\rho^{T_2}\|_1\right)$ (left panel) and $|\langle \mathcal{O}_{\text{Bell}}\rangle_{\max}|$ (right panel) for the qubit-qutrit model described by the density matrix of Eq.(33). The model is entangled ($E > 0$) in the whole physical region, except for $x = y = 1/3$, while it violates local realism for $|\langle \mathcal{O}_{\text{Bell}}\rangle_{\max}| > 2$.

For the analysis of the Bell-violation, we first express ρ in the form (3), which amounts to the following $\beta-$matrices:

$$\beta_0 = \frac{1}{2}\begin{pmatrix} 1-y & 0 & 0 \\ 0 & x+y & 0 \\ 0 & 0 & 1-x \end{pmatrix}, \; \beta_1 = \frac{1}{2}\begin{pmatrix} 0 & x & -x-y+1 \\ x & 0 & y \\ -x-y+1 & y & 0 \end{pmatrix},$$

$$\beta_2 = \frac{1}{2}\begin{pmatrix} 0 & ix & i(x+y-1) \\ -ix & 0 & iy \\ -i(x+y-1) & -iy & 0 \end{pmatrix}, \; \beta_3 = \frac{1}{2}\begin{pmatrix} 2x+y-1 & 0 & 0 \\ 0 & y-x & 0 \\ 0 & 0 & -x-2y+1 \end{pmatrix}. \tag{34}$$

Plugging these expressions in Eq.(16) and performing a simple numerical optimization we can obtain the maximal Bell-violation in the $x-y$ plane, which is shown in Fig.1, right panel. Similarly to the Werner qubit-qubit states, there is a sizeable region in which the state is entangled but $|\langle O_{\text{Bell}}\rangle| \leq 2$, so local realism is not violated.

6 Summary and conclusions

We have considered the violation of Bell-like inequalities in the context of a qubit-qudit system with arbitrary dimension. These inequalities represent a crucial test of local realism, i.e the possibility that the outputs of physical measurements on the system could be reproduced by a (classical) theory of hidden variables. The violation of such inequalities requires that the state is entangled, but (for mixed states) the opposite is not necessarily true. In previous literature [5] it was shown that for these systems, the "classical" polytope, i.e. the region of probability distribution of observables A, A', B, B'

which is compatible with local realism, is bounded by CHSH-type [1] inequalities. However, given a state ρ, this does not solve the problem of determining the maximum Bell violation and thus whether the system can be described by a classical (local-realistic) theory. The usual recipes for a qubit-qubit system [3] cannot be applied beyond the lowest dimensionality. Hence, in principle one should explore all possibilities for the A, A', B, B' observables involved in a CHSH inequality, an expensive computational task, which entails to optimize $\sim 2d^2$ parameters and thus increases quickly with the dimension of the qudit.

In this paper we have addressed the task of evaluating the maximal Bell violation for a generic qubit-qudit system, obtaining easily computable expressions. Our central result, given in Eq.(16), generically amounts to a simple optimization in three angles, independently of the qudit dimension, and it automatically selects the strongest CHSH inequality among all the possible ones. Moreover, this result also holds when considering a larger number of observables acting on the qudit space, since for that scenario the "classical" polytope is still bounded by CHSH-type inequalities [5]. We also give lower and upper bounds on the Bell-violation, which can be immediately computed. Besides, we have shown that it is not possible to improve the amount of Bell-violation by embedding Bob's Hilbert space in one of larger dimension and thus choosing new (higher dimensional) observables. Finally, as an example of the use of our results we have considered a 2-parameter family of density matrices in the context of a qubit-qutrit system and determined the region of such parameter space in which the state is entangled and the region where local realism is violated, showing that both are correlated but the former is broader than the latter.

The results presented here can be used for any qubit-qudit system, independently of its physical nature; e.g. in the analysis of non-local correlations in top-W [14,15] or photon-Z production [16,17] at the LHC, or even (in the large-d limit) hybrid discrete-continuous systems such as a cavity atom-light system [18].

Acknowledgements

We are grateful to J.A. Aguilar-Saavedra for useful discussions. The authors acknowledge the support of the Spanish Agencia Estatal de Investigacion through the grants "IFT Centro de Excelencia Severo Ochoa CEX2020-001007-S", PID2019-110058GB-C22 and PID2022-142545NB-C22 funded by MCIN/AEI/10.13039/501100011033 and by ERDF. The work of A.B. is supported through the FPI grant PRE2020-095867 funded by MCIN/AEI/10.13039/501100011033.

References

[1] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, *Proposed experiment to test local hidden variable theories*, *Phys. Rev. Lett.* **23** (1969) 880–884.

[2] N. Gisin, *Bell's inequality holds for all non-product states*, *Physics Letters A* **154** (1991) 201–202.

[3] R. Horodecki, P. Horodecki and M. Horodecki, *Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition*, *Physics Letters A* **200** (1995) 340–344.

[4] D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu, *Bell Inequalities for Arbitrarily High-Dimensional Systems*, *Phys. Rev. Lett.* **88** (2002) 040404.

[5] S. Pironio, *All Clauser–Horne–Shimony–Holt polytopes*, *Journal of Physics A: Mathematical and Theoretical* **47** (2014) 424020.

[6] P. Horodecki, M. Lewenstein, G. Vidal and I. Cirac, *Operational criterion and constructive checks for the separability of low-rank density matrices*, *Phys. Rev. A* **62** (2000) 032310.

[7] B. Kraus, J. I. Cirac, S. Karnas and M. Lewenstein, *Separability in* $2 \times n$ *composite quantum systems*, *Phys. Rev. A* **61** (2000) 062302.

[8] B. Bylicka and D. Chruściński, *Witnessing quantum discord in* $2 \times n$ *systems*, *Phys. Rev. A* **81** (2010) 062102.

[9] T. Chatterjee, A. Das, S. K. Bala, A. Saha, A. Chattopadhyay and A. Chakrabarti, *Qudiet: A classical simulation platform for qubit-qudit hybrid quantum systems*, *IET Quantum Communication* **4** (2023) 167–180.

[10] L. J. Landau, *On the violation of Bell's inequality in quantum theory*, *Physics Letters A* **120** (1987) 54–56.

[11] A. Peres, *Separability criterion for density matrices*, *Phys. Rev. Lett.* **77** (1996) 1413–1415.

[12] M. Horodecki, P. Horodecki and R. Horodecki, *On the necessary and sufficient conditions for separability of mixed quantum states*, *Phys. Lett. A* **223** (1996) 1, [quant-ph/9605038].

[13] G. Vidal and R. F. Werner, *Computable measure of entanglement*, *Phys. Rev. A* **65** (2002) 032314, [quant-ph/0102117].

[14] J. A. Aguilar-Saavedra, *Postdecay quantum entanglement in top pair production*, *Phys. Rev. D* **108** (2023) 076025, [2307.06991].

[15] A. Subba and R. Rahaman, *On bipartite and tripartite entanglement at present and future particle colliders*, 2404.03292.

[16] R. A. Morales, *Exploring Bell inequalities and quantum entanglement in vector boson scattering*, *Eur. Phys. J. Plus* **138** (2023) 1157, [2306.17247].

[17] R. A. Morales, *Tripartite entanglement and Bell non-locality in loop-induced Higgs boson decays*, 2403.18023.

[18] P. Halder, R. Banerjee, S. Roy and A. S. De, *Hybrid nonlocality via atom photon interactions with and without impurities*, 2302.11513.

Photonic quantum-to-quantum Bernoulli factory

Francesco Hoch[1] *

[1] *Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro 5, I-00185 Roma, Italy*

Abstract. Many applications in information technology depend on the creation and manipulation of randomness, and quantum mechanics has proven useful in this area. One promising model for randomness manipulation is the Bernoulli factory. Initially, this framework was explored in a classical context. However, recent extensions into the quantum realm have demonstrated new interesting features.

We propose two Bernoulli factory schemes that use quantum states as both input and output, one employing the dual-rail and the other the polarization encoding. Our schemes are modular, universal and operate independently of the input bias We present the theoretical analysis and the experimental implementations, showcasing the practicality of our method.

Keywords: Bernoulli factory, Randomness manipulation, Quantum computation, Quantum information, Quoin

1 Introduction

Randomness plays a crucial role in various research fields and everyday applications, particularly those related to sensitive data protection. Several deterministic techniques can generate randomness, with their security and efficiency depending on the specific algorithms used. Quantum mechanics offers intrinsic randomness, theoretically unbreakable but challenging to ensure experimentally due to inevitable noise and imperfect device control. This unique property of quantum theory provides significant advantages in information manipulation, communication, and processing, as demonstrated by several quantum communication protocols and quantum computational algorithms. A recent proposal called Quantrum-to-quantum Bernoulli factory aims at using quantum resources to manipulate randomness in Bernoulli processes.

In a classical contest, a Bernoulli factory is an algorithm that processes instances of a Bernoulli variable (flips of a biased coin), with the goal of generating an output Bernoulli variable whose bias is a desired function of the (unknown) input bias. More formally a Bernoulli factory is a function $G_f : \{0,1\}^\infty \to \{0,1\}$, associated with a function $f : \mathcal{D} \subseteq [0,1] \to [0,1]$, such that its application to a sample following a Bernoulli distribution $\mathcal{B}(p)$ with bias p is equivalent to sampling exactly from a different Bernoulli distribution with bias parameter $f(p)$. In formula $G_f(\mathcal{B}(p)^\infty) = \mathcal{B}(f(p))$. An essential requirement is that the function G_f must not depend on p, which reflects the assumption of the user's ignorance about the value of the input bias. In Ref. [1] they provide a necessary and sufficient condition on the function $f : \mathcal{D} \subseteq [0,1] \to [0,1]$ such that the associated Bernoulli factory exists. In particular, they show that not all functions are exactly implementable as a Bernoulli factory. As became clear later this type of the protocol is called classical-to-classical Bernoulli factory (CCBF).

In recent years the problem has been extended to the quantum domain by analyzing the possibility of replacing the input and/or the output Bernoulli variables with quantum counterparts. In Ref. [2, 3], the first quantum version of this process, named Quantum-To-Classical Bernoulli Factory (QCBF), was defined by considering a quantum input and a classical output. This QCBF extension simulates a Bernoulli variable given a quantum coin (or quoin) as an input parameter. A quoin with bias p is a qubit in the pure state $|C_p\rangle \coloneqq \sqrt{1-p}\,|0\rangle + \sqrt{p}\,|1\rangle$, such that when measured in the computational basis, returns a classical Bernoulli variable with the same bias. In Ref. [2] the authors characterized the space of simulable functions for a QCBF showing that it is strictly large compared to the sef of the CCBF. Moreover, there is experimental evidence that a quantum advantage can be achieved [4, 5] in terms of the average number of inputs coins/quoins required.

A more complex quantum extension of the Bernoulli factory was later proposed by Jiang et al. [6], where both input and output are quantum states, aptly named a Quantum-to-Quantum Bernoulli Factory (QQBF). In detail, a QQBF takes as input a set of quoins, all with the same bias parameter p, and returns a quoin with parameter $f(p) : \mathcal{D} \subseteq [0,1] \to [0,1]$. More in general we define the following parameterization of single-qubit states that proved to be helpful in the analysis of Bernoulli factories:

$$|\mathbf{z}\rangle \coloneqq \frac{z\,|0\rangle + |1\rangle}{\sqrt{1+|z|^2}}, \tag{1}$$

where z is a complex variable. For a general input qubit $|\mathbf{z}\rangle$ a QQBF associated to a complex function $g(z) : \mathbb{C} \to \mathbb{C}$ is a process that generates at the output a qubit in the state $|\mathbf{g}(\mathbf{z})\rangle$. In Ref. [6] it was demonstrated that a necessary and sufficient condition for a QQBF to exist is that the associated function belongs to the complex field generated by the element z, i.e. that $g(z)$ is a complex rational function in the parameter z. Using the previous result and the algebraic theory of the field, the necessary and sufficient condition to demonstrate the feasibility of implementing all the complex rational functions, i.e. all the simulable QQBF, relies on showing the possibility of implementing the quantum version of the field operations which are inversion, addition and product, and the possibility to combine them. The quantum input and output

*francesco.hoch@uniroma1.it

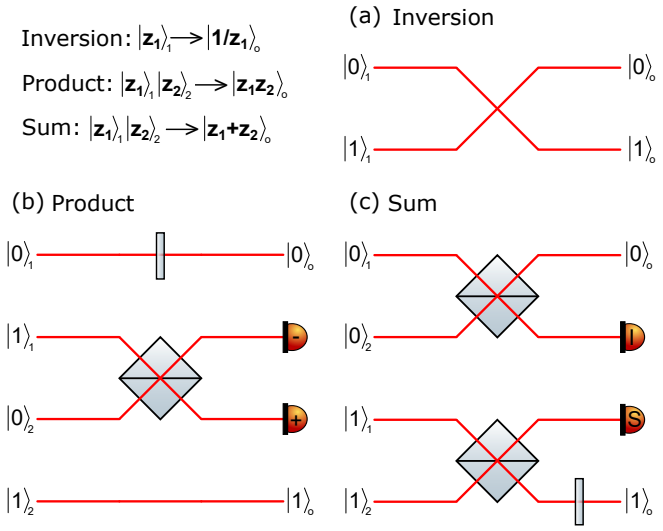


Figure 1: **Building blocks for dual-rail encoding.** Interferometric schemes that implement the basic operations to build a generic QQBF with dual-rail encoded qubits. The inputs of the interferometers are labelled by numbers 1 and 2 while the outputs are labelled as O. (a) The inversion operation is performed by swapping the two modes of the input dual-rail qubit. (b) The product operation is performed by sending one waveguide from each dual rail qubit ($|1\rangle_1$ and $|0\rangle_2$) into a balanced BS, and measuring the outgoing modes. Detection of a single photon in the modes labelled "+" or "−" signals success (up to a global phase). (c) The addition operation is implemented by directing the modes, representing the same state of the two qubits, to equally unbalanced BSs, and measuring one output mode for each BS. When one photon is found in the detector labelled as S, and the other photon is in output modes $|0\rangle_o$ or $|1\rangle_o$, the output state is the sum of the input ones (up to a global phase).

enable its use as a subroutine in quantum algorithms. For example, QQBF-like operations have been used for delegated quantum computing in Ref. [7] to obtain genuine secure quantum state preparation.

2 Our work

In this work, we propose a modular approach to implement a genuine QQBF and we report its experimental realization using integrated quantum photonics with dual-rail encoding or bulk optics with polarization encoding.

To demonstrate the feasibility of a generic QQBF using integrated photonics, we will explicitly construct an appropriate scheme to implement the field operations with photons. Previous attempts to experimentally implement the field operations [8, 9] were limited, as they substantially relied on prior knowledge of the input state. This is in stark contrast to the fundamental requirement for a correct implementation of the protocol, i.e. full ignorance of the input state. In our we present three interferometers, each of them implementing a particular field operation that can be concatenated at will.

In Fig. 1 we present the schemes that employ the dual-rail encoding for photonic qubits, where logical states $|0\rangle$ and $|1\rangle$ are encoded as the presence of a photon in one of two possible optical paths. This choice is motivated by the current state-of-the-art integrated photonic technologies, that allows the implementation of complex architectures [10] based on beam splitters (BS) and phase shifters.

We also implement similar interferometers for the polarization encoding.

3 experimental results

A first step towards characterizing the modular QQBF described above involves the demonstration of the individual building blocks. The operation of every single block is characterized by preparing a set of random input states $(|\mathbf{z_1}\rangle, |\mathbf{z_2}\rangle)$ sampled from a uniform distribution on the Bloch sphere. After the transformation, the output is validated by measuring the success probability of the post-selection used, and the fidelity reached with respect to the target state. The overall figure of merit defining the quality of the implementation is provided by the mean fidelity over the set of sampled states. From a direct comparison of the obtained results with the theoretical expectations, we find that the operations implemented by the circuit are performed with fidelities close to a unitary value (0.99 ± 0.01), thus demonstrating the realization of the building blocks of a QQBF. In this case, corresponding to the verification of each standalone operation, the effect of experimental noise due to photon distinguishability is almost negligible. Indeed, the inversion operation scheme does not rely on photon interference, while both product and addition implementations are verified via two-photon experiments, which, in our source, belong to the same generated pair, and thus possess a high degree of indistinguishability.

As a second step, we demonstrate the modularity of our scheme by showing the possibility of concatenating the individual operations. This aspect is necessary to fulfil all requirements for the correct implementation of a complete Bernoulli factory. Also in this case we measure the output fidelity for a particular set of states corresponding to relevant choices of the input. To compare the experimental data with the theoretical prediction, partial photon distinguishability between the input photons has to be taken into account. All the fidelities experimentally measured are compatible with the theoretical one reconstructed by the noisy model that takes into account the partial distinguishability of the photons. These demonstrate the successful implementation of the concatenation and that the relevant noise in our apparatus is only the photon distinguishability.

We performed the same experiment with a quantum dot source and a bulk optics system to test the protocol implemented for polarization encoding. We apply the same validation method as described previously with mean fidelities of $F = 0.95 \pm 0.01$. The obtained results are compatible with the ones retrieved by the noisy model that take into account the partial distinguishability since,

on the contrary to the SPDC sources that have near unitary indistinguishability, our dot source has a visibility of $V = 0.92 \pm 0.02$.

References

[1] M. S. Keane and George L. O'Brien. A bernoulli factory. *ACM Trans. Model. Comput. Simul.*, 4(2):213–219, April 1994.

[2] Howard Dale, David Jennings, and Terry Rudolph. Provable quantum advantage in randomness processing. *Nature Communications*, 6(1), September 2015.

[3] Howard Dale. Quantum coins and quantum sampling, 2016.

[4] Xiao Yuan, Ke Liu, Yuan Xu, Weiting Wang, Yuwei Ma, Fang Zhang, Zhaopeng Yan, R. Vijay, Luyan Sun, and Xiongfeng Ma. Experimental quantum randomness processing using superconducting qubits. *Physical Review Letters*, 117(1), June 2016.

[5] Raj B. Patel, Terry Rudolph, and Geoff J. Pryde. An experimental quantum bernoulli factory. *Science Advances*, 5(1):eaau6668, January 2019.

[6] Jiaqing Jiang, Jialin Zhang, and Xiaoming Sun. Quantum-to-quantum bernoulli factory problem. *Physical Review A*, 97(3), March 2018.

[7] Elham Kashefi and Anna Pappa. Multiparty delegated quantum computing. *Cryptography*, 1(2):12, July 2017.

[8] Yong Liu, Jiaqing Jiang, Pingyu Zhu, Dongyang Wang, Jiangfang Ding, Xiaogang Qiang, Anqi Huang, Ping Xu, Jialin Zhang, Guojing Tian, Xiang Fu, Mingtang Deng, Chunqing Wu, Xiaoming Sun, Xuejun Yang, and Junjie Wu. General quantum bernoulli factory: framework analysis and experiments. *Quantum Science and Technology*, 6(4):045025, sep 2021.

[9] Xiang Zhan, Kunkun Wang, Lei Xiao, Zhihao Bian, and Peng Xue. Experimental demonstration of quantum-to-quantum bernoulli factory. *Physical Review A*, 102:012605, Jul 2020.

[10] Jianwei Wang, Fabio Sciarrino, Anthony Laing, and Mark G. Thompson. Integrated photonic quantum technologies. *Nature Photonics*, 14(5):273–284, May 2020.

Multiplexed Quantum Communication with Surface and Hypergraph Product Codes

Shin Nishio[1 2 3 *] Nicholas Connolly[2 †] Nicolò Lo Piparo[2] William John Munro[2 3]
Thomas Rowan Scruby[2] Kae Nemoto[2 3 ‡]

[1] *SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan*
[2] *Okinawa Institute of Science and Technology Graduate University, Onna-son, Kunigami-gun, Okinawa, Japan*
[3] *National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan*

Abstract. Connecting multiple processors via photonic interconnects could help to overcome issues of scalability in single-processor quantum computers. Transmission via these interconnects can be performed more efficiently using quantum multiplexing, where information is encoded in high-dimensional photonic degrees of freedom. We study the effects of multiplexing on logical error rates in surface codes and hypergraph product codes. We show that, although multiplexing makes loss errors more damaging, assigning qubits to photons in an intelligent manner can minimize these effects, and the ability to encode higher-distance codes in a smaller number of photons can result in overall lower logical error rates.

Keywords: Quantum Communication, Quantum Error Correction, Surface Codes, HGP Codes, Quantum Multiplexing, Quantum Interconnect

Topological stabilizer codes such as surface codes [3] are regarded as one of the most promising candidates for fault-tolerant quantum computation (FTQC) and quantum communication [7]. This is due in part to the fact that they have a high error threshold and local stabilizer generators which are feasible in 2D systems. Hypergraph product (HGP) codes [21], a generalization of the surface code, are another class of quantum codes considered practical candidates for FTQC. Constructed from two classical codes, HGP codes are particularly interesting because they have asymptotically finite rate and minimum distance proportional to the square root of the classical code lengths. This is in contrast to the surface code, which has a fixed number of logical code words and hence rate approaching zero.

Although the size of quantum processors has increased in recent years, it has become clear that large-scale quantum computation on a single processor is limited by various physical constraints [9, 19]. To solve this problem, a method of connecting multiple quantum processors with photonic quantum interconnects has been proposed [2]. In such a system, the processors would use matter qubits while the qubits in the interconnects would be photonic, resulting in different dominant error mechanisms in the two cases. To address this, hybrid systems using multiple codes have been proposed, but this introduces new overheads such as code-switching [1]. Alternatively, it is possible to address different types of noise within a single code by using different decoders [18].

A single photon has multiple degrees of freedom such as polarization [22], time bin [4, 10, 20], path (e.g. dual rail) [8], orbital angular momentum[23], and frequency [17, 16]. Quantum multiplexing [14] is a method of encoding high-dimensional quantum information into a single photon using these multiple degrees of freedom. It has been shown that multiplexing can be used to reduce the resource cost associated with quantum communication [12, 13] and quantum circuits [11]. In this work we consider encoding 2^m-dimensional quantum information using m two-level degrees of freedom per photon (where m is an integer and $m = 1$ corresponds to no multiplexing, i.e. a single degree of freedom is used). This work analyzes the performance of quantum communication on an erasure channel using surface and HGP codes with quantum multiplexing. Fig. 1 shows a sequence of steps illustrating the quantum multiplexing technique applied to the surface code.

While quantum multiplexing allows for efficient communication it may also affect the logical error rate. The loss of a photon causes the simultaneous loss of multiple qubits encoded in that photon. Surface codes are highly tolerant of uniformly random errors but such classical correlations can degrade performance.

We propose three methods utilizing multiplexing for quantum communication:

1. Sending m different codewords with the same number of photons as the $m = 1$ case.
2. Sending $\sqrt{m} \times \sqrt{m}$ larger codewords with the same number of photons as the $m = 1$ case.
3. Sending the same number of codewords as the $m = 1$ case with fewer photons ($1/m$ times the original).

The first method introduces a classical correlation of errors between m independent codes, but this does not affect the performance of those codes. The second method introduces correlations in errors between the qubits in the code, which may degrade the performance. However, if m is sufficiently small relative to the code size, the benefit gained by increasing the code size is more significant. Fig. 2 (a) shows a Monte Carlo simulation of the logical error rate for the second method using a surface code. The second and third methods have no restriction on the number of codewords and can improve the

*parton@nii.ac.jp
†nicholas.connolly@oist.jp
‡kae.nemoto@oist.jp

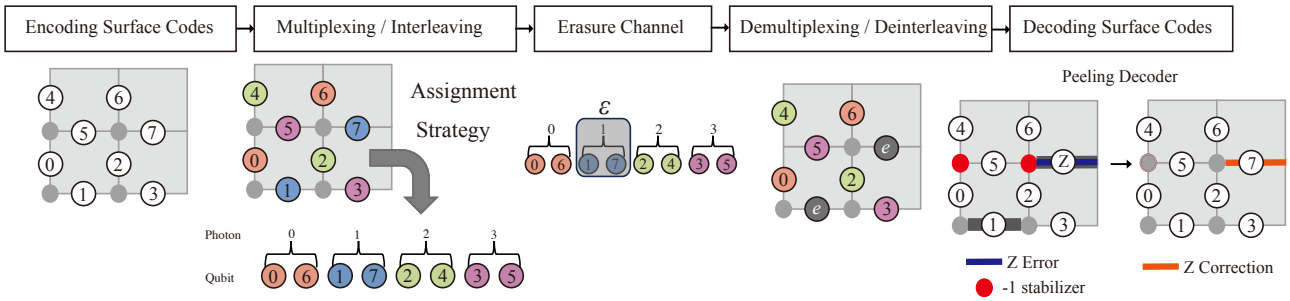


Figure 1: Flow of surface code communication using multiplexed photons over the erasure channel. Each numbered circle represents the physical qubit of data, and the color of the qubit indicates its assigned photon.

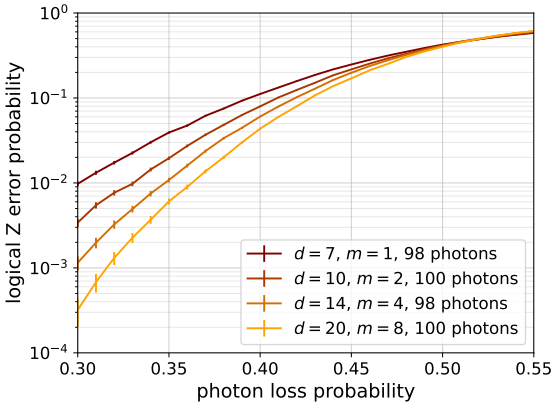
efficiency of quantum communication in general. However, since these methods introduce classical correlation to the errors of multiple qubits in a single code word, it is necessary to be aware of the resulting performance degradation. Fig. 2 (b) shows how increasing m can also increase this degradation.

Assignment Strategies

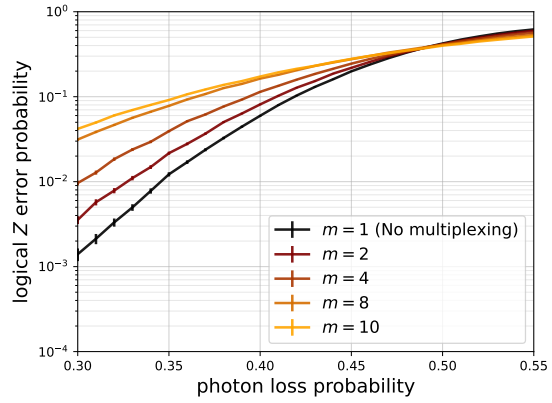
To address the correlations in the error and reduce their effect on performance, we introduce and compare a number of assignment strategies. We propose five assignment strategies for surface codes and five strategies for HGP codes, which are adapted to the code structure and the decoder. A full explanation of these assignment strategies is included in the Appendix, but we briefly discuss the most promising techniques here.

For the surface code, the distance between qubits within the same photon is a crucial factor when considering the impact of correlated errors, motivating us to compare strategies that minimize and maximize this distance. Furthermore, these strategies can be realized with simple calculations on the surface code lattice. Fig. 3 shows an example of these two strategies in a small $d = 2$ surface code, and Fig. 4 shows the simulated performance of these and other strategies applied using a $d = 10$ surface code. Observe that max-distance outperforms min-distance, which is explained by the fact that Pauli errors on nearby qubits quickly grow into clusters when there are multiple erasures.

Errors with strong classical correlation are similar to burst errors in classical communication in the sense that the errors have spatial locality. Interleaving [15] is a technique used to eliminate locality by permuting the rows and columns of the code's generator matrix. The random and random + threshold assignment strategies are inspired by this technique. While the former method assigns uniform-randomly selected qubits to photons, the latter modifies this method with the addition of a variable threshold distance to avoid assigning nearby qubits to the same photon. The random + threshold strategy is designed both to leverage randomness and to increase the distance between qubits in the same photon. The numerical results of Fig. 4 show that this strategy comes the closest to the no-multiplexing case and thus has the

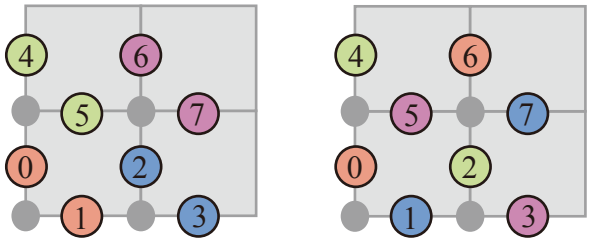


(a) method 2 with surface codes of different size



(b) method 3 with fixed $d = 10$ surface code

Figure 2: (a) Erasure channel performance of the second method (sending a larger codeword with the same number of photons as the no-multiplexing case) using surface codes of different sizes and about 100 photons each. (b) Erasure channel performance of the third method (sending codewords with the same size as the no-multiplexing case using fewer photons) for the $d = 10$ surface code at different values of m (the number of qubits per photon), where qubits are assigned to photons at random.



(a) min-distance (b) max-distance

Figure 3: Examples of photon assignment strategies for the qubits in a $d = 2$ toric code. Numbered circles indicate qubits and colors indicate the assigned photon.

smallest effect on performance.

Our numerical simulations for surface codes used an efficient linear-time maximum-likelihood (ML) decoder [6], but our simulations for HGP codes used an efficient non-ML erasure decoder designed specifically for HGP codes [5]. One drawback of this decoder is that it can fail to return to the code space, and hence decoder failures may occur in addition to logical errors. Decoder failures are the result of certain local configurations of erased qubits referred to as stopping sets. Multiplexing can have a significant effect on the probability of obtaining a stopping set and hence a decoder failure.

We propose another five multiplexing assignment strategies adapted to HGP codes. The first strategy is based on random assignment, identical to the surface code strategy of the same name. The second strategy exploits the fact that HGP codes are a type of stabilizer code; our decoder can often correct erased qubits covering a stabilizer. The stabilizer strategy assigns qubits to photons so that photons cover stabilizers. The last three assignment strategies (sudoku, row-col, and diagonal) are all designed to address decoder failures. Sudoku and diagonal strategies attempt to avoid stopping sets and hence reduce the likelihood of a decoder failure. By contrast, the row-col strategy seeks to maximize the probability of stopping sets and decoder failures; this strategy is of theoretical interest as a worst-case scenario. An example showing how the performance collapses for the row-col strategy is shown in Fig. 5 (a).

Fig. 5 (b) shows a comparison of the performance for all five HGP strategies. In this example, we see that the diagonal strategy outperforms all others, including the baseline no-multiplexing case. An examination of the numerical results shows that, in addition to reducing the number of decoder failures, the diagonal strategy also reduced the number of logical errors in the simulations for this code. Although this result is not always true for other HGP codes, it shows that decoder-designed multiplexing has the possibility to improve performance while reducing the required physical resources.

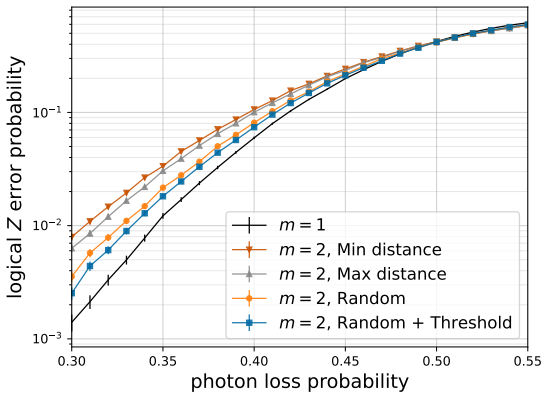
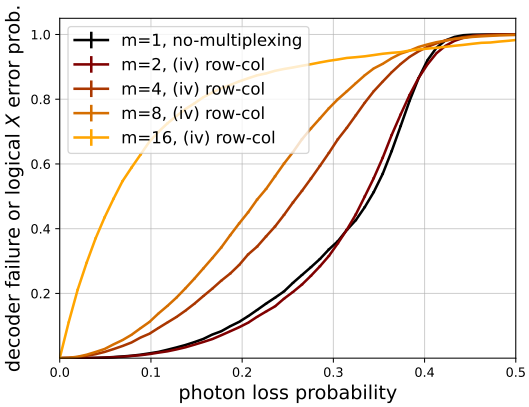
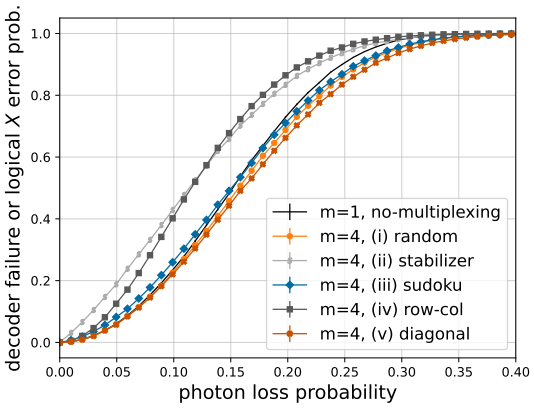


Figure 4: Performance comparison of multiplexing strategies for the ⟦200,2,10⟧ surface code.



(a) ⟦512,8⟧ HGP code



(b) ⟦320,82⟧ HGP code

Figure 5: (a) Examination of the worst-case scenario performance collapse when using multiplexing with the row-col strategy. (b) Comparison of all five HGP multiplexing strategies at fixed $m = 4$. In this example, the diagonal strategy is seen to outperform all other strategies, including the no-multiplexing case.

References

[1] J. T. Anderson, G. Duclos-Cianci, and D. Poulin. Fault-tolerant conversion between the steane and reed-muller quantum codes. *Physical review letters*, 113(8):080501, 2014.

[2] D. Awschalom, K. K. Berggren, H. Bernien, S. Bhave, L. D. Carr, P. Davids, S. E. Economou, D. Englund, A. Faraon, M. Fejer, et al. Development of quantum interconnects (quics) for next-generation information technologies. *PRX Quantum*, 2(1):017002, 2021.

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

[4] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594, 1999.

[5] N. Connolly, V. Londe, A. Leverrier, and N. Delfosse. Fast erasure decoder for a class of quantum ldpc codes. *arXiv preprint arXiv:2208.01002*, 2022.

[6] N. Delfosse and G. Zémor. Linear-time maximum likelihood decoding of surface codes over the quantum erasure channel. *Physical Review Research*, 2(3):033042, 2020.

[7] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. Hollenberg. Surface code quantum communication. *Physical review letters*, 104(18):180503, 2010.

[8] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of modern physics*, 79(1):135, 2007.

[9] S. Krinner, S. Storz, P. Kurpiers, P. Magnard, J. Heinsoo, R. Keller, J. Luetolf, C. Eichler, and A. Wallraff. Engineering cryogenic setups for 100-qubit scale superconducting circuit systems. *EPJ Quantum Technology*, 6(1):2, 2019.

[10] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin. Femtosecond time-bin entangled qubits for quantum communication. *arXiv preprint quant-ph/0205144*, 2002.

[11] S. Nishio, N. L. Piparo, M. Hanks, W. J. Munro, and K. Nemoto. Resource reduction in multiplexed high-dimensional quantum reed-solomon codes. *Physical Review A*, 107(3):032620, 2023.

[12] N. L. Piparo, M. Hanks, C. Gravel, K. Nemoto, and W. J. Munro. Resource reduction for distributed quantum information processing using quantum multiplexed photons. *Physical Review Letters*, 124(21):210503, 2020.

[13] N. L. Piparo, M. Hanks, K. Nemoto, and W. J. Munro. Aggregating quantum networks. *Physical Review A*, 102(5):052613, 2020.

[14] N. L. Piparo, W. J. Munro, and K. Nemoto. Quantum multiplexing. *Physical Review A*, 99(2):022337, 2019.

[15] J. Proakis and M. Salehi. Digital communications, vol. 1221, 1987.

[16] S. Ramelow, L. Ratschbacher, A. Fedrizzi, N. Langford, and A. Zeilinger. Discrete tunable color entanglement. *Physical review letters*, 103(25):253601, 2009.

[17] Y. Shih and A. Sergienko. Observation of quantum beating in a simple beam-splitting experiment: Two-particle entanglement in spin and space-time. *Physical Review A*, 50(3):2564, 1994.

[18] Y. Suzuki, T. Sugiyama, T. Arai, W. Liao, K. Inoue, and T. Tanimoto. Q3de: A fault-tolerant quantum computer architecture for multi-bit burst errors by cosmic rays. In *2022 55th IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pages 1110–1125. IEEE, 2022.

[19] S. Tamate, Y. Tabuchi, and Y. Nakamura. Toward realization of scalable packaging and wiring for large-scale superconducting quantum computers. *IEICE Transactions on Electronics*, 105(6):290–295, 2022.

[20] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Physical Review A*, 66(6):062304, 2002.

[21] J.-P. Tillich and G. Zémor. Quantum ldpc codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2013.

[22] A. B. U'Ren, K. Banaszek, and I. A. Walmsley. Photon engineering for quantum information processing. *arXiv preprint quant-ph/0305192*, 2003.

[23] A. M. Yao and M. J. Padgett. Orbital angular momentum: origins, behavior and applications. *Advances in optics and photonics*, 3(2):161–204, 2011.

Appendix: Multiplexed Quantum Communication with Surface and Hypergraph Product Code

I. INTRODUCTION

Quantum computation has an advantage in computational complexity over classical computation [1, 2]; however, the speed of the basic operations that make up computation is not as fast as that of classical computers. Therefore, it is necessary to realize a large-scale quantum computing system to take advantage of the complexity. Modern quantum devices cannot ignore the effects of various noises in quantum systems, making obtaining meaningful computational results in large-scale computation difficult. To address this issue, various quantum error-correcting codes (QECCs) [3, 4] and fault-tolerant quantum computation (FTQC) [5, 6] utilizing these codes have been proposed, and small-scale experimental implementations are already in progress [7–9]. Topological stabilizer codes such as surface codes [10] are regarded as one of the most promising candidates for FTQC, not only because they have a high error threshold but also because they are regarded as relatively easy to implement on a two-dimensional quantum processor because stabilizers are locally defined.

While the number of qubits in quantum processors has been increasing in recent years, it has become clear that there are various difficulties in achieving large-scale quantum computation only by scaling a single processor for FTQC due to various physical constraints [11, 12]. To address this problem, a method of connecting multiple quantum processors with a quantum interconnect or quantum internet has been proposed [13]. It provides a way to apply a remote gate between processors or send/receive qubits from other processors. Also, one can use quantum memory attached to quantum processors, which can store quantum information even if the processor does not have a large enough number of qubits to manipulate all the qubits in the information processor. Optical systems are regarded as one of the best candidates for quantum interconnects [14] and also as quantum memories [15] due to long coherence time [16].

In a quantum computation system with quantum interconnects, the quantum processor and the quantum interconnect may use different physical systems. In such cases, two systems may have different types of error sources. To cope with this, hybrid systems using multiple codes have been proposed, but they introduce new overheads [17–19]. On the other hand, several different types of noise can also be addressed by a single code [20, 21]. In this work, we consider the use of surface codes and HGP codes in quantum communications, which are also suitable for quantum computation.

However, quantum interconnects and quantum memory will introduce bottlenecks for quantum computation. Operations for inter-processors tend to be slower than the ones inside a single processor. Therefore, it is necessary to ease the bottlenecks by reducing the amount of resources required for interconnects, which is primarily the number of photons.

Quantum multiplexing [22] has been proposed recently. It can be used to reduce the resource costs, such as the number of gates, qubits, and photons associated with quantum communication [23, 24] using quantum Reed-Solomon codes [25], which have good performance for loss error channels. Furthermore, a more generalized method of reducing the number of gates for implementing multi-qubit gates using quantum multiplexing has also been proposed [26]. A single photon has multiple degrees of freedom (polarization, time-bins, etc.), and some degrees of freedom (DOF) have multiple components. Quantum multiplexing is a method of encoding high-dimensional quantum information into a single photon using these multiple components of the same DOF or different DOFs.

In this work, we apply quantum multiplexing to the surface code and hypergraph product codes (HGP), which can be understood as a generalization of the surface code.

The rest of this paper is organized as follows: We overview the flow of quantum communication with surface codes in Sec. II. In Sec. III, we review the concept of quantum multiplexing. We also review the erasure channel, which is the dominant error source in optical systems, and how to correct erasure errors in Sec. IV. We then overview the surface code communication on the erasure channel and how quantum multiplexing affects its performance in Sec. V. Quantum Multiplexing introduces correlated errors on multiple qubits encoded in the same photons. This correlation increases the logical error rate for the channel. In Sec. VI, we show several strategies for assigning qubits in the code into photons. It mitigates the gap in performance caused by the effect of the correlation of errors. We also briefly introduce hypergraph product codes and their decoder in Sec. VII and show assignment strategies for the codes in Sec. VIII. The comparison of several interleaving methods and discussions is shown in Sec. IX.

II. MULTIPLEXED QUANTUM COMMUNICATION ON LOSSY CHANNEL

In this section, we overview the flow of multiplexed quantum communication which is shown in Fig. 1.

Surface codes, a type of topological stabilizer code, have an excellent error threshold. Moreover, the stabilizer generators of these codes have both constant weight and locality. Therefore, they are regarded as relatively feasible for qubits arranged on two-dimensional chips. Furthermore, surface codes have excellent methods for

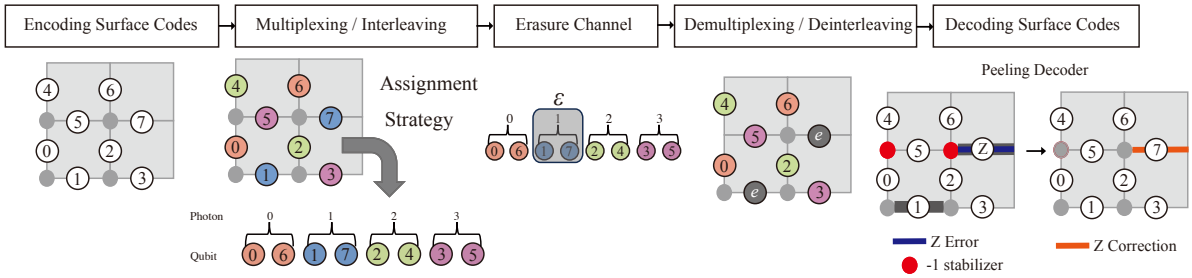


FIG. 1. Flow of surface code communication using multiplexed photons. In the first step, a quantum state is encoded into a surface code. Each circle with a number inside is the physical data qubit, and the grey circles without any number are auxiliary qubits used for stabilizer measurement. Next, in a quantum multiplexing scenario, one assigns each physical qubit of the codeword to single photons using different assignment strategies, as depicted in the second step. For instance, in this figure, two components of the time-bin DOF of each photon are used so that each photon can encode two qubits. We call this encoding multiplexing. There is a degree of freedom in which qubit is assigned to which photon, so it is required to make a map function. We call this function the interleaving assignment strategy. Here, the colors of the qubits indicate which photon the qubit is encoded to, which is the result of the assignment strategy. Then, the encoded photons go over a lossy channel. Here, we assume that we know which photons have been lost during the transmission (erasure channel). If a photon has been lost, all the qubits in the photon have been lost. Finally, we demultiplex and decode it to a code word of the surface code using the peeling decoder [27] and a correction method for erasure error shown in Sec. IV.

implementing two-qubit Clifford gates, including defect braiding [28] and lattice surgery [29] as well as single-qubit Clifford gates. Because of these promising properties, surface codes are regarded as one of the most promising candidate codes for fault-tolerant quantum computation.

For the first step of the communication, we prepare an encoded quantum state in surface codes. Then, as the second step, the sender freely assigns each data qubit to a photon, which can affect the logical error rate of the communication. For the third step, the codeword then goes through an optical channel, which has a loss error. Note that when a photon is lost, all the qubits encoded in that photon are lost. This can lead to strong correlations in the errors of those qubits in the same photon. In the fourth step, the codeword is received and mapped onto the 2D lattice for the surface codes. The photon losses are mapped into multiple qubit erasure errors by exploiting stabilizer measurement, which is described in Sec. IV. As the final step, the decoder estimates the errors based on the syndrome of the stabilizer measurement and corrects them.

III. QUANTUM MULTIPLEXING

This section outlines the methods and benefits of introducing quantum multiplexing. In photon-based quantum information processing, photons' various degrees of freedom (DOF) can be utilized to encode qubits. Polarizations [30], time-bins [31–33], paths (e.g., dual rail) [34], orbital angular momentum[35], and frequencies [36, 37] are typical examples of DOF in a single photon which various experiments and theoretical works have used. Exploring multi-level time-bins makes it especially easy to encode high-dimensional quantum information in a single photon. For instance, Fig. 2 shows a method for encoding higher dimensional information (2^3-dimension) in a time-bin photon. This circuit takes a photon whose polarization is encoded with quantum information as input. This input photon has one qubit of information. After passing through this circuit, the photon has both polarization and time-bin degrees of freedom. The polarization encodes a two-dimensional Hilbert space, and the time-bin encodes a four-dimensional one. Therefore, we can say that this photon exploits an 8-dimensional Hilbert space and so encodes 3 qubits of information. Significantly, encoding high-level time-bin states only requires linear optical elements and classical optical switches.

Quantum multiplexing [22] is a method to encode higher dimensional quantum information in a single photon using these multiple degrees of freedom. In this work, we consider encoding 2^m-dimensional quantum information using m DOFs per photon where m is an integer, and all the DOFs are two-level as shown in Fig. 3.

In this work, we consider a two-level encoding for transmitting quantum information over lossy optical channels, with logical information encoded into one or more surface codes and m physical qubits of these surface codes encoded into each transmitted photon (with $m = 1$ corresponding to no multiplexing).

While quantum multiplexing allows for efficient communication, it also changes the error model. In a communication channel over a photon-loss channel, the loss of a photon causes the simultaneous loss of multiple qubits encoded in that photon.

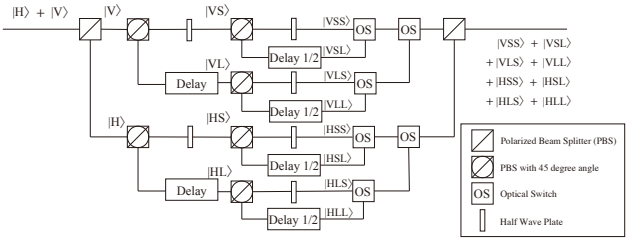


FIG. 2. An example of an optical circuit encoding 2^3-dimensional quantum information into a single photon. The elements on the circuit are the polarized beam splitter (PBS), the PBS on the diagonal basis (the one with a circle inside the box), the delay line, and the optical switch (OS). This circuit is feasible because it only requires optical linear elements.

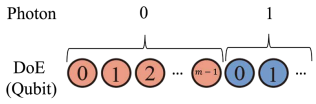


FIG. 3. Quantum multiplexing enables encoding multiple qudits by exploiting multiple components of DOFs in a single photon. Here, we use m time-bin qubits in each single photon. We use colors to indicate the photon to which a qubit belongs.

IV. ERASURE CHANNEL AND CORRECTION

Let us now describe the erasure channel and decoding, which are the last three steps of Fig.1. Erasure error is the dominant source of errors in optical systems [38, 39] because photons can be lost due to imperfect photon generation, detection, as well as scattering and absorption in optical components. Moreover, theoretical [40–43] and experimental [44–48] works have been proposed on methods to map errors from different sources to erasure errors in multiple physical systems recently.

The erasure channel is given by

$$\rho \to (1-\varepsilon)\rho + \varepsilon\,|e\rangle\langle e| \tag{1}$$

where $|e\rangle$ indicates the erased state, which is not in the original Hilbert space of the system, and ε is the probability of erasure. Since the erased state is not in the original Hilbert space, detecting such errors without destroying the quantum states is possible.

Several methods have been proposed to detect and correct erasure errors with QECCs [49]. It is possible to correct erasure by deforming the original logical operator [50, 51], as well as by converting erasure errors into random Pauli errors by replacing the lost qubits with mixed states:

$$\frac{\mathbb{I}}{2} = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z). \tag{2}$$

After replacing the qubits, one can perform stabilizer measurements as usual for surface codes. Then, the erasure is converted into random Pauli errors with the exact probabilities (1/4) for $\{I, X, Y, Z\}$. This random Pauli can also be regarded as independent X and Z errors with a probability of 1/2. This allows for the decoding of an erasure error. The (surface code) peeling decoder [27] is a linear-complexity erasure decoder using this procedure which has been proposed as a maximum-likelihood decoder for erasure errors in the surface code.

Peeling decoder refers to a linear-complexity erasure decoding algorithm originally designed for classical codes [52]. This algorithm corrects an erasure error by examining the subgraph of the Tanner graph corresponding to erased bits, whereby degree-1 check nodes in this subgraph give perfect information about adjacent bit nodes. Because this algorithm only uses the Tanner graph, it can be directly applied to CSS codes as well. The *surface code peeling decoder* refers to a generalization of this algorithm adapted to surface codes [27], which uses additional information about stabilizers. The surface code peeling decoder first identifies a spanning tree in the erasure-induced subgraph of the Tanner graph, and then performs peeling on this subgraph. This modified algorithm is a linear-complexity, maximum-likelihood decoder for the surface code. We use the surface code peeling decoder in our numerical simulations.

V. THE SURFACE CODE USED FOR QUANTUM COMMUNICATION OVER ERASURE CHANNEL

We propose three scenarios **(A, B, and C)** for efficient quantum communication and quantum memory with surface codes exploiting quantum multiplexing and discuss their performance. Table. I shows the code parameters and the number of codes, data qubits, and photons for these scenarios. We compare these scenarios to the case without multiplexing, which sends codewords of a $[\![2d^2, 1, d]\!]$ surface code with $2d^2$ qubits and $2d^2$ photons.

A. Sending m different codewords

The first scenario transmits multiple codewords. One can send m codewords using the same number of photons as the case without multiplexing. The effect of multiplexing on the logical error rate can be ignored by assigning the i-th qubit in each code word to the i-th photon. This introduces a correlation of errors between m distinct codes, but no set of qubits in the same code gets a correlation of errors. This does not affect the performance of the individual codes.

B. Sending $\sqrt{m} \times \sqrt{m}$ bigger codewords

The second scenario sends a single code with a larger size, thus achieving a greater code distance. It intro-

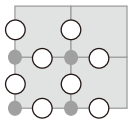
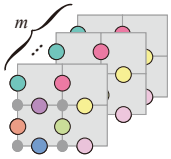
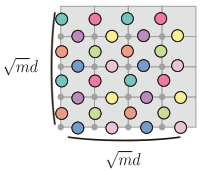
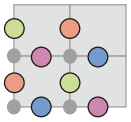
Scenarios	 without multiplexing	 (A)	 (B)	 (C)
Code parameters	$[\![2d^2, 2, d]\!]$	$[\![2d^2, 2, d]\!]$	$[\![2md^2, 2, \sqrt{md}]\!]$	$[\![2d^2, 2, d]\!]$
Number of Codes	1	m	1	1
Number of Data Qubits	$2d^2$	$2md^2$	$2md^2$	$2d^2$
Number of Photons	$2d^2$	$2d^2$	$2d^2$	$\lfloor 2d^2/m \rfloor$
Logical Error Rate	-	Same as without quantum multiplexing	Affected by correlation	Affected by correlation

TABLE I. Comparison of the surface code communication without multiplexing and three scenarios with multiplexing. Parameters that are improved by multiplexing are in red fonts. The case without multiplexing requires one qubit per photon. (A) The first scenario is only applicable when sending multiple codewords. This enables one to send more codewords with the same number of photons, drastically improving the channel's throughput. (B) The second scenario sends the same number of codewords with the bigger code, improving the error tolerance. (C) The third scenario sends the same codeword with fewer photons, drastically improving the channel's throughput. The number of photons required in scenario (C) is $\lfloor 2d^2/m \rfloor$, where $\lfloor x \rfloor$ is the floor function of x.

duces correlations in errors between the qubits in the code, which may degrade the performance. However, if m is sufficiently small relative to the code size, the benefit gained by increasing the code size is more significant. Fig. 4 shows a Monte Carlo simulation of the logical error rate for this scenario. Each data point in the simulation is obtained from 10^5 shots, and the error bar is given by the Agresti–Coull interval [53]. The logical error rate significantly decreases as the code size and m increase.

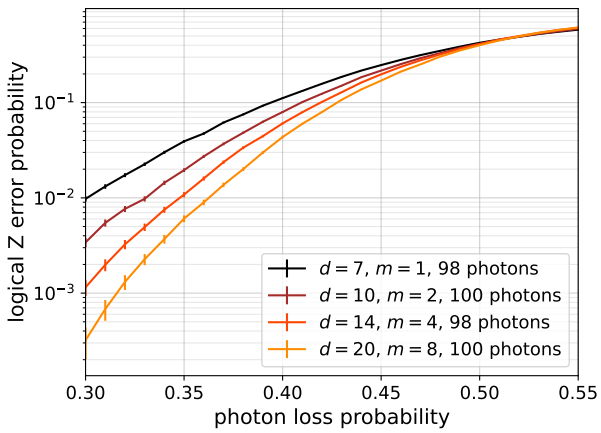


FIG. 4. Performance of $[\![2d^2, 2, d]\!]$ toric codes in scenario (B). Logical Z error rate versus photon loss probability for the surface code communication with about 100 photons. Each curve shows the case for toric codes with different code sizes. By increasing both the number of qubits per photon m and the code distance d, the logical error rate can be reduced.

C. Sending original code words with fewer photons

The third scenario sends a single codeword with a smaller number of photons. The code parameters are the same as the case without multiplexing. It has no restriction on the number of codewords and can improve the efficiency of surface code communication in general. However, since this method introduces correlation to the errors of multiple qubits in a single code word, it is necessary to be aware of that correlation can increase the error rate. Fig. 5 shows this scenario's logical error rate versus the photon loss probability for different choices of m. It shows that as m increases, the logical error rate decreases.

While the benefits of each scenario are obvious, the impact on the logical error rate when multiple qubits are encoded to the same photon is non-trivial. We evaluate this in the next section.

VI. ASSIGNMENT STRATEGIES FOR SURFACE CODES

In this section, we describe five strategies for assigning qubits that take advantage of multiplexing and evaluate their impact on performance. We assume surface code communication scenario **(C)**, where we send the original code with $\lfloor 2d^2/m \rfloor$ photons. In such a multiplexed system, each multiplexed photon is assumed to have the same number of qubits m.

Strategy i and ii: pair with minimum and maximum distance The distance between qubits within the same photon is crucial when considering the impact of correlated errors. To begin, we compare two strategies for the $m = 2$ case that minimize and maximize this distance. One can minimize the distance by

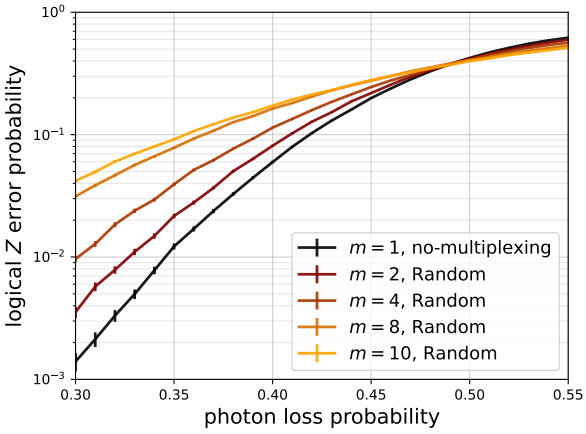


FIG. 5. Scenario (C) multiplexing performance for 10×10 toric code. Logical Z error rate versus photon loss probability for the $[\![200, 2, 10]\!]$ surface code communication with multiplexing using different values of m (the number of qubits per photon). The assignment of qubits to photons is uniformly random. Increasing m allows code words to be transmitted with fewer photons, but the logical error rate increases because multiple qubits in the same photon have strongly correlated errors.

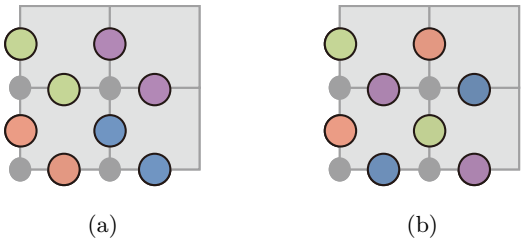


FIG. 6. Examples showing possible assignments of qubits to photons. Each numbered circle denotes a qubit, and the color indicates the photon to which the qubit is assigned. Strategy i, shown in (a), minimizes the distance between qubits in the same photon, while strategy ii in (b) maximizes this distance. Note that this code is defined on the torus represented as a lattice with periodic boundary conditions.

grouping together two qubits that share a stabilizer using an L shape. Also, the distance can be maximized by grouping together two qubits with the position (i, j) and $(i + d/2 - 1 \bmod d, j + d/2 - 1 \bmod d)$ where $i, j < d$. These qubits are as far apart as possible in the standard $d \times d$ periodic lattice used to represent the toric code. Fig. 6 shows an example of the arrangements on the 2×2 lattice when these two strategies are employed. These strategies are deterministic and can be realized with simple calculations. Fig. 7 shows the simulated surface code performance using these two methods in brown and gray. The performance of the distance-maximizing strategy outperforms the distance-minimizing strategy.

Logical errors in the toric codes correspond to errors covering a longitude or meridian curve on the torus (a vertical or horizontal closed loop in the periodic lattice). When decoding erasure errors, logical errors are likely to occur when the qubit-support of one of these vertical or horizontal loops is entirely erased. When adjacent qubits in the lattice are erased, as in the case with the distance-minimizing photon assignment strategy, clusters of errors are more likely to cover such loops in the torus. Hence, it is not surprising that the distance-maximizing strategy outperforms the distance-minimizing strategy in our numerical simulations.

with close distances.

Errors with strong correlation are similar to burst errors in classical communication in the sense that the errors have spatial locality. This locality of errors can be addressed by classical error-correcting codes using two methods. The first method treats multiple bits as a single symbol (an element of a finite field), such as BCH codes and Reed-Solomon codes [54]. Thanks to the high ability to correct burst errors, Reed-Solomon codes are used in many classical systems, including QR codes [55], CDs, and satellite communications. Another method is the interleaving [56] technique. Interleaving eliminates locality by permuting the rows and columns of the code's generator matrix. There is also a method to apply interleaving to QECCs[57]. Inspired by interleaving, we have constructed two more strategies for quantum multiplexing.

Strategy iii: random The third strategy is a method in which qubits are uniform-randomly selected and assigned to photons. The same effect as interleaving can be expected.

Strategy iv: random + threshold The fourth strategy is a modified version of the third strategy. The pseudo-code is shown below in Algorithm 1. The flow of the algorithm is as follows: A "threshold" T is set as $2/d-1$, which is the maximal distance between two qubits in the $[\![2d^2, 1, d]\!]$ toric codes. This value will be used to check that the set of qubits in the same photon has enough distance between each other. Then, it randomly assigns qubits for each photon while respecting the distance threshold. It randomly selects the first qubit of the photon, then it randomly selects a qubit again and takes it as a candidate to assign it to this photon. When the distance between the candidate qubit and the qubit(s) already in the photon is greater than the threshold, the qubit is accepted, and when it is less, it is rejected. This procedure is repeated until the photon has been fulfilled. If no qubit satisfies the threshold, the threshold value is lowered by one. By repeating this process, we can assign all the qubits to photons. This strategy is designed to have randomness and to increase the distance between qubits in the same photon.

This algorithm requires calculating the distance between two qubits, which is easy for the surface codes because the taxicab metric defines the distance (Manhattan distance). Note that this and other assignment

strategies can still be applied even if the number m of qubits per photon is not a divisor of the total number of qubits. In this case, we allow for a final "remainder" photon containing fewer than m qubits.

Algorithm 1: Strategy iv. random + threshold

Input: $P = \{p_i\}$ (the set of photons) where initially $p_i = \{\emptyset\}$ (the set of qubits to be encoded in the i^{th} photon), $Q = \{q_j\}$ (the list of all physical qubits in the code), and the number m of qubits in a single photon.

Output: $P = \{p_i\}$ (set of set of qubits in i^{th} photon).

```
Initialize the threshold with T := d/2 − 1;
for photon p_i ∈ P do
    Pick a qubit q_j ∈ Q randomly.;
    Move q_j from Q to p_i;
    while |p_i| < m do
        while |p_i| < m and Q ≠ ∅ do
            Pick a candidate qubit q_k ∈ Q randomly;
            if q_k has minimum distance greater than T
             from all the qubits in p_i then
                Move q_k from Q to p_i;
            else
                Move q_k from Q to a waiting list Q′;
        Move all qubits in Q′ to Q;
        Update T := T − 1;
Return P;
```

We compared the logical error rates of the four strategies discussed above. Fig. 7 shows the comparison of all the assignment strategies suitable for $m = 2$ case, and Fig. 9 shows the case for $m = 4$. Our numerical results showed that the strategy combining randomness + threshold outperformed the other strategies. Maximizing the distance between qubits while also introducing randomness gives the largest boost in performance against logical errors. Note that no assignment strategy does better than the case with $m = 1$ where no multiplexing is used.

Strategy v: stabilizer Error correction on the surface code is always considered up to multiplication by a stabilizer. This suggests that it may be useful to define photons using the qubit-support of a stabilizer check. Since the stabilizer generators for the surface code correspond to squares and crosses in the lattice, they have weight 4. On a $d \times d$ lattice, if d is divisible by 4, it will always be possible to partition the lattice into squares and crosses. In this perspective, the L-shapes used in the minimum-distance strategy can be thought of as "half-stabilizers" in the lattice. Since the usual strategy for converting an erasure problem into an error correction problem involves assigning erased qubits Pauli errors randomly, this stabilizer assignment strategy uses a mix of Z and X-type stabilizer generators from both squares and crosses. In this case, qubits are equally partitioned into the two types of stabilizers by tiling the lattice with alternating diagonal lines of squares and crosses. Examples of these photon assignment strategies on a 4×4 lattice are shown in Fig 8.

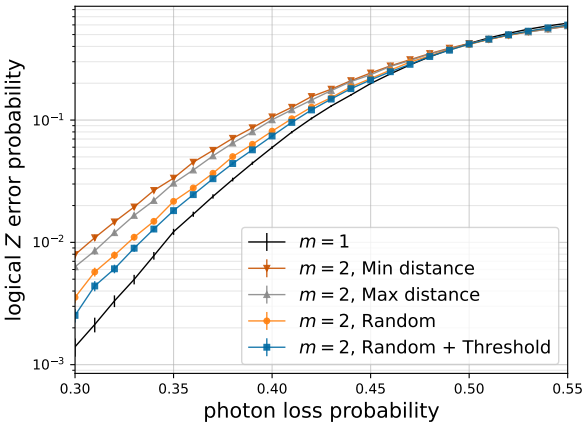


FIG. 7. Comparison of multiplexing photon-assignment strategies for $[\![200, 2, 10]\!]$ toric code. Logical Z error rate versus photon loss probability for the different assignment strategies. The black curve shows the case without multiplexing, and the others show the case for $m = 2$ with different interleaving assignment strategies. The gray/brown curve shows the case for $m = 2$ with the assignment strategy for minimizing (strategy i) / maximizing (strategy ii) the distance between a pair of qubits in the same photon. The orange curve shows the case for uniformly random (strategy iii), and the blue line shows strategy iv, based on the algorithm 1.

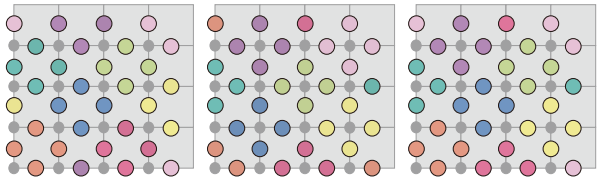


FIG. 8. Examples of the stabilizer-based photon assignment strategy for a surface code on a 4×4 lattice. Edges representing qubits in the lattice are marked with colored nodes indicating photon assignment. In this lattice picture, the qubit support of Z-type stabilizer generators corresponds to squares, and of X-type stabilizer generators corresponds to crosses. Each photon in the stabilizer assignment strategy represents the qubit-support of one of these stabilizers. The three images above show examples of photon assignments using only disjoint Z-stabilizer generators (squares), only disjoint X-stabilizer generators (crosses), or a combination of the two.

Restricting to one type of stabilizer creates a bias in the correction of errors matching the stabilizer type, as shown in Fig.9. Strategy v can be generalized to any stabilizer codes, and this result implies that some biased codes may be useful in multiplexed quantum communication systems.

We also analyzed the performance for different code sizes of the surface code communication as shown in Fig. 10. This indicates that the correlation affects a lot

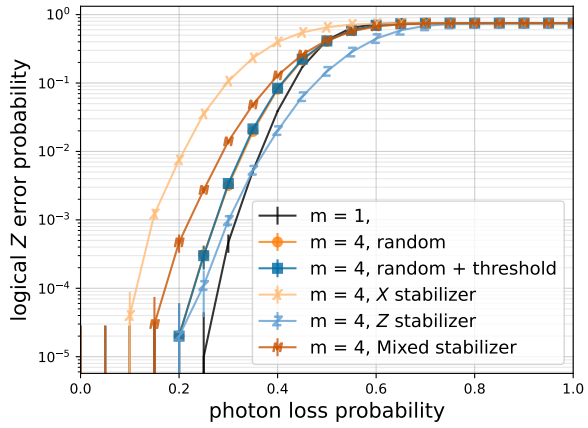


FIG. 9. Comparison of photon-assignment strategies for $[\![288, 2, 12]\!]$ toric code. Z stabilizer-based assignment with light blue curve outperformed X stabilizer-based assignment with light orange curve for logical Z error. The mixed stabilizer-based assignment strategy performs between X and Z. Random (orange, strategy iii) and random + threshold (blue, strategy iv) outperform other assignment strategies for low error rate areas.

in small-size code, but one can suppress such a gap by increasing the size of the code.

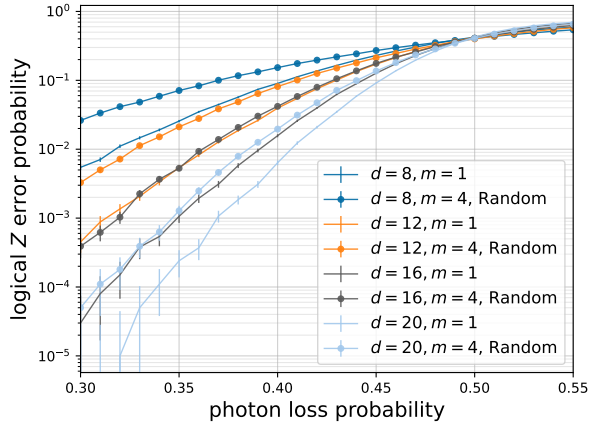


FIG. 10. Comparison of the logical error rates for the case with quantum multiplexing and without it. The Logical error rates of the surface code communication with $d = 8, 12, 16$ and 20 versus the photon loss probability. As d increases, the gap between the non-multiplexed ($m = 1$) and multiplexed ($m = 4$) cases decreases.

VII. HGP CODES AND THE PRUNED PEELING + VH DECODER

In addition to our study of the surface code, we also consider the use of multiplexing with hypergraph product (HGP) codes [58]. HGP codes are of particular interest because they have asymptotically finite rates and minimum distance proportional to the square root of the classical code lengths. They are also considered practical candidates for FTQC codes.

HGP codes are a special class of CSS code defined using any two classical codes. Given classical parity check matrices H_1 and H_2 with sizes $r_1 \times n_1$ and $r_2 \times n_2$, respectively, we may define the matrices H_X and H_Z of a CSS code via the formulas

$$H_X = (H_1 \otimes I_{n_2} | I_{r_1} \otimes H_2^T) \tag{3}$$
$$H_Z = (I_{n_1} \otimes H_2 | H_1^T \otimes I_{r_2}). \tag{4}$$

These matrices satisfy the condition $H_X H_Z^T = 0$ by construction and hence define a valid CSS code $\mathrm{HGP}(H_1, H_2)$. When H_1 and H_2 are low-density parity check (LDPC), H_X and H_Z will also be LDPC. The sizes of H_X and H_Z are also determined by the sizes of the input classical matrices according to the formulas

$$H_X = [r_1 n_2 \times (n_1 n_2 + r_1 r_2)] \tag{5}$$
$$H_Z = [r_2 n_1 \times (n_1 n_2 + r_1 r_2)]. \tag{6}$$

These both simplify to $rn \times (n^2 + r^2)$ in the special case where $r_1 = r_2 = r$ and $n_1 = n_2 = n$.

HGP codes have a geometrically rich Tanner graph structure which can be visualized as the graph product of the Tanner graphs for two classical codes as shown in Fig. 11. The subgraph corresponding to each row and column in this Tanner graph block structure can be understood as the classical Tanner graph for one of the classical codes used in the construction. Qubits in this Tanner graph are represented by the nodes in the $n_1 \times n_2$ and $r_1 \times r_2$ blocks; X- and Z-type stabilizer generators are represented by the nodes in the $r_1 \times n_2$ and $n_1 \times r_2$ blocks, respectively. Hence, the number of qubits and stabilizer checks are controlled by the size of the input classical matrices. Choosing matrices of the same size ensures an equal number of stabilizer checks in the HGP code, but a biased code can also be constructed by using matrices of different sizes. Furthermore, using $H_2 = H_1^T$ yields a symmetric construction for H_X and H_Z and guarantees that the two blocks of qubits in this product graph picture are squares of equal size. In our numerical simulations, we consider two types of HGP code construction: an *equal block* case coming from the symmetric construction, and a non-equal block case using $r_1 = r_2 = r$ and $n_1 = n_2 = n = 2r$.

Surface codes may also be recovered as a special case of hypergraph product code. Using parity check matrices H_1 and H_2 for a classical repetition code, $\mathrm{HGP}(H_1, H_2)$ is exactly the toric code. Hence, adapting the multiplexing strategies discussed in Sec. V to this more general class of codes is a natural next question. However,

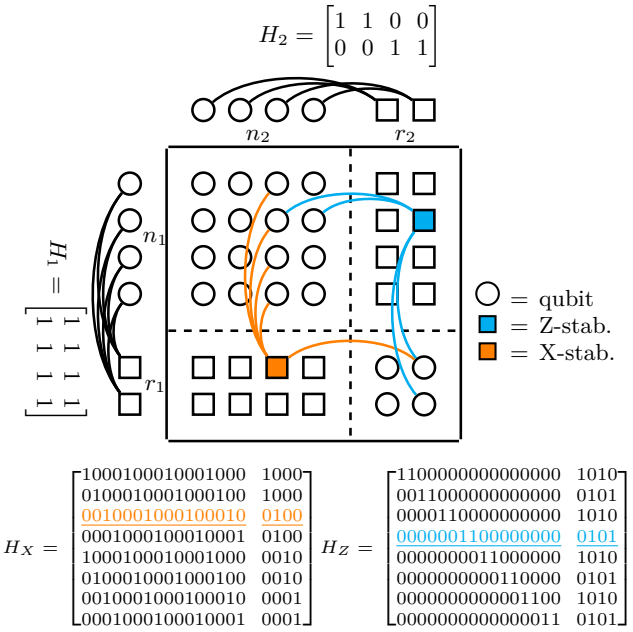


FIG. 11. Example of the Tanner graph for a simple HGP code $\mathrm{HGP}(H_1, H_2)$ constructed from two classical codes with parity check matrices H_1 and H_2. This is the graph product of two classical Tanner graphs, and the subgraph corresponding to each row and column in the product is a copy of one of these classical Tanner graphs. This product structure can be partioned into four quadrants, each representing a different structural component of the HGP code. The nodes in the upper-left and lower-right blocks denote qubits. The nodes in the upper-right block denote Z-stabilizer generators; these correspond to the rows of H_Z. Similarly, the nodes in the lower-left block denote X-stabilizer generators; these correspond to the rows of H_X.

the linear-time maximum-likelihood peeling decoder [27] used in our previous simulations is only defined for the special case of the surface code. Instead, we consider a closely related generalization of the peeling decoder designed for HGP codes, which has quadratic complexity and close to maximum-likelihood performance at low erasure rate [59].

The *pruned peeling + VH decoder* is a modified version of the standard classical peeling decoder based on analysis and correction of two common types of *stopping sets*, which are patterns of erased qubits which cannot be corrected by simple peeling. *Stabilizer stopping sets* occur when the erasure contains the qubit-support of an X- or Z-type stabilizer. Such a stopping set can be modified by fixing a value at random for one qubit of the stabilizer and removing this qubit from the erasure, possibly allowing the standard peeling algorithm to become unstuck. This technique is valid because there exists a solution on the remaining erased qubits in the stabilizer-support such that the combined contribution to the error is at most a stabilizer. This procedure, known as *pruned peeling*, is applicable to any CSS code, not just HGP codes.

Classical stopping sets are another common type of peeling decoder stopping set unique to HGP codes. These refer to patterns of erased qubits supported entirely on a single row or column in the HGP Tanner graph block structure of Fig. 11. In the simplest case, these can also be understood as peeling decoder stopping sets for the classical code obtained by restricting to this row or column in the Tanner graph, although this need not always be true. Any HGP peeling decoder stopping set can be decomposed into a union of vertical and horizontal classical stopping sets. The *VH decoder* algorithm functions by ordering and efficiently solving each of these classical stopping sets in sequence, although this is not always possible for certain erasure configurations.

The *combined decoder* (peeling + pruned peeling + VH) is not a maximum likelihood decoder. Patterns of erased qubits still exist where the decoder becomes stuck in a stopping set, leading to a decoder failure. These are distinct from logical errors, which can only be identified in numerical simulations where the decoding algorithm successfully terminates. The maximum-likelihood decoder always terminates, and thus, logical errors are the only source of failures. Hence, in our numerical analysis, we make a distinction between decoder failures and non-decoder-failure logical errors, as illustrated in Fig. 12. However, the pruned peeling + VH decoder is still practically useful for our numerical simulations since decoder failures are infrequent at low erasure rates.

Note that peeling + pruned peeling is theoretically a maximum likelihood decoder in the special case of the surface code. This is equivalent to the spanning-tree-based ML decoder for the surface code [27]. However, our implementation of pruned peeling is not perfect since it cannot identify the support of an arbitrary erased stabilizer. For the *combined decoder*, the simplest classical stopping sets correspond to a fully erased row or column in the HGP Tanner graph. These are exactly the stopping sets of a repetition code, coinciding with logical errors for the surface code. In general, there do not exist erasure patterns giving a VH decoder failure which do not also cover a logical error.

Figure 13 shows the performance of the *combined decoder* applied to the 10×10 surface code. Comparing this to Figure 5, which uses the ML decoder for the same surface code, we see a noticeable degradation in performance. This gap is explained by the existence of decoder failures in the combinded case which do not exist for the ML decoder. Furthermore, the failure rate of the combined decoder converges to 1 as the erasure rate goes to 1, in contrast with the convergence to 0.75 for the ML decoder. This is because the erasure pattern is always a VH decoder stopping set when all qubits are erased, guaranteeing a decoder failure. Since there are no stopping sets in the ML case, however, a 100% erasure rate is equivalent to generating a uniformly random physical Pauli error on the code. We see a convergence to 0.75 logical error rate because this error is identity 25% of the

time.

Failure rate in the literature usually refers to the logical error rate, which is the only source of errors for a maximum-likelihood decoder. Logical errors for the erasure channel can only occur when the erasure covers a logical code word. However, there may exist erasure patterns covering a logical error which result in a decoder failure, and hence are not properly identified as logical errors. This distinction is stated visually by the Venn diagram of Fig. 12. The failure rate computed in our numerical simulations for the *combined decoder* is the cummulative effect of these two possibilities. We label the vertical axis as such in Fig. 13 and later simulations to make a clear distinction between these two ways of failing. Note that failures at low erasure rates are almost exclusively due to logical errors, and so this distinction can be regarded as negligible in the practical regime.

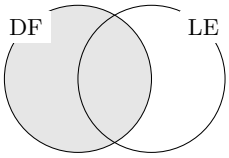


FIG. 12. Venn diagram distinguishing between the types of failures possible using the pruned peeling + VH decoder. A decoding failure (DF) occurs when the decoder becomes stuck in a stopping set it cannot correct. A logical error (LE) occurs when the decoder successfully terminates with a predicted error, but the actual and predicted errors combine to give a logical code word.

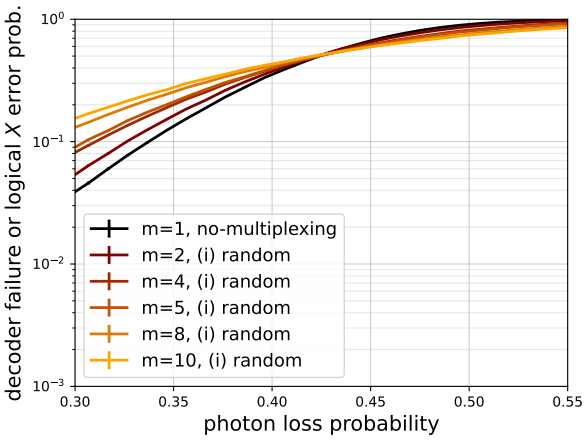


FIG. 13. Comparison of the $[\![200, 2, 10]\!]$ toric code using the uniformly random assignment strategy with different numbers of qubits in a single photon, m. In general, increasing the multiplexing number m also increases the failure rate. These simulations use the non-maximum-likelihood *combined decoder* (peeling + pruned peeling + VH). The vertical axis denotes the cumulative effect of logical errors and decoder failures. Since the decoder is not ML, the curves intersect at a threshold of approximately 0.43 ± 0.01, which is below the value 0.5 for the *surface code peeling decoder* in Fig. 5 used in Sec. VI.

VIII. ASSIGNMENT STRATEGY FOR HGP CODES

Quantum multiplexing can also be utilized in quantum communication using HGP codes. In this section, we analyze the performance of HGP code communication in scenario **(C)**. The scenarios previously proposed in Sec. V are also valid for HGP codes, but unlike the special case of the surface code, the distance between any two qubits in a generic HGP code is not easily inferred from a grid. Hence, we do not consider the previously introduced strategies which use distance. We also introduce several new strategies for HGP codes based on stopping sets for the pruned peeling + VH decoder. These are summarized in Table II.

Strategy i: random The simplest assignment strategy is based on assigning qubits to photons at random.

Strategy ii: stabilizer The stabilizer strategy was initially introduced in Sec. V for the surface code, but it can be applied to CSS codes more generally. The erased qubit-support of a stabilizer will be a peeling decoder stopping set, but these are precisely the stopping sets which the pruned peeling algorithm attempts to correct. Hence, this strategy is motivated by the idea that losing a photon corresponding to a single stabilizer individually induces a correctable erasure pattern.

In the special case of the surface code with a $d \times d$ lattice, where d is divisible by 4, it is always possible to partition the qubits into a combination of disjoint X- and Z-type stabilizer generators as seen in Fig. 8, each of which is supported on 4 qubits. For a more general HGP code, we may attempt a similar assignment strategy by identifying the qubit-support of the stabilizer generators from the rows of H_X and H_Z. However, we cannot guarantee that a partition of qubits into disjoint stabilizers is possible without placing constraints on the number of qubits and the row and column weights in the parity check matrices. Instead, we adopt an imperfect but simpler strategy for generic HGP codes, which does not require any additional assumptions about the code except that H_X and H_Z are LDPC. This strategy can be used with stabilizers coming only from H_X, only from H_Z, or a combination of both, provided that these matrices have the same row weight. Note that restricting to a single type of stabilizer creates a bias in the error correction, as was commented in the surface code case.

In the HGP stabilizer assignment strategy, we search for a partition of the qubits into disjoint stabilizers. To do this, we begin by choosing a row at random from H_X or H_Z; the nonzero entries in this row represent the qubit-support of a single stabilizer. We then eliminate any overlapping stabilizers by deleting the rows from the matrices that share columns with nonzero entries with

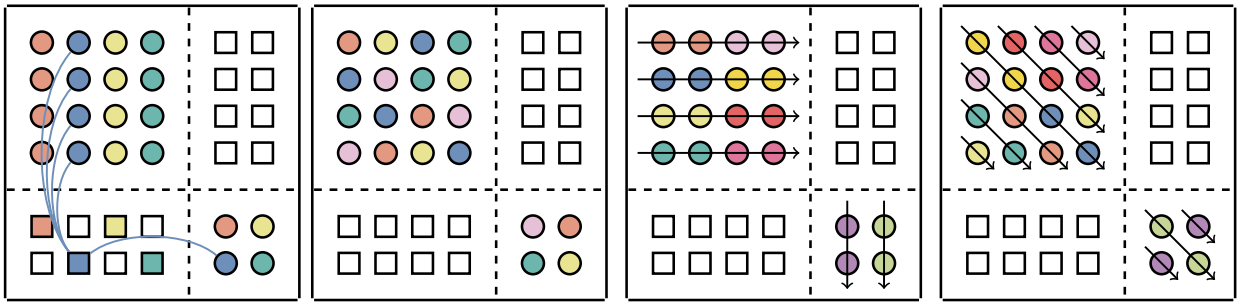


TABLE II. Examples of four different photon assignment strategies for the simple HGP code shown in Fig. 11. **(ii.)** Each photon in the stabilizer strategy is the qubit-support of an X or Z-type stabilizer generator, identified as a row of H_X or H_Z. The number of qubits per photon is a fraction or multiple of the weight of the corresponding row. **(iii.)** In the sudoku strategy, each qubit of a given photon is contained in a different row or column of the HGP Tanner graph. **(iv.)** Using the row-column strategy, each qubit of a given photon is contained in the same row or column of the HGP Tanner graph. **(v.)** Photons from the diagonal strategy contain qubits from the same diagonal of the HGP Tanner graph, allowing diagonal lines to wrap around. For strategies iii., iv., and v., the number of qubits per photon is a fraction or multiple of the shortest side length in the block structure.

the previously selected row. Then we repeat this strategy until either all qubits have been divided into disjoint stabilizers or we exhaust the remaining rows that do not overlap with our previous selections. The result is that as many qubits as possible have been divided into non-overlapping sets corresponding to the qubit-support of disjoint stabilizers, possibly with some remaining ungrouped qubits.

Finally, the qubits are assigned to photons based on the disjoint sets identified in the previous step. Ordering the qubits by their stabilizer assignments, we then redistribute these into photons. The remaining ungrouped qubits are assigned after exhausting the chosen stabilizers. When the multiplexing number matches the stabilizer weight (that is, the row weight of H_X or H_Z), each photon ideally matches a stabilizer, possibly with some remainder photons at the end for the ungrouped qubits. When the multiplexing number matches a fraction or multiple of the stabilizer weight, then the photons represent a partial stabilizer or multiple stabilizers, respectively. Allowing for the leftover qubits at the end ensures that this strategy can be applied with various multiplexing numbers, even when a perfect partition of qubits into stabilizers is not found. Because stabilizers are selected at random, this assignment strategy can be understood as a combination of the random and stabilizer strategies introduced before.

Strategy iii: sudoku The VH decoder is designed to address classical stopping sets for the peeling decoder, but there exist combinations of classical stopping sets that cannot be solved using this technique and result in a decoder failure. However, we may reduce the likelihood of a decoder failure by reducing the number of classical stopping sets in general. Classical stopping sets are supported on a single row or column of the HGP code Tanner graph. Thus, we propose an assignment strategy based on choosing qubits in the same photon from different rows and columns. We name this the sudoku strategy due to its resemblance to the popular game. The strategy is outlined in Algorithm 2.

This strategy assumes that the number of qubits per photon does not exceed the minimum length of a row or column in the Tanner graph, although this condition may be relaxed by instead allowing for a minimal number of qubits from the same row or column to be added to the same photon. Qubits are assigned to photons at random, checking that each newly added qubit is not supported on the same row or column as any qubit already assigned to a given photon. In the case of a fixed number of photons where no valid qubit assignments remain, we drop the condition and default to random assignment.

Strategy iv: row-column Although not a practical assignment strategy, the case where only qubits from the same row or column of the HGP code Tanner graph are assigned to the same photon is of theoretical interest. This strategy attempts to maximize the number of classical stopping sets resulting from photon loss and thus increase the likelihood of a VH decoder failure. Verifying that this assignment strategy performs very poorly in numerical simulations serves as a proof of concept for the VH decoder and also justifies the preferred strategies using qubits from different rows and columns.

Fig. 14 shows the performance of this strategy for a $[\![512,8]\!]$ HGP code at several multiplexing numbers. Although surprisingly the $m = 2$ case seems to outperform the no-multiplexing case, the failure rate otherwise increases as m increases. Failures of the VH decoder are the result of certain configurations of classical stopping sets, and hence increasing the latter also increases the former. In particular, this explains the dramatic jump between the $m = 8$ and $m = 16$ cases. Since the blocks in this code's Tanner graph are 16×16, each photon in

Algorithm 2: Strategy iii. sudoku

Input: $P = \{p_i\}$ (the set of photons) where initially $p_i = \emptyset$ (the set of qubits to be encoded in the i^{th} photon), $Q = \{q_j = (j, r_j, c_j, b_j)\}$ (a list of 4-tuples with information about the index, row, column, and block of each physical qubit in the HGP code), and the number m of qubits per photon.

Output: $P = \{p_i\}$ (set of sets of qubits in i^{th} photon).

for *photon* $p_i \in P$ **do**
  Pick a qubit $q_j \in Q$ randomly;
  Move q_j from Q to p_i;
  while $|p_i| < m$ *and* $Q \neq \emptyset$ **do**
    Pick a candidate qubit $q_k \in Q$ randomly;
    if q_k *is in a different row and column (or block) from each previously selected* $q_j \in p_i$ *(*$(r_k \neq r_j$ *and* $c_k \neq c_j)$ *or* $b_k \neq b_j$*)* **then**
      Move q_k from Q to p_i;
    else
      Move q_k from Q to a waiting list Q';
  Move all qubits in Q' back to Q;
  while $|p_i| < m$ **do**
    Pick a qubit $q_k \in Q$ randomly;
    Move q_k from Q to p_i;
Return P;

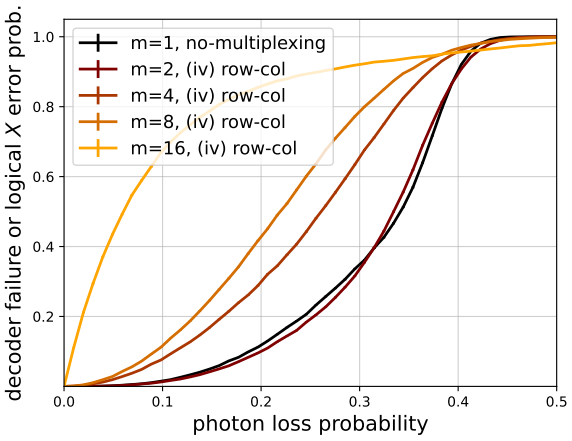


FIG. 14. Multiplexing decoder performance for a ⟦512,8⟧ equal-block (16 × 16) HGP code obtained from the symmetric construction using $r = n = 16$ with assignment strategy (iv) row-column. Increasing the number of qubits per photon using this strategy rapidly increases the failure rate. At $m = 16$, each photon corresponds to an entire row or column in the HGP Tanner graph, whereby losing even one photon guarantees a classical stopping set.

the $m = 16$ case corresponds to an entire row or column. Loss of any photon yields a classical stopping set, and hence VH decoder failures are common. This also confirms the significance of designing assignment strategies to avoid classical stopping sets in our simulations of HGP codes. In general, we expect the performance of the row-column strategy to drop significantly as m becomes equal to or larger than the side length of the block in the HGP Tanner graph.

Strategy v: diagonal The final assignment strategy is a modified version of the sudoku strategy. Whereas the previous strategy assigns qubits at random subject to the sudoku condition, qubits in the HGP code Tanner graph may also be grouped diagonally within each block. A $d \times d$ grid can be divided into d non-overlapping diagonal slices, where we allow slices to wrap around. Since no two qubits in the same diagonal slice are contained in the same row or column of the grid, this technique also guarantees that we avoid classical stopping sets within a single photon. Photon assignment is thus based on grouping together the qubits in the same diagonal slice. Each of the two qubit-squares in the HGP code Tanner graph is considered separately, but if we require that the ratio of the squares' side lengths is a whole number, then the qubits can be cleanly partitioned into photons of size matching the side length of the smaller square. HGP codes with rectangular Tanner graph block sizes call also use the diagonal strategy, provided that the length of the diagonal slice does not exceed the length of the shortest side. If longer slices are permitted in the rectangular case, then instead a minimal number of qubits in the same row or column are allowed.

Algorithm 3: Strategy v. diagonal

Input: $P = \{p_i\}$ (the set of photons) where initially $p_i = \emptyset$ (the set of qubits to be encoded in the i^{th} photon), $Q = \{q_j\}$ (a list of physical qubits in the HGP code ordered along the diagonal), and the number m of qubits per photon.

Output: $P = \{p_i\}$ (set of sets of qubits in i^{th} photon).

for *photon* $p_i \in P$ **do**
  for *qubits with indices* $j \in \{im, \cdots, (i+1)m\}$ **do**
    Move q_j from Q to p_i
return P;

The implementation of this strategy as described in Algorithm 3 is simple, provided one precomputes a *diagonal ordering* on the qubits in the HGP Tanner graph. Referring to the block structure of Fig. 11, the qubits in a given block are indexed along the non-overlapping diagonal slices. These slices are allowed to wrap around the sides of the square, which guarantees that no two qubits in the same slice are contained in the same row or column. The qubits in the second block are indexed sequentially after the first block. In our numerical implementation, a separate function to compute this ordering on the qubits in a HGP code is used along with the assignment function.

To compare the effectiveness of these strategies, we have simulated their performance for several codes at different multiplexing values as shown in Fig. 15 and Fig. 16. To understand these results, the case with no-multiplexing ($m = 1$) is used as the baseline. An assignment strategy is considered good if its failure rate is

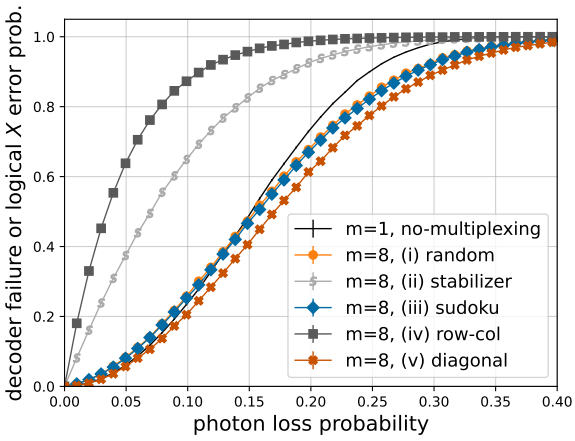


FIG. 15. Multiplexing decoder performance for a ⟦320,82⟧ non-equal block (16×16 and 8×8) HGP code at fixed $m=8$. In this example, strategy (v) diagonal outperforms all other strategies, including the no-multiplexing case.

not significantly worse than the $m=1$ case. Interestingly, our numerical simulations consistently show that the performance of some strategies (random, sudoku, and diagonal) is basically equivalent to or even exceeds the $m=1$ case, even at high multiplexing values. However, the row-col and stabilizer strategies are never seen to be effective in our results.

Fig. 15 shows an example of a code where the diagonal strategy consistently outperforms all other strategies, even the no-multiplexing case and even at low erasure rates. This result is significant because even though multiplexing reduces the number of required physical resources, it is possible to improve the decoding performance while doing so. In fact, an analysis of these results reveals that the diagonal strategy yields fewer logical errors than the no-multiplexing case at the same physical erasure rate. This appears to be a feature of the logical code words in the randomly generated code used in this simulation, even though the strategy was not designed with this in mind. This also explains the gap between the sudoku and diagonal strategies, both of which have similar amounts of decoder failures but differ with respect to logical errors. What these results show is that strategies designed to avoid decoder failures have comparable performance to no-multiplexing, and in some cases are capable of exceeding.

Although not identical, we see similarly good numerical results in the simulations of Fig. 16. The random, sudoku, and diagonal strategies have nearly identical performance to the no-multiplexing case regardless of the chosen multiplexing number. (Simulations include $m\in\{2,4,8,16\}$, although only plots for $m=4$ and $m=16$ are shown.) Furthermore, these results hold consistently at a low erasure rate, which is the regime of practical interest. This is significant because it implies there is no loss in performance when multiplexing, even though fewer physical resources are required, provided the assignment strategy is adapted to the decoder. If a ML decoder were used (e.g. Gaussian elmination rather than peeling + pruned peeling + VH), a gap is expected between the multiplexing and no-multiplexing cases. However, given that the combined decoder is a faster, more efficient alternative to a true ML decoder for HGP codes, these results are very promising.

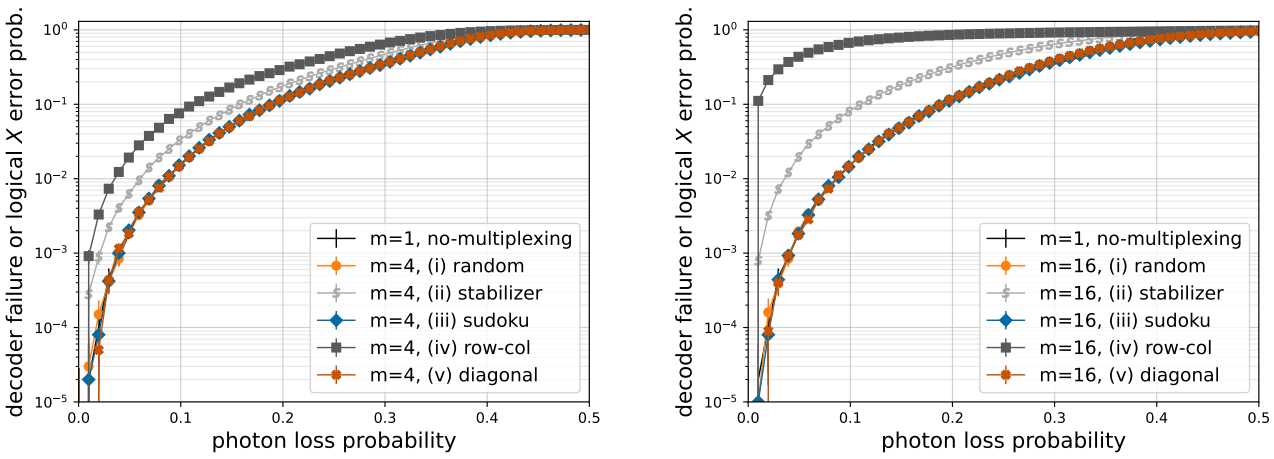
IX. CONCLUSION AND DISCUSSION

We proposed efficient error-corrected quantum information processing scenarios for quantum memory storage and communication with quantum multiplexing over an erasure channel. We have shown that Quantum multiplexing can improve throughput or resilience to errors, easing the bottleneck in quantum systems. This work can be adapted to surface code quantum communication with quantum interconnects, quantum repeaters [60], and multimode quantum memory.

For multiplexed quantum communication, we have found that if multiple qubits in a single code word are encoded into the same photon, a correlation of errors in those qubits will be introduced. The simulation results show that it leads to an increase in the logical error rate. We showed that this performance gap can be significantly mitigated by introducing a code-aware (or decoder-aware) strategy to assign qubits to photons, which exploits code structure. In particular for the surface codes, randomness and also distance maximization are important factors for achieving this. For HGP codes with the VH decoder, minimizing decoder failures was found to be the most important factor. These techniques can also be exploited to benefit other families of codes and decoders. It is also possible to deal with the gap by increasing the code size. We have also shown that it is possible to introduce biased error by using a stabilizer-based assignment strategy. In the special case of the diagonal strategy for the HGP code of Fig. 15, we see that the photon-correlated errors offer an improvement over the no-multiplexing case. In this example, the improvement can be explained by the fact that the diagonal strategy reduces logical errors in addition to decoder failures. Furthermore, this shows the existence of strategies that improve over no-multiplexing, despite the fact that fewer resources are used.

Although we propose several promising candidates, the optimal interleaving strategy is still unknown for both surface codes and HGP codes. Furthermore, in the actual communication with quantum multiplexing, various errors may occur when converting from qubits in the quantum processor to photons, measuring stabilizers, and substituting erased qubits with mixed states. How to deal with these errors is a practically important next question.

It may be practical to use the assignment information for decoding in cases where we do not know the positions



(A) $m = 4$ (B) $m = 16$

FIG. 16. Comparisons of multiplexing decoder performance for a ⟦512,8⟧ equal-block (16×16) HGP code obtained from the symmetric construction with $r = n = 16$ using various assignment strategies for $m = 4$ and $m = 16$. In both cases, the random, sudoku, and diagonal strategies are seen to be effectively equivalent to the no-multiplexing case, even at low erasure rates.

of errors (e.g., unitary error).

ACKNOWLEDGEMENTS

SN acknowledges Dan Browne, Antonio deMarti iOlius, and Hon Wai Lau for valuable discussions throughout this project. This work was supported by JSPS KAKENHI Grant Number JP21H04880, JP22J20882, the MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0118069605, the JST Moonshot R&D Grant Number JPMJMS2061, and the travel budget of National Institute of Informatics.

[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] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (1996) pp. 212–219.
[3] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Physical Review A **54**, 1098 (1996).
[4] D. Gottesman, Stabilizer codes and quantum error correction, arXiv preprint quant-ph/9705052 (1997).
[5] D. Gottesman, Fault-tolerant quantum computation with higher-dimensional systems, in *NASA International Conference on Quantum Computing and Quantum Communications* (Springer, 1998) pp. 302–313.
[6] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Annals of physics **303**, 2 (2003).
[7] M. Gong, X. Yuan, S. Wang, Y. Wu, Y. Zhao, C. Zha, S. Li, Z. Zhang, Q. Zhao, Y. Liu, *et al.*, Experimental exploration of five-qubit quantum error-correcting code with superconducting qubits, National Science Review **9**, nwab011 (2022).
[8] W. P. Livingston, M. S. Blok, E. Flurin, J. Dressel, A. N. Jordan, and I. Siddiqi, Experimental demonstration of continuous quantum error correction, Nature communications **13**, 2307 (2022).
[9] Suppressing quantum errors by scaling a surface code logical qubit, Nature **614**, 676 (2023).
[10] S. B. Bravyi and A. Y. Kitaev, Quantum codes on a lattice with boundary, arXiv preprint quant-ph/9811052 (1998).
[11] S. Krinner, S. Storz, P. Kurpiers, P. Magnard, J. Heinsoo, R. Keller, J. Luetolf, C. Eichler, and A. Wallraff, Engineering cryogenic setups for 100-qubit scale superconducting circuit systems, EPJ Quantum Technology **6**, 2 (2019).
[12] S. Tamate, Y. Tabuchi, and Y. Nakamura, Toward realization of scalable packaging and wiring for large-scale superconducting quantum computers, IEICE Transactions on Electronics **105**, 290 (2022).
[13] D. Awschalom, K. K. Berggren, H. Bernien, S. Bhave, L. D. Carr, P. Davids, S. E. Economou, D. Englund, A. Faraon, M. Fejer, *et al.*, Development of quantum interconnects (quics) for next-generation information technologies, PRX Quantum **2**, 017002 (2021).
[14] J. Wang, D. Bonneau, M. Villa, J. W. Silverstone, R. Santagati, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, *et al.*, Chip-to-chip quantum photonic interconnect by path-polarization interconversion, Optica **3**, 407 (2016).

[15] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Optical quantum memory, Nature photonics **3**, 706 (2009).

[16] Y.-W. Cho, G. Campbell, J. Everett, J. Bernu, D. Higginbottom, M. Cao, J. Geng, N. Robins, P. Lam, and B. Buchler, Highly efficient optical quantum memory with long coherence time in cold atoms, Optica **3**, 100 (2016).

[17] S. Nagayama, B.-S. Choi, S. Devitt, S. Suzuki, and R. Van Meter, Interoperability in encoded quantum repeater networks, Physical Review A **93**, 042338 (2016).

[18] C. D. Hill, A. G. Fowler, D. S. Wang, and L. C. Hollenberg, Fault-tolerant quantum error correction code conversion, Quantum Information & Computation **13**, 439 (2013).

[19] J. T. Anderson, G. Duclos-Cianci, and D. Poulin, Fault-tolerant conversion between the steane and reed-muller quantum codes, Physical review letters **113**, 080501 (2014).

[20] Y. Suzuki, T. Sugiyama, T. Arai, W. Liao, K. Inoue, and T. Tanimoto, Q3de: A fault-tolerant quantum computer architecture for multi-bit burst errors by cosmic rays, in *2022 55th IEEE/ACM International Symposium on Microarchitecture (MICRO)* (IEEE, 2022) pp. 1110–1125.

[21] F. Kobayashi and S. Nagayama, Erasure-tolerance protocol for the surface codes on rydberg atomic quantum computers, arXiv preprint arXiv:2404.12656 (2024).

[22] N. L. Piparo, W. J. Munro, and K. Nemoto, Quantum multiplexing, Physical Review A **99**, 022337 (2019).

[23] N. L. Piparo, M. Hanks, C. Gravel, K. Nemoto, and W. J. Munro, Resource reduction for distributed quantum information processing using quantum multiplexed photons, Physical Review Letters **124**, 210503 (2020).

[24] N. L. Piparo, M. Hanks, K. Nemoto, and W. J. Munro, Aggregating quantum networks, Physical Review A **102**, 052613 (2020).

[25] M. Grassl, W. Geiselmann, and T. Beth, Quantum reed—solomon codes, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Springer, 1999) pp. 231–244.

[26] S. Nishio, N. L. Piparo, M. Hanks, W. J. Munro, and K. Nemoto, Resource reduction in multiplexed high-dimensional quantum reed-solomon codes, Physical Review A **107**, 032620 (2023).

[27] N. Delfosse and G. Zémor, Linear-time maximum likelihood decoding of surface codes over the quantum erasure channel, Physical Review Research **2**, 033042 (2020).

[28] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation, Physical Review A **86**, 032324 (2012).

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

[30] A. B. U'Ren, K. Banaszek, and I. A. Walmsley, Photon engineering for quantum information processing, arXiv preprint quant-ph/0305192 (2003).

[31] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Pulsed energy-time entangled twin-photon source for quantum communication, Physical Review Letters **82**, 2594 (1999).

[32] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin, Femtosecond time-bin entangled qubits for quantum communication, arXiv preprint quant-ph/0205144 (2002).

[33] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, Experimental investigation of the robustness of partially entangled qubits over 11 km, Physical Review A **66**, 062304 (2002).

[34] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Linear optical quantum computing with photonic qubits, Reviews of modern physics **79**, 135 (2007).

[35] A. M. Yao and M. J. Padgett, Orbital angular momentum: origins, behavior and applications, Advances in optics and photonics **3**, 161 (2011).

[36] Y. Shih and A. Sergienko, Observation of quantum beating in a simple beam-splitting experiment: Two-particle entanglement in spin and space-time, Physical Review A **50**, 2564 (1994).

[37] S. Ramelow, L. Ratschbacher, A. Fedrizzi, N. Langford, and A. Zeilinger, Discrete tunable color entanglement, Physical review letters **103**, 253601 (2009).

[38] S. Slussarenko and G. J. Pryde, Photonic quantum information processing: A concise review, Applied Physics Reviews **6** (2019).

[39] A. Joshi, K. Noh, and Y. Y. Gao, Quantum information processing with bosonic qubits in circuit qed, Quantum Science and Technology **6**, 033001 (2021).

[40] Y. Wu, S. Kolkowitz, S. Puri, and J. D. Thompson, Erasure conversion for fault-tolerant quantum computing in alkaline earth rydberg atom arrays, Nature communications **13**, 4657 (2022).

[41] A. Kubica, A. Haim, Y. Vaknin, H. Levine, F. Brandão, and A. Retzker, Erasure qubits: Overcoming the t 1 limit in superconducting circuits, Physical Review X **13**, 041022 (2023).

[42] M. Kang, W. C. Campbell, and K. R. Brown, Quantum error correction with metastable states of trapped ions using erasure conversion, PRX Quantum **4**, 020358 (2023).

[43] T. Tsunoda, J. D. Teoh, W. D. Kalfus, S. J. de Graaf, B. J. Chapman, J. C. Curtis, N. Thakur, S. M. Girvin, and R. J. Schoelkopf, Error-detectable bosonic entangling gates with a noisy ancilla, PRX Quantum **4**, 020354 (2023).

[44] C.-Y. Lu, W.-B. Gao, J. Zhang, X.-Q. Zhou, T. Yang, and J.-W. Pan, Experimental quantum coding against qubit loss error, Proceedings of the National Academy of Sciences **105**, 11050 (2008).

[45] S. Ma, G. Liu, P. Peng, B. Zhang, S. Jandura, J. Claes, A. P. Burgers, G. Pupillo, S. Puri, and J. D. Thompson, High-fidelity gates and mid-circuit erasure conversion in an atomic qubit, Nature **622**, 279 (2023).

[46] P. Scholl, A. L. Shaw, R. B.-S. Tsai, R. Finkelstein, J. Choi, and M. Endres, Erasure conversion in a high-fidelity rydberg quantum simulator, arXiv preprint arXiv:2305.03406 (2023).

[47] H. Levine, A. Haim, J. S. Hung, N. Alidoust, M. Kalaee, L. DeLorenzo, E. A. Wollack, P. A. Arriola, A. Khalajhedayati, Y. Vaknin, *et al.*, Demonstrating a long-coherence dual-rail erasure qubit using tunable transmons, arXiv preprint arXiv:2307.08737 (2023).

[48] K. S. Chou, T. Shemma, H. McCarrick, T.-C. Chien, J. D. Teoh, P. Winkel, A. Anderson, J. Chen, J. Curtis, S. J. de Graaf, *et al.*, Demonstrating a superconducting dual-rail cavity qubit with erasure-detected logical measurements, arXiv preprint arXiv:2307.03169 (2023).

[49] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl, and M. Mussinger, Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes, Physical Review Letters **86**, 4402 (2001).

[50] T. M. Stace, S. D. Barrett, and A. C. Doherty, Thresholds for topological codes in the presence of loss, Physical review letters **102**, 200501 (2009).

[51] S. D. Barrett and T. M. Stace, Fault tolerant quantum computation with very high threshold for loss errors, Physical review letters **105**, 200502 (2010).

[52] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, Efficient erasure correcting codes, IEEE Transactions on Information Theory **47**, 569 (2001).

[53] A. Agresti and B. A. Coull, Approximate is better than "exact" for interval estimation of binomial proportions, The American Statistician **52**, 119 (1998).

[54] S. B. Wicker and V. K. Bhargava, *Reed-Solomon codes and their applications* (John Wiley & Sons, 1999).

[55] M. Hara, M. Watabe, T. Nojiri, T. Nagaya, and Y. Uchiyama, Two-dimensional code (Japan Patent, 07-254037,A(1995)), Toyota Central Research & Development Lab Inc.

[56] J. Proakis and M. Salehi, Digital communications, vol. 1221 (1987).

[57] S. Kawabata, Quantum interleaver: quantum error correction for burst error, Journal of the Physical Society of Japan **69**, 3540 (2000).

[58] J.-P. Tillich and G. Zémor, Quantum ldpc codes with positive rate and minimum distance proportional to the square root of the blocklength, IEEE Transactions on Information Theory **60**, 1193 (2013).

[59] N. Connolly, V. Londe, A. Leverrier, and N. Delfosse, Fast erasure decoder for a class of quantum ldpc codes, arXiv preprint arXiv:2208.01002 (2022).

[60] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. Hollenberg, Surface code quantum communication, Physical review letters **104**, 180503 (2010).

First-quantized adiabatic time evolution for quantum chemistry

Yusuke Nishiya[1 2 *] Hirofumi Nishi[1 2] Yannick Couzinié[1 2] Taichi Kosugi[1 2]
Yu-ichiro Matsushita[1 2 3]

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*
[2] *Quemix Inc., Taiyo Life Nihombashi Building, 2-11-2, Nihombashi Chuo-ku, Tokyo 103-0027, Japan*
[3] *Quantum Material and Applications Research Center, National Institutes for Quantum Science and Technology (QST), 2-12-1, Ookayama, Meguro-ku, Tokyo 152-8552, Japan*

Abstract. We propose an adiabatic time evolution (ATE) method for obtaining the ground state of a quantum many-electron system on a quantum circuit based on first quantization. It consists of only unitary operations representing real-time evolution, which can be implemented efficiently in the first-quantized formalism. We also provide a way to prepare an antisymmetrized and non-degenerate initial ground state that is suitable as an input to an ATE circuit. In addition, by considering a first-quantized Hamiltonian for quantum mechanical electron system and classical nuclear system, we design a quantum circuit for optimal structure search based on ATE.

Keywords: state preparation, first quantization, quantum chemistry

1 Introduction

Efficient calculation for the ground state of a given Hamiltonian is of crucial importance in a wide range of fields. This is because solving practically interesting problems can often be paraphrased as finding the ground state of a properly defined Hamiltonian. To this end, several schemes have been proposed realizing non-unitary operations to the system of interest on quantum circuits, such as imaginary-time evolution (ITE) [1, 2, 3, 4, 5]. On the other hand, there are widely known methods for ground-state calculation called adiabatic quantum computation (AQC) or quantum annealing (QA) [6, 7, 8], and these have attracted attention in the field of combinatorial optimization [9, 10] as well as quantum chemistry [11, 12, 13]. As examples of the application of AQC to quantum chemistry, some schemes utilizing adiabatic real-time evolution (RTE) for ground-state preparation have been proposed [14, 15, 16, 17, 18], all of which are based on second quantization. Kassal et al. [19] actually demonstrated that quantum computers can simulate the RTE within the first-quantized formalism in polynomial time while the computational cost using classical computers increases exponentially with system size. Moreover, the advantage of employing first quantization over second quantization is discussed in Ref. [20, 2, 3]. Specifically, the operation number per RTE step is evaluated as $\mathcal{O}(n_e^2 \mathrm{poly}(\log n_e))$ for the first quantization while it is $\mathcal{O}(n_e^4)$ for the second quantization due to the two-electron integrals in the Hamiltonian [21]. In this study, we describe a method to obtain the ground state of a many-electron system and the optimal ionic configuration using first-quantized adiabatic time evolutioin (ATE) on a quantum circuit and give an example of the construction of an appropriate initial Hamiltonian and its ground state.

*ynishiya@quemix.com

2 Construction of the quantum circuit

Encoding of wave function We encode the n_e-electron wavefunction confined in a cubic cell of size L using n_{qe} qubits for each spatial direction per electron, as usual in the first-quantized formalism [22, 23, 19, 2, 20, 24]. We refer to the $3n_e n_{qe}$ qubits collectively as the electronic register. We generate uniform grid points in the cell to encode the wavefunction ψ as

$$|\psi\rangle = \Delta V^{n_e/2} \sum_{\boldsymbol{k}_0,\ldots,\boldsymbol{k}_{n_e-1}} \psi\left(\boldsymbol{r}^{(\boldsymbol{k}_0)},\ldots,\boldsymbol{r}^{(\boldsymbol{k}_{n_e-1})}\right) \times |\boldsymbol{k}_0\rangle_{3n_{qe}} \otimes \cdots \otimes |\boldsymbol{k}_{n_e-1}\rangle_{3n_{qe}}\,, \tag{1}$$

where $\boldsymbol{k}_l$ is the vector of the three integers specifying the position eigenvalue $(k_{l_x}\boldsymbol{e}_x + k_{l_y}\boldsymbol{e}_y + k_{l_z}\boldsymbol{e}_z)\Delta x$ for the l-th electron. $\Delta x \equiv L/N_{qe}$ is the grid spacing of $N_{qe} \equiv 2^{n_{qe}}$ grid points in each spatial direction. $\Delta V \equiv \Delta x^3$ is the volume element for the normalization of $|\psi\rangle$.

Electronic structure optimization We define the time-dependent Hamiltonian for adiabatic time evolution (ATE) as

$$\hat{\mathcal{H}}(t) = \hat{T} + \hat{V}(t), \tag{2}$$

where $\hat{T}$ is the kinetic part and $\hat{V}(t)$ is the potential part. The boundary conditions of the potential part are $\hat{V}(0) = V_{\mathrm{ini}}$ and $\hat{V}(t_{\mathrm{f}}) = V_{\mathrm{fin}}$. By employing a first-order Suzuki-Trotter expansion in conjunction with the adiabatic theorem, the ground state $|\psi_{t_{\mathrm{f}}}^{\mathrm{gs}}\rangle$ of the objective Hamiltonian $\hat{\mathcal{H}}_{\mathrm{fin}} \equiv \hat{T} + \hat{V}_{\mathrm{fin}}$ is approximately given as

$$|\psi_{t_{\mathrm{f}}}^{\mathrm{gs}}\rangle \approx \prod_{m=N}^{1} \left[e^{-i\hat{T}\Delta t} e^{-i\hat{V}(t_m)\Delta t}\right] |\psi_0^{\mathrm{gs}}\rangle, \tag{3}$$

where $|\psi_0^{\mathrm{gs}}\rangle$ is the ground state of $\hat{\mathcal{H}}(0)$. The n_{qe}-qubit real-time evolution (RTE) operator generated by the kinetic energy per electron and per direction, $\hat{T}_\nu$ (ν =

x, y, z), can be implemented by using the centered quantum Fourier transform (CQFT) [25, 26] as

$$\mathrm{CQFT} U_{\mathrm{kin}}(\Delta t) \mathrm{CQFT}^{\dagger} = e^{-i\hat{T}_{\nu}\Delta t}, \tag{4}$$

where U_{kin} is diagonal matrix. $U_{\mathrm{pot}}^{(m)}$ is the real-time evolution by the potential part at $t = t_m$:

$$U_{\mathrm{pot}}^{(m)} \equiv e^{-i\hat{V}(t_m)\Delta t}. \tag{5}$$

If $\hat{V}(t)$ consists of the sum of the two-body interactions and the one-body external potential terms for all t, the same method as in Ref. [3] can be employed in order to implement $U_{\mathrm{pot}}^{(m)}$, and the operation number of one ATE step $e^{-i\hat{\mathcal{H}}(t_m)\Delta t}$ is estimated as $\mathcal{O}(n_e^2 \mathrm{poly}(\log n_e))$, thanks to the employment of position eigenstates in the basis of each electron's register.

Initial Hamiltonian and its ground state We describe an example of how to create an initial ground state that is non-degenerate and antisymmetric with respect to the exchange of any two electrons. This is important because antisymmetry of the electron wavefunction must be intentionally introduced in the first-quantized formalism, and if there is degeneracy in the initial ground state, the output state could be a superposition of the ground and excited states. This is achieved by considering as an initial state an n_e-electron system independently dominated by the one-electron Hamiltonian $\hat{\mathcal{H}}_1$ of an anisotropic harmonic oscillator as follows:

$$\hat{\mathcal{H}}_1 = \sum_{\mu=x,y,z} \left[\frac{\hat{p}_\mu^2}{2m_e} + \frac{1}{2} m_e \omega_\mu^2 \hat{r}_\mu^2 \right]. \tag{6}$$

The ground state is then obtained by the single Slater determinant created by the bottom n_e one-electron orbitals, which can be proved to be non-degenerate when, for instance, $(\omega_x, \omega_y, \omega_z) = (1, \sqrt{2}, \sqrt{3})$.

Ionic structure optimization Here we consider n_e quantum mechanical electrons and n_{nucl} classical nuclei system as in the case of structural optimization of molecular systems using probabilistic imaginary-time evolution (PITE) [3]. Thus the objective Hamiltonian is

$$\begin{aligned}\hat{\mathcal{H}}_{\mathrm{fin}} = &\underbrace{\sum_{l=1}^{n_e} \frac{\hat{\boldsymbol{p}}_l^2}{2m_e}}_{\equiv \hat{T}_{\mathrm{el}}} + \underbrace{\sum_{l=1}^{n_e} v_{\mathrm{ext}}(\hat{\boldsymbol{r}}_l)}_{\equiv \hat{V}_{\mathrm{ext}}} + \underbrace{\frac{1}{2}\sum_{l\neq l'} v_{ll'}^{(\mathrm{ee})}(|\hat{\boldsymbol{r}}_l - \hat{\boldsymbol{r}}_{l'}|)}_{\equiv \hat{V}_{\mathrm{ee}}} \\ &+ \underbrace{\sum_{l=1}^{n_e}\sum_{\lambda=1}^{n_{\mathrm{nucl}}} v_{l\lambda}^{(\mathrm{en})}(|\hat{\boldsymbol{r}}_l - \boldsymbol{R}_\lambda|)}_{\equiv \hat{V}_{\mathrm{en}}} \\ &+ \underbrace{\frac{1}{2}\sum_{\lambda\neq\lambda'} v_{\lambda\lambda'}^{(\mathrm{nn})}(|\boldsymbol{R}_\lambda - \boldsymbol{R}_{\lambda'}|)}_{\equiv \hat{V}_{\mathrm{nn}}},\end{aligned} \tag{7}$$

where v_{ext}, $v^{(\mathrm{ee})}$, $v^{(\mathrm{en})}$, and $v^{(\mathrm{nn})}$ represent the external potential for an electron, electron-electron interaction, electron-nucleus interaction, and nucleus-nucleus interaction, respectively. Note that the kinetic term of nuclei is ignored and the nuclear position $\boldsymbol{R}_\lambda$ appears as a classical parameter. To find the ground state of this Hamiltonian, we consider a quantum register using a total of $3n_e n_{qe} + n_{qn}$ qubits as

$$|\Psi\rangle = \sum_{\boldsymbol{J}} \sqrt{w_{\boldsymbol{J}}} |\psi[\boldsymbol{J}]\rangle_{3n_e n_{qe}} \otimes |\boldsymbol{J}\rangle_{n_{qn}}, \tag{8}$$

where n_{qn} is the number of qubits allocated to a register $|\boldsymbol{J}\rangle_{n_{qn}}$ representing a possible nuclear configuration specified by the vector $\boldsymbol{J}$. Due to the quantum superposition, up to $2^{n_{qn}}$ different structures can be entered at once. $|\psi[\boldsymbol{J}]\rangle_{3n_e n_{qe}}$ is an $3n_e n_{qe}$-qubit register representing the many-electron wavefunction for each configuration $\boldsymbol{J}$ in three dimensional space. The overall quantum register $|\Psi\rangle$ can be written as a superposition of $|\psi[\boldsymbol{J}]\rangle_{3n_e n_{qe}} \otimes |\boldsymbol{J}\rangle_{n_{qn}}$, and when $|\Psi_{\mathrm{f}}^{\mathrm{gs}}\rangle$ is obtained as the ground state of $\hat{\mathcal{H}}_{\mathrm{fin}}$, the most stable nuclear configuration can be determined by measuring the n_{qn} qubits assigned to the nuclear configuration part. To find the ground state of $\hat{\mathcal{H}}_{\mathrm{fin}}$ in Eq. (7) by ATE, we consider the time-dependent Hamiltonian

$$\begin{aligned}\hat{\mathcal{H}}(t) = &\hat{T}_{\mathrm{el}} \otimes \hat{I}_{\mathrm{nucl}} + A_1(t)\hat{V}_{\mathrm{ext}} \otimes \hat{I}_{\mathrm{nucl}} \\ &+ A_2(t)\hat{V}_{\mathrm{ee}} \otimes \hat{I}_{\mathrm{nucl}} + A_3(t)\hat{V}_{\mathrm{en}} \\ &+ A_4(t)\hat{I}_{\mathrm{el}} \otimes \hat{V}_{\mathrm{nn}} \\ &+ (1 - A_5(t))\hat{V}_0 \otimes \hat{I}_{\mathrm{nucl}} \\ &- (1 - A_6(t))\, \hat{I}_{\mathrm{el}} \otimes J_x \sum_{l=1}^{n_{qn}} \hat{X}_l,\end{aligned} \tag{9}$$

where $\hat{X}_l$ denotes the Pauli-X gate $\hat{\sigma}_x$ acting on the l-th qubit of the nuclear register and the boundary conditions for functions A_i ($i \in \{1, 2, 3, \cdots\}$) are $A_i(0) = 0$ and $A_i(t_{\mathrm{f}}) = 1$. Since there is no interaction between the electronic part and the nuclear part at $t = 0$, the ground state $|\Psi_0^{\mathrm{gs}}\rangle$ of the initial Hamiltonian $\hat{\mathcal{H}}(0)$ can be straightforwardly constructed as the tensor product of the ground states of each part as

$$|\Psi_0^{\mathrm{gs}}\rangle = |\psi_0^{\mathrm{gs}}\rangle_{3n_e n_{qe}} \otimes |+\rangle^{\otimes n_{qn}}, \tag{10}$$

where $|\psi_0^{\mathrm{gs}}\rangle_{3n_e n_{qe}}$ and $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ are the ground states of $\hat{T}_{\mathrm{el}} + \hat{V}_0$ and $-\hat{\sigma}_x$, respectively. The overview of the quantum circuit in this case is shown in Fig. 1. Note that the RTE by $\hat{\sigma}_x$ is represented by x-rotation R_x.

3 Results

This method is applied to some simple models for electronic structure calculation and ionic-position optimization. Fig. 2 shows the output of the electron density for a one-electron system in 1D space when the harmonic potential is introduced according to a linear schedule. Here, the time width δt is constant, and the output approaches the exact solution as the number of ATE steps N is increased and the change of the Hamiltonian with time is slowed down. Fig. 3 illustrates the results of the bond

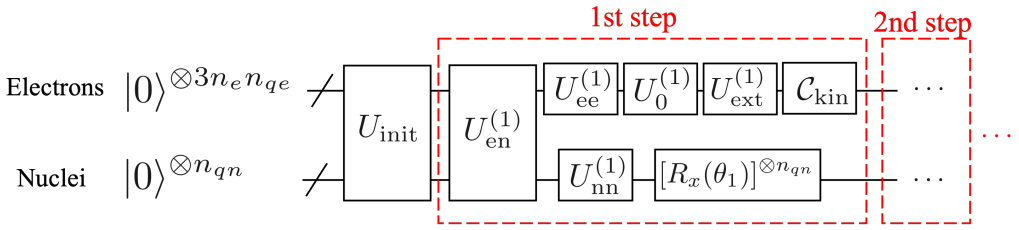


Figure 1: Quantum circuit to find the most stable nuclear configuration among up to $2^{n_{qn}}$ candidates. n_e-electron system in three-dimensional space are modelled and $3n_{qe}$ qubits per electron are used to represent the wavefunction of the electron system. After the ground state of the initial Hamiltonian is created by $U_{\rm init}$, ATE operation discretized into N steps follows. $\mathcal{C}_{\rm kin}, U_{\rm ext}^{(m)}, U_{\rm ee}^{(m)}, U_{\rm en}^{(m)}, U_{\rm nn}^{(m)}$, and $U_0^{(m)}$ represent the RTE generated by $\hat{T}, A_1(t_m)\hat{V}_{\rm ext}, A_2(t_m)\hat{V}_{\rm ee}, A_3(t_m)\hat{V}_{\rm en}, A_4(t_m)\hat{V}_{\rm nn}$, and $(1 - A_5(t_m))\hat{V}_0$, respectively.

length optimization for the H_2^+ molecular model. Here, $J = 0, 1, 2, 3$ correspond to bond lengths of 2,4,6,8 bohr, respectively, indicating that the probability of obtaining the most stable structure, $J = 0$, is highest for sufficiently large N.

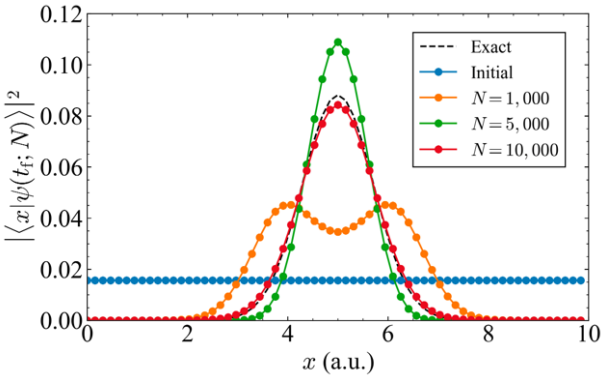


Figure 2: The simulation results of ATE for one electron system under the parabolic potential.The squared wavefunction of a electron after ATE over N steps with the linear scheduling function. The black dashed line represents the exact ground state obtained from the numerical diagonalization of the final Hamiltonian. The blue circles represent the ground state of initial Hamiltonian. The orange, green, and red circles represent the output state of ATE over 1000, 5000, and 10000 steps, respectively.

4 Conclusions

We have applied the first-quantized real-time evolution circuit and varied it adiabatically to construct a quantum circuit for the ground state calculation of the objective Hamiltonian. We also show that a non-degenerate and anti-symmetrized initial ground state in the case of general electron numbers can be prepared using the Slater determinant of a anisotropic harmonic oscillator. We further demonstrate that the method can be extended to search for the most stable structure among various ion configurations entered as quantum superposition states, and present a circuit for this purpose. We believe that our method is useful as one of the ground state calculation algorithms on fault-tolerant quantum computers,

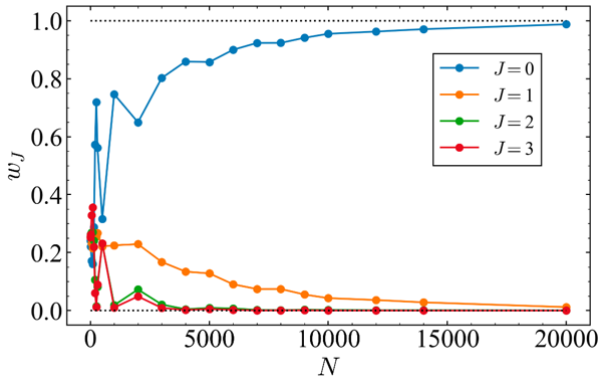


Figure 3: The simulation results of ATE for the search for the optimal bond length of an H_2^+ molecule. Plots of the probability w_J of obtaining the J-th structure when the nuclear register is observed with the linear scheduling function.

since it makes maximum use of the previously proposed efficient implementation of real-time evolution within the first-quantized formalism.

References

[1] T. d. L. Silva, M. M. Taddei, S. Carrazza, and L. Aolita. Fragmented imaginary-time evolution for early-stage quantum signal processors. quant-ph/2110.13180, 2021.

[2] T. Kosugi, Y. Nishiya, H. Nishi, and Y. Matsushita. Imaginary-time evolution using forward and backward real-time evolution with a single ancilla: First-quantized eigensolver algorithm for quantum chemistry. *Phys. Rev. Research*,4,033121, 2022.

[3] T. Kosugi, H. Nishi, and Y.-i. Matsushita. Exhaustive search for optimal molecular geometries using imaginary-time evolution on a quantum computer. *npj Quantum Information*, 9, 112, 2023.

[4] H.-N. Xie, S.-J. Wei, F. Yang, Z.-A. Wang, C.-T. Chen, H. Fan, and G.-L. Long. A Probabilistic Imaginary Time Evolution Algorithm Based on

Non-unitary Quantum Circuit. quant-ph/2210.05293, 2022.

[5] H. H. S. Chan, D. Muñoz-Ramo, and N. Fitzpatrick. Simulating non-unitary dynamics using quantum signal processing with unitary block encoding. quant-ph/2303.06161, 2023.

[6] T. Kadowaki and H. Nishimori. Quantum annealing in the transverse Ising model. *Phys. Rev. E*,58,5355, 1998.

[7] B. Apolloni, C. Carvalho, and D. de Falco. Quantum annealing in the transverse Ising model. *Stochastic Processes and their Applications*,33,233, 1989.

[8] T. Albash and D. A. Lidar. Adiabatic quantum computation. *Rev. Mod. Phys.*,90,015002, 2018.

[9] A. Lucas. Ising formulations of many NP problems. *Frontiers in Physics.*,2,5, 2014.

[10] W. Lechner., P. Hauke, and P. Zoller. A quantum annealing architecture with all-to-all connectivity from local interactions. *Science Advances.*,1,e1500838, 2015.

[11] R. Xia, T. Bian, and S. Kais. Electronic Structure Calculations and the Ising Hamiltonian. *J. Phys. Chem. B*,13,3384, 2018.

[12] J. Copenhaver, A. Wasserman, and B. Wehefritz-Kaufmann. Using quantum annealers to calculate ground state properties of molecules. *The Journal of Chemical Physics*,3,034105, 2021.

[13] A. Teplukhin, B. Kendrick, K. Brian, S. Tretiak, and P. A. Dub. Using quantum annealers to calculate ground state properties of molecules. *Scientific Reports*,10,20753, 2020.

[14] R. Babbush, P. J. Love, and A. Aspuru-Guzik. Adiabatic Quantum Simulation of Quantum Chemistry. *Scientific Reports*,4,6603, 2014.

[15] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon. Simulated Quantum Computation of Molecular Energies. *Science*,309,1704, 2005.

[16] L. Veis and J. Pittner. Adiabatic state preparation study of methylene. *The Journal of Chemical Physics*,140,214111, 2014.

[17] T. Shirakawa, K. Seki, and S. Yunoki. Discretized quantum adiabatic process for free fermions and comparison with the imaginary-time evolution. *Phys. Rev. Research*,3,013004, 2021.

[18] K. Sugisaki, K. Toyota, K. Sato, D. Shiomi, and T. Takui. Adiabatic state preparation of correlated wave functions with nonlinear scheduling functions and broken-symmetry wave functions. *Communications Chemistry*,5, 2022.

[19] I. Kassal, S. P. Jordan, P. J. Love, M. Mohseni, and A. Aspuru-Guzik. Polynomial-time quantum algorithm for the simulation of chemical dynamics. *Proceedings of the National Academy of Sciences*, 105, 18681, 2008.

[20] N. C. Jones, J. D. Whitfield, P. L. McMahon, M.-H. Yung, R. V. Meter, A. Aspuru-Guzik, and Y. Yamamoto. Faster quantum chemistry simulation on fault-tolerant quantum computers *New Journal of Physics*, 14, 115023, 2012.

[21] T. Helgaker, P. Jørgensen, and J. Olsen. Faster quantum chemistry simulation on fault-tolerant quantum computers In *Molecular Electronic-Structure Theory*, 2000.

[22] S. Wiesner. Simulations of Many-Body Quantum Systems by a Quantum Computer quant-ph/9603028, 1996.

[23] C. Zalka. Simulating quantum systems on a quantum computer *Proc. R. Soc. Lond. A.*, 454, 313, 1998.

[24] H. H. S. Chan, R. Meister, T. Jones, D. P. Tew, and S. C. Benjamin. Grid-based methods for chemistry simulations on a quantum computer *Science Advances*, 9, eabo7484, 2023.

[25] R. D. Somma. Quantum simulations of one dimensional quantum systems quant-ph/1503.06319, 2015.

[26] R. D. Somma. Nonadiabatic Molecular Quantum Dynamics with Quantum Computers *Phys. Rev. Lett.*, 125, 260511, 2020.

Secure Two-Party Computation using Photonic Graph States

Maxwell Gold[1] * Jianlong Lin[2] † Eric Chitambar[2] ‡ Elizabeth A. Goldschmidt[1] §

[1] *Department of Physics, University of Illinois Urbana-Champaign, Urbana, IL 61801*
[2] *Department of Electrical and Computer Engineering, Coordinated Science Laboratory, University of Illinois Urbana-Champaign, Urbana, IL 61801*

Abstract. Secure multi-party computation is a cryptographic primitive that enables two or more parties to privately compute some joint function of their inputs. While classical protocols are known for this task, they typically require private channels and/or multiple rounds of communication. In this work we introduce a method for two-party computation and restricted multi-party computation using small-sized photonic graph states and two rounds of public communication. The inputs of all honest parties are kept secure in our protocol. We also propose an experimental method for generating the necessary graph states used in the protocol and analyze its performance on current hardware.

Keywords: Multi-party computation, measurement-based computation, experimental implementations

1 Introduction

Secure multi-party computation (MPC) is a task in which two or more parties compute some function on their individually held variables without revealing the values of the variables to each other [1, 2]. MPC is a deeply-studied topic in both classical and quantum cryptography, and a variety of MPC protocols have been proposed achieving different levels of security and relying on different operational assumptions [3].

We propose an unconditionaly secure method for restricted MPC that includes all two-party computations and requires only two rounds of public communication regardless of the size of the computational input. Our scheme follows a well-known approach of decomposing MPC into "offline" and "online" phases [4, 5, 6]. In the offline phase, some universal computational resource is distributed to all the parties. Crucially, this resource does not depend on the particular function being computed other than its input size. Then in the online phase this resource is used to compute some chosen function of the parties' inputs. For example, in the classical setting one well-known computational resource is a special form of shared randomness known as "Beaver triples," which can be used to efficiently compute logical AND gates in the online phase [7]. The problem of MPC then reduces to secure and efficient methods for distributing Beaver triples in the offline phase. In a similar spirit, our protocol involves distributing certain quantum graph states in the offline phase which then enable the computation of a logical AND in the online phase. Beyond its relatively low communication costs, a significant advantage of our protocol is that the parties can, in principle, use self-testing methods to verify that some untrusted source is faithfully distributing the correct graph state [8, 9], an ability that does not exist for classical shared randomness.

*mjgold2@illinois.edu
†jl131@illinois.edu
‡echitamb@illinois.edu
§goldschm@illinois.edu

2 Contributions

This work provides a full theory-to-practice proposal for implementing secure two-party computation. The protocol uses eight-qubit graph states and works for functions of arbitrary size. We describe a realistic method for building these states using quantum emitters that also applies to the construction of more general graph states. The proposed use-case of secure computation and its practical implementation motivates a direction for developing quantum information deliverables in the near term.

3 Protocol Description

Boolean functions $f : \{0,1\}^{\times n} \to \{0,1\}$ are building blocks for arbitrary discrete functions. Suppose that N parties $\mathbf{P}_1, \mathbf{P}_2, \cdots, \mathbf{P}_N$ wish to compute some Boolean function $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$, where $\mathbf{x}_i$ is a string of bits representing the input for party i. In addition to correctness, the evaluation of f should be done securely such that the parties learn no more information about the individual $\mathbf{x}_1, \cdots, \mathbf{x}_N$ beyond their own input and what is revealed in the function value $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$. To achieve this task, we propose a method of delegated computation in which a non-collaborating Referee is introduced to assist in the computation of $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$. To maintain privacy, the Referee also should not learn any more information about the $\mathbf{x}_i$ beyond what is implied by the computed value $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$, nor does the Referee reveal anymore information to the other parties than this value.

The protocol uses the fact that every Boolean function f can be expressed in an algebraic normal form (ANF), which presents f as a sum (mod 2) of different variable conjunctions. That is, we can write $f = \sum_{i=1}^{\mathfrak{R}} c_i$, where each c_i is the logical AND of a certain group of input variables. By combining variables belonging to the same party, every c_i becomes the conjunction of at most N variables, each one belonging to a different party. In this work we restrict attention to functions f that admit an ANF whose conjunctions involve no

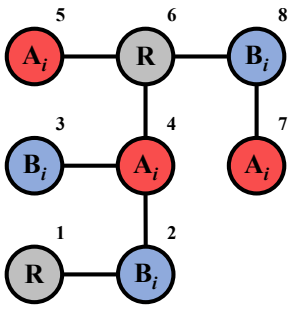


Figure 1: In Stage I, each computation of a padded AND, $b_i = x_i y_i + p_i$, is accomplished using a graph state $|G_I\rangle$ of this form. The qubits are distributed to parties $\mathbf{A}_i$ (Alice), $\mathbf{B}_i$ (Bob), and $\mathbf{R}$ (the Referee) as shown. The numeric script k above each qubit reflects an example photon emission order.

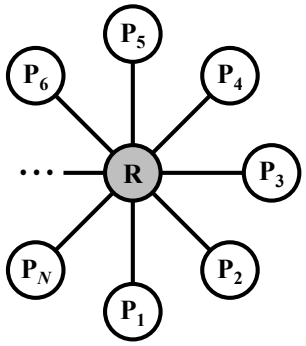


Figure 2: The graph state $|G_{\rm II}\rangle$ used to compute values p in Stage II. The numeric subscript labels both the party $\mathbf{P}_k$ and an example photon emission ordering. In total, $n_p = N + 1$ photons are required for the N parties and the Referee.

more than two variables. This covers the entire class of two-party functions, but it also includes certain multi-party functions, such as the three-party majority function $\varphi_3(x, y, z) = xy + xz + yz \mod 2$, which outputs the majority value among inputs $x, y, z \in \{0, 1\}$. In general, the functions we consider have the form $f = \sum_{i=1}^{\mathfrak{R}_1} x_i y_i + \sum_{i=1}^{N} z_i$, which is separated into linear and quadratic parts. By again combining variables, we can assume that z_i is held by party $\mathbf{P}_i$ and computed from her input $\mathbf{x}_i$. Furthermore, if each $\mathbf{x}_i$ is no more than M bits, then $\mathfrak{R}_1 \leq \binom{N}{2} M^2$.

The protocol involves performing Pauli observables, X, Y, Z, on two types of graph states, $|G_I\rangle$ and $|G_{II}\rangle$, depicted in Figs. 1 and 2 respectively. The distribution of these states is conducted during the offline phase of the protocol. In practice, the states can be generated by some untrusted quantum source, and their correctness can be certified using established self-testing methods [8, 9]. The online phase of the protocol then involves specific sequences of Pauli measurements and public communication, and these sequences take place in two different stages.

Stage I uses $|G_I\rangle$ to compute the bit values

$$b_i = x_i y_i + p_i, \qquad i = 1, \cdots, \mathfrak{R}_1, \tag{1}$$

where each p_i is an independent one-time pad bit that is private from all the parties, including the Referee.

Stage I. *Input:* Parties $\mathbf{A}_i$ (Alice) and $\mathbf{B}_i$ (Bob) input bits x_i and y_i, respectively.

1. The Referee and Bob measure X and Z on qubits 1 and 2, respectively, obtaining a common measurement outcome $s = m_1 = m_2$.

2. Bob measures Z on qubit 3, obtaining m_3. He announces $\delta_i = y_i + m_3$. Alice applies Z^{δ_i} to qubit 4.

3. Alice measures $W^{x_i} Z (W^\dagger)^{x_i}$ on qubits 4 and 5, where $W \equiv (iX)^{1/2}$, computing $\alpha_i = x_i + m_4 + m_5$ from her outcomes. Note that $WZW^\dagger = Y$.

4. The Referee measures $V^s X (V^\dagger)^s$ on qubit 6, where $V \equiv (-iZ)^{1/2}$, obtaining $b_i = m_6$. Note, $VXV^\dagger = Y$.

5. Alice measures Z on qubit 7, obtaining m_7. She announces $\gamma_i = x_i + m_7$. Bob applies Z^{γ_i} to qubit 8.

6. Bob measures $W^s Z (W^\dagger)^s$ on qubit 8 obtaining $\beta_i = m_8$.

It is not difficult to see that the Referee's measurement outcome in step 4. satisfies $b_i = x_i y_i + p_i$, where $p_i = \alpha_i + \beta_i$ (see the full manuscript for details). The above sequence is repeated on a fresh copy of $|G_I\rangle$ for each $i = 1, \cdots, \mathfrak{R}_1$, with the values of α_i and β_i possibly being obtained by different parties in each iteration. Note that if the Referee added all the b_i at the end of Stage I, the computed value would be

$$\sum_{i=1}^{\mathfrak{R}_1} b_i = f + \sum_{i=1}^{N} z_i + \sum_{i=1}^{\mathfrak{R}_1} (\alpha_i + \beta_i) = f + \sum_{i=1}^{N} \mu_i, \tag{2}$$

where μ_i denotes the sum of the variables in the set $\{\alpha_i, \beta_i\}_{i=1}^{\mathfrak{R}_1} \cup \{z_i\}_{i=1}^{N}$ belonging to party i. Stage II then amounts to removing the term $\sum_{i=1}^{N} \mu_i$ from the RHS of Eq. (2).

Stage II is performed using an $(N+1)$-party GHZ state $|G_{II}\rangle$ (see Fig. 2) shared between the Referee and the N parties. The following steps are then taken.

Stage II. *Input:* Parties $\mathbf{P}_i$ input their respective bits $\{\mu_i\}_{i=1}^{N}$ obtained from the set $\{\alpha_i, \beta_i\}_{i=1}^{\mathfrak{R}_1} \cup \{z_i\}_{i=1}^{N}$, as in Eq. (2). The Referee inputs $\{b_i\}_{i=1}^{\mathfrak{R}_1}$ from Stage I.

1. Party $\mathbf{P}_k$ measures Z on qubit k for qubits $1, \cdots, N$. She then announces $\nu_k = \mu_k + m_k$.

2. The Referee measures X to learn $\sum_{k=1}^{N} m_k$ and then adds this to $\sum_{k=1}^{N} \nu_k$ to obtain $\sum_{k=1}^{N} \mu_k$. The latter is then added to the sum $\sum_{i=1}^{\mathfrak{R}_1} b_i$ to obtain f, which is then announced to all the parties.

It should be noted that by parallelization, both Stages I and II can be performed using just two rounds of simultaneous communication. Indeed, each party needs

to broadcast at most two public messages, the first being no more than $\log \mathfrak{R}_1$ bits, and the second being one bit. When run in parallel, all the Stage I messages can be broadcast concurrently, and likewise for the Stage II messages.

Intuitively, this protocol is secure due to the one-time pad bits that are generated with each measurement on the graph states. While there are a variety of different approaches to defining security in multipartite computation, in this work we demand as a security condition that playing honestly does not reveal any more information about one's input than what can be inferred from the final function output. We demonstrate in the full version of this paper that our protocol satisfies this level of information-theoretic security. We also show how classical error correction can be incorporated in the protocol to suppress the effects of experimental error. Realistic estimates of performance are given in Figure 4.

4 Experimental Proposal

Photonic graph states can be generated using coherent emitters such as trapped neutral atoms or ions in vacuum [10, 11, 12, 13], physical systems which are attractive from an experimental perspective since they exhibit long coherence times ($10^0 - 10^3$ seconds) [14, 15] and host high-fidelity deterministic entangling gates ($> 99\%$) [16, 17, 18]. However, efficient collection from individual quantum emitters is a challenge that remains largely out of reach today, making the previous schemes impractical for generating large graph states on even near-term hardware [19].

In this work, we show how protocol described in Section 3 can be implemented using a single emitting spin and a fixed number of auxiliary spins, without any requirement on the collection efficiency of the emitted photons or any need for quantum memories. The rate and size of feasible graph states generated by the proposed method has polynomial dependence on the collection efficiency, compared to the exponential suppression of the feasible graph size for the successive detection of photons required in previous schemes. This enhanced performance is achieved by recognizing the possibility of adding each photon to the graph only after successful spin-photon entanglement generation has been heralded.

While a general method for building photonic graph states is comprehensively presented in the full paper, here we provide a high-level description of how $|G_I\rangle$ and $|G_{II}\rangle$ can be generated and used in the above protocol. The process involves a Herald-on-Detection scheme depicted in Fig. 3. To produce $|G_I\rangle$ (resp. $|G_{II}\rangle$) one needs to use a single spin emitter and two (resp. one) auxiliary spins. Entangling gates are performed on the spin systems in such a way that the emitted photons are transformed into the desired graph states [11]. In our scheme, we measure each photon immediately as its emitted as prescribed by the steps in Stage I and Stage II of the above protocol. These measurements not only herald the event of a successful emission, but as shown in the paper, up to classical post-processing they also generate the same

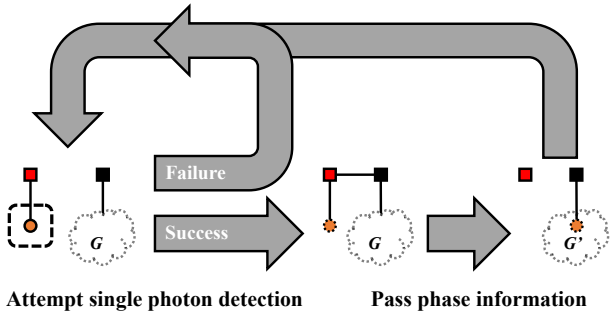


Figure 3: Herald-on-detection (HoD) scheme. An auxiliary spin (black square) is entangled to a graph G. A spin emitter (red square) is pumped, and if an emitted photon is detected, entangling gates between the two spins adds the now-measured photon to a new graph G'. The photonic graph state constructed in this case is virtual (represented by dashed boundaries) and exists as a set of conditional phases stored on auxiliary spins, which can be corrected by classical post-processing.

outcomes as if the measurements had taken place after the full graph were generated. The ability to convert stabilizer measurements into classical post-processing is well-known in the theory of measurement-based quantum computing [20]. However, to our knowledge this is the first time this principle has been being used as a heralding mechanism in an emitter-based protocol. Based on experimentally realistic parameters, Figure 4 shows an overall estimate for the rate of secure function evaluation using the protocol of Section 3 and its implementation described here in Section 4, given some error tolerance ϵ_f in the computation.

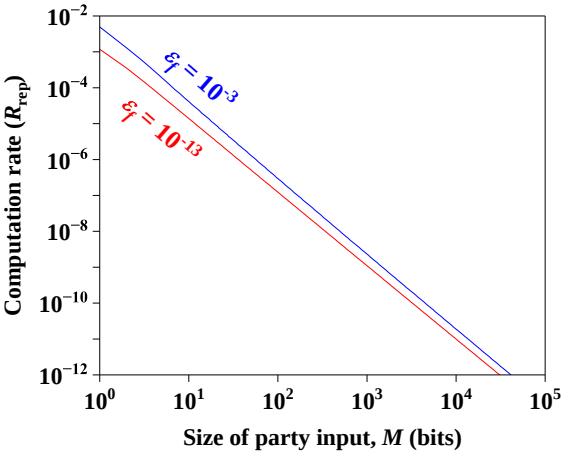


Figure 4: Error corrected two-party computation rate versus the number of input bits to f using our HoD scheme, shown for two acceptable error probabilities on the computation (ϵ_f). The rate is expressed in units of the repetition rate of excitation of the chosen quantum emitter, R_{rep}, which is typically in the range of $10^6 - 10^9$ s^{-1} for highly coherent emitters. Details of this calculation are explained in the full paper.

References

[1] Andrew C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 160–164, 1982.

[2] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM conference on Theory of computing - STOC '87*, STOC '87. ACM Press, 1987.

[3] Chuan Zhao, Shengnan Zhao, Minghao Zhao, Zhenxiang Chen, Chong-Zhi Gao, Hongwei Li, and Yu-an Tan. Secure multi-party computation: Theory, practice and applications. *Information Sciences*, 476:357–372, February 2019.

[4] Donald Beaver. *Efficient Multiparty Protocols Using Circuit Randomization*, page 420–432. Springer Berlin Heidelberg, 1992.

[5] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. *A New Approach to Practical Active-Secure Two-Party Computation*, page 681–700. Springer Berlin Heidelberg, 2012.

[6] Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. *Multiparty Computation from Somewhat Homomorphic Encryption*, page 643–662. Springer Berlin Heidelberg, 2012.

[7] Ashish Choudhury and Arpita Patra. An efficient framework for unconditionally secure multiparty computation. *IEEE Transactions on Information Theory*, 63(1):428–468, January 2017.

[8] Yuki Takeuchi, Atul Mantri, Tomoyuki Morimae, Akihiro Mizutani, and Joseph Fitzsimons. Resource-efficient verification of quantum computing using serfling's bound. *npj Quantum Information*, 5, 2019.

[9] Anupama Unnikrishnan and Damian Markham. Verification of graph states in an untrusted network. *Phys. Rev. A*, 105:052420, May 2022.

[10] Sophia E. Economou, Netanel Lindner, and Terry Rudolph. Optically generated 2-dimensional photonic cluster state from coupled quantum dots. *Phys. Rev. Lett.*, 105:093601, Aug 2010.

[11] Antonio Russo, Edwin Barnes, and Sophia E Economou. Generation of arbitrary all-photonic graph states from quantum emitters. *New Journal of Physics*, 21(5):055002, May 2019.

[12] Paul Hilaire, Leonid Vidro, Hagai S Eisenberg, and Sophia E Economou. Near-deterministic hybrid generation of arbitrary photonic graph states using a single quantum emitter and linear optics. *Quantum*, 7:992, 2023.

[13] Yuan Zhan and Shuo Sun. Deterministic generation of loss-tolerant photonic cluster states with a single quantum emitter. *Physical Review Letters*, 125(22):223601, 2020.

[14] Dolev Bluvstein, Harry Levine, Giulia Semeghini, Tout T. Wang, Sepehr Ebadi, Marcin Kalinowski, Alexander Keesling, Nishad Maskara, Hannes Pichler, Markus Greiner, Vladan Vuletić, and Mikhail D. Lukin. A quantum processor based on coherent transport of entangled atom arrays. *Nature*, 604(7906):451–456, April 2022.

[15] Pengfei Wang, Chun-Yang Luan, Mu Qiao, Mark Um, Junhua Zhang, Ye Wang, Xiao Yuan, Mile Gu, Jingning Zhang, and Kihwan Kim. Single ion qubit with estimated coherence time exceeding one hour. *Nature communications*, 12(1):1–8, 2021.

[16] Simon J. Evered, Dolev Bluvstein, Marcin Kalinowski, Sepehr Ebadi, Tom Manovitz, Hengyun Zhou, Sophie H. Li, Alexandra A. Geim, Tout T. Wang, Nishad Maskara, Harry Levine, Giulia Semeghini, Markus Greiner, Vladan Vuletić, and Mikhail D. Lukin. High-fidelity parallel entangling gates on a neutral-atom quantum computer. *Nature*, 622(7982):268–272, October 2023.

[17] R. Srinivas, S. C. Burd, H. M. Knaack, R. T. Sutherland, A. Kwiatkowski, S. Glancy, E. Knill, D. J. Wineland, D. Leibfried, A. C. Wilson, D. T. C. Allcock, and D. H. Slichter. High-fidelity laser-free universal control of trapped ion qubits. *Nature*, 597(7875):209–213, September 2021.

[18] Craig R. Clark, Holly N. Tinkey, Brian C. Sawyer, Adam M. Meier, Karl A. Burkhardt, Christopher M. Seck, Christopher M. Shappert, Nicholas D. Guise, Curtis E. Volin, Spencer D. Fallek, Harley T. Hayden, Wade G. Rellergert, and Kenton R. Brown. High-fidelity bell-state preparation with $^{40}CA^{+}$ optical qubits. *Physical Review Letters*, 127(13), September 2021.

[19] Dan Cogan, Zu-En Su, Oded Kenneth, and David Gershoni. Deterministic generation of indistinguishable photons in a cluster state. *Nature Photonics*, 17(4):324–329, February 2023.

[20] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, Aug 2003.

Heralded arbitrary graph states with inefficient quantum emitters

Maxwell Gold,[1,*] Jianlong Lin,[2,*] Eric Chitambar,[2] and Elizabeth A. Goldschmidt[1]

[1] *Department of Physics, University of Illinois Urbana-Champaign, Urbana, IL 61801*
[2] *Department of Electrical and Computer Engineering, University of Illinois Urbana-Champaign, Urbana, IL 61801*

(Dated: May 21, 2024)

Quantum emitter-based schemes for the generation of photonic graph states offer a promising, resource efficient methodology for realizing distributed quantum computation and communication protocols on near-term hardware. We present a heralded scheme for making photonic graph states that is compatible with the typically poor photon collection from state-of-the-art coherent quantum emitters. We demonstrate that the construction time for large graph states can be polynomial in the photon collection efficiency, as compared to the exponential scaling of current emitter-based schemes, which assume deterministic photon collection. The additional overhead to achieve this advantage consists of an extra spin system plus one additional spin-spin entangling gate per photon added to the graph. While the proposed scheme enables the generation of graph states for arbitrary applications, we show how it can be further simplified for the specific task of measurement-based computation, leading to significantly higher rates and removing the need for photonic memory in certain computations. As an example use-case of our scheme, we construct a protocol for secure two-party computation that can be implemented efficiently on current hardware. Estimates of the fidelity to produce graph states used in the computation are given, based on current trapped ion experimental benchmarks.

I. INTRODUCTION

The vast promise of quantum information technologies for faster and more secure computational and information systems relies on entanglement as a primary resource. Traditional gate-based quantum computing requires the ability to perform sequences of joint operations across multiple qubits.An alternative paradigm, known as measurement-based quantum computation (MBQC), realizes universal computation through sequences of single qubit measurements made on an initially prepared entangled resource state [1]. This is an appealing approach for photonic quantum systems as single photon rotations and measurements are straightforward using commercial optical elements, and fast efficient routing solutions are readily available [2]. Furthermore, the sequential nature of photon emission allows entangled states to be built from photons emitted at different times by the same emitter [3]. By using entangled emitters, it then becomes possible to simulate entangling gates between photons and overcome the difficulty of realizing direct photon-photon interactions [4]. Indeed, it is known that computationally useful graph states of photons can be generated using either a small number of coherent quantum emitters [5], a combination of a single emitter and fusion gates [6], or a single quantum emitter in a feedback scheme [7].

All of these aforementioned schemes assume a photon is successfully added to the graph every time an emitter is excited, and we thus term this class of schemes as being "deterministic". However, efficient collection from individual quantum emitters is a challenge that remains largely out of reach today, making deterministic schemes impractical for generating large graph states on even near-term hardware [8].

We introduce a procedure for building arbitrary photonic graph states using a single emitting spin and a fixed number of auxiliary spins, without any requirement on the collection efficiency of the emitted photons. The rate and size of feasible graph states generated by the proposed method has polynomial dependence on the collection efficiency, compared to the exponential suppression of the feasible graph size for the successive detection of photons required in current deterministic schemes. This enhanced performance is achieved by recognizing the possibility of adding each photon to the graph only after successful spin-photon entanglement generation has been heralded.

In Section II of this work, we describe a non-destructive method for this heralding that is implementable on current hardware by swapping the entanglement to another photon, termed the herald-on-swap (HoS) method. More generally, any non-destructive detection of the photon would be suitable to implement this "emit-then-add" method of building graphs for arbitrary use. We explain in Section III how we can herald on destructive detection of the photon in certain cases, including MBQC. This enables much higher production rates and fidelities than any feasible non-destructive heralding method. In this case, the emitted photon is measured prior to adding it to the graph, thereby abrogating the need for entanglement swapping or photon storage, and dramatically speeding up graph construction. In this case, the graph state is built only virtually as every photon in the graph is necessarily measured. We refer to this as a herald-on-detection (HoD) method, and Section III provides more detail on when the HoD method can be applied.

In both the HoS and HoD schemes we propose, the

* These two authors contributed equally

photons are emitted over a longer time compared to other emitter-based methods for building photonic graph states; this is because most attempts to add a photon to the graph will result in an unsuccessful herald. Consequently, it is the number of excitation attempts that can be made during the coherence time of the emitter that sets the practical limit on the graph size, rather than the collection efficiency. Trapped neutral atoms and ions in vacuum are well suited to this scheme as they exhibit long coherence times ($10^0 - 10^3$ seconds) [9, 10] and host high-fidelity deterministic entangling gates ($> 99\%$) [11–13] with moderate collection efficiencies ($\gtrsim 10\%$ with high-NA optics and $\gtrsim 40\%$ with parabolic reflectors) [14–17]. We note here that some solid-state systems, such as rare-earth emitters, can also exhibit excellent coherence, spin-spin entangling gates, and reasonable photon collection via integration into photonic devices [18]. In Section IV we provide estimates of the rate and fidelity for the production of heralded graph states via both of our schemes assuming state-of-the-art trapped ion and photon pair source architectures, which include realistic sources of loss, noise, and decoherence.

Lastly, in Section V we propose a protocol for performing secure two-party classical computation, in which two parties privately compute a function of their input variables with the help of an untrusted referee. Compared to universal quantum computation, our protocol only requires Pauli measurements, and so the entire procedure can be performed using only our HoD method. We demonstrate how secure two-party computation can be achieved using just a single quantum emitter and two auxiliary spin qubits, regardless of the size of the party's input. We provide fidelity estimates to produce the graph states on current hardware, which suggests this is a highly feasible use-case for quantum networks in the near term. A security analysis and the resulting bit error rates with and without classical error correction are also provided.

II. SPIN-PHOTON ENTANGLEMENT SCHEMES

We first describe the HoS scheme, shown in Figure 1, for making graph states for arbitrary applications. Given the technical challenges associated with photon non-demolition measurement [19], this swapping step is required to herald without destructive measurement of the photonic qubit on near-term hardware. Compared to the deterministic scheme described in [5], we include a local entanglement swapping step between an emitter-photon entangled pair and a pair of entangled photons, and only add the final photon to the graph upon success of that swap. A single emitter is initialized into an unentangled state and excited to produce a single photon that is entangled with its long-lived internal spin state and collected with some overall efficiency η_e. This can be implemented with a wide variety of quantum emitters including laser-cooled atoms or ions, quantum dots, and defects or dopants in wide-bandgap semiconductors [3, 8, 20–22]. Photons can be encoded in various degrees of freedom including polarization, time-bin, and frequency [23–27]. Simultaneously, a pair of entangled photons is probabilistically produced, which can be implemented via standard nonlinear optical processes, such as spontaneous parametric down conversion (SPDC) [28, 29]. One member of the photon pair, the signal photon, is wavelength and bandwidth matched to the emitter photon, and the entangled pair is encoded in the same degree of freedom as the emitter photon. The emitter photon and signal photon are sent to a joint measurement apparatus which, upon a successful measurement outcome, projects the emitter spin and the unmeasured photon, the idler photon, into an entangled Bell state [30]. Since only certain measurement outcomes correspond to entanglement between the emitter spin and idler photon, and imperfect collection and detection means that fewer than two photons are detected on most attempts, the procedure is repeated until a successful herald is flagged. Following each failed attempt, the emitter is measured and reinitialized for the subsequent attempt at a successful herald.

We assume the emitter is among a set of spin qubits that can be controllably entangled in a pair-wise way via local and deterministic two-qubit spin-spin entangling gates, such as an array of trapped atomic ions or neutral atoms. Upon a successful herald, the emitter spin is deterministically entangled with an auxiliary spin, which may already be part of a larger graph state. The emitter spin is then rotated to a conjugate basis and projectively measured, removing it from the graph without disturbing any of the other qubits. Following a correction to the photon based on the outcome of this measurement, the state of the system is as if the auxiliary spin had directly emitted the photon itself. This "emit then add" method then allows for the construction of arbitrary photonic graph states using the methods described in [5]. Namely, the graph states are built using sequences of two-qubit gates on the spins and local Clifford gates on the photons. The local gates on each photon can all be combined and applied as a single rotation prior to using the graph state in subsequent applications.

The key improvement in our scheme is that the idler photon can be collected with near unit efficiency upon a successful herald [31]. Attaining the improvement of this scheme requires one additional two-qubit spin-spin entangling gate per photon added to the graph plus one additional spin (the emitter), compared to the requirements for generating graphs via known deterministic schemes [32]. In addition, the graph is emitted over a much longer time and thus requires longer spin coherence times. We note an additional benefit of the scheme in that the idler photon can be at virtually any wavelength due to the flexibility of standard entangled photon pair sources [33–36], which overcomes common challenged due to the inconvenient emission colors of many atomic qubits. We show here that current state-of-the-art trapped ion sys-

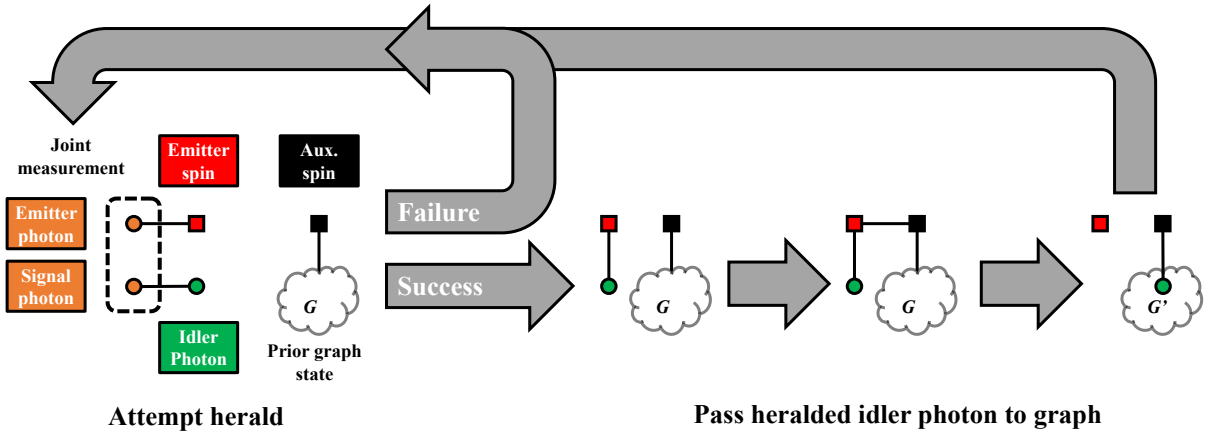


FIG. 1. Herald-on-swap (HoS) scheme. The components are two initial entangled pairs: an emitter spin (red square) entangled with a photon (orange circle) and a signal-idler entangled photon pair (orange and green circle, respectively). We also assume an existing graph G that contains one or more auxiliary spins (black square). Entanglement swapping is attempted between the two initial entangled pairs. Upon success, a two-qubit spin-spin gate deterministically entangles the emitter spin and auxiliary spin. A local complementation operation is then performed on the emitter spin, which is subsequently measured out of the graph. This leaves the idler photon a part of the graph and the emitter spin reinitialized for the next attempted emission.

tems can be designed to produce graph states of tens to hundreds of photons using the proposed method, where extending to thousands would be made possible with reasonable improvements [10, 12, 14].

III. A HERALDING SCHEME FOR MBQC

The HoS scheme described in the previous section, or any non-destructive heralding of successful collection of the emitter photon, can be used to build arbitrary photonic graph states. However for many applications, including MBQC, the nodes are measured sequentially with the choice of measurement basis on one node depending on outcomes of previous ones. It is not necessary in this case to build the full graph state before beginning these measurements [37]. Instead, an emitted photon can be destructively measured as soon as the correct basis for measurement is determined. This measurement thus serves doubly as a prescribed step in the MBQC protocol and as a way for detecting the emitted photon. Upon failure to detect the photon, we re-initialize the emitter and attempt generation again, having left the larger graph undisturbed, as in the HoS scheme. Upon successful detection, we perform all required gates on the emitter and auxiliary spins, measure the emitter out of the graph, and re-initialize the emitter to attempt generation of the next photon in the graph.

This simpler HoD scheme is shown in Figure 2, and it has the advantage that it requires no storage time for the emitted photon prior to measurement. There are limitations for when this scheme can be employed. Namely, a photon can be measured using HoD provided the two conditions are satisfied: (1) the correct measurement basis for that photon, as set by the MBQC protocol, is determined prior to its emission, and (2) this measurement is either Pauli Z or of the form $\cos\phi X + \sin\phi Y$. Condition (1) can be met in general, as the emission order can be chosen to match the measurement of order of the computation, albeit at the cost of using extra auxiliary spins and two-qubit gates in some cases [32]. The second condition can also be met in principle, since the specified gates sets are sufficient for universal MBQC [1, 38].

To understand condition (2) in more detail, note that if the full graph state were built using HoS and two-qubit gates on the auxiliary spins, then each emitted photon would have a local Clifford error of the form UZ^m, where U is a fixed Clifford and $m \in \{0, 1\}$ is determined by the decoupling measurement on the emitter spin. If M is the measurement to be subsequently performed on the photon in the MBQC protocol, then when correcting for the Clifford error, the effective measurement would be $M' = UZ^m M Z^m U^\dagger$. When $M = Z$, then $M' = UZU^\dagger$; or when $M = \cos\phi X + \sin\phi Y$, then $M' = (-1)^m UZU^\dagger$. In the first case, the dependence on m is completely removed, and the photon can be equivalently measured with $UZU^\dagger$ immediately after it is emitted in the HoD scheme. In the second case, it can also be immediately measured with $UZU^\dagger$, but now one must perform a bit flip on the classical measurement outcome if $m = 1$; this is because an overall -1 factor on a spin observable simply flips the spin-up/spin-down outcomes. In summary, the correct computation can be attained through HoD and classical post-processing for observables of the specified form.

While satisfying conditions (1) and (2) above is suffi-

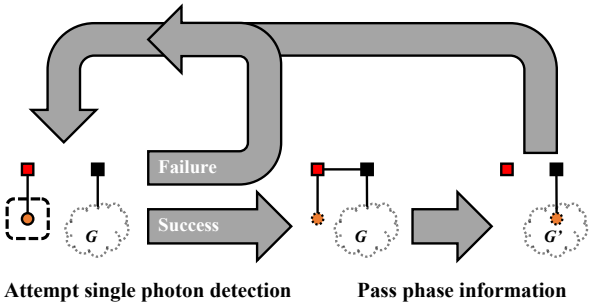


FIG. 2. Herald-on-detection (HoD) scheme. For certain MBQC protocols, it is sufficient to perform the deterministic entangling gate between the emitter and auxiliary spin only upon successful detection of the emitted photon. The photonic graph state constructed in this case is virtual (represented by dashed boundaries) and exists as a set of conditional phases stored on auxiliary spins.

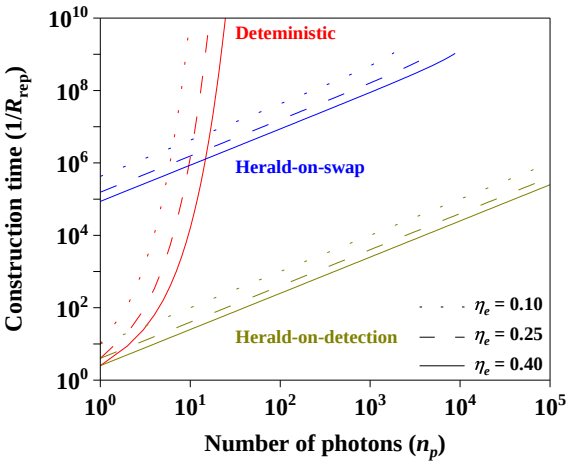


FIG. 3. Time to make photonic graph states of size n_p in units of the repetition period. The deterministic (red), HoS (blue), and HoD (yellow) schemes are compared. The three curves of each color represent emitter photon detection efficiencies $\eta_e \in \{0.1, 0.25, 0.4\}$. Polynomial scaling in the heralded schemes allows for the construction of larger graphs. Results are omitted where decoherence and false heralds bring the fidelity under 50% for reasonable experimental parameters. In the HoS scheme, fidelity can be sacrificed to improve the rate for the construction of small graph states if desired. Details of the fidelity estimates are introduced in Section I, with a full description given in Appendix D.

cient for universal MBQC using HoD, this is often not the most efficient method in terms of the overall number of photons used to drive the computation. For example, building out the graph to a certain depth and measuring in a different sequence than the emission order can lead to more compact gate implementations [38]. Also, using MBQC measurements outside of the x-y plane allows for more general forms of information flow [39]. Nevertheless, as we show in the next section, the HoD scheme can enable dramatically faster construction and higher fidelity with no photon storage required. For the HoS (or any non-destructive heralding) scheme, photon storage is required for at least the time to perform the spin-spin entangling gates and the decoupling measurement on the emitter.

IV. SCALING AND FIDELITY FOR HERALDED SCHEMES

A major benefit of both schemes comes in scaling up the size of graph states using near term hardware. The average time to successfully generate an n_p-photon graph by directly collecting photons from an emitter in n_p subsequent excitation events for computation is $\mathcal{O}(\eta_e^{-n_p})$, where η_e is the emitter collection efficiency, because any failed detection event truncates the graph. In typical deterministic quantum emitter-based schemes, any inefficiency in collection therefore leads to exponentially bad scaling with graph size. Given current hardware, this severely limits the size and rate of generation for photonic graph states, particularly those that require multiple spin qubits. We note that there are loss tolerance and percolation thresholds that improve this scaling, but they require much better collection efficiency than is feasible in near-term systems [40–42]. For the heralded schemes, any failed detection of the emitter photon simply results in the reinitialization of the emitter and another attempt at the joint or single photon detection, while the graph under construction remains unaffected. Therefore, an n_p-photon graph state will be created over a time that is $\mathcal{O}(n_p\eta_e^{-1})$. As a comparison, the time to make an n_p-photon graph state (in units of the repetition period) is shown in Figure 3 for $\eta_e \in \{0.1, 0.25, 0.4\}$ for the deterministic (red), HoS (blue), and HoD (yellow) schemes. We assume that the emitter coherence does not limit the graph size for the deterministic scheme ($n_p/\tau R_{\rm rep} \ll 1$ where τ is the spin coherence time and $R_{\rm rep}$ is the repetition rate of excitation). In practice, however, the short coherence times of the most efficient photon emitters further limit the size of graphs that can be produced in the deterministic scheme [8, 27]. For the heralded schemes, all auxiliary spins must remain coherent for the entire time they are a part of the graph, which is much longer than the n_p repetition cycles over which the graph is generated in the deterministic scheme. Thus, moving from the deterministic scheme to one proposed here effectively means moving from a scheme limited by the photon collection efficiency to a scheme limited by spin coherence. If a hybrid of the HoS and HoD schemes is employed, the generation time falls somewhere between the curves for those schemes, with the fraction of photons generated via each method determining exactly where.

For the two proposed schemes, there are additional factors that affect the fidelity not present in the determinis-

tic scheme including decoherence of the emitter and auxiliary spin(s) during the construction time and multiple photon pair production that limits the fidelity of entanglement swapping for the the HoS scheme. Here we investigate the scaling of these sources of infidelity and compare them to the limits set by imperfect two-qubit spin-spin entangling gates, as well the initial entanglement fidelities of the emitter-photon and photon pair sources. We require one such gate per photon added to the graph over and above any gates required to make the desired final graph [32], which exponentially suppresses the ability to make large photonic graph states if the gates are not perfect. Additionally, any infidelity of the photon-pair source in the HoS scheme adds to the overall infidelity. Here, we demonstrate that if sufficient error correction or entanglement purification is possible [43], the additional sources of infidelity inherent to our scheme do not themselves prohibit exceeding large graph states. For a full discussion of our experimental model and relevant sources of infidelity, see Appendix D.

In modeling decoherence under the usual dephasing map, any emitters or auxiliary spins will remain invariant with a probability $D(t,\tau) = \frac{1}{2}(1+e^{-t/\tau})$, for the duration t until they are projectively measured. In either scheme, the emitter is reinitialized with each attempt to add a new photon to the larger graph, and hence the time its required to remain coherent is reset. Furthermore, the classical conditioning offered by this "emit then add" method means the emitter is only required to remain coherent for the attempts where the relevant joint or single photon measurements are a success. Any auxiliary spins, on the other hand, are required to remain coherent for the duration of time they remain a part of the larger graph state in construction. The average time for successful addition of a new photon to the larger graph goes as t_{rep}/P_s, where $t_{\text{rep}} = R_{\text{rep}}^{-1}$ is the repetition period of the excitation, and P_s is the probability of a successful joint or single photon measurement for the HoS or HoD schemes, respectively. Note that in the HoD scheme we assume $P_s = \eta_e$. Hence, the total contribution to the final state fidelity from the emitter and any auxiliary spins is

$$F_D^{(e)}(n_p) = \left(\frac{1}{2}\left(1+e^{-t_{\text{rep}}/\tau}\right)\right)^{n_p}, \tag{1a}$$

$$\langle F_D^{(s)}(n_p,P_s)\rangle = \frac{1}{2}\left(1+e^{-n_p t_{\text{rep}}/P_s\tau}\right), \tag{1b}$$

where we include a superscript to denote emitter (e) and auxiliary spin (s) qubits, and we have used the same coherence time τ for the emitter and auxiliary spins in the system.

For the HoS scheme we assume a standard SPDC source to generate the required entangle photons pairs [44]. The multi-pair emission of such a source introduces an additional infidelity in the entanglement swapping procedure. We denote P_t as the the overall probability that a true Bell state is heralded and measured after constructing the graph. In general, $P_t < P_s$ due to false heralding. A primary source of false heralding is when the emitter photon is not collected but the SPDC source produces two or more photon pairs that lead to a detection pattern falsely signalling a successful swap. False heralding due to two signal photons is a well known and ubiquitous problem in entanglement swapping with photon pair sources based on nonlinear optics [33]. We can write an expression for the fidelity of the entanglement swapping procedure, P_t/P_s, using the known statistical distribution of entangled photon pairs produced via SPDC. Here, we assume photon number-resolved detection and perfect collection and detection of the signal photon once produced. This is because loss on that channel can generally be minimal and primarily affects the rate rather than the swapping fidelity (see Appendix D for the full calculation, including further experimental factors not discussed here). Furthermore, the intention here is to show that even quite low efficiency collection of the emitter photon can allow the generation of graph states. The probability of producing two entangled photon pairs is proportional to the square of the probability of producing a single entangled pair, and is controllable via the pump power of the SPDC (parameterized here by the quantity ξ [33]), thus introducing a tradeoff between rate and fidelity. The fidelity, $F_{\text{swap}} = P_t/P_s$, is given by

$$P_t(\eta_e,\xi) = \eta_e(1-\xi)^2\xi, \tag{2a}$$

$$P_s(\eta_e,\xi) = \left[\eta_e\xi + (1-\eta_e)\xi^2\right](1-\xi)^2, \tag{2b}$$

$$F_{\text{swap}}(\eta_e,\xi) = \frac{\eta_e}{\eta_e + (1-\eta_e)\xi}. \tag{2c}$$

In the absence of decoherence of the spins, we could simply work at $\xi \ll 1$ (very low pair generation rate) to reduce the false heralding and increase the overall fidelity. However, this slows the rate of the graph production and introduces infidelity due to decoherence of the auxiliary spin(s). Given a set of experimental parameters, the rate of pair production can be optimized by tuning ξ to maximize the overall fidelity of the desired graph state, balancing the infidelity due to false heralds against the decoherence.

We present a simple example comparing these additional sources of infidelity to the limits set by spin-spin entangling gates and initial entanglement fidelities, for case of the constructing a graph state on a single auxiliary spin. Figure 4 depicts these estimates over a few regimes. The combined effect of false heralds and decoherence (blue) set the fidelity as

$$F(n_p,\eta_e,\xi) = F_{\text{swap}}(\eta_e,\xi)^{n_p} F_D^{(e)}(n_p) \times \langle F_D^{(s)}(n_p, P_s(\eta_e,\xi))\rangle, \tag{3}$$

which we optimize over ξ, for fixed n_p and η_e. We assume the same coherence time for the emitter and auxiliary spin. When only limited by decoherence (yellow), we can employ the same Equation 3, except now fixing $F_{\text{swap}}(\eta_e,\xi) = 1$ and removing the need to optimize the fidelity. These estimates are applicable when construction large star graph states—the local-unitary equivalent

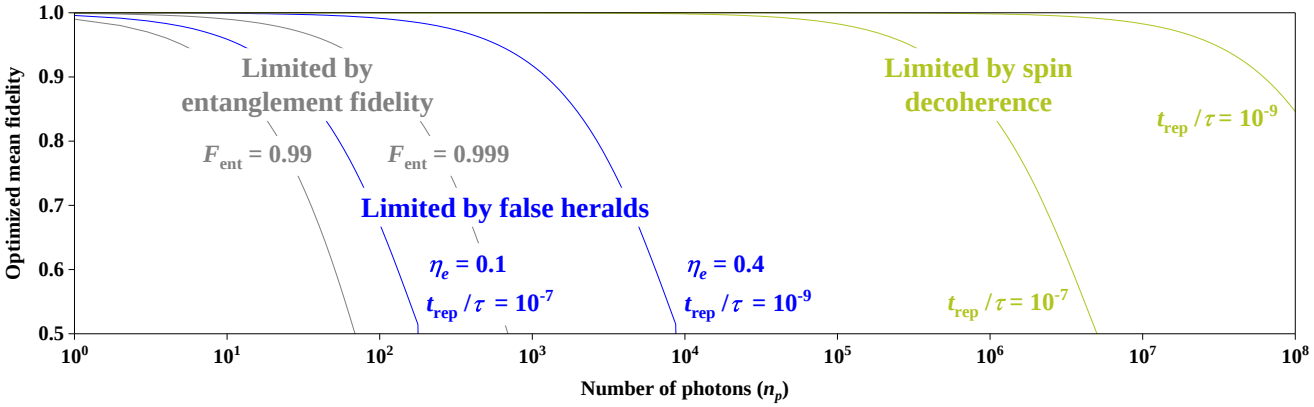


FIG. 4. Graph state fidelity versus photon number (n_p) for several different regimes of operations, and variable emitter-photon collection efficiencies (η_e) and dephasing timescales ($t_{\rm rep}/\tau$). Gate and pair generation fidelities (grey) exponentially preclude the construction of large graph states in any scheme utilizing our "emit then add" method. With sufficient error correction or purification around these gate fidelities, regimes limited by false heralds and decoherence (blue) and decoherence alone (yellow), allow for the construction of significantly larger graph states.

to a Greenberger-Horne-Zeilinger (GHZ) state—and 1D cluster states.

V. REALIZING SECURE TWO-PARTY COMPUTATION

As one application of our HoD scheme, we describe a method for securely computing an arbitrary Boolean function $f : \{0,1\}^{\times n} \to \{0,1\}$ of either two parties or a restricted class of multi-party functions. As a special type of MBQC, our protocol performs the calculation through a sequence of measurements on distributed graph states. Only Pauli measurements are needed and the protocol can be implemented using the HoD method, for which the generation of the requisite resource state happens in parallel with the computation and no photonic memory is required.

Secure multi-party computation (MPC) is a task in which two or more parties compute some function on their individually held variables without revealing the values of the variables to each other [45, 46]. For example, in Yao's famous millionaire problem, two parties want to determine whose bank account has the most money without actually revealing how much money is in each account. MPC is a deeply-studied topic in both classical and quantum cryptography, and a variety of MPC protocols have been proposed achieving different levels of security and relying on different operational assumptions [47]. We propose an unconditionaly secure method for restricted MPC that includes all two-party computations and requires only two rounds of public communication regardless of the size of the computational input. Our scheme follows a well-known approach of decomposing MPC into "offline" and "online" phases [48–50]. In the offline phase, some universal computational resource is distributed to all the parties. Crucially, this resource does not depend on the particular function being computed other than its input size. Then in the online phase this resource is used to compute some chosen function of the parties' inputs. For example, in the classical setting one well-known computational resource is a special form of shared randomness known as "Beaver triples," which can be used to efficiently compute logical AND gates in the online phase [51]. The problem of MPC then reduces to secure and efficient methods for distributing Beaver triples in the offline phase. In a similar spirit, our protocol involves distributing certain quantum graph states in the offline phase which then enable the computation of a logical AND in the online phase. Beyond its relatively low communication costs, a significant advantage of our protocol is that the parties can, in principle, use self-testing methods to verify that some untrusted source is faithfully distributing the correct graph state [52, 53], an ability that does not exist for classical shared randomness.

Suppose that N parties $\mathbf{P}_1, \mathbf{P}_2, \cdots, \mathbf{P}_N$ wish to compute some Boolean function $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$, where $\mathbf{x}_i$ is a string of bits representing the input for party i. In addition to correctness, the evaluation of f should be done securely such that the parties learn no more information about the individual $\mathbf{x}_1, \cdots, \mathbf{x}_N$ beyond their own input and what is revealed in the function value $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$. To achieve this task, we propose a method of delegated computation in which a non-collaborating Referee is introduced to assist in the computation of $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$. To maintain privacy, the Referee also should not learn any more information about the $\mathbf{x}_i$ beyond what is implied by the computed value $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$, nor does the Referee reveal anymore information to the other parties than this value.

The protocol uses the fact that every Boolean function f can be expressed in an algebraic normal form (ANF), which presents f as a sum (mod 2) of different vari-

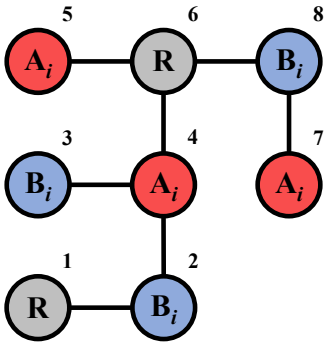


FIG. 5. In Stage I, each computation of a padded AND, $b_i = x_i y_i + p_i$, is accomplished using a graph state $|G_I\rangle$ of this form. The qubits are distributed to parties $\mathbf{A}_i$ (Alice), $\mathbf{B}_i$ (Bob), and $\mathbf{R}$ (the Referee) as shown. The numeric script k above each qubit reflects an example photon emission order.

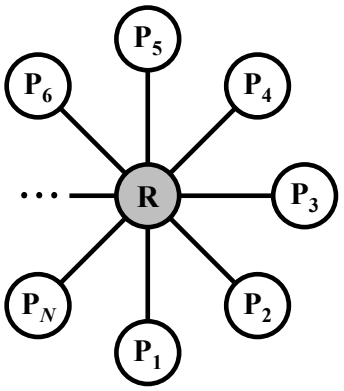


FIG. 6. The graph state $|G_{\rm II}\rangle$ used to compute values p in Stage II. The numeric subscript labels both the party $\mathbf{P}_k$ and an example photon emission ordering. In total, $n_p = N + 1$ photons are required for the N parties and the Referee.

able conjunctions. That is, we can write $f = \sum_{i=1}^{\mathfrak{R}} c_i$, where each c_i is the logical AND of a certain group of input variables. By combining variables belonging to the same party, every c_i becomes the conjunction of at most N variables, each one belonging to a different party. In this work we restrict attention to functions f that admit an ANF whose conjunctions involve no more than two variables. This covers the entire class of two-party functions, but also includes certain multi-party functions, such as the three-party majority function $\varphi_3(x, y, z) = xy + xz + yz \mod 2$, which outputs the majority value among inputs $x, y, z \in \{0, 1\}$. In general, the functions we consider have the form $f = \sum_{i=1}^{\mathfrak{R}_1} x_i y_i + \sum_{i=1}^{N} z_i$, which is separated into linear and quadratic parts. By again combining variables, we can assume that z_i is held by party $\mathbf{P}_i$ and computed from her input $\mathbf{x}_i$. Furthermore, if each $\mathbf{x}_i$ is no more than M bits, then $\mathfrak{R}_1 \leq \binom{N}{2} M^2$.

The protocol involves performing Pauli observables, X, Y, Z, on two types of graph states, $|G_I\rangle$ and $|G_{II}\rangle$, depicted in Figs. 5 and 6 respectively. The distribution of these states is conducted during the offline phase of the protocol. In practice, the states can be generated by some untrusted quantum source, and their correctness can be certified using self-testing methods (see Appendix B 4). Specific steps for building both $|G_I\rangle$ and $|G_{II}\rangle$ using a quantum emitter is presented in Appendix C 2. We note that the nontrivial emission order on $|G_I\rangle$ set by our MPC requires two auxiliary spins to produce [32]. The online phase of the protocol then involves specific sequences of Pauli measurements and public communication, and these sequences take place in two different stages.

Stage I uses $|G_I\rangle$ to compute the bit values

$$b_i = x_i y_i + p_i, \qquad i = 1, \cdots, \mathfrak{R}_1, \tag{4}$$

where each p_i is an independent one-time pad bit that is private from all the parties, including the Referee.

Stage I. *Input:* Parties $\mathbf{A}_i$ (Alice) and $\mathbf{B}_i$ (Bob) input bits x_i and y_i, respectively.

1. The Referee and Bob measure X and Z on qubits 1 and 2, respectively, obtaining a common measurement outcome $s = m_1 = m_2$.

2. Bob measures Z on qubit 3, obtaining m_3. He announces $\delta_i = y_i + m_3$. Alice then applies Z^{δ_i} to qubit 4.

3. Alice measures $W^{x_i} Z (W^\dagger)^{x_i}$ on qubits 4 and 5, where $W \equiv (iX)^{1/2}$, computing $\alpha_i = x_i + m_4 + m_5$ from her outcomes. Note that $WZW^\dagger = Y$.

4. The Referee measures $V^s X (V^\dagger)^s$ on qubit 6, where $V \equiv (-iZ)^{1/2}$, obtaining $b_i = m_6$. Note that $VXV^\dagger = Y$.

5. Alice measures Z on qubit 7, obtaining m_7. She announces $\gamma_i = x_i + m_7$. Bob then applies Z^{γ_i} to qubit 8.

6. Bob measure $W^s Z (W^\dagger)^s$ on qubit 8 obtaining $\beta_i = m_8$.

As shown in Appendix B 1, the Referee's measurement outcome in step 4. satisfies $b_i = x_i y_i + p_i$, where $p_i = \alpha_i + \beta_i$. The above sequence is repeated on a fresh copy of $|G_I\rangle$ for each $i = 1, \cdots, \mathfrak{R}_1$, with the values of α_i and β_i possibly being obtained by different parties in each iteration. Note that if the Referee added all the b_i at the end of Stage I, the computed value would be

$$\sum_{i=1}^{\mathfrak{R}_1} b_i = f + \sum_{i=1}^{N} z_i + \sum_{i=1}^{\mathfrak{R}_1} (\alpha_i + \beta_i) = f + \sum_{i=1}^{N} \mu_i, \tag{5}$$

where μ_i denotes the sum of the variables in the set $\{\alpha_i, \beta_i\}_{i=1}^{\mathfrak{R}_1} \cup \{z_i\}_{i=1}^{N}$ belonging to party i. Stage II then amounts to removing the term $\sum_{i=1}^{N} \mu_i$ from the RHS of Equation (5).

Stage II is performed using an $(N+1)$-party GHZ state $|G_{II}\rangle$ (see Figure 6) shared between the Referee and the N parties. The following steps are then taken.

Stage II. *Input:* Parties $\mathbf{P}_i$ input their respective bits $\{\mu_i\}_{i=1}^{N}$ obtained from the set $\{\alpha_i, \beta_i\}_{i=1}^{\mathfrak{R}_1} \cup \{z_i\}_{i=1}^{N}$, as in Equation (5). The Referee inputs $\{b_i\}_{i=1}^{\mathfrak{R}_1}$ obtained from Stage I.

1. Party $\mathbf{P}_k$ measures Z on qubit k for qubits $1, \cdots, N$. She then announces $\nu_k = \mu_k + m_k$.

2. The Referee measures X to learn $\sum_{k=1}^{N} m_k$ and then adds this to $\sum_{k=1}^{N} \nu_k$ to obtain $\sum_{k=1}^{N} \mu_k$. The latter is then added to the sum $\sum_{i=1}^{\mathfrak{R}_1} b_i$ to obtain f, which is then announced to all the parties.

It should be noted that by parallelization, both Stages I and II can be performed using just two rounds of simultaneous communication. Indeed, each party needs to broadcast at most two public messages, the first being no more than $\log \mathfrak{R}_1$ bits, and the second being one bit. When run in parallel, all the Stage I messages can be broadcast concurrently, and likewise for the Stage II messages.

Intuitively, this protocol is secure due to the one-time pad bits that are generated with each measurement on the graph states. While there are a variety of different approaches to defining security in multipartite computation, in this work we demand as a security condition that playing honestly does not reveal any more information about one's input than what can be inferred from the final function output. We prove in Appendix B 3 that our protocol satisfies this condition.

Performance. To handle experimental errors in the above protocol, we can employ a simple repetition code to suppress the effects of any infidelity in our ability to make $|G_I\rangle$ and $|G_{II}\rangle$ on the output of the computation f. By determining the total bit error probability when computing each b_i in Stage I and p in Stage II, an arbitrarily small total bit error probability ϵ_f on the computation output f can be chosen to set the number of repetitions required for each Stage I and II, respectively. We use this information to estimate the lower bound rate of computation at which N parties can compute f on their M-bit inputs. Details are proved in Appendix B 2.

Functionally, our protocol allows for the secure implementation of any two-party Boolean function, f. Using the fidelity estimates established in Sec I and detailed in App D, we can conservatively estimate the maximum possible bit error probability in either Stage from the compliment of the probability that no bit error occurs, that is, the probability to successfully generate $|G_I\rangle$ and $|G_{II}\rangle$ in our proposed HoD scheme. In Figure 7, we plot

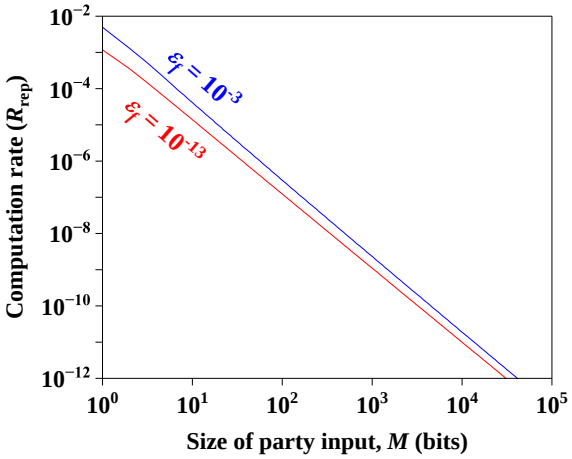


FIG. 7. Error corrected two-party computation rate versus the number of input bits to f using the HoD scheme, shown for two acceptable error probabilities on the computation (ϵ_f). The rate is expressed in units of the repetition rate of excitation of the chosen quantum emitter, R_{rep}, which is typically in the range of $10^6 - 10^9$ s^{-1} for highly coherent emitters. The individual bit error probabilities for Stage I and Stage II, respectively, are 0.008 and 0.003, assuming $\eta_e = 0.4$, $F_{\text{ent}} = 0.999$, and $t_{\text{rep}}/\tau = 10^{-9}$ (see. Appendix D for details). We see that these parameters allow virtually unlimited reduction in the total error probability with minimal change in the overall rate.

the lower bound rate of computation at which our protocol can operate with error correction, in units R_{rep}, against the size of each parties input, M, for total acceptable error probabilities $\epsilon_f = \{10^{-3}, 10^{-13}\}$.

VI. DISCUSSION AND CONCLUSION

The schemes introduced here naturally lend themselves to various extensions and modifications to increase functionality. First, combining with a high degree of multiplexing, such as between many arrays of atoms or ions, would increase the generation rate with a linear factor in the degree of multiplexing. Incorporating this with heralding means that photons can be routed upon successful generation of spin-photon entanglement. Another extension is the opportunity for substantial spectral engineering of the idler photon in the HoS scheme. As mentioned above, the idler photon can be produced at virtually any arbitrary wavelength regardless of the emission wavelength of the emitter spin (including using a superconducting qubit as the spin and generating a signal-idler pair with a microwave signal and an optical idler [54]). We also point out that the bandwidth of the idler photon can be different than the, typically narrow and fixed, bandwidth of the emitter. Filtering, time lensing [55], and/or source engineering [22, 56] can enable substantial

broadening or narrowing of the idler photon compared to the emitter photon.

In this work we have demonstrated the feasibility of generating photonic graph states with inefficient quantum emitters, and give a central example of its applications to secure multi-party computation. Significantly, our schemes offer polynomial scaling in the time to construct graph states of hundreds of photons with a high fidelity on current generation trapped ion experiments [12, 13], even when the collection efficiency of emitter photons is poor. The "emit-then-add" approach requires additional resource costs for making graph states, but we show that it is feasible with current and near-term experimental hardware. Our scheme is a toolbox for making large entangled photonic states for MBQC and other applications that are limited by spin decoherence rather than photon collection efficiency. We specifically show an application to realization distributed multi-party computation with reasonable improvements to current hardware.

ACKNOWLEDGMENTS

We acknowledge helpful discussions with Kejie Fang. E.C. thanks Christian Schaffner for some helpful guidance on mutli-party computation. This work was supported by the NSF Quantum Leap Challenge Institute on Hybrid Quantum Architectures and Networks (NSF Award No. 2016136).

Appendix A: Preliminaries on graph states

For an arbitrary graph $G = (V, E)$ with vertices $V = \{a_1, \cdots, a_n\}$ and edge set $E \subset V \times V$, consider the n-qubit operator obtained by performing a controlled$-Z$ gate, $CZ_{a,b}$, between every $(a, b) \in E$. We denote this global operator by

$$U_G = \prod_{(a,b)\in E} CZ_{a,b}. \tag{A1}$$

The graph state associated with the graph G is the n-qubit state

$$|G\rangle = U_G |+\rangle^{\otimes V}. \tag{A2}$$

Note that $|+\rangle^{\otimes n}$ is stabilized by n commuting operators $\{X_a\}_{a\in V}$. Hence the stabilizer of $|G\rangle$ can be understood by examining the how the X_a transform under U_G. Since $CZ_{a,b}(X_a)CZ_{a,b} = X_a Z_b$, it follows that the stabilizer of $|G\rangle$ is generated by the operators $\{K_a\}_{a\in V}$, where

$$\begin{aligned} K_a &= U_G X_a U_G \\ &= X_a \prod_{b\in N_a} Z_b \\ &= X_a \prod_{b\in V} Z_b^{\Gamma_{a,b}} \qquad \forall a \in V, \end{aligned} \tag{A3}$$

and Γ is the adjacency matrix of G.

For any n-qubit graph state $|G\rangle$, we can generate an orthonormal basis for $\mathbb{C}_2^N$, called the associated graph basis. The basis vectors have the form

$$Z^{\mathbf{r}} |G\rangle \quad \text{where} \quad Z^{\mathbf{r}} := Z_1^{r_1} \otimes Z_2^{r_2} \otimes \cdots \otimes Z_N^{r_N}, \tag{A4}$$

and we will call $\mathbf{r} = (r_1, r_2, \cdots, r_n) \in \mathbb{Z}_2^n$ a conditional phase vector and each bit r_k *phase information* for qubit k. To see that these states are orthogonal, let $\mathbf{r}$ and $\mathbf{r}'$ be two distinct conditional phase vectors, and suppose their bit values differ in position a. Then K_a will anti-commute with $Z^{\mathbf{r}} Z^{\mathbf{r}'}$, and so

$$\langle G| Z^{\mathbf{r}} Z^{\mathbf{r}'} |G\rangle = \langle G| Z^{\mathbf{r}} Z^{\mathbf{r}'} K_a |G\rangle = -\langle G| K_a Z^{\mathbf{r}} Z^{\mathbf{r}'} |G\rangle = -\langle G| Z^{\mathbf{r}} Z^{\mathbf{r}'} |G\rangle. \tag{A5}$$

We will be particularly interested in how the graph basis states transform under the local Pauli measurements of Y and Z. For a binary vector $\mathbf{r} \in \mathbb{Z}_2^n$ and subset of nodes $S \subset V$, let $\mathbf{r} - S$ denote the vector of length $n - |S|$ obtained from $\mathbf{r}$ by removing the coordinates in S. Suppose that for an initial graph basis state $Z^{\mathbf{r}} |G\rangle$, either Y or

Z is measured on qubit a and outcome $m_a \in \{0,1\}$ is received. The initial state transforms as follows:

$$Z_a: \quad Z^{\mathbf{r}} |G\rangle \mapsto \left(\prod_{b \in N_a} Z_b^{m_a} \right) Z^{\mathbf{r}-a} |G-a\rangle , \tag{A6a}$$

$$Y_a: \quad Z^{\mathbf{r}} |G\rangle \mapsto \left(\prod_{b \in N_a} (-iZ_b)^{1/2} Z_b^{r_a+m_a} \right) Z^{\mathbf{r}-a} |\tau_a(G)-a\rangle , \tag{A6b}$$

where $\tau_a(G)$ is the local complementation of G at vertex a, i.e. $\tau_a(G)$ is the graph $(V, E\Delta E(N_a, N_a))$, and $\tau_a(G)-a$ is the graph obtained by removing a from $\tau_a(G)$ [57]. Explicitly,

$$|\tau_a(G)\rangle = (-iX_a)^{1/2} \left(\prod_{b \in N_a} (iZ_b)^{1/2} \right) |G\rangle , \tag{A7}$$

describes a set of single-qubit rotations comprising a local complementation. Note that the Y_a post-measurement state can always be transformed back to the associated graph basis by performing $(iZ_b)^{1/2}$ on each $b \in N_a$. For the special case of measurement at a leaf in the graph, a vertex with only a single neighbor such that $\tau_a(G) = G$, the Y_a post-measurement state after rotation back to the graph basis is effectively a Z_a post-measurement state up to the conditional phase flip $Z_b^{r_a}$.

1. Phase transmission along a chain

Consider the effect of locally measuring along some linear chain in graph G. Let $a_1, a_2, a_3, \cdots, a_n, a_{n+1}$ denote the constituent qubits, with a_1 being the first node in the chain and a_{n+1} being the final node, which is connected to the remainder of the graph and left unmeasured in this sub-routine. The specific measurement sequence consists of measuring Y on a_1 and $(-iZ)^{1/2} Y (iZ)^{1/2} = -X$ on a_k for all $k = 2, \cdots, n-1$. If the total state prior to measurement is a graph basis state $Z^{\mathbf{r}} |G\rangle$ and $(m_{a_1}, \cdots, m_{a_{n-1}})$ is the binary sequence of outcomes from these measurements, then by Equation (A6b) the overall state evolution is

$$Y_{a_1}, (-X_{a_2}), \cdots, (-X_{a_{n-1}}): \quad Z^{\mathbf{r}} |G\rangle \mapsto [-iZ_{a_n}]^{1/2} Z_{a_n}^{\Omega} Z^{\mathbf{r}-\{a_1,\cdots,a_{n-1}\}} |G-\{a_1,\cdots,a_{n-1}\}\rangle , \tag{A8}$$

where $\Omega = \sum_{i=1}^{n-1} (r_{a_i} + m_{a_i}) \mod 2$. Crucially, each m_{a_k} is a random bit uncorrelated from $\mathbf{r}$ and any other measurement data. Hence, we can think of each m_{a_k} as a one-time pad that is added to the conditional phase information r_{a_k} when passing from node a_k to a_{k-1}.

2. Phase transmission at a fork

Consider the effect of measuring two qubits, a and b, that are connected to a single common node c. Suppose the total state prior to measurement is a graph basis state $Z^{\mathbf{r}} |G\rangle$. If m_a and m_b denote the binary outcomes when either Y or Z is measured on both qubits, the respective state transformations are given by

$$Y_a, Y_b: \quad Z^{\mathbf{r}} |G\rangle \mapsto Z_c^{r_a+r_b+1} Z_c^{m_a+m_b} Z^{\mathbf{r}-\{a,b\}} |G-\{a,b\}\rangle , \tag{A9a}$$

$$Z_a, Z_b: \quad Z^{\mathbf{r}} |G\rangle \mapsto Z_c^{m_a+m_b} Z^{\mathbf{r}-\{a,b\}} |G-\{a,b\}\rangle , \tag{A9b}$$

up to an overall phase. Hence, the key difference between the two measurements is that Y_a, Y_b transfers the conditional phase flip $Z_c^{r_a+r_b+1}$ onto the state $|G-\{a,b\}\rangle$ while Z_a, Z_b does not.

Appendix B: Secure multi-party computation

We verify correctness and prove security of our multi-party computation protocol detailed in Section II, using the preliminaries of Appendix A. The measurement sequences described in Stages 1 and 2 together accomplish the computation of any Boolean function up to quadratic order in the parties' inputs. We verify these sequences by tracing through the transformation of the graph states $|G_I\rangle$ and $|G_{II}\rangle$ used in each part of the protocol, and the information that is transmitted along the graph in the form of phase flips conditioned on both the parties' inputs and their measurements. We establish the security of this process by demonstrating that the classically communicated information in the protocol reveals no new information to any of the other parties about their input, other than what they would learn from the final output of the computation.

1. Correctness

To verify correctness for the computation of f, we track the evolution of phase information as defined in Appendix A through both phases of the protocol. A graph state $|G\rangle$ consisting of n qubits, labelled $1, \cdots, n$, is initialized. We denote $\mathbf{m} = (m_1, \cdots, m_n)$ as the binary vector of measurement outcomes for each of the qubits. In general, measurements change the shape of the graph disconnecting the measured qubit and applying conditional phase flips on its neighbors. As the labeling we assigned represents a possible photon emission ordering for generating the graph state in a quantum emitter based experimental scheme, it is convenient to keep this labeling for each qubit despite transformations in the graph induced by the measurement sequence.

a. Stage I

Stage I details the measurement sequence performed on $|G_I\rangle$, requisite for computing each $b_i = x_i y_i + p_i$ in the first phase. Let x_i and y_i be the input for the parties $\mathbf{A}_i$ and $\mathbf{B}_i$, respectively. We will refer to $\mathbf{A}_i$ and $\mathbf{B}_i$ as Alice and Bob, although in general these labels change for different $i \in \{1, 2, \cdots, \mathfrak{R}_1\}$. The measurement outcome m_k denotes the measurement m of the k^{th} qubit in the eight-qubit graph state, depicted in Figure 5. For simplicity, we suppress any additional subscript denoting the iteration of Stage I and reset these labels with each new copy of $|G_I\rangle$.

In step (1.), the Referee's X measurement on qubit 1 decouples Bob's qubit 2 from the rest of the graph. This leads to correlated outcomes $s = m_1 = m_2$ as the parties are each measuring an independent component of the generator $X_1 Z_2$ that stabilizes the state. From Eqs. A6a and A8, we see this adds the conditional phase flip Z_4^s to Alice's qubit. In step (2.), Bob's measurement of qubit 3 introduces a conditional phase flip $Z_4^{m_3}$ on Alice's qubit. Her subsequent rotation of the qubit, using Bob's announced $\delta_i = y_i + m_3$, transforms the state such that the total conditional phase on her qubit is described by $Z_4^{y_i+s}$. Alice then in step (3.) performs a measurement at a fork on qubits 4 and 5, conditioned on her own input x_i, and obtains $\alpha_i = x_i + m_4 + m_5$. From Eqs. A9a and A9b, we see that the total conditional phase applied to the Referee's qubit 6 from this step is $Z_6^{x_i(y_i+s+1)+m_4+m_5} = Z_6^{x_i(y_i+s)+\alpha_i}$. In steps (4.) and (6.), the pad s informs the Referee and Bob the correct basis to measure their respective qubits, in order to obtain a correlated outcome. In more detail, the parties each measure their independent component of the generator $X_6 Z_8$ or $Y_6 Y_8$, conditioned on whether $s = 0$ or $s = 1$, respectively. Note that if $s = 0$ the Referee's measurement in step (4.) decouples the remaining two qubits, shared between Alice and Bob, and leaves Bob's qubit invariant under the action of step (5.) That is, the combined action of Alice and Bob in step (5.) produces a conditional phase $Z_8^{sx_i}$ on Bob's qubit. Hence, step (6.) produces a correlated outcome between the parties' measurements and prior phase information such that

$$(x_i(y_i + s) + \alpha_i) + b_i + (sx_i) + \beta_i = 0. \tag{B1}$$

where we denote $b_i = m_6$ belonging to the Referee and $\beta_i = m_8$ belonging to Bob, and the Referee obtains

$$b_i = x_i y_i + p_i \qquad (\text{where } p_i = \alpha_i + \beta_i), \tag{B2}$$

as desired.

b. Stage II

Correctness is proved for Stage II in the same way as before, where now each party is labeled by a $\mathbf{P}_k$, for $k = 1, \cdots, N$. We again let $\mathbf{m} = (m_1, \cdots, m_N, m_{\text{R}})$ represent the binary vector of measurement outcomes from each party on the $N + 1$ qubit graph state, depicted in Figure 6. We note that the ordering of the labels need not be tied to a particular photon emission ordering, as all the measurements performed commute with each other and all classically communicated information need only be shared after each party's measurement.

We first recognize that each party is measuring an independent component of the generator, $X_{\text{R}} Z_1 \cdots Z_N$, of this graph state. This implies for the Referee's outcome m_{R} that

$$m_{\text{R}} + \sum_{k=1}^{N} m_k = 0. \tag{B3}$$

This is equivalent to the notion that the measurement of each party $\mathbf{P}_k$ in step (1.) introduces a conditional phase flip Z^{m_k} on the Referee's qubit, such that total action on the Referee's qubit is $\prod_k Z^{m_k}$. The Referee can determine

the value of p by adding their outcome m_k to sum of the parties announces $\nu_k = \mu_k + m_k$, such that

$$p = m_{\rm R} + \sum_{k=1}^{N} \nu_k = \sum_{i=1}^{\mathfrak{R}_1} (\alpha_i + \beta_i) + \sum_{k=0}^{\mathfrak{R}_2} z_i, \tag{B4}$$

and subsequently the output of the computation

$$f = p + \sum_{i=1}^{\mathfrak{R}_1} b_i = \sum_{i=1}^{\mathfrak{R}_1} x_i y_i + \sum_{i=1}^{\mathfrak{R}_2} z_i. \tag{B5}$$

2. Including Error Correction

In practice, each bit conjunction computed in Stage I of the protocol as well as the final summation computed in Stage II will have some error. In this section we describe a basic error correction method that can be employed to suppress the overall computational error as much as desired.

Let ϵ_* denote the largest probability of a bit error in each iteration of Stage I, and let Ξ_i be the indicator variable for the occurrence of an error in iteration i. Thus, while the noiseless protocol generates bit value $b_i = x_i y_i + p_i$ in iteration i, the actual implementation generates bit value

$$b_i = x_i y_i + p_i + \Xi_i. \tag{B6}$$

To deal with this, the Referee can employ a simple repetition code. That is, each iteration i is repeated K_I times, from which the Referee obtains values $b_{(i,1)}$, $b_{(i,2)}, \cdots, b_{(i,K_I)}$, where $b_{(i,j)} = x_i y_i + p_{(i,j)} + \Xi_{(i,j)}$. Recalling that $p_{(i,j)} = \alpha_{(i,j)} + \beta_{(i,j)}$ is the sum of Alice and Bob's private bits, for each $j = 2, \cdots, K_I$, Alice and Bob announce to the Referee messages $\alpha_{(i,1)} + \alpha_{(i,j)}$ and $\beta_{(i,1)} + \beta_{(i,j)}$, respectively. The Referee adds these to each corresponding $b_{(i,j)}$ so that his K_I bit values have the form $b_{(i,j)} = x_i y_i + p_i + \Xi_{(i,j)}$, where $p_i = \alpha_{(i,1)} + \beta_{(i,1)}$. Note that each $\alpha_{(i,j)}$ and $\beta_{(i,j)}$ is an independent private random bit for Alice and Bob, so the announcements of $\alpha_{(i,1)} + \alpha_{(i,j)}$ and $\beta_{(i,1)} + \beta_{(i,j)}$ do not reveal any information about $\alpha_{(i,1)}$ and $\beta_{(i,1)}$. The Referee then performs majority voting on the bit values $b_{(i,j)}$, accepting the value appearing the most among the K_I sub-iterations. By Hoeffding's inequality, this value will be $b_i = x_i y_i + p_i$ with a bit error rate $\delta \leq \exp\Big[-2K_I(\frac{1}{2} - \epsilon_* - \frac{1}{2K_I})^2\Big]$. Then, the combined bit error rate in computing $\sum_{i=1}^{\mathfrak{R}_1} b_i$ is equal to the probability that an odd number of bit errors occur among the b_i. A counting argument shows this probability to be

$$\epsilon_I = \frac{1}{2}[1 - (1-2p)^{\mathfrak{R}_1}] \leq \delta \mathfrak{R}_1 \leq \mathfrak{R}_1 \cdot \exp\Big[-2K_I(\tfrac{1}{2} - \epsilon_* - \tfrac{1}{2K_I})^2\Big]. \tag{B7}$$

Note that to suppress the bit error rate, the number of repetitions K_I needed for each iteration i is exponentially smaller than the total number of iterations $\mathfrak{R}_1$.

Moving to Stage II, there will be a separate bit error rate ϵ_+ in the Referee's computation of p using the state $|G_{II}\rangle$. Again, a repetition code can be used by repeating this step K_{II} times and achieving an overall bit error rate on p of $\epsilon_{II} \leq \exp\Big[-2K_{II}(\frac{1}{2} - \epsilon_+ - \frac{1}{2K_{II}})^2\Big]$. Therefore, the total error rate in computing f is $\epsilon_I + \epsilon_{II} - 2\epsilon_I\epsilon_{II}$, which is exponentially small in the repetitions K_I and K_{II}. In particular, to obtain a bit error probability ϵ_f on the computation of f for fixed ϵ_* and ϵ_+, it suffices to take

$$K_I = \left\lceil \frac{1}{(\frac{1}{2} - \epsilon_*)^2} \ln \sqrt{\frac{\mathfrak{R}_1}{\epsilon_f}} \right\rceil \leq \left\lceil \frac{1}{(\frac{1}{2} - \epsilon_*)^2} \ln \left(\frac{MN}{\sqrt{2\epsilon_f}} \right) \right\rceil, \tag{B8a}$$

$$K_{II} = \left\lceil \frac{1}{(\frac{1}{2} - \epsilon_+)^2} \ln \sqrt{\frac{1}{\epsilon_f}} \right\rceil. \tag{B8b}$$

In total, the N-party computation of f on each party's M-bit input can be implemented with error correction in our protocol at a lower bound unit rate of

$$\frac{R}{R_0} \geq \frac{MN}{4M^2N^2 \left\lceil \frac{\ln(MN/\sqrt{2\epsilon_f})}{(\frac{1}{2} - \epsilon_*)^2} \right\rceil + (N+1) \left\lceil \frac{\ln(1/\sqrt{\epsilon_f})}{(\frac{1}{2} - \epsilon_+)^2} \right\rceil}, \tag{B9}$$

where R_0 is the scheme-dependant average rate to add a new photon to a graph state. For the HoD scheme we propose, $R_0 = \eta_e R_{\rm rep}$.

3. Security

Having established correctness of the proposed protocol, we now prove that it is secure under the requirements defined in Section III. Recall, we demand as a security condition that playing honestly does not reveal any more information about one's input than what can be inferred from the final function output. We will show this is true under the assumption that the Referee does not collaborate with any of the parties by supplying them with side information.

In the first phase, each state $|G_I\rangle^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}$ is a tripartite state, held by Alice, Bob, and the Referee. Suppose that Alice is playing honestly and a dishonest Bob is trying to learn about input based on his local quantum information and whatever Alice discloses in an honest execution of the protocol. The only information he obtains in Stage I is the public message $\gamma_i = x_i + m_7$ announced from Alice. Hence, suppose that Alice's input is described by the random variable $\mathbf{X}_i$ with values x_i having a prior distribution $p(x_i)$, which is known to all parties. Bob's initial state of knowledge of variable $\mathbf{X}_i$ given his share of $|G_I\rangle^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}$ is described by the density matrix

$$\sigma^{\mathbf{X}_i\mathbf{B}_i} = \sum_{x_i=0}^{1} p(x_i)\,|x_i\rangle\langle x_i|^{\mathbf{X}_i} \otimes \mathrm{tr}_{\mathbf{A}_i\mathbf{R}}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right). \tag{B10}$$

After Alice's measurement and Bob's learning of the value γ_i, his updated state of knowledge conditioned on this new information is

$$\sigma_{\gamma_i}^{\mathbf{X}_i\mathbf{B}_i} = \sum_{x_i=0}^{1}\sum_{m_7=0}^{1} p(x_i, m_7|\gamma_i)\,|x_i\rangle\langle x_i|^{\mathbf{X}_i} \otimes \mathrm{tr}_{\mathbf{A}_i\mathbf{R}}\left(|m_7\rangle\langle m_7|_7\,|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right)/p(m_7). \tag{B11}$$

A calculation shows that

$$\begin{aligned}\mathrm{tr}_{\mathbf{A}_i\mathbf{R}}\left(|m_7\rangle\langle m_7|_7\,|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right) &= \frac{\mathbb{I}_2}{2}\otimes\frac{\mathbb{I}_3}{2}\otimes\mathrm{tr}_7\left(|m_7\rangle\langle m_7|_7\,\frac{|{+}0\rangle\langle{+}0|_{78} + |{-}1\rangle\langle{-}1|_{78}}{2}\right)\\ &= \frac{1}{2}\left(\frac{\mathbb{I}_2}{2}\otimes\frac{\mathbb{I}_3}{2}\otimes\frac{\mathbb{I}_8}{2}\right)\\ &= \frac{1}{2}\,\mathrm{tr}_{\mathbf{A}_i\mathbf{R}}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right).\end{aligned} \tag{B12}$$

In other words, the post-measurement state of Bob's subsystem is independent of Alice's measurement outcome. Since m_7 is a uniform random bit independent of x_i, we have $p(m_7) = \frac{1}{2}$ and $p(x_i|\gamma_i) = p(x_i)$. Thus,

$$\begin{aligned}\sigma_{\gamma_i}^{\mathbf{X}_i\mathbf{B}_i} &= \sum_{x_i=0}^{1}\sum_{m_i=0}^{1} p(x_i, m_7|\gamma_i)\,|x_i\rangle\langle x_i|^{\mathbf{X}_i} \otimes \mathrm{tr}_{\mathbf{A}_i\mathbf{R}}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right)\\ &= \sum_{x_i=0}^{1} p(x_i)\,|x_i\rangle\langle x_i|^{\mathbf{X}_i} \otimes \mathrm{tr}_{\mathbf{A}_i\mathbf{R}}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right)\\ &= \sigma^{\mathbf{X}_i\mathbf{B}_i}.\end{aligned} \tag{B13}$$

This shows that Bob's knowledge of Alice's input does not change throughout the course of Stage I. The same is also clearly true for Stage II since the $\mathrm{tr}_{\mathbf{R}}\,|G_{II}\rangle\langle G_{II}| = \frac{1}{2}(|{+}\cdots{+}\rangle\langle{+}\cdots{+}| + |{-}\cdots{-}\rangle\langle{-}\cdots{-}|)$, and so the measurement outcomes m_k of the honest parties $\mathbf{P}_k$ measuring Z are independent of each other and of the values μ_k. Therefore, the only new information Bob learns about Alice's input comes through the announcement of $f(\mathbf{x}_1, \cdots, \mathbf{x}_N)$ by the Referee at the end of the protocol. A similar conclusion is reached in the scenario of an honest Bob and a dishonest Alice.

Now we consider the Referee. Since there is no collusion with parties $\mathbf{P}_1, \cdots, \mathbf{P}_k$, from the Referee's perspective, either all parties are playing fairly or some are acting maliciously; in the latter case, it is unknown who these parties are or what attacks they are employing. Therefore, a corrupt Referee wanting to learn the inputs of one or more honest parties should proceed by assuming that all parties are playing honestly. Like before, in each iteration of $|G_I\rangle^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}$, the Referee's initial state and description of the variables $\mathbf{X}_i$ and $\mathbf{Y}_i$ is given by

$$\sigma^{\mathbf{X}_i\mathbf{Y}_i\mathbf{R}} = \sum_{x_i,y_i=0}^{1} p(x_i)p(y_i)\,|x_i\rangle\langle x_i|^{\mathbf{X}_i} \otimes |y_i\rangle\langle y_i|^{\mathbf{Y}_i} \otimes \mathrm{tr}_{\mathbf{A}_i\mathbf{B}_i}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right). \tag{B14}$$

Note that tracing out qubits 2, 4, 5, and 8 completely dephase all the remaining qubits in $|G_I\rangle$:

$$\mathrm{tr}_{2,4,5,8}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right) = \frac{\mathbb{I}_1}{2}\otimes\frac{\mathbb{I}_3}{2}\otimes\frac{\mathbb{I}_6}{2}\otimes\frac{\mathbb{I}_7}{2}. \tag{B15}$$

Hence,

$$\mathrm{tr}_{\mathbf{A}_i\mathbf{B}_i}\left(|m_3\rangle\langle m_3|_3\otimes|m_7\rangle\langle m_7|_7\,|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right) = \mathrm{tr}_{\mathbf{A}_i\mathbf{B}_i}\left(|G_I\rangle\langle G_I|^{\mathbf{A}_i\mathbf{B}_i\mathbf{R}}\right) = \frac{\mathbb{I}_1}{2}\otimes\frac{\mathbb{I}_6}{2}, \tag{B16}$$

from which it follows that Alice and Bob's announcements of $\gamma_i = x_i + m_7$ and $\delta_i = y_i + m_3$ reveal no information to the referee about x_i and y_i; i.e. $\sigma^{\mathbf{X}_i\mathbf{Y}_i\mathbf{R}} = \sigma^{\mathbf{X}_i\mathbf{Y}_i\mathbf{R}}_{\gamma_i,\delta_i}$. Likewise, it is easy to see that in Stage II, the Referee's reduced state is completely mixed until all N messages are received, at which point it encodes the bit value $\sum_{k=1}^{N} m_k$.

Now since $f = \sum_{k=1}^{N}(m_k+\nu_k) + \sum_{i=1}^{\mathfrak{N}_1} b_i$, we have that

$$p\left(\mathbf{x}_1,\cdots,\mathbf{x}_N\middle|\sum_k m_k,\{\nu_k\}_k,\{b_i\}_i\right) = p\left(\mathbf{x}_1,\cdots,\mathbf{x}_N|\{\nu_k\}_k,\{b_i\}_i,f\right) = p\left(\mathbf{x}_1,\cdots,\mathbf{x}_N|f\right), \tag{B17}$$

where the last equality follows from the fact that the ν_k and b_i are independent of the $\{\mathbf{x}_i\}_{i=1}^N$ due to the padded bits from the measurements. Hence, the Referee's knowledge of the inputs $\{\mathbf{x}_i\}_{i=1}^N$ given the data $(\sum_k m_k, \{\nu_k\}_k, \{b_i\}_i)$ is equivalent to his knowledge of the $\{\mathbf{x}_i\}_{i=1}^N$ given $f(\mathbf{x}_1,\cdots,\mathbf{x}_N)$.

4. Self-testing of graph states

We can further secure the computation against an untrustworthy Source, via a self-testing procedure, which allows the parties and the Referee to validate the state distributed by the Source. If the parties indeed have the correct state, measuring the independent components of a uniformly randomly chosen stabilizer of the state will lead to a correlated outcome, hence implementing a partial test of the state's validity. By repeating the protocol and partitioning rounds between these stabilizer tests, discarded rounds of computation, and a single accepted target round of computation, the parties can upper bound the probability of receiving the incorrect state during the target round [52]. In implementing our multi-party protocol within our HoD scheme for generating the requisite states, we require the set of instructions, detailing which rounds to test, compute, and ultimately accept, be a private source of shared randomness between the parties and the Referee, which could be generated initially from a set of GHZ states distributed to the participants in the computation [58]. Without knowledge of which rounds are stabilizer tests and which are computations, the Source is prevented from modifying the state they distribute in order to fool the participants during rounds of self-testing. Conversely, the HoS scheme allows for the requisite graph states to be produced prior to the measurement-based computation protocol. Hence, the instruction set directing the participants when to self-test can be decided after the state has already been generated. In these schemes, we therefore do not require a distinct Source and Referee, at the cost of necessitating memory—in requiring the full set of photonic states be generated in advance, as well as additional rounds of self-testing [53].

Appendix C: Constructing graph states with "emit then add"

Building graph states in either of the HoS and HoD schemes necessities additional experimental overhead from typical deterministic quantum emitter-based schemes in both the number of qubits required and entangling operations between them. We demonstrate through an inductive argument that these additional resource costs scale at worst linearly. Subsequently, we present a resource-efficient set of subroutines used to produce the requisite states for our multi-party computation protocol, described in Section II. As the whole of our protocol is Clifford, we can employ the HoD scheme to produce and measure these graph states efficiently in practice, without the need of a quantum memory whatsoever. We briefly discuss how phase corrections, resulting from these construction subroutines, are handled classical in this scheme. The subroutines we introduce are thereafter employed in Appendix D to estimate the fidelity to make the states used in our protocol. In what follows, a superscript (p), (s), or (e) denotes the kind of physical qubit associated with the relevant subspace on which an operator acts on a photon, auxiliary spin, or emitter, respectively.

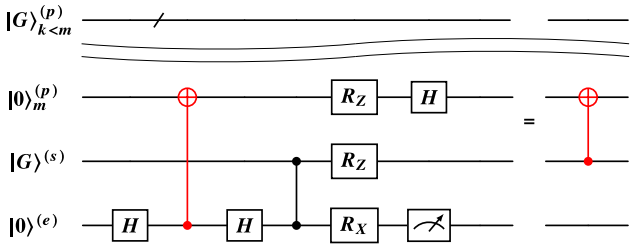


FIG. 8. A subcircuit equivalent to a $CX_{s,p}$ gate, up to a conditional phase correction, for transferring entanglement (conditional phase information) in our proposed HoS (HoD) scheme. This example "emit then add" procedure replaces every pumping gate in typical deterministic schemes for generating arbitrary photonic graph states. Entanglement (conditional phase information) between a photon (p) and a coherently pumped emitter (e) (represented by a red $CX_{e,p}$ gate) is exchanged to an auxiliary spin (s) via a two-qubit entangling $CZ_{e,s}$ gate and local complementation. The emitter is measured out thereafter and reinitialized for the next iteration of the procedure. Rotations about X and Z are by $\pi/2$ and $-\pi/2$, respectively, as noted in Equation A7. The measurement of the emitter is with respect to the Z basis. All previously added photons at iterations $k < m$ are unaffected.

1. Additional overhead

Let $|G\rangle$ define an existing graph state in which there is at least a single edge between an auxiliary spin and the set of photons previously added to the the graph. We label each of these photons by an emission order $1, \cdots, m-1$. Let V_m define the additional vector space describing the emitter and the next photon, m, to be added to the graph, both of which start in $|0\rangle$. The set of generators which stabilizes the collective vector space $V_G + V_m$, consisting of the graph and subsequent emitter-photon pair, has the form below

$$S_{V_G+V_m} = \langle \cdots, \cdots Z_k^{(p)} \cdots X^{(s)}, Z^{(e)}, Z_m^{(p)} \rangle, \tag{C1}$$

where $\langle \cdots \rangle$ denotes a set of generators and the notation $\cdots Z_k^{(p)} \cdots$ is used to keep track of an arbitrary edge between the auxiliary spin and a photon previously added to the graph at some emission step $k < m$. The subcircuit depicted Figure 8 demonstrates an example of how to transfer entanglement (or conditional phase information) from the emitter-photon sub-system to $|G\rangle$, with a single two-qubit spin-spin entangling gate and local complementation. In implementing the example, we transform the stabilizer of the combined vector space in Equation C1 as

$$S'_{V_G+V_m} = \langle \cdots, (-1)^{c_m} \cdots Z_k^{(p)} \cdots X_m^{(p)} X^{(s)}, (-1)^{c_m} Z_m^{(p)} Z^{(s)}, (-1)^{c_m} Z^{(e)} \rangle \tag{C2}$$

where $c_m \in \{0, 1\}$ is a classical bit value conditioned on the measurement of the emitter.

The result of these operations produces the same stabilizer we would have arrived at had we instead pumped the auxiliary spin itself. With these additional operations, any graph state accessible in the deterministic scheme can be constructed in the HoS or HoD schemes. As we restrict those auxiliary spins already entangled with any previously added photons from being pumped, it follows that one additional spin, the emitter, and one two-qubit spin-spin entangling gate per photon in G are the minimum additional overhead in our proposed schemes for making arbitrary graph states. Furthermore we can define a new vector space V'_G, containing the existing graph state and a newly entangled photon, with a dimension that increases by one with each new photon. The new space V'_G is stabilized by a unique set of generators that can be rotated back to a graph state basis of the same general form as Equation C1, now defined by a new graph state $|G'\rangle$.

2. Construction subroutines

We also offer a pair subroutines the simplifies the construction and overhead for the graph states $|G_I\rangle$ and $|G_{II}\rangle$, described in Section III. Representations of the graph transformations associated with the two subroutines, along with example circuits, are depicted in Figs. 9 and 10. These transformations can be performed successively with no additional operations, transforming the previous graph G built on the auxiliary spin to a new graph G' with any new photons sharing an edge to the auxiliary spin. Despite their intended application in our MPC protocol, we make no assumptions about the measurement of the photons in these subroutines, such that they can be applied generally across experimental implementations.

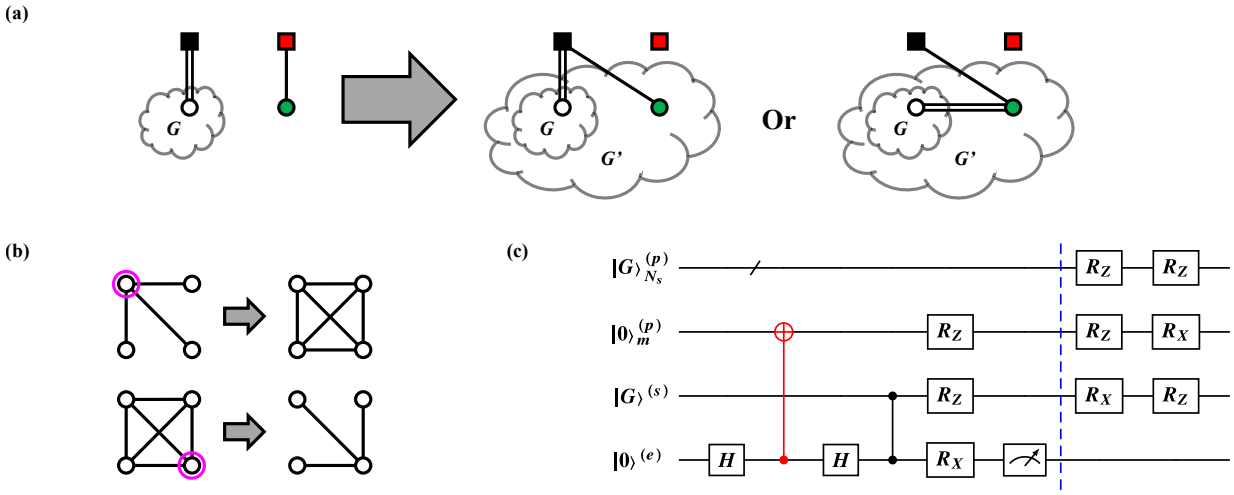


FIG. 9. Passing-subroutine for adding new photons to an existing graph, G. (a) A graph transformation of passing a new photon (green) from the emitter (red) to an auxiliary spin (black), which is connected to one or more previously added photons (white, denoted with double edge for the multiplicity). This subroutine consists of two variations: (left) leaving all previously added photons invariant, (right) transplanting those edges to the newly added photon. (b) An example of how local complementations on a target qubit (magenta circle) can be used to add or remove edges. (c) A quantum subcircuit which implements the graph transformation. The right variation of the graph transformation above is achieved with the additional two local complementations (blue dashed line, depicting the deviation). Rotations and measurements follow the same notation as in Figure 8.

One "passing"-subroutine, shown in Figure 9 consists of two variations: "join" and "extend". The join-subroutine adds a new photon to an existing graph and leaves all previously existing edges invariant. The extend-subroutine transfers all edges from the auxiliary spin to the new photon. The two are achieved without or with the additional two local complementations depicted at the end of the example circuit, respectively. Both variations only act on previously added photons in the neighborhood of the auxiliary spin, N_s. Repeatedly applying the join-subroutine or extend-subroutine on a single auxiliary spin produces a star graph or linear cluster state, respectively for each variation.

We note briefly that in practice with each implementation of the passing-subroutine, the newly added photon to graph carries a conditional phase that is a byproduct of the decoupling measurement made on the emitter, as shown in Equation C2. This byproduct phase determines the precise basis state of the graph, and may require correction for general measurement-based quantum computation. In the HoD scheme photons are measured before they are decoupled from the emitter, and hence any requisite phase corrections need be commuted after each measurement. The Clifford nature of the computations employed in our MPC simplifies all of these corrections to bits flips that can be handled classically. Furthermore, correction of this phase is not always necessary as certain measurements made by the parties destroy this phase information, while other measurements allow the parties to absorb this phase information into their own pad. Conversely, conditional measurements, such as the ones made by Alice in step (4.) of Stage I of our protocol, couple these byproduct phases to the phase information input into the computation. Therefore classical communication is required here between Alice and the Source. A simple solution is for the Source to make public the outcomes of each of these decoupling measurement, at no cost to security of the computation.

The other "patching"-subroutine, shown in Figure 10, serves to attach two subgraphs G_1 and G_2 by a common edges between photons. This process requires additional two-qubit spin-spin entangling gates from the passing-subroutine. For further simplicity we only consider the case when G_1 and G_2 each have a single edge to all previously added photons in their respective subgraphs. Operations in this subroutine are restricted locally to only the emitter, spin, and the two photons we ultimately require to share an edge, labeled in the figure by arbitrary emission steps j, k in $1, \cdots, n_p$. This subroutine mirrors the one employed in the production of large 2D cluster states in [5], and can be applied in the either scheme we propose for the same purpose.

Application of these subroutines to the construction of the graph states discussed in Section III is straightforward. The state $|G_I\rangle$, consisting of $n_p = 8$ photons, labeled by an emission ordering depicted in Figure 5, can be built following the sequence of steps in Build I. This procedure requires 11 two-qubit spin-spin entangling gates in total: 8 from passing operations, and 3 from a single patching step (as we are patching between the final two photons in

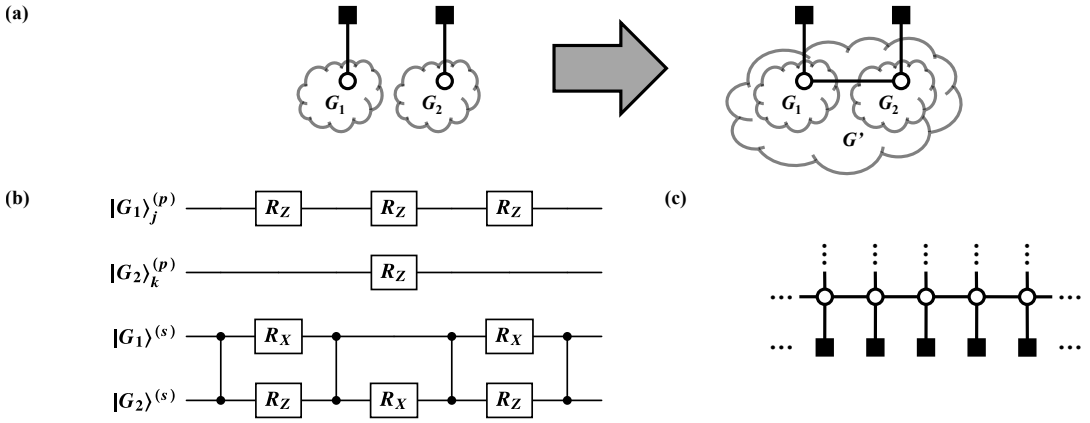


FIG. 10. Patching-subroutine for attaching two subgraphs G_1 and G_2 by a common edge between photons. (a) The graph transformation depicting the patching. (b) The corresponding circuit diagram. Additional two-qubit spin-spin entangling gates are required for this subroutine, over the passing-subroutine. Rotations follow the same notation as in Figure 8. (c) A 2D cluster state built on an array of auxiliary spins. Edges can be generated between photons in the layer neighboring the array of spins with this patching.

each subgraph and can therefore neglect the fourth spin-spin entangling gate in the subroutine). It is known that the sequential nature of photon emission events imparts on an ordering on the graph state, limiting the kinds of photonic graphs accessible by construction on a single quantum emitter [59]. The private nature of the padded AND being computed in Stage I sets a nontrivial emission ordering, which, following the results of [32], requires two auxiliary spins to construct. The state $|G_{II}\rangle$, consisting of $n_p = N+1$ photons for an N party computation, can be constructed entirely out of the passing-subroutine on a single auxiliary spin. This graph state can be built following Build II. Trivially, this construction requires $N+1$ two-qubit spin-spin entangling gates.

Build I. $|G_I\rangle$. *Input:* A photon emission order labeling photons $(p_1), \cdots, (p_8)$, corresponding to the $n_p = 8$ photons in $|G_I\rangle$, an emitting spin, and two auxiliary spins, labeled (s_1) and (s_2).

1. Pass photon (p_1) to auxiliary spin (s_1) with join.
2. Pass photons (p_2) and (p_3) to (s_1), utilizing extend for (p_2) and join for (p_3).
3. Repeat step the previous step for photons (p_4) and (p_5).
4. Pass photon (p_6) to (s_1) with extend.
5. Pass photons (p_7) and (p_8) to auxiliary spin (s_2), utilizing join for (p_7) and extend for (p_8).
6. Patch subgraphs on (s_2) and (s_1).

Build II. $|G_{II}\rangle$. *Input:* A photon emission order labeling photons $(p_1), \cdots, (p_N), (p_R)$, corresponding to the $n_p = N+1$ photons in $|G_{II}\rangle$, an emitting spin, and a single auxiliary spin, labeled (s).

1. Pass photons $(p_1), \cdots, (p_N)$ to the auxiliary spin (s) with join, where photon (p_k) is routed to party k.
2. Pass the final photon (p_R), belonging to the Referee, to (s) with extend.

Appendix D: Experimentally realizable fidelity calculations

We now consider an experimental realization of our schemes for constructing the graph states utilized in our multi-party computation. While the nature of the herald and the computation itself are device-independent, we assume here

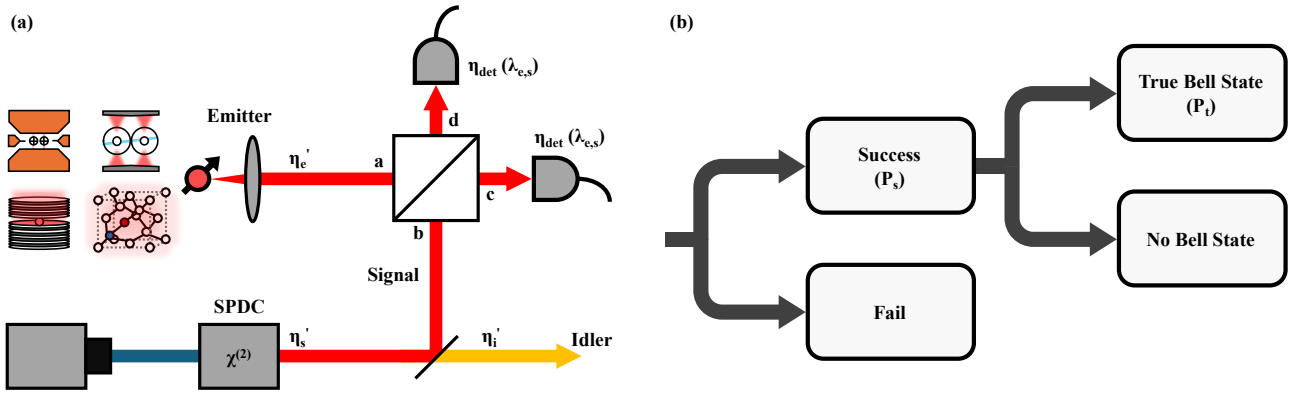


FIG. 11. Entanglement swapping in the HoS scheme. (a) Schematic of a generalized Hong-Ou-Mandel interferometer applied as a joint measurement apparatus. A photon entangled with an emitter is sent through port a of the beamsplitter, and a photon from a spontaneous parametric down-conversion (SPDC) photon-pair source is sent through port b. Detection of two single-photon orthonormal states $|u\rangle$, $|v\rangle$ in either output ports c or d results in entanglement between the emitter and the idler photon from the pair source. Various loss factors denoted by η are modelled. Additional elements for qubit rotations are not shown. (b) Probability tree showing the outcomes of a Bell state measurement attempt. The "success" probability P_s for the Bell state measurement denotes the probability of measuring a set of specific click patterns that indicate entanglement swapping. P_t denotes the probability of projecting the emitter and idler onto a Bell state from the measurement.

trapped ions as our quantum emitters, due to their high fidelity benchmarks for two-qubit spin-spin entangling gates [12, 13] and reasonable collection efficiency with high numerical aperture optics [14]. We outline our fidelity model for two schemes; the HoS scheme involving the heralding of a Bell state between an emitter and a photon for general cases involving non-destructive heralding of photons, and the HoD scheme where emitter photons are measured directly in the basis required for the measurement-based computation protocol.

1. Experimental apparatus

For the HoS scheme, heralding a Bell state between an emitter and photon is implemented via entanglement swapping between a photon from an emitter and a photon from a nonlinear pair-source. We use spontaneous parametric down-conversion (SPDC) as our pair-source for the heralding. SPDC is an optical process based on a crystal with $\chi^{(2)}$ nonlinearity whereby a photon from a pump is converted to a signal and idler photon pair of lower energy. It is often used to produce entangled photon pairs in various degrees of freedom, or as a heralded single photon source [28]. The joint measurement apparatus required for the entanglement swapping in the heralding scheme we describe here can be accomplished via a generalized Hong-Ou-Mandel interferometer [60] depicted in Figure 11(a), where the emitter photon and signal photon from the pair-source are sent to a 50:50 beamsplitter. Elements from these experiments are modeled in our estimates of the fidelity to successfully produce graph states.

We briefly consider the set of states employed in heralding a Bell state in a device-independent form. The internal state of an emitter (e) is entangled with a photon (p_e) in an arbitrary basis, and an entangled photon pair is produced from the SPDC source labeled as the signal (p_s) and idler (p_i) photons. We can express both the idealized entangled states $|\Psi_E\rangle$ and $|\Psi_P\rangle$ respectively, as

$$|\Psi_E\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{(e)}|1;0\rangle^{(p_e)} - |1\rangle^{(e)}|0;1\rangle^{(p_e)}), \tag{D1}$$

$$|\Psi_P\rangle = \frac{1}{\sqrt{2}}(|1;0\rangle^{(p_s)}|0;1\rangle^{(p_i)} - |0;1\rangle^{(p_s)}|1;0\rangle^{(p_i)}), \tag{D2}$$

where $|0\rangle^{(e)}$ and $|1\rangle^{(e)}$ is the computational basis for the emitter, and the notation $|m;n\rangle$ is used to denote the photonic Fock state representation for a particular basis $\{|u\rangle, |v\rangle\}$, such as orthogonal polarizations, with m in $|u\rangle$ and n in $|v\rangle$. The relationship between the input modes a and b and output modes c and d of the 50:50 beamsplitter can be described by the unitary transformation on the creation operators $\hat{a}^\dagger = \frac{1}{\sqrt{2}}(\hat{c}^\dagger + \hat{d}^\dagger)$ and $\hat{b}^\dagger = \frac{1}{\sqrt{2}}(\hat{c}^\dagger - \hat{d}^\dagger)$. With the emitter photon entering port a, and the signal photon entering port b, the overall state after applying the transformation can be expressed in the form

$$
\begin{aligned}
|\Psi_E\rangle\,|\Psi_P\rangle =& \frac{(\hat{c}_u^\dagger)^2-(\hat{d}_u^\dagger)^2}{4}\,|vac\rangle_{c,d}\,|0\rangle^{(e)}\,|0;1\rangle^{(p_i)} + \frac{\hat{d}_u^\dagger\hat{d}_v^\dagger-\hat{c}_u^\dagger\hat{c}_v^\dagger}{2\sqrt{2}}\,|vac\rangle_{c,d}\,|\Psi^+\rangle^{(e,p_i)} \\
&+\frac{\hat{c}_u^\dagger\hat{d}_v^\dagger-\hat{c}_v^\dagger\hat{d}_u^\dagger}{2\sqrt{2}}\,|vac\rangle_{c,d}\,|\Psi^-\rangle^{(e,p_i)} + \frac{(\hat{c}_v^\dagger)^2-(\hat{d}_v^\dagger)^2}{4}\,|vac\rangle_{c,d}\,|1\rangle^{(e)}\,|1;0\rangle^{(p_i)}\,,
\end{aligned}
\tag{D3}
$$

where

$$
|\Psi^\pm\rangle^{(e,p_i)} = \frac{1}{\sqrt{2}}(|0\rangle^{(e)}\,|1;0\rangle^{(p_i)} \pm |1\rangle^{(e)}\,|0;1\rangle^{(p_i)}). \tag{D4}
$$

We are interested in projecting onto either $|\Psi^+\rangle^{(e,p_i)}$ or $|\Psi^-\rangle^{(e,p_i)}$ which can be realized by detecting specific click patterns on photon counting detectors at the output ports capable of resolving the orthonormal components. From Equation (D3), we can see that detecting orthonormal one-photon states in either ports c or d results in a projection onto $|\Psi^+\rangle^{(e,p_i)}$ while detection in opposite ports results in $|\Psi^-\rangle^{(e,p_i)}$. The overall probability of projection onto either of the Bell states is $\frac{1}{2}$ for each heralded measurement attempt. Upon the detection of $|\Psi^-\rangle^{(e,p_i)}$, we can perform a qubit rotation to produce the state $|\Psi^+\rangle^{(e,p_i)}$ for phase consistency. We can then perform a series of one- and two-qubit gates to add a photon to a graph. Upon failure to detect the correct detection pattern, we reinitialize the emitter and photon-pair and attempt the measurement again. We assume number-resolving detectors at the output ports of the beamsplitter capable of detecting photons in the basis $\{|u\rangle\,,|v\rangle\}$. For example, two polarizing beamsplitters and four detectors would be used after the output ports for photons entangled in a polarization basis.

The initial state of the emitter can be described by the state defined in Equation (D1). The output state of SPDC is a multi-mode squeezed state where the photon-pair production probability is dependent on the pump amplitude. Assuming a classical pump, we take the Hamiltonian for the SPDC process to approximately be of the form [33, 61]

$$
\hat{H} = e^{i\phi}\kappa\hat{K}^\dagger + e^{-i\phi}\kappa\hat{K}, \tag{D5}
$$

where $\hat{K}^\dagger = \hat{a}_{u;s}^\dagger\hat{a}_{v;i}^\dagger - \hat{a}_{v;s}^\dagger\hat{a}_{u;i}^\dagger$ represents the creation of entangled signal and idler pairs denoted s and i in the basis $\{|u\rangle\,,|v\rangle\}$. The time evolution operator $\hat{U}(t) = \exp\Big(i\hat{H}t/\hbar\Big)$ yields the resulting state

$$
|\Psi_{SPDC}\rangle = N\sum_{n=0}^{\infty}\tanh^n r\sum_{m=0}^{n}(-1)^m\,|n-m;m\rangle^{(p_s)}\,|m;n-m\rangle^{(p_i)}\,, \tag{D6}
$$

where $r=\kappa t/\hbar$ is the interaction parameter that is dependent on the pump field amplitude, t is the interaction time of the pump through the crystal, and N is the normalization constant with $N=1-\tanh^2 r$. By tuning the interaction parameter r, we can change the probability of producing a single pair ($n=1$ in Equation (D6) leading to Equation (D2)) to optimize the fidelity of the HoS scheme. Note that increasing the pump power also increases the relative contribution of the higher order terms ($n>1$), which increases the probability of detecting multiple photon-pairs.

The above is applicable for polarization-entangled photon pairs directly produced in type-II SPDC described in refs. [33, 61]; the output state and choice of degree-of-freedom for entanglement will of course be dependent on the specific properties of the photon-pair source and pump. However, we note that we are assuming the pump can be treated as a classical, single-mode source, and we use a simplified Hamiltonian and output state for the photon pairs entangled in $\{|u\rangle\,,|v\rangle\}$. Moreover, factors such as the multi-modal nature of the pump, phase differences or instabilities between the orthonormal components in the optical path, or distinguishability between the photons from the emitter and the SPDC source can degrade the fidelity of the scheme.

2. Sources of infidelity

Several experimentally relevant sources of infidelity are considered in our model. Photonic loss and detector dark counts can induce false heralding events, leading to a failure to resolve a true Bell state and subsequent addition of a photon to the graph. Decoherence across the emitter and any auxiliary spins utilized in building the graph will produce errors on any computation done on the graph state. The fidelity of each two-qubit spin-spin entangling gate performed in the construction is considered as well. We can also consider the fidelity of the initial entanglement between the emitter and its photon, as well as the entanglement of the photon-pair, used in the entanglement swapping procedure.

a. Photonic loss

The standard approach to modelling photonic losses is to introduce a fictitious beamsplitter with transmittance η and reflectance $1-\eta$ on the lossy channel. This is equivalent to applying the transformation on the creation operator $\hat{a}^\dagger = \sqrt{\eta}\hat{a}_T^\dagger + \sqrt{1-\eta}\hat{a}_R^\dagger$ [62] where T and R denote the transmitted and reflected paths respectively. The Fock state $|n\rangle$ serving as the input transforms as $|n\rangle \to \sum_{k=0}^{n}\sqrt{\binom{n}{k}\eta^{n-k}(1-\eta)^k}\,|n-k\rangle_T\,|k\rangle_R$ and the reflected path is traced out. We assume, for simplicity, that η is independent of the photonic degrees of freedom for each loss channel modelled. Applying this to an emitter with an initial state given by Equation (D1) and performing the partial trace over the reflected path, the resulting density matrix $\hat{\rho}_E$ for the emitter-photon pair incorporating losses is

$$\begin{aligned}\hat{\rho}_E =& \frac{1}{2}(1-\eta_e)\,|0\rangle\langle 0|^{(e)} \otimes |vac\rangle\langle vac|^{(p_e)} + \frac{1}{2}(1-\eta_e)\,|1\rangle\langle 1|^{(e)} \otimes |vac\rangle\langle vac|^{(p_e)} \\ &+\frac{1}{2}\eta_e\,|0\rangle\langle 0|^{(e)} \otimes |1;0\rangle\langle 1;0|^{(p_e)} + \frac{1}{2}\eta_e\,|1\rangle\langle 1|^{(e)} \otimes |0;1\rangle\langle 0;1|^{(p_e)} \\ &-\frac{1}{2}\eta_e\,|0\rangle\langle 1|^{(e)} \otimes |1;0\rangle\langle 0;1|^{(p_e)} - \frac{1}{2}\eta_e\,|1\rangle\langle 0|^{(e)} \otimes |0;1\rangle\langle 1;0|^{(p_e)}\,. \end{aligned} \tag{D7}$$

Similarly, the density matrix for the SPDC source $\hat{\rho}_{SPDC}$ becomes

$$\begin{aligned}\hat{\rho}_{SPDC} = \sum_{n,n^*=0}^{\infty}\sum_{m=0}^{n}\sum_{m^*=0}^{n^*}\sum_{k_s,k_i'=0}^{\min\{n-m,n^*-m^*\}}\sum_{k_s',k_i=0}^{\min\{m,m^*\}} & c_{n,m,k_s,k_s',k_i,k_i'}c^*_{n^*,m^*,k_s,k_s',k_i,k_i'} \\ & |n-m-k_s;m-k_s'\rangle\,\langle n^*-m^*-k_s;m^*-k_s'|^{(p_s)} \\ \otimes\, & |m-k_i;n-m-k_i'\rangle\,\langle m^*-k_i;n^*-m^*-k_i'|^{(p_i)}\,,\end{aligned} \tag{D8}$$

where

$$c_{n,m,k_s,k_s',k_i,k_i'} = (1-\xi)(\sqrt{\xi})^n(-1)^m\sqrt{\binom{n-m}{k_s}\binom{m}{k_s'}\binom{m}{k_i}\binom{n-m}{k_i'}\eta_s^{n-k_s-k_s'}(1-\eta_s)^{k_s+k_s'}\eta_i^{n-k_i-k_i'}(1-\eta_i)^{k_i+k_i'}}, \tag{D9}$$

and we have used $\xi = \tanh^2 r$. Here, we have made the additional substitutions $\eta_e = \eta_e'\eta_{det}(\lambda_e)$ and $\eta_s = \eta_s'\eta_{det}(\lambda_s)$, where η_e and η_s are the combined collection and photodetection efficiencies for the emitter and signal photons respectively in the interferometry setup. η' accounts for the collection efficiency of the optical path as shown in Figure 11(a), and $\eta_{det}(\lambda)$ is the photodetection efficiency which may be wavelength dependent (in the joint measurement, we require $\lambda_e = \lambda_s$). $\eta_i = \eta_i'$ is the collection efficiency of the idler for the SPDC setup, neglecting user-specific losses such as transmission losses through an optical fiber network and imperfect detection from the user. Since we are interested in retrieving the photon from the emitter and a single pair from the SPDC source for entanglement swapping, under the loss model the resulting probabilities for $|\Psi_E\rangle$ and $|\Psi_P\rangle$ as defined in Equation (D1) and Equation (D2) are

$$\langle\Psi_E|\,\hat{\rho}_E\,|\Psi_E\rangle = \eta_e, \tag{D10}$$

$$\langle\Psi_P|\,\hat{\rho}_{SPDC}\,|\Psi_P\rangle = \frac{\eta_s\eta_i\xi(\bar{\eta}_s\bar{\eta}_i\xi+2)(1-\xi)^2}{(1-\bar{\eta}_s\bar{\eta}_i\xi)^4}, \tag{D11}$$

where $\bar{\eta}_e = 1-\eta_e$, $\bar{\eta}_s = 1-\eta_s$, and $\bar{\eta}_i = 1-\eta_i$.

b. Photodetector metrics

In this work, we provide practical estimates of the fidelity achievable using photon number-resolving detectors for entanglement swapping. We assume each detector in the setup has some efficiency η_{det} and also model dark counts which arise due to inherent electronic noise in a detector. Each dark count event is assumed to be independent and generated at a constant rate R_d cps, and typically dark count rates can be low ($< 10^{-2}$ cps) for single-photon detectors such as Transition Edge Sensors [63]. Furthermore, we assume the exposure time of the detectors, t_{exp} is much longer than the time scale over which dark counts emerge. The probability for n_d dark counts on a detector during each measurement cycle can then be approximated by a Poisson distribution [64]

$$P_d(n_d) = e^{-R_d t_{\text{exp}}}\frac{(R_d t_{\text{exp}})^{n_d}}{n_d!}. \tag{D12}$$

The joint measurement in the heralding involves the use of detectors in output ports c and d in Figure 11. Therefore, we need to consider the effect of four detection outcomes for the herald – two detectors each with two orthonormal results, and the probability of dark counts for each. We assume identical dark count distributions for the detectors used in the herald.

c. *Entanglement swapping and heralded success probability*

A successful herald occurs at a probability which we define as P_s. For the HoD scheme, $P_s = \eta_e$ as we perform additional single and two-qubit operations on a graph only when the photon from the emitter is successfully measured. In the HoS scheme, P_s is the probability of detecting the set of detector click patterns requisite for the entanglement swap.

An extra source of infidelity for the heralded Bell state measurement occurs from the joint measurement itself. We define P_t as the overall probability of projecting the idler photon and emitter onto a Bell state for each joint measurement attempt. The probabilities are indicated in Figure 11(b). This will be a function of the detection efficiencies of the photons as well as the probability of zero dark count events detected. From Equation D10, Equation D11, and Equation D12, P_t is given by

$$\begin{aligned} P_t(\eta_e, \eta_s, \eta_i, \xi) &= \frac{1}{2} \langle \Psi_E | \hat{\rho}_E | \Psi_E \rangle \langle \Psi_P | \hat{\rho}_{SPDC} | \Psi_P \rangle P_d^4(0) \\ &= \frac{1}{2} \frac{\eta_e \eta_s \eta_i \xi (\bar{\eta}_s \bar{\eta}_i \xi + 2)}{(1 - \bar{\eta}_s \bar{\eta}_i \xi)^4} (1 - \xi)^2 P_d^4(0). \end{aligned} \tag{D13}$$

The heralded success probability P_s for the joint measurement is conditioned on a detection pattern representing the orthonormality of the photon states after the beamsplitter. This is a source of infidelity as the joint detection of states such as $|0;0\rangle^{(p_e)} |1;1\rangle^{(p_s)}$, representing two signal photons that are orthonormal to each other from the photon pair source and no photons from the emitter, possible due to detection or collection losses, would not result in entanglement swapping. We can identify the set of states that would result in a "success":

$$S = \{|1;0\rangle^{(p_e)} |0;1\rangle^{(p_s)}, |0;1\rangle^{(p_e)} |1;0\rangle^{(p_s)}, |0;0\rangle^{(p_e)} |1;1\rangle^{(p_s)}\} \tag{D14}$$

For each state in the set S, dark counts can lead to a false detection of the state. For example, the state $|1;0\rangle^{(p_e)} |0;1\rangle^{(p_s)}$ with zero dark counts is indistinguishable from the state $|1;0\rangle^{(p_e)} |0;0\rangle^{(p_s)}$ with one dark count falsely attributed to the measurement of a signal photon in the state $|0;1\rangle^{(p_s)}$. The former has an additional associated dark count probability of $P_d^4(0)$ and the latter $P_d(1)P_d^3(0)$. Thus, we can compute P_s by considering the probability of measuring all states in S, and all dark count combinations and photon states that reconstruct each element of S. By taking the partial trace of the emitter and idler photon from Equation D7 and Equation D8, and considering the probabilities mentioned in the overall set of joint measurement outcomes, we arrive at the probability P_s for the joint measurement,

$$\begin{aligned} P_s(\eta_e, \eta_s, \xi) =& \frac{3\bar{\eta}_e}{(1 - \bar{\eta}_s \xi)^2} (1 - \xi)^2 P_d^2(1) P_d^2(0) \\ &+ \left[\frac{\eta_e}{(1 - \bar{\eta}_s \xi)^2} + \frac{4\bar{\eta}_e \eta_s \xi}{(1 - \bar{\eta}_s \xi)^3} \right] (1 - \xi)^2 P_d(1) P_d^3(0) \\ &+ \left[\frac{\eta_e \eta_s \xi}{(1 - \bar{\eta}_s \xi)^3} + \frac{\bar{\eta}_e \eta_s^2 \xi^2}{(1 - \bar{\eta}_s \xi)^4} \right] (1 - \xi)^2 P_d^4(0). \end{aligned} \tag{D15}$$

In this paper, we consider the case where heralding is repeated until a "success" is flagged for each idler photon added to the graph. Thus, the fidelity of the entanglement swapping procedure is $F_{\text{swap}} = P_t / P_s$.

d. *Decoherence*

The emitter used to generate photons, as well as any auxiliary spin(s) entangled with an existing graph, will dephase across the duration until they are measured and projected back to a known state. For an emitter or auxiliary spin represented by a density matrix $\hat{\rho}$, we model the dephasing process via the map

$$\hat{\rho} \to \mathcal{D}(\hat{\rho}; t, \tau) = \frac{1}{2}(1 + e^{-t/\tau})\hat{\rho} + \frac{1}{2}(1 - e^{-t/\tau}) Z \hat{\rho} Z, \tag{D16}$$

where τ is the coherence time of the emitter or auxiliary spin and t is a timescale for the dephasing process. Clearly this process leaves the state invariant with probability $\frac{1}{2}(1+e^{-t/\tau})$, or conjugates it by Z with probability $\frac{1}{2}(1-e^{-t/\tau})$. It is straightforward to verify that this map describes a Markovian process such that

$$\mathcal{D}(\hat{\rho};t_1+t_2,\tau)=\mathcal{D}(\hat{\rho};t_2,\tau)\circ\mathcal{D}(\hat{\rho};t_1,\tau). \tag{D17}$$

We assume that each attempted herald happens on a short, regular timescale $t_{\text{rep}}=R_{\text{rep}}^{-1}$, which is simply the inverse repetition rate of the experiment. Furthermore, we assume each qubit gate operation time is near-instantaneous compared to t_{rep}, so that the dephasing takes place during the attempted herald only. As the emitter is measured out and reinitialized with each cycle of the experiment, it is evident that it will only dephase for at most t_{rep}. This implies that for each iteration of HPSE the contribution to the graph state fidelity from the decoherence of the emitter is $\frac{1}{2}(1+e^{-t_{\text{rep}}/\tau_e})$, such that

$$F_D^{(e)}(n_p)=\left(\frac{1}{2}\left(1+e^{-t_{\text{rep}}/\tau_e}\right)\right)^{n_p}, \tag{D18}$$

is the total contribution towards building an n_p photon graph state, and τ_e is the coherence time for the emitter.

We now model the contribution to the final state fidelity from any auxiliary spins in the system, which dephase for the entirety of their presence in the graph. Consider a mixed state density operator $\hat{\rho}_n=\sum_\lambda p_\lambda|\Phi_\lambda\rangle\langle\Phi_\lambda|$, described by a convex combination of n-qubit pure stabilizer states $|\Phi_\lambda\rangle$, where p_λ are the corresponding classical probabilities. This could represent the mixture of states one expects for an existing graph state built on a set of auxiliary spins, when under the action of its environment—including the prior action of the dephasing map itself. The system is initially stabilized by a set of generators $S_{|\Phi_\lambda\rangle}=\langle g_{1,\lambda},g_{2,\lambda},\cdots,g_{n,\lambda}\rangle$. Under the dephasing map the state evolves as

$$\mathcal{D}^{(s)}(\hat{\rho}_n;t,\tau_s)=\frac{1}{2}(1+e^{-t/\tau_s})\sum_\lambda p_\lambda|\Phi_\lambda\rangle\langle\Phi_\lambda|+\frac{1}{2}(1-e^{-t/\tau_s})\sum_\lambda p_\lambda Z^{(s)}|\Phi_\lambda\rangle\langle\Phi_\lambda|Z^{(s)}, \tag{D19}$$

which is once again a convex combination of stabilizer states with generators

$$\begin{aligned}S_{|\Phi_\lambda\rangle}&=\langle g_{1,\lambda},g_{2,\lambda},\cdots,g_{n,\lambda}\rangle,\\ S_{Z^{(s)}|\Phi_\lambda\rangle}&=\langle Z^{(s)}g_{1,\lambda}Z^{(s)},Z^{(s)}g_{2,\lambda}Z^{(s)},\cdots,Z^{(s)}g_{n,\lambda}Z^{(s)}\rangle.\end{aligned} \tag{D20}$$

τ_s is the coherence time of the auxiliary spins in the system, which we treat as identical. Since we are interested in graph states, $\hat{\rho}_{G=(V,E)}=|G\rangle\langle G|$, whose stabilizers are generated by the operators $\{K_a\}_{a\in V}$ defined in Equation A3, the dephasing map only acts on the generators proportional to $X^{(s)}$, for any auxiliary spin (s) in the system. Hence, a graph state consisting of n_p photons and n_s auxiliary spins would evolve under the dephasing map as the mixture

$$\mathcal{D}^{(s)}(\hat{\rho}_G;t,\tau_s)=\sum_{\mathbf{b}\in\mathbb{Z}_2^{n_s}}p(\mathbf{b})|G_{\mathbf{b}}\rangle\langle G_{\mathbf{b}}|, \tag{D21}$$

where $\mathbf{b}=(b_1,b_2,\cdots,b_{n_s})\in\mathbb{Z}_2^{n_s}$ and

$$p(\mathbf{b})=\frac{1}{2^{n_s}}\prod_{i=1}^{n_s}(1+(-1)^{b_i}e^{-t/\tau_s}). \tag{D22}$$

This mixture is stabilized by the set of generators,

$$S_{|G_{\mathbf{b}}\rangle}=\langle K_1^{(p)},\cdots,K_{n_p}^{(p)},(-1)^{b_1}K_1^{(s)},\cdots,(-1)^{b_{n_s}}K_{n_s}^{(s)}\rangle. \tag{D23}$$

The size of the system's stabilizer grows by one with each new photon m added to the graph. For the passing-subroutines we employ in Appendix C 2, we apply this rule, however in choosing either variation of the subroutine we choose whether to rotate the auxiliary spin out of the basis of the dephasing map, and consequentially project the system on to a new mixed state as described above. That is for the m^{th} photon, we generate a new subgroup of the stabilizer as either

$$S_{|G\rangle,\text{join}-m}=\langle(-1)^{b_k}\cdots Z_k^{(p)}\cdots Z_m^{(p)}X^{(s)},X_m^{(p)}Z^{(s)}\rangle, \tag{D24a}$$

$$S_{|G\rangle,\text{extend}-m}=\langle(-1)^{b_k}\cdots Z_k^{(p)}\cdots X_m^{(p)}Z^{(s)},Z_m^{(p)}X^{(s)}\rangle. \tag{D24b}$$

Here, the bit conditioning phase b_k is applied to the generator $K^{(s)}$ during the creation of the k^{th} photon, with $k < m$. If we allow the system to continue dephasing, these subgroups evolve, distinctly, as

$$S_{|G_{\mathbf{b}}\rangle,\text{join}-m} = \langle (-1)^{b_k+b_m} \cdots Z_k^{(p)} \cdots Z_m^{(p)} X^{(s)}, X_m^{(p)} Z^{(s)} \rangle, \tag{D25a}$$

$$S_{|G_{\mathbf{b}}\rangle,\text{extend}-m} = \langle (-1)^{b_k} \cdots Z_k^{(p)} \cdots X_m^{(p)} Z^{(s)}, (-1)^{b_m} Z_m^{(p)} X^{(s)} \rangle. \tag{D25b}$$

We see that in case of executing the extend-subroutine on m^{th} photon, the number of states in the mixture doubles, whereas in the case of the join-subroutine, the symmetry between states where either $b_k = b_m$ or $b_k \neq b_m$ leads to an effective mixture the same size as it was prior to the m^{th} photon's addition. Furthermore, we can express the probability for each state in the mixture in terms of b_k and b_m as

$$P(b_k, b_m) = \frac{1}{4} \left(1 + (-1)^{b_k} e^{-t_k/\tau_s}\right) \left(1 + (-1)^{b_m} e^{-t_m/\tau_s}\right). \tag{D26}$$

where we have defined t_k and t_m as arbitrary times from the probabilistic nature of the herald. For the join-subroutine, the graph state remains unchanged when $b_k, b_m = 0$ or $b_k, b_m = 1$, whereas, for the extend-subroutine, the graph state remains unchanged only when $b_k, b_m = 0$. Hence, the fidelity under the dephasing model scales as $\frac{1}{2}(1 + e^{-(t_k+t_m)/\tau_s})$ for the join-subroutine and $\frac{1}{4}(1+e^{-t_k/\tau_s})(1+e^{-t_m/\tau_s})$ for the extend-subroutine for iterations k and m. This is a subtle distinction that arises from the Markovian nature of the dephasing map when implementing the join-subroutine. It implies the final state fidelity when constructing graph states on a set of auxiliary spins will in general depend on the sequence describing how each photon is passed in to the system. In contrast, we assume $t_{\text{rep}} \ll \tau_s$ in our estimates, such that this distinction is not necessary, as $\frac{1}{4}(1+e^{-t_k/\tau_s})(1+e^{-t_m/\tau_s}) \approx \frac{1}{2}(1+e^{-(t_k+t_m)/\tau_s})$. We provide estimates where t_{rep}/τ_s is of order $10^{-7} - 10^{-9}$ [10, 31]. It is nonetheless important to discuss, when considering auxiliary spins with shorter coherence times or constructing exceedingly large graph states, where the time to build the graph is of order the coherence time.

Lastly, we account for the probabilistic nature of the herald. Building graph states in either scheme we propose can be viewed as a Bernoulli trial with success probability P_s occurring at regular intervals t_{rep}. The cumulative probability that m trials yields r successes is given by the distribution

$$h(m, r, P_s) = \binom{m-1}{r-1} P_s^r (1 - P_s)^{m-r}, \tag{D27}$$

where $m = r, r+1, r+2, \cdots$. For any auxiliary spins in the graph, any failure to herald adds an additional t_{rep} to the dephasing time. Therefore, we model the mean contribution to the state fidelity for an auxiliary spin with r photons passed to it under either passing-subroutine as

$$\begin{aligned} \langle F_D^{(s)}(r, P_s) \rangle &= \sum_{m=r}^{\infty} h(m, r, P_s) \left(\frac{1}{2}\left(1 + e^{-m t_{\text{rep}}/\tau_s}\right)\right) \\ &= \frac{1}{2}\left(1 + \left(\frac{P_s}{P_s + e^{t_{\text{rep}}/\tau_s} - 1}\right)^r\right) \\ &\approx \frac{1}{2}\left(1 + e^{-r t_{\text{rep}}/P_s \tau_s}\right), \end{aligned} \tag{D28}$$

where $\langle \cdots \rangle$ here denotes a classical expectation value, and t_{rep}/P_s is the average time for a successful herald. Note in the HoD scheme, $P_s = \eta_e$, whereas in the HoS scheme it is of the form in Equation D15. For an n_p photon graph state, we take r up to the number of photons that a given auxiliary spin remains a part of the graph. Here, we consider the same coherence times for the emitter and auxiliary spins, $\tau_e = \tau_s = \tau$. Given state-of-art of trapped ion experiments [10], we take the dephasing timescale to be $t_{\text{rep}}/\tau = 10^{-9}$ in our best estimates.

e. Gates

Single-qubit gates applied to photons, the emitter and any auxiliary spins are assumed to be perfect in our model. For all two-qubit spin-spin entangling gates, we assume a fidelity $F_{CZ} = 0.999$ in our best estimates, in line with benchmarks from state-of-the-art trapped ion experiments [12, 13]. We assume the time to implement any single-qubit or two-qubit gate, $t_{\text{gate}} \ll t_{\text{rep}}$, and can therefore be treated as instantaneous.

f. Initial entanglement fidelity

In practice, there will be a non-unit fidelity on initializing the emitter into the state described in Equation D1 as well as Equation D2 for the pair-source. The additional contribution to the overall fidelity using our schemes compared to schemes where an emitter is directly used to generate graphs is the entanglement fidelity of the nonlinear photon-pair source. For example, for SPDC, the main contribution to the degradation of polarization-based entanglement fidelity comes from the spatial-temporal profile of the pump [65] and its interaction with the specific nonlinear medium, in which different spatial and sepctral or temporal components impart different relative phases to the entangled pair described by Equation D2. The fidelity can be optimized by using compensating crystals or filtering techniques, however the latter also lowers the collection efficiency. Nevertheless, some of the best estimated fidelities for polarization-entangled SPDC sources range from ∼97% to ∼99.7% for various free-space and fiber-based setups [66–68]. In terms of overall fidelity estimations, we can introduce additional scaling terms similar to gate fidelity. We denote the initial entanglement fidelities for the emitter-photon pair and photon-photon pair as F_e and F_p respectively. We focus primarily on the fidelity from the SPDC source to highlight the additional infidelity from our scheme.

3. Pair generation rate optimization

Given the infidelity from false heralds, defined in Equations D13 and D15, there exists a trade-off between the rate and fidelity at which large graph states can be generated in the HoS scheme, as set by the dimensionless parameter ξ, controlling the pair generation rate of the SPDC source. Decreasing ξ improves the probability of heralding a true Bell state, at the cost of longer average times between successful heralds. Conversely, the effects of decoherence on any auxiliary spins in the system, through Equation D28, reduces the fidelity of the graph state as the overall time of construction increases. Hence, there is an optimum rate at which HoS can run, controlled by ξ and parameterized by the relevant total collection and detection efficiencies $\{\eta_e, \eta_s, \eta_i\}$, dark count rate, R_d, dephasing timescale, t_{rep}/τ, number of auxiliary spins, n_s, and total number of photons, n_p, required by the graph. Given a fixed set of parameters, this is a straightforward scalar maximization problem that can be accomplished numerically. If necessary, one can optimize within some ϵ of the optimum in order to achieve a speed-up in the rate.

4. Example applications

We briefly demonstrate how the sources of infidelity, presented in Appendix D 2, are combined to produce the fidelity estimates discussed in Section II and Section III. We note from the above that this fidelity is a mean estimate, optimized over ξ. For the estimates discussed in Section II and Section III, we assume a negligible dark count rate, and let $\eta_s = \eta_i = 1$. In practice the signal photon collection efficiency can be near unity [31], and only makes a minor impact on the rate and fidelity that does not affect the overall scaling of either function with the other relevant parameters. We carry out the optimization in numerically, and determine ξ which achieves the optimum fidelity.

a. GHZ states and cluster states

In Section IV, we present the mean final state fidelity to generate arbitrary graph states, requiring a single auxiliary spin in either of our schemes, such as the n_p-photon star graph, which is local-unitary equivalent to a GHZ state, or a 1D cluster state. For these graph states we optimize a function of the form

$$F_{\text{cluster,1D}}(\xi; n_p, \eta_e) = (F_{\text{ent}} F_{\text{swap}}(\xi; \eta_e))^{n_p} F_D^{(e)}(n_p) \langle F_D^{(s)}(n_p, P_s(\eta_e, \xi)) \rangle. \tag{D29}$$

Here, we have defined $F_{\text{ent}} = F_{CZ} F_p$ to combine the spin-spin entangling gate and photon-pair entanglement fidelities respectively. In Figure 4, we compare the effects of false heralds and decoherence against the limits imposed by imperfect spin-spin gate and initial SPDC photon-pair entanglement fidelities, and hence set $F_{\text{ent}} = 1$ when computing estimates in the false herald and decoherence limited regimes. In the decoherence limited regime we additionally set $F_{\text{swap}} = 1$ and subsequently do not require optimization. Computing the fidelity to make large 1D and 2D cluster states in our schemes with perfect spin-spin entangling gates and initial photon-pair entanglement assumes that additional error-correction or purification is employed.

b. Multi-party computation

For the multi-party computation protocol introduced in Section III, fidelity estimates for the generation of $|G_I\rangle$ and $|G_{II}\rangle$ are required to estimate the total bit error probability in Stage I and II, respectively. We assume graph states constructed in the HoD scheme discussed in Section II, where the computation of f happens in parallel with the construction of each state, and no pair source or photonic memory is required. In this scheme we take $P_s = \eta_e = 0.4$, from trapped ion experiments utilizing parabolic reflectors [17]. Additionally, we assume a dephasing timescale $t_{\text{rep}}/\tau = 10^{-9}$, following the best estimates for trapped ions [10]. The production of arbitrarily large graph states using our scheme is predominately limited by the spin-spin entangling gate fidelity and photon-pair entanglement fidelity, F_{CZ} and F_p respectively. However, for a fixed number of parties N, the size of the required graph states for our protocol is also fixed. For each of iteration of Stage I, the source is required to generate a copy of the eight-qubit graph state, $|G_I\rangle$, depicted in Figure 5. From Equations D18 and D28, the mean fidelity to produce each copy of the state is

$$F_{G_I} = F_{\text{ent}}^8 F_{CZ}^3 F_D^{(e)}(8)\langle F_D^{(s_1)}(8,\eta_e)\rangle\langle F_D^{(s_2)}(2,\eta_e)\rangle, \tag{D30}$$

where we have defined again $F_{\text{ent}} = F_{CZ}F_p$. We note additional spin-spin entangling gates are required to make this graph state from Equation D29. In Stage II, the source distributes a single copy of the $N+1$-qubit graph state, $|G_{II}\rangle$, depicted in Figure 6, where N is number of parties involved in the computation. The mean fidelity to produce this state is

$$F_{G_{II}}(N) = F_{\text{ent}}^{N+1} F_D^{(e)}(N+1)\langle F_D^{(s)}(N+1,\eta_e)\rangle, \tag{D31}$$

which is equivalent to fidelity in Equation D29, upon setting $n_p = N+1$.

[1] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[2] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[3] N. H. Lindner and T. Rudolph, Phys. Rev. Lett. **103**, 113602 (2009).
[4] S. E. Economou, N. Lindner, and T. Rudolph, Phys. Rev. Lett. **105**, 093601 (2010).
[5] A. Russo, E. Barnes, and S. E. Economou, New Journal of Physics **21**, 055002 (2019).
[6] P. Hilaire, L. Vidro, H. S. Eisenberg, and S. E. Economou, Quantum **7**, 992 (2023).
[7] Y. Zhan and S. Sun, Physical Review Letters **125**, 223601 (2020).
[8] D. Cogan, Z.-E. Su, O. Kenneth, and D. Gershoni, Nature Photonics **17**, 324–329 (2023).
[9] D. Bluvstein, H. Levine, G. Semeghini, T. T. Wang, S. Ebadi, M. Kalinowski, A. Keesling, N. Maskara, H. Pichler, M. Greiner, V. Vuletić, and M. D. Lukin, Nature **604**, 451–456 (2022).
[10] P. Wang, C.-Y. Luan, M. Qiao, M. Um, J. Zhang, Y. Wang, X. Yuan, M. Gu, J. Zhang, and K. Kim, Nature communications **12**, 1 (2021).
[11] S. J. Evered, D. Bluvstein, M. Kalinowski, S. Ebadi, T. Manovitz, H. Zhou, S. H. Li, A. A. Geim, T. T. Wang, N. Maskara, H. Levine, G. Semeghini, M. Greiner, V. Vuletić, and M. D. Lukin, Nature **622**, 268–272 (2023).
[12] R. Srinivas, S. C. Burd, H. M. Knaack, R. T. Sutherland, A. Kwiatkowski, S. Glancy, E. Knill, D. J. Wineland, D. Leibfried, A. C. Wilson, D. T. C. Allcock, and D. H. Slichter, Nature **597**, 209–213 (2021).
[13] C. R. Clark, H. N. Tinkey, B. C. Sawyer, A. M. Meier, K. A. Burkhardt, C. M. Seck, C. M. Shappert, N. D. Guise, C. E. Volin, S. D. Fallek, H. T. Hayden, W. G. Rellergert, and K. R. Brown, Physical Review Letters **127**, 10.1103/physrevlett.127.130505 (2021).
[14] G. Shu, C.-K. Chou, N. Kurz, M. R. Dietrich, and B. B. Blinov, J. Opt. Soc. Am. B **28**, 2865 (2011).
[15] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, Nature Physics **11**, 37 (2015).
[16] C.-K. Chou, C. Auchter, J. Lilieholm, K. Smith, and B. Blinov, Review of Scientific Instruments **88** (2017).
[17] R. Maiwald, A. Golla, M. Fischer, M. Bader, S. Heugel, B. Chalopin, M. Sondermann, and G. Leuchs, Physical Review A **86**, 043431 (2012).
[18] A. Kinos, D. Hunger, R. Kolesov, K. Mølmer, H. de Riedmatten, P. Goldner, A. Tallaire, L. Morvan, P. Berger, S. Welinski, *et al.*, arXiv preprint arXiv:2103.15743 (2021).
[19] R. Yanagimoto, R. Nehra, R. Hamerly, E. Ng, A. Marandi, and H. Mabuchi, PRX Quantum **4**, 010333 (2023).
[20] S. E. Economou, L. J. Sham, Y. Wu, and D. G. Steel, Phys. Rev. B **74**, 205415 (2006).
[21] M. Gimeno-Segovia, T. Rudolph, and S. E. Economou, Phys. Rev. Lett. **123**, 070501 (2019).
[22] D. Rieländer, A. Lenhard, M. Mazzera, and H. De Riedmatten, New Journal of Physics **18**, 123013 (2016).
[23] J. P. Covey, H. Weinfurter, and H. Bernien, npj Quantum Information **9**, 10.1038/s41534-023-00759-9 (2023).

[24] T. Ward and M. Keller, New Journal of Physics **24**, 123028 (2022).

[25] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, Phys. Rev. Lett. **130**, 050803 (2023).

[26] H. Jayakumar, A. Predojević, T. Kauten, T. Huber, G. S. Solomon, and G. Weihs, Nature Communications **5**, 10.1038/ncomms5251 (2014).

[27] P. Senellart, G. Solomon, and A. White, Nature Nanotechnology **12**, 1026–1039 (2017).

[28] J. Schneeloch, S. H. Knarr, D. F. Bogorin, M. L. Levangie, C. C. Tison, R. Frank, G. A. Howland, M. L. Fanto, and P. M. Alsing, Journal of Optics **21**, 043501 (2019).

[29] C. Zhang, Y.-F. Huang, B.-H. Liu, C.-F. Li, and G.-C. Guo, Advanced Quantum Technologies **4**, 2000132 (2021).

[30] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Physical review letters **80**, 3891 (1998).

[31] S. Ramelow, A. Mech, M. Giustina, S. Gröblacher, W. Wieczorek, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, *et al.*, Optics express **21**, 6707 (2013).

[32] B. Li, S. E. Economou, and E. Barnes, npj Quantum Information **8**, 10.1038/s41534-022-00522-6 (2022).

[33] A. Lamas-Linares, J. C. Howell, and D. Bouwmeester, Nature **412**, 887 (2001).

[34] N. Sangouard, B. Sanguinetti, N. Curtz, N. Gisin, R. Thew, and H. Zbinden, Physical review letters **106**, 120403 (2011).

[35] D. L. P. Vitullo, M. G. Raymer, B. J. Smith, M. Karpiński, L. Mejling, and K. Rottwitt, Phys. Rev. A **98**, 023836 (2018).

[36] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **121**, 250505 (2018).

[37] M. Houshmand, M. Houshmand, and J. F. Fitzsimons, Phys. Rev. A **98**, 012318 (2018).

[38] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).

[39] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix, New Journal of Physics **9**, 250–250 (2007).

[40] S. Bartolucci, P. Birchall, H. Bombín, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, F. Pastawski, T. Rudolph, and C. Sparrow, Nature Communications **14**, 10.1038/s41467-023-36493-1 (2023).

[41] M. C. Löbl, S. Paesani, and A. S. Sørensen, Quantum **8**, 1302 (2024).

[42] M. Pant, D. Towsley, D. Englund, and S. Guha, Nature communications **10**, 1070 (2019).

[43] R. Reichle, D. Leibfried, E. Knill, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Nature **443**, 838 (2006).

[44] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Review of scientific instruments **82**, 071101 (2011).

[45] A. C. Yao, in *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)* (1982) pp. 160–164.

[46] O. Goldreich, S. Micali, and A. Wigderson, in *Proceedings of the nineteenth annual ACM conference on Theory of computing - STOC '87*, STOC '87 (ACM Press, 1987).

[47] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y.-a. Tan, Information Sciences **476**, 357–372 (2019).

[48] D. Beaver, Efficient multiparty protocols using circuit randomization, in *Lecture Notes in Computer Science* (Springer Berlin Heidelberg, 1992) p. 420–432.

[49] J. B. Nielsen, P. S. Nordholt, C. Orlandi, and S. S. Burra, A new approach to practical active-secure two-party computation, in *Advances in Cryptology – CRYPTO 2012* (Springer Berlin Heidelberg, 2012) p. 681–700.

[50] I. Damgård, V. Pastro, N. Smart, and S. Zakarias, Multiparty computation from somewhat homomorphic encryption, in *Advances in Cryptology – CRYPTO 2012* (Springer Berlin Heidelberg, 2012) p. 643–662.

[51] A. Choudhury and A. Patra, IEEE Transactions on Information Theory **63**, 428–468 (2017).

[52] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. Fitzsimons, npj Quantum Information **5**, 10.1038/s41534-019-0142-2 (2019).

[53] A. Unnikrishnan and D. Markham, Phys. Rev. A **105**, 052420 (2022).

[54] S. Meesala, S. Wood, D. Lake, P. Chiappina, C. Zhong, A. D. Beyer, M. D. Shaw, L. Jiang, and O. Painter, Nature Physics , 1 (2024).

[55] S. Mittal, V. V. Orre, A. Restelli, R. Salem, E. A. Goldschmidt, and M. Hafezi, Physical Review A **96**, 043807 (2017).

[56] K.-H. Luo, H. Herrmann, S. Krapick, B. Brecht, R. Ricken, V. Quiring, H. Suche, W. Sohler, and C. Silberhorn, New Journal of Physics **17**, 073039 (2015).

[57] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).

[58] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, Physical Review Letters **124**, 10.1103/physrevlett.124.020402 (2020).

[59] C. Schön, E. Solano, F. Verstraete, J. I. Cirac, and M. M. Wolf, Physical Review Letters **95**, 10.1103/physrevlett.95.110503 (2005).

[60] S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).

[61] P. Kok and S. L. Braunstein, Phys. Rev. A **61**, 042304 (2000).

[62] U. Leonhardt and H. Paul, Progress in Quantum Electronics **19**, 89 (1995).

[63] R. Shah, K.-S. Isleif, F. Januschek, A. Lindner, and M. Schott, Journal of Low Temperature Physics **209**, 355–362 (2022).

[64] H. Lee, U. Yurtsever, P. Kok, G. M. Hockney, C. Adami, S. L. Braunstein, and J. P. Dowling, Journal of Modern Optics **51**, 1517 (2004).

[65] R. Rangarajan, M. Goggin, and P. Kwiat, Opt. Express **17**, 18920 (2009).

[66] M. V. Jabir and G. K. Samanta, Scientific Reports **7**, 12613 (2017).

[67] F. Steinlechner, S. Ramelow, M. Jofre, M. Gilaberte, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **21**, 11943 (2013).

[68] M. Medic, J. B. Altepeter, M. A. Hall, M. Patel, and P. Kumar, Opt. Lett. **35**, 802 (2010).

Concatenate codes, save qubits

Satoshi Yoshida[1] Shiro Tamiya[2] Hayata Yamasaki[1]

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*

[2] *Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

Abstract. The essential requirement for fault-tolerant quantum computation (FTQC) is the total protocol design to achieve a fair balance of all the critical factors relevant to its practical realization, such as the space overhead, the threshold, and the modularity. A major obstacle in realizing FTQC with conventional protocols, such as those based on the surface code and the concatenated Steane code, has been the space overhead, i.e., the required number of physical qubits per logical qubit. Protocols based on high-rate quantum low-density parity-check (LDPC) codes gather considerable attention as a way to reduce the space overhead, but problematically, the existing fault-tolerant protocols for such quantum LDPC codes sacrifice the other factors. Here we construct a new fault-tolerant protocol to meet these requirements simultaneously based on more recent progress on the techniques for concatenated codes rather than quantum LDPC codes, achieving a constant space overhead, a high threshold, and flexibility in modular architecture designs. In particular, under a physical error rate of 0.1%, our protocol reduces the space overhead to achieve the logical CNOT error rates 10^{-10} and 10^{-24} by more than 90% and 97%, respectively, compared to the protocol for the surface code. Furthermore, our protocol achieves the threshold of 2.4% under a conventional circuit-level error model, substantially outperforming that of the surface code. The use of concatenated codes also naturally introduces abstraction layers essential for the modularity of FTQC architectures. These results indicate that the code-concatenation approach opens a way to significantly save qubits in realizing FTQC while fulfilling the other essential requirements for the practical protocol design. The full paper of this work is on arXiv [1].

Keywords: Fault-tolerant quantum computation, Concatenated codes, High threshold and small space overhead, Stabilizer simulation

The realization of fault-tolerant quantum computation (FTQC) requires the total protocol design to meet all the essential factors relevant to its practical implementation, such as the space overhead, the threshold, and the modularity. The recent development of constant-overhead protocols [2–6, 6–8] substantially reduces the space overhead, i.e., the required number of physical qubits per logical qubit, compared to the conventional protocols such as those based on the surface code [9, 10] and the concatenated Steane code [11]. In particular, the most recent development [5] based on the concatenation of quantum Hamming codes [11, 12] is promising for the implementation of FTQC since Ref. [5] explicitly clarifies the full details of the protocol for implementing logical gates and efficient decoders, making it possible to realize universal quantum computation in a fault-tolerant way. Toward the practical implementation, however, it is indispensable to optimize the original protocol in Ref. [5] to improve its threshold, which is, by construction, at least as bad as the concatenated Steane code. Furthermore, even a proper quantitative evaluation of the original protocol in Ref. [5] was still missing due to the lack of the numerical study of the protocols based on the quantum Hamming codes.

In this work, we construct an optimized fault-tolerant protocol by substantially improving the protocol in Ref. [5], achieving an extremely low space overhead (Fig. 1) and a high threshold (2.4% for conventional circuit-level noise, see below) to simultaneously outperform the surface code. The optimization is performed based on our quantitative evaluation of the performance of the fault-tolerant protocols for various choices of quantum error-correcting codes, which we numerically carried out in a unified way under a circuit-level depolarizing error model following the convention of Ref. [13]. The original protocol in Ref. [5] is based on the concatenation of a series of quantum Hamming codes with increasing code sizes. Quantum Hamming code is a family of quantum codes $\mathcal{Q}_r$ parameterized by $r \in \{3, 4, \cdots\}$, consisting of $N_r = 2^r - 1$ physical qubits and $K_r = N_r - 2r$ logical qubits with code distance 3 [11, 12] (i.e., an $[[N_r, K_r, 3]]$ code). By concatenating the quantum Hamming code $\mathcal{Q}_{r_l}$ for a sequence $(r_l = l + 2)_{l=1,2,\cdots}$ of parameters at the concatenation level $l \in \{1, \cdots, L\}$, we obtain a quantum code consisting of $N = \prod_{l=1}^{L} N_{r_l}$ physical qubits and $K = \prod_{l=1}^{L} K_{r_l}$ logical qubits. Its space overhead, defined by the ratio of N and K [3], converges to a finite constant factor $\eta_\infty \approx 36$ as $L \to \infty$ [5]. However, our numerical simulation shows that the threshold of this original protocol is $\sim 10^{-5}$. Advancing over this original protocol, we newly construct and numerically analyze the optimized fault-tolerant protocol achieving the essential requirements for FTQC in the practical regime, such as low space overhead and high threshold, as summarized below.

1 Substantially smaller space overhead and higher threshold than the surface code in a practical regime

We optimize the original protocol in Ref. [5] by replacing the physical qubits of the original protocol with

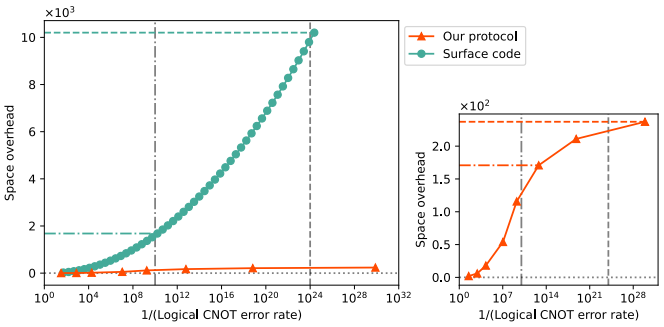


Figure 1: **Comparison of space overhead of the proposed protocol with that for the surface code.** The left figure plots the space overheads and logical error rates of the proposed protocol (▲) and the surface code (●). The right figure enlarges the plot for the proposed protocol. The logical error rate is calculated under a circuit-level depolarizing error model at a physical error rate 0.1%. The dash-dotted lines represent the logical error rate 10^{-10} and the corresponding space overhead, i.e., 1.7×10^2 physical qubits per logical qubit for our protocol. The dashed lines represent the logical error rate 10^{-24} and the corresponding space overhead, i.e., 2.4×10^2 physical qubits per logical qubit for our protocol. Our protocol reduces the space overhead to achieve the logical error rates 10^{-10} and 10^{-24} by more than 90% and 97%, respectively, compared to the protocol for the surface code.

logical qubits of a finite-size quantum code $\mathcal{Q}_0$ (called an underlying quantum code). With this replacement, we aim to improve the threshold determined at the physical level while maintaining the constant space overhead at the large concatenation levels. Here, the logical error rate of the underlying quantum code should be lower than the threshold of the original protocol so that the original protocol can further suppress the logical error rate. If the fixed-size underlying quantum code $\mathcal{Q}_0$ has N_0 physical qubits and K_0 logical qubits, the overall space overhead still converges to a constant value given by $\eta'_\infty = \frac{N_0}{K_0}\eta_\infty$. For our protocol, we propose the following code construction. As an underlying quantum code, we use the C_4/C_6 code [14] as first L' levels of the concatenated code, where the 4-qubit code denoted by $C_4(=[[4,2,2]])$ is concatenated with the 6-qubit code denoted by $C_6(=[[6,2,2]])$ for $L'-1$ times. On top of the underlying quantum code, i.e., at the concatenation levels $L'+1, L'+2, \cdots, L$, we concatenate quantum Hamming codes $\mathcal{Q}_{r_l}$ for an optimized choice of the sequence $(r_l)_{l=1,2,\ldots}$ of parameters, where $\mathcal{Q}_{r_l}$ is used at the concatenation level $L'+l$. The C_4/C_6 code is adopted as the underlying quantum code since it achieves the state-of-the-art high threshold (see Table II of the Technical Manuscript). To avoid the increase of overhead, we use a non-post-selected protocol of the C_4/C_6 code in Ref. [14] rather than a post-selected one.

Under a physical error rate of 0.1%, we compare the space overhead of our proposed protocol to achieve the logical CNOT error rates 10^{-10} and 10^{-24} with a conventional protocol for the surface code. Note that the concatenated Steane code cannot suppress the logical error rate under the physical error rate 0.1% since the threshold is smaller than 0.1% in our circuit-level error model (see Table II of the Technical Manuscript). Factoring of a 2048-bit integer using Shor's algorithm [15] requires the logical error rate 10^{-10} [16], which is relevant to the currently used cryptosystem RSA-2048 [17, 18]. The logical error rate $\sim 10^{-24}$ is a rough estimate of the logical error rate of classical computation.

As shown in Fig. 1, our protocol saves the space overheads by more than 90% and 97% to achieve the logical error rates 10^{-10} and 10^{-24}, respectively, compared to the surface code. Note that our protocol achieves constant space overhead while the protocol for the surface code (as well as that for the concatenated Steane code) has growing space overhead; thus, in principle, the advantage of our protocol can be arbitrarily large as the target logical error rate becomes small. However, our contribution here is to clarify that our protocol indeed offers a space-overhead advantage by orders of magnitude in the practical regimes.

We remark that our protocol is constructed without assuming geometrical constraints on quantum gates. Nonlocal interactions are indispensable to avoid the growing space overhead of FTQC on large scales, which has been a major obstacle to implementing FTQC; in particular, a polylogarithmically growing space overhead is inevitable as long as one sticks to an architecture with two-dimensional two-qubit gate connectivity [19]. By contrast, all-to-all connectivity of physical gates is indeed becoming possible in various experimental platforms, such as neutral atoms [20], trapped ions [21, 22], and optics [23–25]; in such cases, the proposed protocol substantially reduces the space overhead compared to the surface code, as shown in Fig. 1. Consequently, our protocol lends increased importance to such physical platforms with all-to-all connectivity; at the same time, the technological progress on the experimental side may also lead to extra factors to be considered for practical FTQC protocols, and our results and techniques constitute a basis for further optimization of the fault-tolerant protocols in these platforms.

2 Flexible optimization of the quantum code

The quantum code used for our protocol is designed by optimizing the underlying quantum code, and under the physical error rate 0.1%, our optimized choice of the underlying quantum code turns out to be the level-4 C_4/C_6 code (see Table II of the Technical Manuscript). For this optimization, we compare four candidate quantum codes: the C_4/C_6 code [14], the surface code [9, 10], the concatenated Steane code [26], and the C_4/Steane code. The C_4/Steane code is newly constructed in this work by concatenating the $[[4,2,2]]$ code (i.e., the C_4 code) with the Steane code. For each of the physical error rates $p = 0.01\%, 0.1\%, 1\%$, we compare the thresholds and the space overheads of these four candidate quantum codes

to achieve the logical error rate 10^{-24} by concatenating the code with a series of quantum Hamming codes.

As shown in Table II of the Technical Manuscript, the threshold of the protocol for the C_4/C_6 code has the highest threshold of 2.4% among the four candidate quantum codes, and thus, our optimized protocol uses the C_4/C_6 code as the underlying quantum code. For the physical error rates $p = 0.1\%, 1\%$, we show that the C_4/C_6 code indeed has the smallest space overhead among the four candidates. We also note that the optimal protocol may differ depending on the physical error rate; in particular, at $p = 0.01\%$, the C_4/Steane code leads to a smaller space overhead than the C_4/C_6 code. Our contribution here is to perform the numerical simulation of all the codes under the same circuit-level error model in a unified way to make a direct, systematic comparison.

3 Modularity in comparison with the quantum low-density parity-check (LDPC) code

We have so far presented the results of the quantitative analysis of our protocol based on the code-concatenation approach. We here compare this approach with another existing approach toward low-overhead FTQC based on the high-rate quantum LDPC codes originally proposed in Refs. [2–4].

The crucial difference between our approach based on concatenated codes and the approach based on quantum LDPC codes is modularity. In the approach of quantum LDPC code, one needs to realize a single large-size code block. To suppress the logical error rate more and more, each code block may become arbitrarily large, yet an essential assumption for the fault tolerance of the quantum LDPC codes is to keep the physical error rates constant [3, 4]. In experiments, problematically, it is in principle challenging to arbitrarily increase the number of qubits in a single quantum device without increasing physical error rates [27, 28]. By contrast, in the code-concatenation approach, we can realize a fixed-size code at each level of the code concatenation by putting finite efforts into improving a quantum device; that is, each fixed-size code serves as a fixed-size abstraction layer in the implementation. In this way, our code-concatenation approach offers modularity, an essential requirement for the FTQC architectures. (See also Technical Manuscript for more details.)

Apart from the modularity, another advantage is that our protocol based on concatenated codes can implement logical gates faster than the existing protocols for quantum LDPC codes. In the protocol for quantum LDPC codes in Refs. [3, 4], almost all gates, including most of the Clifford gates, are implemented by gate teleportation using auxiliary code blocks; to maintain constant space overhead, gates must be applied sequentially, which incurs a long time overhead. Other Clifford gate schemes are proposed based on code deformation [6] and lattice surgery [7], but they also introduce additional overheads in time and space. Apart from these schemes for logical gate implementations, a stabilizer measurement scheme for a constant-space-overhead quantum LDPC code in thin planar connectivity is presented in Ref. [8]. This protocol implements a quantum memory (i.e., the logical identity gate), but to implement universal quantum computation in a fault-tolerant way, we need to add the components to implement state preparation and logical gates, which incur the overhead issues in the same way as the above. More recent protocols in Refs. [29, 30] aim to improve the implementability of quantum LDPC codes, but in the same way, these protocols can only be used as the quantum memory; problematically, it is currently unknown how to realize logical gates with these protocols, and it is also unknown how to achieve constant-space-overhead FTQC based on these protocols without sacrificing their implementability. In contrast with these protocols, our protocol can implement universal quantum computation within constant space overhead and quasi-polylogarithmic time overhead, by using the concatenated code rather than quantum LDPC codes, as shown in Ref. [5].

Note that, due to this difference, it is not straightforward to obtain numerical results on the existing protocols for the high-rate quantum LDPC codes in the same setting as our protocol; however, if one develops more efficient protocols achieving universal quantum computation using the high-rate quantum LDPC codes, our comparison between our protocol with that of the surface code serves as a useful baseline. We also point out that in the current status, even if one wants to implement constant-space-overhead FTQC using quantum LDPC codes, one eventually needs to use concatenated codes in combination. In particular, as shown in Refs. [3, 4], the existing constant-space-overhead fault-tolerant protocols for such quantum LDPC codes rely on concatenated codes for preparation of logical $|0\rangle$ states, e.g., by using the encoding procedure implemented by the concatenated Steane code [31]. Thus, even though a part of the protocol using the high-rate quantum LDPC codes may be efficient, the part relying on the concatenated codes may become a bottleneck in practice, which should be taken into account in future work for a fair comparison of the overall protocols.

4 Conclusion

This work constructs a fault-tolerant protocol based on the code concatenation achieving all the desired features for its practical realization: a small space overhead, a high threshold, and modularity. Our numerical simulation shows that our protocol substantially outperforms that of the surface code, which implies a promising utility of the concatenated code for the implementation of FTQC. At the same time, our results and techniques for systematic analysis of various quantum codes constitute a basis for further optimization of the fault-tolerant protocols in the practical physical platforms, especially with all-to-all connectivity.

References

[1] S. Yoshida, S. Tamiya, and H. Yamasaki, arXiv:2402.09606 (2024).

[2] A. A. Kovalev and L. P. Pryadko, Phys. Rev. A **87**, 020304 (2013).

[3] D. Gottesman, Quantum Info. Comput. **14**, 1338–1372 (2014).

[4] O. Fawzi, A. Grospellier, and A. Leverrier, in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (2018) pp. 743–754.

[5] H. Yamasaki and M. Koashi, Nature Physics **20**, 247 (2024).

[6] A. Krishna and D. Poulin, Phys. Rev. X **11**, 011023 (2021).

[7] L. Z. Cohen, I. H. Kim, S. D. Bartlett, and B. J. Brown, Science Advances **8**, eabn1717 (2022).

[8] M. A. Tremblay, N. Delfosse, and M. E. Beverland, Phys. Rev. Lett. **129**, 050504 (2022).

[9] S. B. Bravyi and A. Y. Kitaev, arXiv:quant-ph/9811052 [quant-ph] (1998).

[10] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, Journal of Mathematical Physics **43**, 4452 (2002).

[11] A. M. Steane, Phys. Rev. A **54**, 4741 (1996).

[12] R. W. Hamming, The Bell system technical journal **29**, 147 (1950).

[13] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Phys. Rev. A **86**, 032324 (2012).

[14] E. Knill, Nature **434**, 39 (2005).

[15] P. Shor, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.

[16] C. Gidney and M. Ekerå, Quantum **5**, 433 (2021).

[17] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120 (1978).

[18] E. Barker and Q. Dang, NIST, Tech. Rep **16** (2016).

[19] N. Baspin, O. Fawzi, and A. Shayeghi, arXiv:2302.04317 [quant-ph] (2023).

[20] 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).

[21] 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, Phys. Rev. X **11**, 041058 (2021).

[22] L. Egan, D. M. Debroy, C. Noel, A. Risinger, D. Zhu, D. Biswas, M. Newman, M. Li, K. R. Brown, M. Cetina, *et al.*, Nature **598**, 281 (2021).

[23] H. Yamasaki, K. Fukui, Y. Takeuchi, S. Tani, and M. Koashi, arXiv:2006.05416 [quant-ph] (2020).

[24] 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, Quantum **5**, 392 (2021).

[25] D. Litinski and N. Nickerson, arXiv:2211.15465 [quant-ph] (2022).

[26] A. M. Steane, Phys. Rev. A **68**, 042322 (2003).

[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, arXiv:2308.08648 [quant-ph] (2023).

[28] M. Fellous-Asiani, J. H. Chai, Y. Thonnart, H. K. Ng, R. S. Whitney, and A. Auffèves, PRX Quantum **4**, 040319 (2023).

[29] C. A. Pattison, A. Krishna, and J. Preskill, arXiv:2303.04798 [quant-ph] (2023).

[30] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, arXiv:2308.07915 [quant-ph] (2023).

[31] M. Christandl and A. Müller-Hermes, IEEE Transactions on Information Theory **70**, 282 (2022).

Concatenate codes, save qubits

Satoshi Yoshida,[1,*] Shiro Tamiya,[2,†] and Hayata Yamasaki[1,‡]

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*
[2] *Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

(Dated: February 16, 2024)

The essential requirement for fault-tolerant quantum computation (FTQC) is the total protocol design to achieve a fair balance of all the critical factors relevant to its practical realization, such as the space overhead, the threshold, and the modularity. A major obstacle in realizing FTQC with conventional protocols, such as those based on the surface code and the concatenated Steane code, has been the space overhead, i.e., the required number of physical qubits per logical qubit. Protocols based on high-rate quantum low-density parity-check (LDPC) codes gather considerable attention as a way to reduce the space overhead, but problematically, the existing fault-tolerant protocols for such quantum LDPC codes sacrifice the other factors. Here we construct a new fault-tolerant protocol to meet these requirements simultaneously based on more recent progress on the techniques for concatenated codes rather than quantum LDPC codes, achieving a constant space overhead, a high threshold, and flexibility in modular architecture designs. In particular, under a physical error rate of 0.1%, our protocol reduces the space overhead to achieve the logical CNOT error rates 10^{-10} and 10^{-24} by more than 90% and 97%, respectively, compared to the protocol for the surface code. Furthermore, our protocol achieves the threshold of 2.4% under a conventional circuit-level error model, substantially outperforming that of the surface code. The use of concatenated codes also naturally introduces abstraction layers essential for the modularity of FTQC architectures. These results indicate that the code-concatenation approach opens a way to significantly save qubits in realizing FTQC while fulfilling the other essential requirements for the practical protocol design.

The realization fault-tolerant quantum computation (FTQC) requires the total protocol design to meet all the essential factors relevant to its practical implementation, such as the space overhead, the threshold, and the modularity. The recent development of constant-overhead protocols [1–7] substantially reduces the space overhead, i.e., the required number of physical qubits per logical qubit, compared to the conventional protocols such as those based on the surface code [8, 9] and the concatenated Steane code [10]. In particular, the most recent development [4] based on the concatenation of quantum Hamming codes [10, 11] is promising for the implementation of FTQC since Ref. [4] explicitly clarifies the full details of the protocol for implementing logical gates and efficient decoders, making it possible to realize universal quantum computation in a fault-tolerant way. Toward the practical implementation, however, it is indispensable to optimize the original protocol in Ref. [4] to improve its threshold, which is, by construction, at least as bad as the concatenated Steane code. Furthermore, even a proper quantitative evaluation of the original protocol in Ref. [4] was still missing due to the lack of the numerical study of the protocols based on the quantum Hamming codes.

In this work, we construct an optimized fault-tolerant protocol by substantially improving the protocol in Ref. [4], achieving an extremely low space overhead and a high threshold to simultaneously outperform the surface code. The optimization is performed based on our quantitative evaluation of the performance of the fault-tolerant protocols for various choices of quantum error-

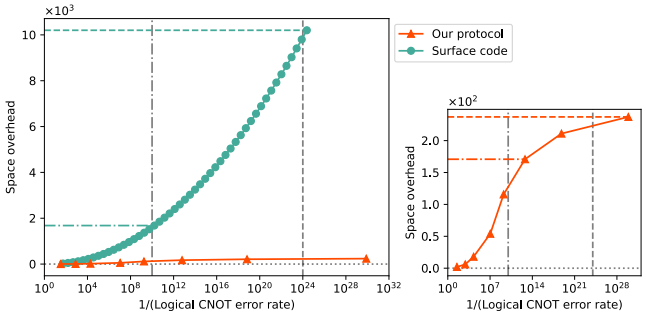


FIG. 1. **Comparison of space overhead of the proposed protocol with that for the surface code.** The left figure plots the space overheads and logical error rates of the proposed protocol (▲) and the surface code (●). The right figure enlarges the plot for the proposed protocol. The logical error rate is calculated under a circuit-level depolarizing error model at a physical error rate 0.1%. The dash-dotted lines represent the logical error rate 10^{-10} and the corresponding space overhead, i.e., 1.7×10^2 physical qubits per logical qubit for our protocol. The dashed lines represent the logical error rate 10^{-24} and the corresponding space overhead, i.e., 2.4×10^2 physical qubits per logical qubit for our protocol. Our protocol reduces the space overhead to achieve the logical error rates 10^{-10} and 10^{-24} by more than 90% and 97%, respectively, compared to the protocol for the surface code.

* satoshiyoshida.phys@gmail.com
† shiro.tamiya01@gmail.com
‡ hayata.yamasaki@gmail.com

TABLE I. **Construction of the proposed protocol.** Our quantum code uses the level-4 C_4/C_6 code as an underlying quantum code, and on top of this, we concatenate a series of quantum Hamming codes. The second column of this table shows a quantum code to be concatenated at each level. The rightmost column of this table shows the space overhead, which is the ratio of the number of physical qubits denoted by N and the number of logical qubits denoted by K.

	Quantum code	N	K	N/K
level-1	$C_4(=[[4,2,2]])$	4	2	2
level-2	$C_6(=[[6,2,2]])$	12	2	6
level-3	$C_6(=[[6,2,2]])$	36	2	18
level-4	$C_6(=[[6,2,2]])$	108	2	54
level-5	$\mathcal{Q}_4(=[[15,7,3]])$	1.6×10^3	14	1.2×10^2
level-6	$\mathcal{Q}_5(=[[31,21,3]])$	5.0×10^4	2.9×10^2	1.7×10^2
level-7	$\mathcal{Q}_6(=[[63,51,3]])$	3.2×10^6	1.5×10^4	2.1×10^2
level-8	$\mathcal{Q}_7(=[[127,113,3]])$	4.0×10^8	1.7×10^6	2.4×10^2

correcting codes (see Tables I and II), which we carried out in a unified way under a circuit-level depolarizing error model following the convention of Ref. [12]. Our numerical study makes it possible to optimize the combination of the quantum codes to be concatenated. Our numerical results show that the threshold of the original protocol for quantum Hamming codes in Ref. [4] is $\sim 10^{-5}$. To improve the threshold, our protocol uses the C_4/C_6 code [13] at the physical level; on top of the C_4/C_6 code, our protocol concatenates the quantum Hamming codes at the larger concatenation levels to achieve the constant space overhead. Under a physical error rate of 0.1%, compared to the conventional protocol for the surface code, our protocol reduces the space overhead to achieve the logical error rate 10^{-10} and 10^{-24} by more than 90% and 97%, respectively, (see Fig. 1). The threshold of our protocol is 2.4%, which substantially outperforms that of the surface code (see Table II). These results establish a basis for the practical fault-tolerant protocols, especially suited for the architectures with all-to-all two-qubit gate connectivity, such as neutral atoms [14], trapped ions [15, 16], and optics [17–19].

RESULTS

Setting. We construct a space-overhead-efficient fault-tolerant protocol by optimizing the protocol presented in Ref. [4]. The original protocol in Ref. [4] is based on the concatenation of a series of quantum Hamming codes with increasing code sizes. Quantum Hamming code is a family of quantum codes $\mathcal{Q}_r$ parameterized by $r \in \{3,4,\cdots\}$, consisting of $N_r = 2^r - 1$ physical qubits and $K_r = N_r - 2r$ logical qubits with code distance 3 [10, 11], which is written as an $[[N_r, K_r, 3]]$ code. By concatenating the quantum Hamming code $\mathcal{Q}_{r_l}$ for a sequence $(r_l = l+2)_{l=1,2,\ldots}$ of parameters at the concatenation level $l \in \{1,\cdots,L\}$, we obtain a quantum code consisting of $N = \prod_{l=1}^{L} N_{r_l}$ physical qubits and $K = \prod_{l=1}^{L} K_{r_l}$ logical qubits. Its space overhead, defined by the ratio of N and K [2], converges to a finite constant factor η_∞ as

$$\frac{N}{K} = \prod_{l=1}^{L} \frac{N_{r_l}}{K_{r_l}} \to \eta_\infty < \infty \quad \text{as} \quad L \to \infty, \tag{1}$$

where η_∞ is given by $\eta_\infty \approx 36$ [4]. However, the threshold of the protocol based on this quantum code is given by $\sim 10^{-5}$, as shown in Supplementary Information. As discussed in Ref. [4], instead of $r_l = l+2$, we can also take an arbitrary sequence $(r_l)_{l=1,2,\ldots}$ satisfying $\eta_\infty = \prod_{l=1}^{\infty} \frac{N_{r_l}}{K_{r_l}} < \infty$ to achieve the constant space overhead, and our choice of r_l will be clarified below.

We optimize this original protocol by replacing the physical qubits of the original protocol with logical qubits of a finite-size quantum code $\mathcal{Q}_0$ (called an underlying quantum code). With this replacement, we aim to improve the threshold determined at the physical level while maintaining the constant space overhead at the large concatenation levels. Here, the logical error rate of the logical qubits of the underlying quantum code should be lower than the threshold of the original protocol so that the original protocol can further suppress the logical error rate. If the underlying quantum code $\mathcal{Q}_0$ has N_0 physical qubits and K_0 logical qubits, the overall space overhead is given by

$$\frac{N}{K} = \frac{N_0}{K_0} \prod_{l=1}^{L} \frac{N_{r_l}}{K_{r_l}} \to \eta'_\infty < \infty \quad \text{as } L \to \infty, \tag{2}$$

which remains a constant value given by $\eta'_\infty = \frac{N_0}{K_0}\eta_\infty$ as long as we use a fixed code as the underlying quantum code.

For our protocol, we propose the following code construction:

- As an underlying quantum code, we use the C_4/C_6 code [13] as first L' levels of the concatenated code, where the 4-qubit code denoted by $C_4(=[[4,2,2]])$ is concatenated with the 6-qubit code denoted by $C_6(=[[6,2,2]])$ for $L'-1$ times.
- On top of the underlying quantum code, i.e., at the concatenation levels $L'+1, L'+2, \cdots, L$, we concatenate quantum Hamming codes $\mathcal{Q}_{r_l}$ for an optimized choice of the sequence $(r_l)_{l=1,2,\ldots}$ of parameters, where $\mathcal{Q}_{r_l}$ is used at the concatenation level $L'+l$.

The C_4/C_6 code is adopted as the underlying quantum code since it achieves the state-of-the-art high threshold. To avoid the increase of overhead, we use a non-post-selected protocol of the C_4/C_6 code in Ref. [13] rather than a post-selected one.

To estimate the space overhead and the threshold, we evaluate the logical CNOT error rate of the fault-tolerant protocols based on the C_4/C_6 code and the quantum

TABLE II. **Comparison of the error threshold and the required space overhead to achieve the logical error rate $P_0 < P_{\text{target}}$ of underlying quantum codes.** The table shows the error threshold and the required space overhead to achieve the logical error rate $P_0 < P_{\text{target}}$ under the physical error rates $p = 0.01\%, 0.1\%, 1\%$ for the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code. Bold values represent the minimum space overheads among the four quantum codes under the same physical error rates. Note that for $p = 1\%$, the C_4/C_6 code is the only one among the four codes that can suppress the logical error rate; similarly, for $p = 0.1\%$, the concatenated Steane code cannot suppress the logical error rate.

	Threshold	Space overhead		
		$p = 0.01\%$	$p = 0.1\%$	$p = 1\%$
C_4/C_6 code	2.4%	18	**54**	**1458**
Surface code	0.31%	121	841	-
Steane code	0.030%	343	-	-
C_4/Steane code	0.15%	**14**	4802	-

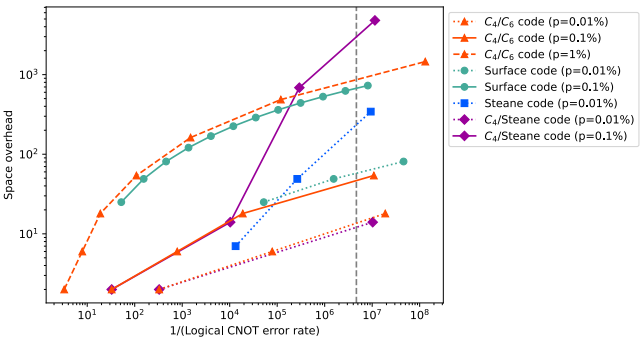


FIG. 2. **Comparison on space overheads of the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code.** The horizontal axis shows the inverse of the logical CNOT error rate, and the vertical axis the space overhead. The simulation is performed under the circuit-level depolarizing error model with the physical error rates given by $p = 0.01\%, 0.1\%, 1\%$. The vertical dashed line represents P_{target}, which is the required logical error rate such that, by concatenating quantum Hamming codes, the overall quantum code achieves a logical error rate below 10^{-24}.

Hamming codes. The logical CNOT error rate is evaluated at each concatenation level using the Monte Carlo sampling method in Refs. [20, 21], which is based on the reference entanglement method [13, 22]. By convention, we describe the noise on physical qubits by a circuit-level depolarizing error model (see Methods for the details of the simulation method and the error model). In the simulation, we assume no geometrical constraints on manipulating quantum gates, which is applicable to neutral atoms [14], trapped ions [15, 16], and optics [17–19]. Our numerical results show that by using the C_4/C_6 code as the underlying quantum code, our protocol achieves a high threshold 2.4% (see Table II), where we use the non-post-selected protocol of the C_4/C_6 code rather than the post-selected one in Ref. [13]. We optimize the combination of the quantum codes, i.e., the choice of parameters L', L, and r_l, based on our simulation results so as to reduce the space overhead. In particular, the optimized parameters that we found are $L' = 4$, $L = 8$, and $r_1 = 4, r_2 = 5, r_3 = 6, r_4 = 7$ (see Table I). Note that the Steane code $\mathcal{Q}_3$ in the original protocol of Ref. [4] is skipped to improve the space overhead of our protocol. To avoid the combinatorial explosion arising from the combinations of these parameters, we performed a level-by-level numerical simulation at each concatenation level (see Methods for the details). With this technique, our simulation makes it possible to flexibly optimize the combination of the quantum codes to be concatenated for designing our protocol.

Large-scale resource estimation. Under a physical error rate of 0.1%, we compare the space overhead of our proposed protocol to achieve the logical CNOT error rates 10^{-10} and 10^{-24} with a conventional protocol for the surface code. Note that another conventional protocol using the concatenated Steane code cannot suppress the logical error rate under the physical error rate 0.1% since the threshold is larger than 0.1% (see Table II). Factoring of a 2048-bit integer using Shor's algorithm [23] requires the logical error rate 10^{-10} [24], which is relevant to the currently used cryptosystem RSA-2048 [25, 26]. The logical error rate $\sim 10^{-24}$ is a rough estimate of the logical error rate of classical computation (see Methods for the details of these estimations).

As shown in Fig. 1, the surface code requires the space overhead $\sim 1.7 \times 10^3$ and $\sim 10.2 \times 10^3$ to achieve the logical error rates $\sim 10^{-10}$ and $\sim 10^{-24}$, respectively. On the other hand, our protocol only requires the space overheads $\sim 1.7 \times 10^2$ and $\sim 2.4 \times 10^2$ to achieve the same logical error rates, saving the space overheads by more than 90% and 97%, respectively, compared to the surface code. Note that our protocol achieves constant space overhead while the protocol for the surface code (as well as that for the concatenated Steane code) has growing space overhead; thus, in principle, the advantage of our protocol can be arbitrarily large as the target logical error rate becomes small. However, our contribution here is to clarify that our protocol indeed offers a space-overhead advantage by orders of magnitude in the practical regimes.

Comparison on underlying quantum codes. The quantum code for our protocol shown in Table I is obtained by optimizing the underlying quantum code, and under the physical error rate 0.1%, our optimized choice of the underlying quantum code turns out to be the level-4 C_4/C_6 code. Here, we show this optimization procedure in more detail. For this optimization, we compare four candidate quantum codes: the C_4/C_6 code [13], the surface code [8, 9], the concatenated Steane code [27], and the C_4/Steane code. The C_4/Steane code is newly constructed in this work by concatenating the $[[4, 2, 2]]$ code (i.e., the C_4 code) with the Steane code (see Supplementary Information for details). For simplicity, we

fix the series of quantum Hamming codes as $\mathcal{Q}_4$, $\mathcal{Q}_5$, $\mathcal{Q}_6$, and $\mathcal{Q}_7$, and compare the required space overhead to achieve the logical error rate 10^{-24}. If the underlying quantum code has a logical error rate smaller than $P_{\text{target}} = 2.2 \times 10^{-7}$, then our numerics shows that by concatenating the quantum Hamming codes, the overall quantum code achieves a logical error rate below 10^{-24}.

In Fig. 2 and Table II, we compare the thresholds and the space overheads of these four candidate quantum codes to achieve the logical error rate $P_0 < P_{\text{target}}$ at the physical error rates $p = 0.01\%$, $p = 0.1\%$, and $p = 1\%$. For a fair comparison, we performed the numerical simulation of implementing logical CNOT gates for all these four codes under the aforementioned circuit-level depolarizing error model. For the decoding of the surface code, we use the minimum-weight perfect matching decoder [28, 29], and for the other concatenated codes, we use a hard-decision decoder to cover practical situations where the efficiency of implementing the decoder matters (see Supplementary Information for more details). Conventionally, the threshold for the surface code is evaluated by implementing a quantum memory (i.e., the logical identity gate) [12], but for a fair comparison, we here evaluate that by the logical CNOT gate, which is implemented by lattice surgery [30, 31] and is simulated using the method in Ref. [32] (see Supplementary Information for details). Similarly, Ref. [27] evaluates the threshold for the concatenated Steane code by implementing the logical identity gate, but we evaluate that by the transversal implementation of the logical CNOT gate. Note that the thresholds evaluated by the logical CNOT gate may be worse than those by the logical identity gate [33], but our setting of the numerical simulation is motivated by the fact that the realization of quantum memory by just implementing the logical identity gate is insufficient for universal quantum computation. We also remark that various numerical simulations have been performed in the literature under different error models from ours, e.g., for the surface code in Refs. [34, 35], for the concatenated Steane code in Refs. [21, 34], and for the C_4/C_6 code in Refs. [13, 36], but our contribution here is to perform the numerical simulation of all the codes under the same circuit-level error model in a unified way to make a direct, systematic comparison.

As shown in Fig. 2 and Table II, for $p = 0.1\%$, the level-4 C_4/C_6 code has the minimum space overhead 54 to achieve $P_0 < P_{\text{target}}$. For $p = 0.01\%$, the level-2 C_4/Steane code has a smaller space overhead to achieve $P_0 < P_{\text{target}}$ than the level-3 C_4/C_6 code. Then, we obtain an overall protocol having the space overhead ~ 61 to achieve the logical error rate 10^{-24}. For $p = 1\%$, the C_4/C_6 code is the only one among the four candidate codes that can suppress the logical error rate since the thresholds for the other codes, such as the surface code, are worse than 1% in our setting. In this case, the level-7 C_4/C_6 code achieves $P_0 < P_{\text{target}}$. Then, we obtain an overall protocol having the space overhead $\sim 6.4 \times 10^3$ to achieve the logical error rate 10^{-24}.

Modularity in comparison with the quantum low-density parity-check (LDPC) code. We have so far offered a quantitative analysis of our protocol based on the code-concatenation approach. We here compare this approach with another existing approach toward low-overhead FTQC based on the high-rate quantum LDPC codes originally proposed in Refs. [1–3].

The crucial difference between our approach based on concatenated codes and the approach based on quantum LDPC codes is modularity. In the approach of quantum LDPC code, one needs to realize a single large-size code block. To suppress the logical error rate more and more, each code block may become arbitrarily large, yet an essential assumption for the fault tolerance of the quantum LDPC codes is to keep the physical error rates constant [2, 3]. In experiments, problematically, it is in principle challenging to arbitrarily increase the number of qubits in a single quantum device without increasing physical error rates [37, 38]. By contrast, in the code-concatenation approach, we can realize a fixed-size code at each level of the code concatenation by putting finite efforts into improving a quantum device; that is, each fixed-size code serves as a fixed-size abstraction layer in the implementation. As shown in Ref [4], as we increase the concatenation levels, the logical error rates are suppressed doubly exponentially, whereas the required number of gates for implementing each gadget grows much more slowly. Once the error rates are suppressed by a concatenated code at some concatenation level, the low error rate of each logical gate provides a margin for using more logical gates (i.e., tolerating more architectural overhead) to implement FTQC at the higher concatenation levels, which provides flexibility for scalable architecture design. For example, once we develop finite-size devices implementing the fixed-size code, we can further scale up FTQC by combining these error-suppressed devices by using quantum channels to connect these devices and implement another fixed-size code to be concatenated at the next concatenation level. These quantum channels can be lossier than the physical gates in each device since the quantum states that will go through the channels are already encoded. In this way, our code-concatenation approach offers modularity, an essential requirement for the FTQC architectures.

Apart from the modularity, another advantage is that our protocol based on concatenated codes can implement logical gates faster than the existing protocols for quantum LDPC codes. In the protocol for quantum LDPC codes in Refs. [2, 3], almost all gates, including most of the Clifford gates, are implemented by gate teleportation using auxiliary code blocks; to maintain constant space overhead, gates must be applied sequentially, which incurs the polynomial time overhead. Other Clifford gate schemes are proposed based on code deformation [5] and lattice surgery [6], but they also introduce additional overheads. In particular, the code deformation scheme may introduce an additional time overhead that may be worse than the gate teleportation method [5].

The lattice surgery scheme requires a large patch of the surface code, which makes the space overhead of the overall protocol non-constant if we want to attain low time overhead [6]. Apart from these schemes for logical gate implementations, a stabilizer measurement scheme for a constant-space-overhead quantum LDPC code in thin planar connectivity is presented in Ref. [7]. This protocol implements a quantum memory (i.e., the logical identity gate), but to implement universal quantum computation in a fault-tolerant way, we need to add the components to implement state preparation and logical gates, which incur the overhead issues in the same way as the above. More recent protocols in Refs. [39, 40] aim to improve the implementability of quantum LDPC codes, but in the same way, these protocols can only be used as the quantum memory; problematically, it is currently unknown how to realize logical gates with these protocols, and it is also unknown how to achieve constant-space-overhead FTQC based on these protocols without sacrificing their implementability. In contrast with these protocols, our protocol can implement universal quantum computation within constant space overhead and quasi-polylogarithmic time overhead, by using the concatenated code rather than quantum LDPC codes, as shown in Ref. [4]. Due to this difference, it is not straightforward to obtain numerical results on the existing protocols for the high-rate quantum LDPC codes in the same setting as our protocol; however, if one develops more efficient protocols achieving universal quantum computation using the high-rate quantum LDPC codes, the current numerical results on comparing our protocol with those of the surface code and the concatenated Steane code also serve as a useful baseline for further comparison, which we leave for future work.

We also point out that in the current status, even if one wants to implement constant-space-overhead FTQC using quantum LDPC codes, one eventually needs to use concatenated codes in combination. In particular, as shown in Refs. [2, 3], the existing constant-space-overhead fault-tolerant protocols for such quantum LDPC codes rely on concatenated codes for preparation of logical $|0\rangle$ states, e.g., by using the encoding procedure implemented by the concatenated Steane code [41]. Thus, even though a part of the protocol using the high-rate quantum LDPC codes may be efficient, the part relying on the concatenated codes may become a bottleneck in practice, which should be taken into account in future work for a fair comparison of the overall protocols.

DISCUSSION

In this work, we have constructed a low-overhead, high-threshold, modular protocol for FTQC based on the recent progress on the code-concatenation approach in Ref. [4]. To design our protocol, we have performed thorough numerical simulations of the performance of fault-tolerant protocols for various quantum codes, under the same circuit-level error model in a unified way, as shown in Figs. 1 and 2 and Tables I and II. Based on these numerical results, we have proposed an optimized protocol, which we have designed by seeking an optimized combination of the underlying quantum code at the physical level and the series of quantum Hamming codes at higher concatenation levels. The proposed protocol (Table I) uses a fixed-size C_4/C_6 code at the physical level to attain a high threshold and, on top of this underlying quantum code, concatenate the quantum Hamming codes to achieve the constant space overhead. This proposed protocol achieves a substantial saving of the space overhead compared to that of the surface code (Fig. 1), has a higher threshold 2.4% than those of the surface code and the concatenated Steane code (Table II), and offers modularity owing to the code-concatenation approach.

At the same time, as shown in Fig. 2, our results show that the optimal choice of the underlying quantum code to minimize the space overhead may change depending on the physical error rate; in particular, we find that the C_4/Steane code that we have developed in this work can outperform the C_4/C_6 code at the physical error rate 0.01% while the C_4/C_6 code is better at the physical error rates 0.1% and 1%. Since our protocol is based on concatenated codes, the proposed protocol has flexibility in the choice of the underlying quantum code and the sequence of quantum Hamming codes to be concatenated, which will also be useful for further optimization of fault-tolerant protocols depending on the advances of experimental technologies in the future.

Lastly, we remark that we have constructed our fault-tolerant protocol without assuming geometrical constraints on quantum gates. Non-local interactions are indispensable to avoid the growing space overhead of FTQC on large scales, which has been a major obstacle to implementing FTQC; in particular, a polylogarithmically growing space overhead is inevitable as long as one sticks to an architecture with two-dimensional two-qubit gate connectivity [42]. By contrast, all-to-all connectivity of physical gates is indeed becoming possible in various experimental platforms, such as neutral atoms [14], trapped ions [15, 16], and optics [17–19]; in such cases, the proposed protocol substantially reduces the space overhead compared to the surface code, as shown in Fig. 1. Consequently, our protocol lends increased importance to such physical platforms with all-to-all connectivity; at the same time, the technological progress on the experimental side may also lead to extra factors to be considered for practical FTQC protocols, and our results and techniques constitute a basis for further optimization of the fault-tolerant protocols in these platforms.

METHODS

In Methods, after summarizing the notations, we first describe the error model used in the numerical simulation and the Monte Carlo simulation method to evaluate

the logical CNOT error rate. Then, we provide the details of our estimation of the required logical error rate of quantum computation, based on the evaluation of the CNOT gate counts of the quantum circuit implementing Shor's algorithm for 2048-bit RSA integer factoring and the required error rates for the classical computation. Finally, we present our method for estimating the logical CNOT error rate of the large-scale concatenated codes using the small-scale level-by-level simulation results at each concatenation level.

Notation. The computational basis (also called the Z basis) of a qubit $\mathbb{C}^2$ is denoted by $\{|0\rangle, |1\rangle\}$, and the complementary basis (also called the X basis) $\{|+\rangle, |-\rangle\}$ is defined by $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. By the convention of Ref. [43], we use the following notation on 1-qubit and 2-qubit unitaries:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{3}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{4}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{5}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{6}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{7}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{8}$$

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{9}$$

where the 1-qubit and 2-qubit unitaries are shown in the matrix representations in the computational bases $\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2$ and $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\} \subset \mathbb{C}^2 \otimes \mathbb{C}^2$, respectively. See also Ref. [44] for terminology on FTQC.

Error model. In this work, the stabilizer circuits for describing the fault-tolerant protocols are composed of state preparations of $|0\rangle$ and $|+\rangle$, measurements in the Z and X bases, single-qubit gates I, X, Y, Z, H, S, and a two-qubit CNOT gate. Each of these preparation, measurement, and gate operations in a circuit is called a location in the circuit. By the convention of Ref. [12], we use a circuit-level depolarizing error model. In this model, independent and ideally distributed (IID) Pauli errors randomly occur at each location, i.e., after state preparations and gates, and before measurements. By convention, we ignore the error and the runtime of polynomial-time classical computation used for decoding in the fault-tolerant protocols.

The probabilities of the errors are given using a single parameter p (called the physical error rate) as follows. State preparations of $|0\rangle$ and $|+\rangle$ are followed by X and Z gates, respectively, with probability p. Measurements in Z and X bases follow X and Z gates, respectively, with probability p. One-qubit gates I, X, Y, Z, H, S are followed by one of the 3 possible non-identity Pauli operators $\{X, Y, Z\}$, each with probability $p/3$. A two-qubit gate CNOT is followed by one of the 15 possible non-identity Pauli products acting on 2 qubits $\{\sigma_1 \otimes \sigma_2\}_{(\sigma_1,\sigma_2)\in\{I,X,Y,Z\}^2} \setminus \{I \otimes I\}$, each with probability $p/15$.

Simulation to evaluate logical CNOT error rates. In our numerical simulation, we evaluate the logical CNOT error rate using the Monte Carlo sampling method presented in Refs. [20, 21], which is based on the reference entanglement method [13, 22]. For a quantum code consisting of N physical qubits and K logical qubits, the circuit that we use for the Monte Carlo sampling method is illustrated in Fig. 3, where we assume that random Pauli errors occur at each location of the circuit according to the error model described above. In particular, starting from two error-free logical Bell states, we repeatedly apply a gate gadget of the logical $\mathrm{CNOT}^{\otimes K}$ gate followed by an error correction gadget, which is repeated ten times. For all the quantum codes (which are Calderbank-Shor-Steane (CSS) codes in this work) except for the surface code, we implement the logical CNOT gates transversally and use Knill's error correction gadget [13] for error correction. For the surface code, by convention, we use the lattice surgery [30, 31] to implement the logical CNOT gates, which includes the error correction. Note that the transversal implementation of the logical CNOT gate is also possible for the surface code, but we performed our numerical simulation based on the lattice surgery since the lattice surgery is more widely used in the literature on resource estimation for FTQC, such as Refs. [45, 46]. Then, we apply the error-free logical Bell measurement on the output quantum state. Any measurement outcomes that do not result in all zeros for the first logical qubits in four code blocks are counted as logical errors. We evaluate the logical CNOT error rate by dividing the empirical logical error probability in the simulation by ten. Since the quantum circuit in Fig. 3, including Pauli errors, is composed of Clifford gates, the sampling of measurement outcomes is efficiently simulated by a stabilizer circuit simulator; in particular, our simulation is conducted with Stim [47].

Logical error rate required for 2048-bit RSA integer factoring. The security of the RSA cryptosystem is ensured by the classical hardness of integer factoring, and factoring 2048-bit integers given as the product of two similar-size prime numbers, which is called RSA integers in Ref. [24] leads to breaking RSA-2048. Previous works have investigated efficient algorithms for RSA integer factoring based on Shor's algorithm [23]. In particular, Ref. [24] proposes an n-bit RSA integer factoring algorithm using $0.3n^3 + 0.0005n^3 \lg n$ Toffoli gates. Since a Toffoli gate can be decomposed into 6 CNOT gates and single-qubit gates [43], this algorithm can be implemented by $1.8n^3 + 0.003n^3 \lg n$ CNOT gates. For

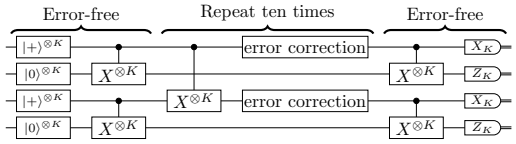


FIG. 3. **A quantum circuit for the reference entanglement method [13, 20–22] to estimate a logical CNOT error rate.** In this simulation, starting from two error-free logical Bell states, we apply a gate gadget of the logical CNOT$^{\otimes K}$ gate followed by the error correction gadget ten times, using a noisy circuit. For the surface code, we use the lattice surgery [30, 31] to implement logical CNOT gates, which includes the error correction. For the other codes, we implement logical CNOT gates transversally and use Knill's error correction gadget [13] for error correction. Finally, we apply the error-free logical Bell measurement on the output quantum state to estimate the logical error rate. The symbol with X_K (Z_K) denotes the measurements in X (Z) basis for all the K logical qubits in a code block.

$n = 2048$, it requires $\sim 10^{10}$ CNOT gates. Thus, we require a logical error rate $\sim 10^{-10}$ to run this algorithm.

Required error rate for classical computation. The required error rate for classical computation is estimated by taking an inverse of the number of elementary gates in a large-scale classical computation that is currently available. In particular, we consider a situation where the supercomputer Fugaku [48] is run for a month. The peak performance at double precision of Fugaku in the normal mode is given 488 petaflops $\sim 5 \times 10^{17}$ s^{-1} [48]. If we run it for 1 month $\sim 2.6 \times 10^6$ s, then the number of elementary gates is roughly estimated as $\sim 10^{24}$. Thus, an upper bound of the logical error rate of classical computation is roughly estimated as $\sim 10^{-24}$.

Estimation of logical error rates of large-scale quantum codes from small-scale level-by-level simulations. In this work, we use an underlying quantum code $\mathcal{Q}_0$ concatenated with a series of quantum Hamming codes $\mathcal{Q}_{r_1}, \mathcal{Q}_{r_2}, \ldots, \mathcal{Q}_{r_L}$. The logical error rate of the overall quantum code under the physical error rate p is evaluated from the level-by-level numerical simulation as

$$P(p) = P_{r_L} \circ \cdots \circ P_{r_2} \circ P_{r_1} \circ P_0(p), \tag{10}$$

where $P_0(p)$ is the logical error rate of $\mathcal{Q}_0$ under the physical error rate p, and $P_{r_l}(p)$ is that of the quantum Hamming code $\mathcal{Q}_{r_l}$. This estimation gives the upper bound of the logical error rate in the cases where the logical CNOT gates (rather than initial-state preparation of $|0\rangle$ and $|+\rangle$, single-qubit Pauli and Clifford gates, and measurements in Z and X bases) have the largest error rate in the set of elementary operations for the stabilizer circuits, which usually holds true since the gadget for the CNOT gate is the largest. The logical error rates $P_0(p)$ and $P_{r_l}(p)$ for each $l \in \{1, \ldots, L\}$ are estimated by the numerical simulation using the circuit described in Fig. 3. See Supplementary Information for more details.

With our numerical simulation, we obtain the parameters of the following fitting curves of the logical error rates (see Supplementary Information for more details). For the quantum Hamming code $\mathcal{Q}_r$ with parameter r, due to distance 3, $P_r(p)$ is approximated for $r \in \{3, 4, 5, 6, 7\}$ by the following fitting curve

$$P_r(p) = a_r p^2. \tag{11}$$

The logical error rate of the level-l C_4/C_6 code, denoted by $P^{(l)}_{C_4/C_6}(p)$, is approximated by a fitting curve

$$P^{(l)}_{C_4/C_6}(p) = A_{C_4/C_6}(B_{C_4/C_6}p)^{F_l}, \tag{12}$$

where F_l is the Fibonacci number defined by $F_1 = 1$, $F_2 = 2$, and $F_l = F_{l-1} + F_{l-2}$ for $l > 2$ [13]. The threshold $p^{(\mathrm{th})}_{C_4/C_6}$ for the C_4/C_6 code is estimated by

$$p^{(\mathrm{th})}_{C_4/C_6} = (B_{C_4/C_6})^{-1}. \tag{13}$$

The logical error rate of the surface code with code distance d, denoted by $P^{(d)}_{\mathrm{surface}}(p)$, is approximated by a fitting curve

$$P^{(d)}_{\mathrm{surface}}(p) = A_{\mathrm{surface}}(B_{\mathrm{surface}}p)^{\frac{d+1}{2}}. \tag{14}$$

Based on the critical exponent method in Ref. [49], the threshold $p^{(\mathrm{th})}_{\mathrm{surface}}$ of the surface code is estimated as a fitting parameter of another fitting curve given by

$$P^{(d)\prime}_{\mathrm{surface}}(p) = C_{\mathrm{surface}} + D_{\mathrm{surface}}x + E_{\mathrm{surface}}x^2, \tag{15}$$

$$x = (p - p^{(\mathrm{th})}_{\mathrm{surface}})d^{1/\mu}. \tag{16}$$

The logical error rate of the level-l concatenated Steane code, denoted by $P^{(l)}_{\mathrm{Steane}}(p)$, is approximated for $l \in \{1, 2\}$ by a fitting curve

$$P^{(l)}_{\mathrm{Steane}}(p) = a^{(l)}_{\mathrm{Steane}}p^{2^l}. \tag{17}$$

For $l \geq 3$, due to the limitation of computational resources, we did not directly perform the numerical simulation to determine $a^{(l)}_{\mathrm{Steane}}$ in (17), but using the results for $l \in \{1, 2\}$ in (17), we recursively evaluate the logical error rates $P^{(l)}_{\mathrm{Steane}}(p)$ of level-l concatenated Steane code as

$$P^{(l)}_{\mathrm{Steane}}(p) = \begin{cases} P^{(1)}_{\mathrm{Steane}} \circ P^{(l-1)}_{\mathrm{Steane}}(p) & (l \text{ is odd}) \\ P^{(2)}_{\mathrm{Steane}} \circ P^{(l-2)}_{\mathrm{Steane}}(p) & (l \text{ is even}) \end{cases}. \tag{18}$$

The threshold $p^{(\mathrm{th})}_{\mathrm{Steane}}$ of the concatenated Steane code is estimated by that satisfying $P^{(2)}_{\mathrm{Steane}}(p^{(\mathrm{th})}_{\mathrm{Steane}}) = p^{(\mathrm{th})}_{\mathrm{Steane}}$, i.e.,

$$p^{(\mathrm{th})}_{\mathrm{Steane}} = [a^{(2)}_{\mathrm{Steane}}]^{-1/3}. \tag{19}$$

The logical error rates of the level-l C_4/Steane codes for $l \in \{1, 2\}$, denoted by $P^{(l)}_{C_4/\mathrm{Steane}}(p)$, are approximated by fitting curves

$$P^{(1)}_{C_4/\mathrm{Steane}}(p) = a^{(1)}_{C_4/\mathrm{Steane}} p, \tag{20}$$

$$P^{(2)}_{C_4/\mathrm{Steane}}(p) = a^{(2)}_{C_4/\mathrm{Steane}} p^3, \tag{21}$$

where $a^{(1)}_{C_4/\mathrm{Steane}}$ is given by $a^{(1)}_{C_4/\mathrm{Steane}} = A_{C_4/C_6} B_{C_4/C_6}$ from the logical error rate of the level-1 C_4/C_6 since the level-1 C_4/Steane code coincides with the level-1 C_4/C_6 code. For $l \geq 3$, similar to the concatenated Steane code, logical error rates $P^{(l)}_{C_4/\mathrm{Steane}}(p)$ of the level-l C_4/Steane code are evaluated by

$$P^{(l)}_{C_4/\mathrm{Steane}}(p) = P^{(l-2)}_{\mathrm{Steane}} \circ P^{(2)}_{C_4/\mathrm{Steane}}(p). \tag{22}$$

Since the C_4/Steane code at concatenation levels 2 and higher becomes the same as the concatenated Steane code, the threshold $p^{(\mathrm{th})}_{C_4/\mathrm{Steane}}$ of the C_4/Steane code is determined by the physical error rate that can be suppressed below $p^{(\mathrm{th})}_{\mathrm{Steane}}$ at level 2, estimated as that satisfying $P^{(2)}_{C_4/\mathrm{Steane}}(p^{(\mathrm{th})}_{C_4/\mathrm{Steane}}) = p^{(\mathrm{th})}_{\mathrm{Steane}}$, i.e.,

$$p^{(\mathrm{th})}_{\mathrm{Steane}} = [a^{(2)}_{\mathrm{Steane}}]^{-1/9} [a^{(2)}_{C_4/\mathrm{Steane}}]^{-1/3}. \tag{23}$$

Using the fitting parameters of these fitting curves obtained from the level-by-level numerical simulations, we evaluate the overall logical error rate according to (10).

ACKNOWLEDGMENTS

S.Y. was supported by Japan Society for the Promotion of Science (JSPS) KAKENHI Grant Number 23KJ0734, FoPM, WINGS Program, the University of Tokyo, and DAIKIN Fellowship Program, the University of Tokyo. 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. was supported by 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 [50].

SUPPLEMENTARY INFORMATION

Supplementary Information of "Concatenate codes, save qubits" is organized as follows. In Sec. A, we present the details of the fault-tolerant protocols for the concatenated quantum Hamming code, the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code. In Sec. B, we show the numerical results of the logical CNOT error rates for these quantum codes.

Appendix A: Implementation of fault-tolerant protocols

In this section, we summarize the details of the implementation of fault-tolerant protocols for the quantum codes relevant to our analysis. For a concatenated code, the set of logical qubits of the concatenated code at the concatenation level l is called a level-l register, where a level-0 register refers to a physical qubit [4]. For the concatenated quantum Hamming codes, the C_4/C_6 code, the concatenated Steane code, and the C_4/Steane code (which are the Calberback-Shor-Steane (CSS) codes), the Pauli gate gadgets, the CNOT gate gadget, and the measurement gadget are implemented transversally as shown in Fig. S1. To run the circuits for the simulation, the error correction gadget and the initial-state preparation gadget are also required, and we will describe these gadgets in this section. In Sec. A 1, we describe the protocol for the concatenated quantum Hamming code. In Sec. A 2, we describe the protocols for the underlying quantum codes, i.e., the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code. In addition, the measurement gadgets include the classical processing of decoding using the measurement outcomes, and in Sec. A 3, we describe the decoders.

1. Concatenated quantum Hamming code

We summarize the details of the protocol for the concatenated quantum Hamming code. A level-l register refers to $K^{(l)} = \prod_{l'=1}^{l} K_{r_{l'}}$ logical qubits of the concatenated quantum Hamming code at the concatenation level $l \in \{1, 2, \ldots\}$, as shown in Ref. [4]. To form a level-l register, we use N_{r_l} level-$(l-1)$ registers; in particular, from each of the N_{r_l} level-$(l-1)$ registers, we pick up the kth qubit ($k \in \{1, \ldots, K^{(l-1)}\}$) and encode K_{r_l} out of $K^{(l)}$ qubits of the level-l register into these picked N_{r_l} qubits as the K_{r_l} logical qubits of the quantum Hamming code $\mathcal{Q}_{r_l}$. The logical Pauli operators acting on the ith logical qubit of the level-l register for $l \geq 2$, denoted by $P_i^{(1)}$ for $P \in \{I, X, Y, Z\}$, are written in terms of the level-$(l-1)$ logical Pauli operators acting on the jth logical qubit of the nth level-$(l-1)$ register, denoted by $P_{n,j}^{(l-1)}$ for $P \in \{I, X, Y, Z\}$, as

$$\begin{aligned} X_i^{(l)} &= \bigotimes_{n=1}^{N_{r_l}} X_{n,j}^{(l-1)b_n^{(k)}}, \\ Z_i^{(l)} &= \bigotimes_{n=1}^{N_{r_l}} Z_{n,j}^{(l-1)b_n^{(k)}}, \end{aligned} \tag{A1}$$

where $i = K^{(l-1)}(k-1) + j$ for $k \in \{1, \cdots, K_{r_l}\}$ and $j \in \{1, \cdots, K^{(l-1)}\}$, and $b_n^{(k)}$ represent the logical operators of the quantum Hamming code $\mathcal{Q}_{r_l}$. The explicit forms of the logical operators, i.e., $b_n^{(k)}$ in (A1), can be determined by the method shown in Refs. [51, 52]. Our simulation calculates the logical CNOT error rate on the first logical qubit; thus, we here show $b_n^{(k)}$ only for $k = 1$, which is given by

$$b_n^{(k=1)} = \begin{cases} 1 & (n \in \{1, 2, 3\}) \\ 0 & (n \in \{4, 5, \cdots, N_{r_l}\}) \end{cases}. \tag{A2}$$

The level-l initial-state preparation gadget for the logical $|0\rangle$ ($|+\rangle$) of the concatenated quantum Hamming code is recursively defined using the level-$(l-1)$ gadgets as shown in Fig. S2. The Z (X) stabilizer generators and the logical Z (X) operator are measured for verification from the measurement outcomes. If the verification fails, the output quantum state is discarded, and the initial-state preparation is rerun without additional verification. In our simulation, the leading-order effect of the verification failure is included in the estimation of the logical CNOT error rate as

$$P_L = P_{\text{CNOT}}^{(0)} + P_{\text{verification}} \sum_i P_{\text{CNOT}}^{(i)}, \tag{A3}$$

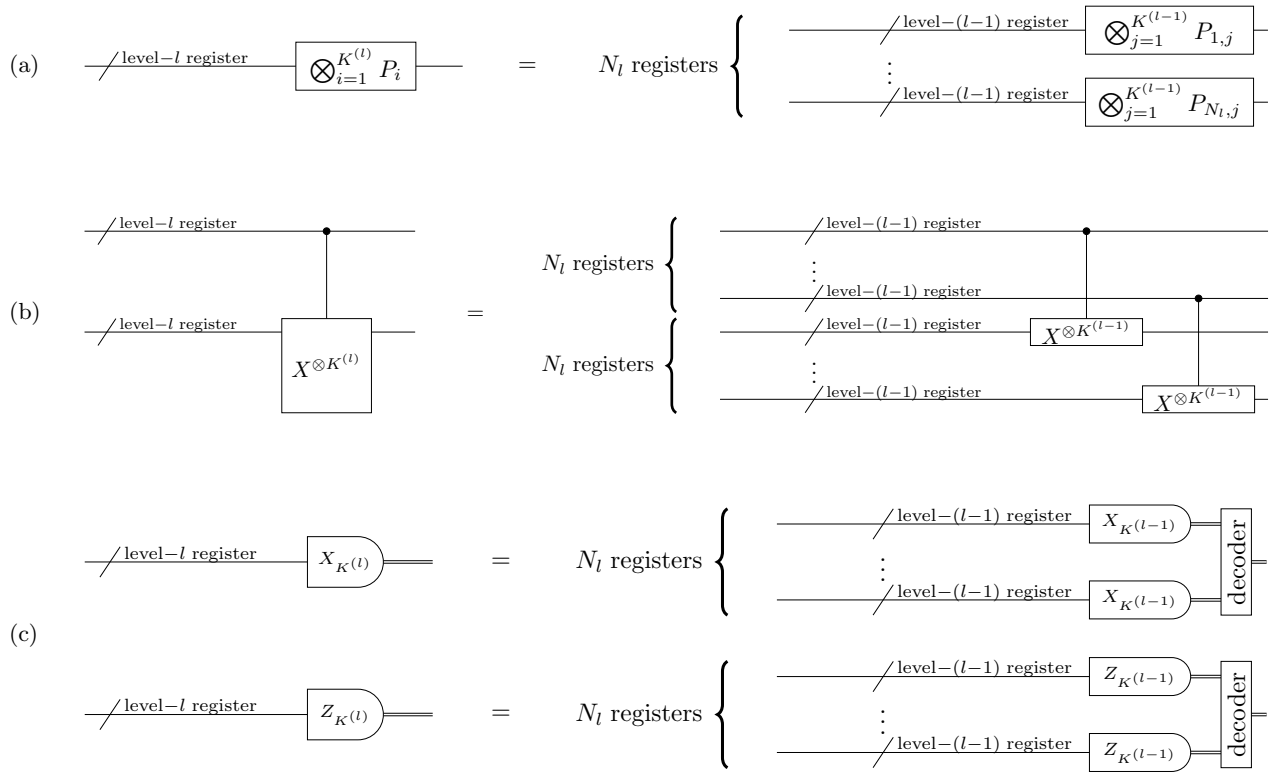


FIG. S1. Level-l Pauli gate, CNOT gate, and measurement gadgets for the CSS codes using level-$(l-1)$ operations, which are used for the concatenated quantum Hamming codes, the C_4/C_6 code, the concatenated Steane code, and the C_4/Steane code in our analysis. (a) The level-l Pauli gate gadget implements the logical Pauli operator $\bigotimes_{i=1}^{K^{(l)}} P_i$ for $P_i \in \{I, X, Y, Z\}$. It is implemented by the level-$(l-1)$ Pauli gadget as $\bigotimes_{n=1}^{N_l} \bigotimes_{j=1}^{K^{(l-1)}} P_{n,j}$, where $P_{n,j}$ is chosen from the logical Pauli operators $\{I, X, Y, Z\}$ of the level-$(l-1)$ code, which will be explained for each code in (A1), (A17), (A18), (A21) and (A23). (b) The level-l CNOT gate gadget implements the logical $\mathrm{CNOT}^{\otimes K^{(l)}}$ gate. It is implemented by the N_l transversal level-$(l-1)$ CNOT gate gadgets as shown on the right-hand side. (c) The X (Z) measurement gadget implements the measurement of the logical X (Z) operator on the ith logical qubit for $i \in \{1, \cdots, K^{(l)}\}$. It is implemented by the transversal level-$(l-1)$ X (Z) measurement gadgets, followed by the classical computation decoding the measurement outcomes of level-$(l-1)$ logical operators. See Sec. A 3 for the details of the decoder.

where $P^{(0)}_{\mathrm{CNOT}}$ is the logical CNOT error rate evaluated in the post-selected simulation runs that all the verification succeed, $P_{\mathrm{verification}}$ is the failure probability of the verification, and $P^{(i)}_{\mathrm{CNOT}}$ is the logical CNOT error rate evaluated in the post-selected simulation runs that all the verifications but the ith one succeed. We use the error correction gadget shown in Ref. [4]. See also Ref. [4] for details of the full fault-tolerant protocol for implementing universal quantum computation using the quantum Hamming code while we have described here a part of the protocol relevant to our analysis.

Initial-state preparation unitaries U_{encode} for the quantum Hamming code $\mathcal{Q}_r = [[N_r, K_r, 3]]$ for $r \in \{3, 4, 5, 6, 7\}$ are constructed using Steane's Latin rectangle encoding method [53]. In the initial state preparation of the logical $|0\rangle$ state, the 2^{i-1}th qubits for $i \in \{1, \cdots, r\}$ are initialized to be $|+\rangle$ states, and the jth qubits for $j \in \{1, \cdots, K_r\} \setminus \{2^0, \cdots, 2^{r-1}\}$ are initialized to be $|0\rangle$ states. Steane's Latin rectangle L for the quantum Hamming codes $[[N_r, K_r, 3]]$ is given by a $r \times N_r$ matrix whose elements $L_{i,j}$ for $i \in \{1, \cdots, r\}$ and $j \in \{1, \cdots, N_r\}$ specify the ordering of the CNOT gates to be applied. If $L_{i,j} = l$ for $l \in \{1, \cdots\}$, a CNOT gate is applied between the 2^{i-1}th qubit (control) and the jth qubit (target) on the depth l. If $L_{i,j} = 0$, no CNOT gate is applied. The initial state preparation of the logical $|+\rangle$ state is done by replacing $|0\rangle$ ($|+\rangle$) with $|+\rangle$ ($|0\rangle$), swapping the control qubit and target qubit of the CNOT gates, and replacing the Z measurements with the X measurements in the initial state preparation of the logical $|0\rangle$ state In particular, we use the Latin rectangles L_r for the $\mathcal{Q}_r$ codes for $r \in \{3, 4, 5, 6, 7\}$ given by

$$L_3 = \begin{pmatrix} 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 \end{pmatrix}, \tag{A4}$$

$$L_4 = \begin{pmatrix} 0 & 0 & 3 & 0 & 7 & 0 & 1 & 0 & 4 & 0 & 5 & 0 & 2 & 0 & 6 \\ 0 & 0 & 5 & 0 & 0 & 1 & 3 & 0 & 0 & 4 & 6 & 0 & 0 & 7 & 2 \\ 0 & 0 & 0 & 0 & 2 & 7 & 6 & 0 & 0 & 0 & 0 & 1 & 4 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 3 & 7 & 6 & 1 & 5 & 4 \end{pmatrix}, \tag{A5}$$

$$L_5 = \begin{pmatrix} 0 & 0 & 7 & 0 & 2 & 0 & 9 & 0 & 14 & 0 & 3 & 0 & 11 & 0 & 13 & 0 & 12 & 0 & 1 & 0 & 8 & 0 & 6 & 0 & 15 & 0 & 4 & 0 & 10 & 0 & 5 \\ 0 & 0 & 8 & 0 & 0 & 9 & 15 & 0 & 0 & 13 & 11 & 0 & 0 & 5 & 14 & 0 & 0 & 2 & 12 & 0 & 0 & 1 & 10 & 0 & 0 & 6 & 7 & 0 & 0 & 4 & 3 \\ 0 & 0 & 0 & 0 & 14 & 12 & 4 & 0 & 0 & 0 & 0 & 8 & 3 & 1 & 10 & 0 & 0 & 0 & 0 & 2 & 13 & 6 & 9 & 0 & 0 & 0 & 0 & 11 & 5 & 7 & 15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 10 & 7 & 5 & 4 & 6 & 15 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 12 & 14 & 8 & 9 & 13 & 2 & 11 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 15 & 1 & 13 & 7 & 11 & 4 & 12 & 8 & 5 & 3 & 9 & 6 & 2 & 14 & 10 \end{pmatrix}, \tag{A6}$$

$$L_6 = \begin{pmatrix} L_{6,1} & L_{6,2} & L_{6,3} \end{pmatrix}, \tag{A7}$$

$$L_7 = \begin{pmatrix} L_{7,1} & L_{7,2} & L_{7,3} & L_{7,4} & L_{7,5} \end{pmatrix}, \tag{A8}$$

where L_6 and L_7 are given by horizontally concatenating the matrices defined as

$$L_{6,1} = \begin{pmatrix} 0 & 0 & 13 & 0 & 24 & 0 & 5 & 0 & 6 & 0 & 3 & 0 & 7 & 0 & 10 & 0 & 27 & 0 & 28 & 0 & 20 \\ 0 & 0 & 15 & 0 & 0 & 28 & 13 & 0 & 0 & 19 & 25 & 0 & 0 & 26 & 16 & 0 & 0 & 12 & 30 & 0 & 0 \\ 0 & 0 & 0 & 0 & 15 & 9 & 26 & 0 & 0 & 0 & 0 & 24 & 3 & 17 & 25 & 0 & 0 & 0 & 0 & 6 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 14 & 12 & 27 & 19 & 5 & 20 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 8 & 18 & 23 & 11 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{A9}$$

$$L_{6,2} = \begin{pmatrix} 0 & 17 & 0 & 16 & 0 & 9 & 0 & 26 & 0 & 22 & 0 & 18 & 0 & 23 & 0 & 1 & 0 & 2 & 0 & 4 & 0 \\ 8 & 3 & 0 & 0 & 9 & 14 & 0 & 0 & 23 & 2 & 0 & 0 & 24 & 20 & 0 & 0 & 29 & 7 & 0 & 0 & 6 \\ 27 & 4 & 0 & 0 & 0 & 0 & 30 & 19 & 10 & 29 & 0 & 0 & 0 & 0 & 2 & 5 & 14 & 31 & 0 & 0 & 0 \\ 0 & 0 & 11 & 18 & 21 & 10 & 1 & 28 & 15 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 6 & 3 \\ 19 & 27 & 2 & 21 & 13 & 5 & 15 & 31 & 14 & 17 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 & 6 & 3 & 22 & 4 & 20 & 10 & 19 & 9 & 13 \end{pmatrix}, \tag{A10}$$

$$L_{6,3} = \begin{pmatrix} 29 & 0 & 19 & 0 & 31 & 0 & 11 & 0 & 8 & 0 & 25 & 0 & 12 & 0 & 14 & 0 & 30 & 0 & 21 & 0 & 15 \\ 22 & 0 & 0 & 17 & 21 & 0 & 0 & 4 & 31 & 0 & 0 & 5 & 11 & 0 & 0 & 27 & 10 & 0 & 0 & 18 & 1 \\ 0 & 20 & 7 & 23 & 11 & 0 & 0 & 0 & 0 & 13 & 21 & 28 & 22 & 0 & 0 & 0 & 0 & 18 & 16 & 1 & 12 \\ 2 & 29 & 13 & 7 & 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 26 & 22 & 23 & 24 & 31 & 17 & 4 & 25 \\ 0 & 0 & 0 & 0 & 0 & 24 & 1 & 30 & 6 & 16 & 28 & 29 & 20 & 22 & 10 & 9 & 3 & 25 & 7 & 12 & 26 \\ 18 & 17 & 14 & 25 & 7 & 15 & 24 & 27 & 16 & 12 & 29 & 8 & 1 & 2 & 5 & 30 & 21 & 28 & 26 & 11 & 31 \end{pmatrix}, \tag{A11}$$

$$L_{7,1} = \begin{pmatrix} 0 & 0 & 19 & 0 & 1 & 0 & 21 & 0 & 54 & 0 & 10 & 0 & 55 & 0 & 45 & 0 & 61 & 0 & 47 & 0 & 33 & 0 & 51 & 0 & 2 & 0 \\ 0 & 0 & 17 & 0 & 0 & 50 & 59 & 0 & 0 & 41 & 38 & 0 & 0 & 28 & 51 & 0 & 0 & 39 & 23 & 0 & 0 & 54 & 4 & 0 & 0 & 42 \\ 0 & 0 & 0 & 0 & 59 & 18 & 33 & 0 & 0 & 0 & 0 & 61 & 40 & 41 & 37 & 0 & 0 & 0 & 0 & 24 & 63 & 29 & 31 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 35 & 23 & 24 & 15 & 26 & 14 & 33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 4 & 57 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 15 & 32 & 21 & 47 & 13 & 33 & 41 & 27 & 60 & 39 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{A12}$$

$$L_{7,2} = \begin{pmatrix} 59 & 0 & 31 & 0 & 17 & 0 & 24 & 0 & 63 & 0 & 13 & 0 & 29 & 0 & 53 & 0 & 30 & 0 & 16 & 0 & 27 & 0 & 22 & 0 & 34 & 0 \\ 26 & 0 & 0 & 21 & 19 & 0 & 0 & 36 & 62 & 0 & 0 & 46 & 34 & 0 & 0 & 16 & 29 & 0 & 0 & 45 & 57 & 0 & 0 & 27 & 61 & 0 \\ 0 & 21 & 46 & 17 & 6 & 0 & 0 & 0 & 0 & 47 & 28 & 50 & 3 & 0 & 0 & 0 & 0 & 4 & 1 & 11 & 43 & 0 & 0 & 0 & 0 & 56 \\ 5 & 47 & 40 & 16 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 20 & 10 & 17 & 28 & 54 & 2 & 32 & 49 & 0 & 0 & 0 & 0 & 0 \\ 45 & 44 & 50 & 51 & 26 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 38 & 9 & 55 & 62 & 40 \\ 0 & 0 & 0 & 0 & 0 & 0 & 23 & 62 & 9 & 26 & 53 & 60 & 14 & 46 & 19 & 51 & 58 & 56 & 47 & 35 & 3 & 11 & 34 & 13 & 32 & 54 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{A13}$$

$$L_{7,3} = \begin{pmatrix} 37 & 0 & 35 & 0 & 26 & 0 & 42 & 0 & 23 & 0 & 3 & 0 & 41 & 0 & 40 & 0 & 32 & 0 & 11 & 0 & 20 & 0 & 44 & 0 & 50 & 0 \\ 0 & 52 & 6 & 0 & 0 & 58 & 12 & 0 & 0 & 7 & 55 & 0 & 0 & 18 & 56 & 0 & 0 & 49 & 47 & 0 & 0 & 31 & 14 & 0 & 0 & 8 \\ 8 & 19 & 36 & 0 & 0 & 0 & 0 & 13 & 32 & 27 & 51 & 0 & 0 & 0 & 0 & 34 & 30 & 53 & 14 & 0 & 0 & 0 & 0 & 57 & 42 & 10 \\ 0 & 0 & 0 & 22 & 21 & 63 & 13 & 58 & 60 & 42 & 43 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 29 & 53 & 7 & 56 & 3 & 1 \\ 4 & 11 & 7 & 48 & 37 & 31 & 58 & 34 & 17 & 22 & 56 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 41 & 59 & 31 & 27 & 5 & 15 & 2 & 4 & 50 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 56 & 47 & 4 & 1 & 59 & 16 & 6 & 46 & 49 & 2 & 30 & 23 & 21 & 17 \end{pmatrix}, \tag{A14}$$

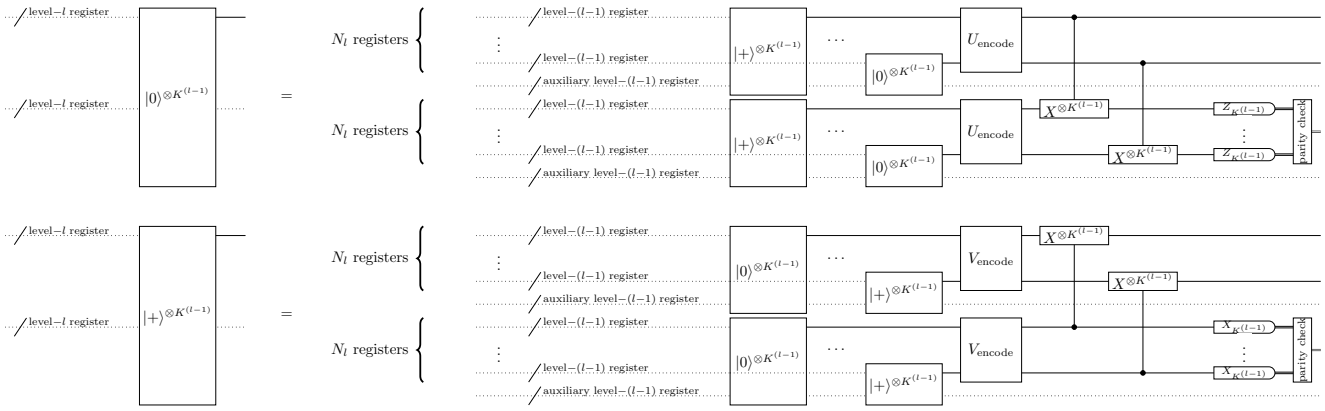


FIG. S2. Level-l initial-state preparation gadgets for the logical $|0\rangle$ ($|+\rangle$) state of the concatenated quantum Hamming code are implemented by using the level-$(l-1)$ gadgets. The Z (X) stabilizer generators and the logical Z (X) operator are measured for verification from the measurement outcomes. If the verification fails, the output quantum state is discarded, and the initial-state preparation is rerun without additional verification.

$$L_{7,4} = \begin{pmatrix} 7 & 0 & 57 & 0 & 25 & 0 & 39 & 0 & 43 & 0 & 6 & 0 & 56 & 0 & 46 & 0 & 15 & 0 & 36 & 0 & 9 & 0 & 60 & 0 & 52 & 0 \\ 9 & 0 & 0 & 2 & 15 & 0 & 0 & 40 & 22 & 0 & 0 & 43 & 25 & 0 & 0 & 24 & 5 & 0 & 0 & 11 & 48 & 0 & 0 & 20 & 13 & 0 \\ 58 & 0 & 0 & 0 & 0 & 39 & 60 & 15 & 26 & 0 & 0 & 0 & 0 & 52 & 38 & 7 & 54 & 0 & 0 & 0 & 0 & 12 & 62 & 9 & 45 & 0 \\ 34 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 61 & 55 & 31 & 51 & 59 & 6 & 52 & 41 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 48 \\ 0 & 52 & 25 & 42 & 6 & 36 & 8 & 2 & 28 & 20 & 24 & 1 & 35 & 5 & 16 & 49 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 44 & 6 & 7 & 29 & 17 & 55 & 52 & 21 & 1 \\ 51 & 28 & 55 & 38 & 24 & 54 & 53 & 14 & 20 & 48 & 36 & 42 & 18 & 27 & 50 & 61 & 29 & 22 & 19 & 9 & 10 & 5 & 15 & 13 & 7 & 31 \end{pmatrix}, \tag{A15}$$

$$L_{7,5} = \begin{pmatrix} 62 & 0 & 4 & 0 & 58 & 0 & 49 & 0 & 18 & 0 & 12 & 0 & 38 & 0 & 14 & 0 & 5 & 0 & 28 & 0 & 48 & 0 & 8 \\ 0 & 37 & 63 & 0 & 0 & 30 & 10 & 0 & 0 & 32 & 53 & 0 & 0 & 1 & 3 & 0 & 0 & 44 & 33 & 0 & 0 & 60 & 35 \\ 0 & 0 & 0 & 55 & 44 & 5 & 23 & 0 & 0 & 0 & 0 & 49 & 16 & 20 & 22 & 0 & 0 & 0 & 0 & 48 & 35 & 2 & 25 \\ 9 & 45 & 27 & 19 & 37 & 36 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 30 & 38 & 25 & 62 & 50 & 46 & 39 & 44 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 54 & 57 & 43 & 29 & 3 & 63 & 12 & 46 & 19 & 14 & 23 & 10 & 53 & 59 & 61 & 18 \\ 20 & 28 & 30 & 39 & 24 & 18 & 42 & 25 & 40 & 57 & 37 & 33 & 22 & 61 & 38 & 36 & 49 & 10 & 63 & 12 & 43 & 45 & 48 \\ 63 & 52 & 26 & 12 & 45 & 35 & 37 & 41 & 8 & 39 & 33 & 32 & 62 & 25 & 60 & 34 & 44 & 3 & 57 & 11 & 40 & 58 & 43 \end{pmatrix}. \tag{A16}$$

The Latin rectangle for the $[[7,1,3]]$ code is taken from Ref. [54], and the others are heuristically chosen to minimize the circuit depth as much as possible.

2. Underlying quantum codes

In this section, we describe the protocols for the underlying quantum codes, i.e., the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code. In Sec. A 2 a, we describe the C_4/C_6 code. In Sec. A 2 b, we describe the surface code. In Sec. A 2 c, we describe the concatenated Steane code. In Sec. A 2 d, we describe the C_4/Steane code.

a. C_4/C_6 code

We summarize the details of the protocol for the C_4/C_6 code. We call the two logical qubits of the C_4 code (i.e., the $[[4,2,2]]$ code) a level-1 register. Similarly, the level-l register for $l \in \{2,3,\cdots\}$ refers to the two logical qubits of the C_4/C_6 code at the concatenation level l. To form the level-l register, the C_4/C_6 code uses three level-$(l-1)$ registers (i.e., six qubits) of the level-$(l-1)$ code to encode the level-l register as the logical qubits of the C_6 code, as shown in Ref. [13]. The logical Pauli operators acting on the ith logical qubit of the level-1 register, denoted by $P_i^{(1)}$

for $P \in \{I, X, Y, Z\}$, are given by the physical Pauli operators as [13]

$$\begin{aligned} X_1^{(l)} \otimes I_2^{(l)} &= X \otimes X \otimes I \otimes I, \\ Z_1^{(l)} \otimes I_2^{(l)} &= Z \otimes I \otimes Z \otimes I, \\ I_1^{(l)} \otimes X_2^{(l)} &= I \otimes X \otimes I \otimes X, \\ I_1^{(l)} \otimes Z_2^{(l)} &= Z \otimes I \otimes Z \otimes I. \end{aligned} \tag{A17}$$

The logical Pauli operators acting on the ith logical qubit of the level-l register for $l \geq 2$, denoted by $P_i^{(1)}$ for $P \in \{I, X, Y, Z\}$, are given by the level-$(l-1)$ logical Pauli operators acting on the jth logical qubit of the nth level-$(l-1)$ register, denoted by $P_{n,j}^{(l-1)}$ for $P \in \{I, X, Y, Z\}$, as [13]

$$\begin{aligned} X_1^{(l)} \otimes I_2^{(l)} &= I_{1,1}^{(l-1)} \otimes X_{1,2}^{(l-1)} \otimes X_{2,1}^{(l-1)} \otimes I_{2,2}^{(l-1)} \otimes I_{3,1}^{(l-1)} \otimes I_{3,2}^{(l-1)}, \\ Z_1^{(l)} \otimes I_2^{(l)} &= Z_{1,1}^{(l-1)} \otimes I_{1,2}^{(l-1)} \otimes I_{2,1}^{(l-1)} \otimes Z_{2,2}^{(l-1)} \otimes Z_{3,1}^{(l-1)} \otimes Z_{3,2}^{(l-1)}, \\ I_1^{(l)} \otimes X_2^{(l)} &= X_{1,1}^{(l-1)} \otimes X_{1,2}^{(l-1)} \otimes X_{2,1}^{(l-1)} \otimes I_{2,2}^{(l-1)} \otimes I_{3,1}^{(l-1)} \otimes X_{3,2}^{(l-1)}, \\ I_1^{(l)} \otimes Z_2^{(l)} &= Z_{1,1}^{(l-1)} \otimes Z_{1,2}^{(l-1)} \otimes Z_{2,1}^{(l-1)} \otimes I_{2,2}^{(l-1)} \otimes I_{3,1}^{(l-1)} \otimes Z_{3,2}^{(l-1)}. \end{aligned} \tag{A18}$$

Level-l initial-state preparation gadgets of the C_4/C_6 code are recursively defined using level-$(l-1)$ gadgets as shown in Figs. S3 and S4. The initial-state preparation gadget uses $*u$ and $*u^2$ gate gadgets [13], which are shown in Fig. S5, implementing the logical 2-qubit unitary operations given by

$$\begin{aligned} *u &= \mathrm{CNOT} \cdot \mathrm{SWAP}, \\ *u^2 &= \mathrm{SWAP} \cdot \mathrm{CNOT}, \end{aligned} \tag{A19}$$

where SWAP is defined by

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{A20}$$

The parity of the measurement outcomes is checked for verification. If it fails, the output quantum state is discarded, and the initial-state preparation gadget is rerun. Using the Bell-state preparation gadget shown in Fig. S6 [36], we implement Knill's error correction gadget as shown in Fig. S7. In the error correction and detection gadgets, measurement outcomes of X and Z measurements are decoded to apply logical Pauli gates for correcting byproducts. In the error correction gadget, if an uncorrectable error is detected in the decoding process, random numbers are assigned to the logical measurement outcomes. In the error detection gadget, if an uncorrectable error is detected in the decoding process, the output quantum state is discarded, which incurs an erasure error. In the Bell-state preparation gadget, an error detection gadget is applied after preparing the logical Bell state. If an uncorrectable error is detected in the error detection, the output quantum state is discarded and the Bell-preparation gadget is rerun by replacing the error detection gadget with an error correction gadget. Since the effect of the verification failure on the logical CNOT error rate is in a sub-leading order, we omit to include this effect in the numerical simulation. See also Ref. [13] for details of the full fault-tolerant protocol for implementing universal quantum computation using the C_4/C_6 code while we have described here a part of the protocol relevant to our analysis. Note that the protocol described here is the non-post-selected protocol while Ref. [13] also proposes a post-selected protocol, which we do not use to avoid the increase of overhead.

b. Surface code

We summarize the details of the protocol for the surface code and its numerical simulation. The surface code is a planar version [8, 55] of the toric code [56, 57], and we here consider a rotated version [58] of the planar surface code that requires fewer auxiliary qubits for the syndrome measurement. The distance-d rotated surface code is a $[[d^2, 1, d]]$ code, defined on a square lattice consisting of $d \times d$ data physical qubits. In the rotated surface codes, as shown in Fig. S8, data qubits are located at the vertices of the square plaquettes, while auxiliary qubits are placed at

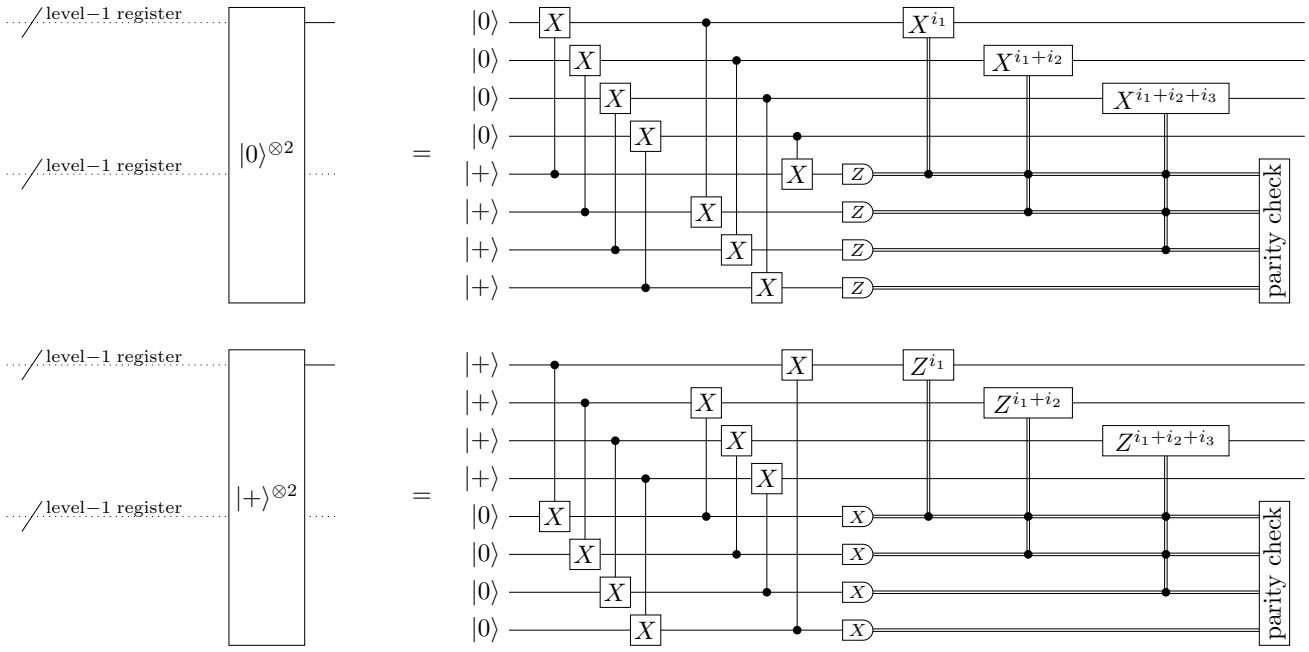


FIG. S3. Level-1 initial-state preparation gadgets for the C_4/C_6 code and the C_4/Steane code implements preparations of the logical $|0\rangle^{\otimes 2}$ and $|+\rangle^{\otimes 2}$ states. Pauli gates are applied depending on the measurement outcomes i_j of the $(j+4)$th qubits for $j \in \{1, \cdots, 4\}$. The parity of the measurement outcomes is checked for verification. If $i_1 + i_2 + i_3 + i_4 \neq 0 \pmod 2$ holds, the output quantum state is discarded and the initial-state preparation is rerun.

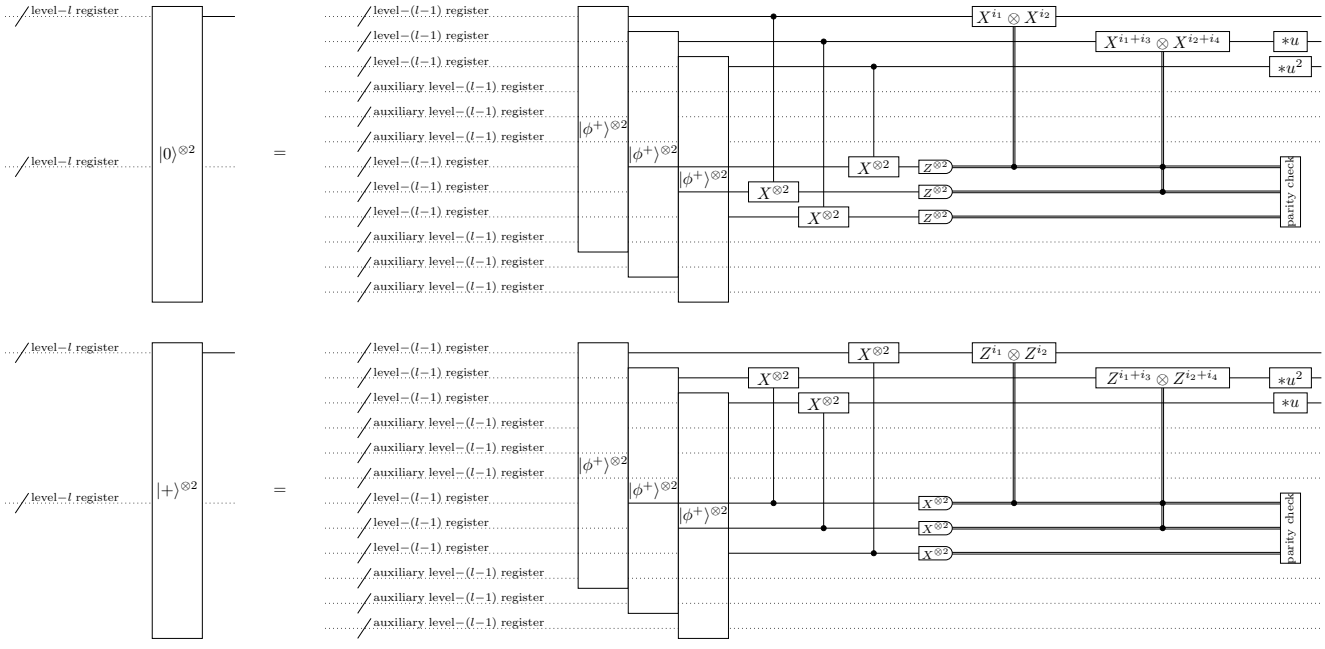


FIG. S4. Level-l initial-state preparation gadgets ($l \geq 2$) for the C_4/C_6 code implements preparations of the logical $|0\rangle^{\otimes 2}$ and $|+\rangle^{\otimes 2}$ states, implemented by using level-$(l-1)$ gadgets. Pauli gates are applied depending on the measurement outcomes (i_{2j-1}, i_{2j}) of the $(j+6)$th code block for $j \in \{1, \cdots, 3\}$. The parity of the measurement outcomes is checked for verification. If $i_1 + i_3 + i_5 \neq 0 \pmod 2$ or $i_2 + i_4 + i_6 \neq 0 \pmod 2$ hold, the output quantum state is discarded and the initial-state preparation is rerun.

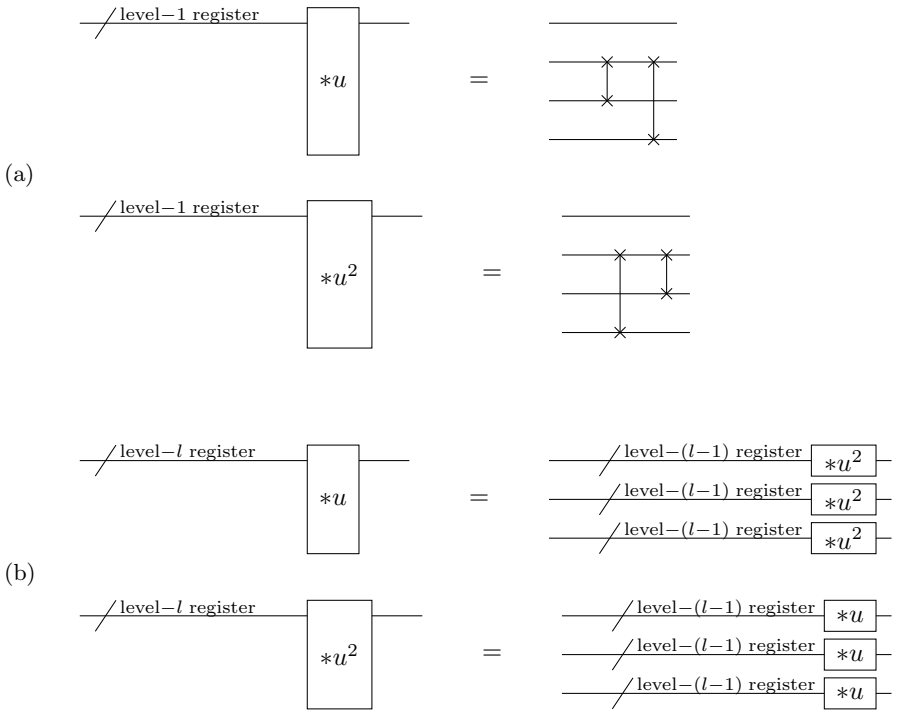


FIG. S5. (a) Level-1 $*u$ and $*u^2$ gate gadgets for the C_4/C_6 code implement the logical $*u$ and $*u^2$ operations given in (A19). (b) Level-l ($l \geq 2$) $*u$ and $*u^2$ gate gadgets for the C_4/C_6 code are implemented by using the level-$(l-1)$ gadgets.

the centers of the squares; the X-type and Z-type stabilizer generators are arranged in an alternating checkerboard pattern.

We employ the lattice surgery [30, 31] to implement a logical CNOT gate on logical qubits encoded in the surface codes. The lattice surgery is a widely used technique for measuring logical Pauli operators acting on logical qubits encoded in the specially separated code blocks of the surface code only using the nearest-neighbor interaction of physical qubits aligned in a two-dimensional plane. The lattice surgery also provides a way to perform a logical CNOT gate between logical qubits of the surface code blocks, which is given by a quantum circuit shown in Fig. S8 (a). The circuit is described by logical I, X, Z gates, and the measurements of logical $X \otimes X$, $Z \otimes Z$, and Z operators, denoted by M_{XX}, M_{ZZ}, and M_Z, respectively, and implemented by the lattice surgery. The layout of physical qubits for performing a logical CNOT gate through the lattice surgery is shown in Fig. S8 (b). The space between code blocks of surface codes in our layout is called the routing space, which should be at least as large as the size of each code block to allow for the lattice surgery between distant code blocks [59, 60]. Also note that the lattice surgery, in combination with magic state injection and magic state distillation, leads to a protocol for implementing universal quantum computation while we here present a lattice-surgery part relevant to our analysis; see Ref. [30] for further details of the protocol.

Given a physical error rate p of the circuit-level depolarizing error model and the distance d, we evaluate the logical error rates of logical I, X, Z, M_{XX}, M_{ZZ}, and M_Z operations, in the circuit to perform the CNOT gate in Fig. S8 (a). In particular, we estimate the logical error rate of I, M_{XX}, and M_{ZZ} is estimated through the memory experiment and stability experiment based on the method in Ref. [61]. On the one hand, the memory experiment evaluates the probability of logical X or Z errors occurring on the logical qubit encoded in the surface code after t rounds of syndrome measurement; on the other hand, the stability experiment evaluates the logical error probability of the product of the measurement outcomes of multiple stabilizer generators after t rounds of syndrome measurement. We use the minimum-weight perfect matching algorithm for decoding implemented by PyMatching package [28, 29].

For the $|+\rangle$-state preparation operation in Fig. S8 (a), we initialize the logical qubit of surface codes in the logical state $|+\rangle$ by initializing all data physical qubits of the surface code in the physical state $|+\rangle$, measuring all stabilizer generators, and running the decoder to correct errors. However, since these operations can be performed simultaneously with the subsequent M_{ZZ} operation using lattice surgery, we assume that we can subsume the logical error rate of the $|+\rangle$ state preparation operation into the logical error rate of the subsequent lattice surgery and thus can ignore it here.

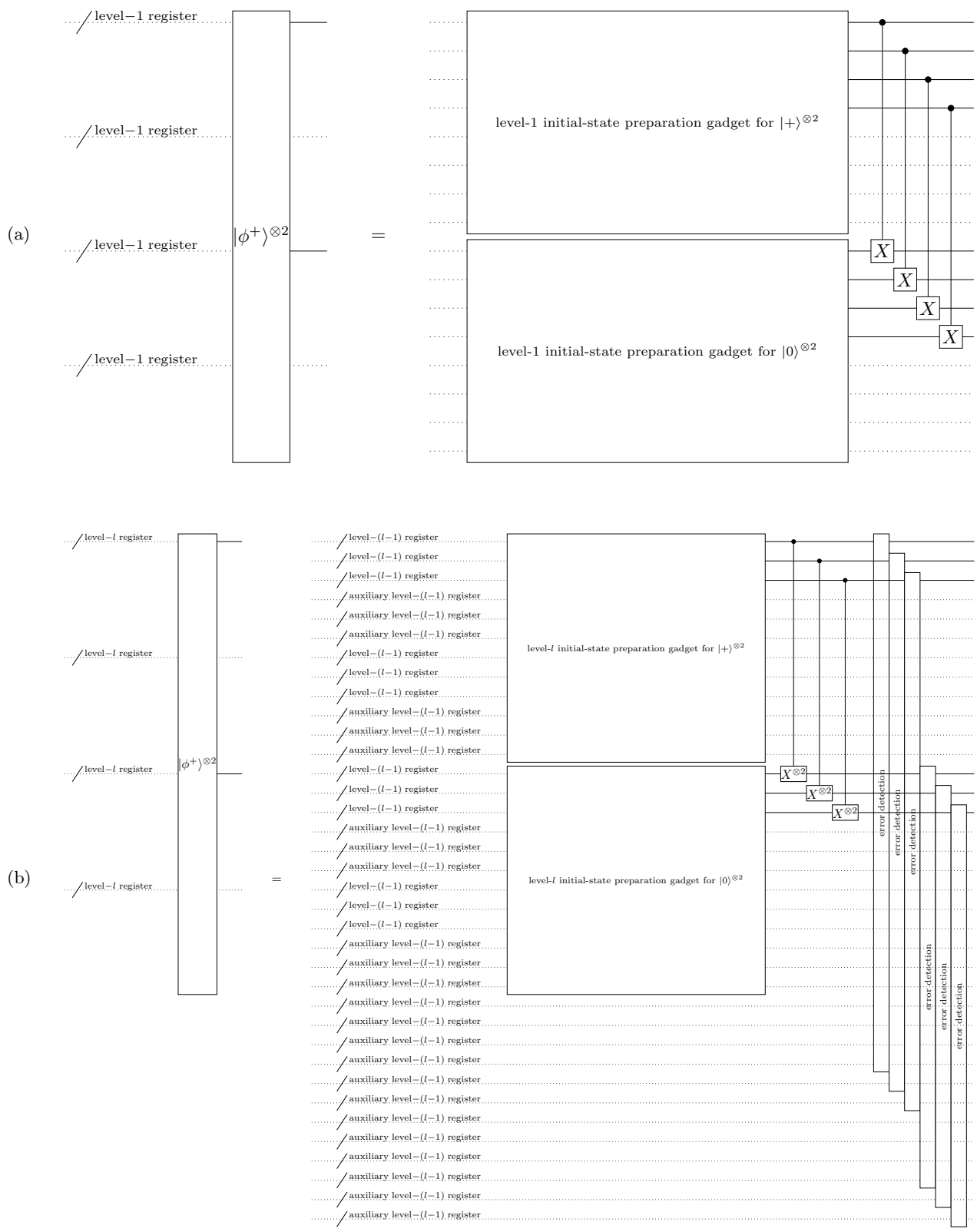


FIG. S6. (a) A level-1 Bell-state preparation gadget for the C_4/C_6 code implements preparation of the logical Bell state $|\phi^+\rangle^{\otimes 2} = \left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)^{\otimes 2}$. (b) A level-$l$ ($l \geq 2$) Bell-state preparation gadget for the C_4/C_6 code is implemented by using the level-$(l-1)$ gadgets.

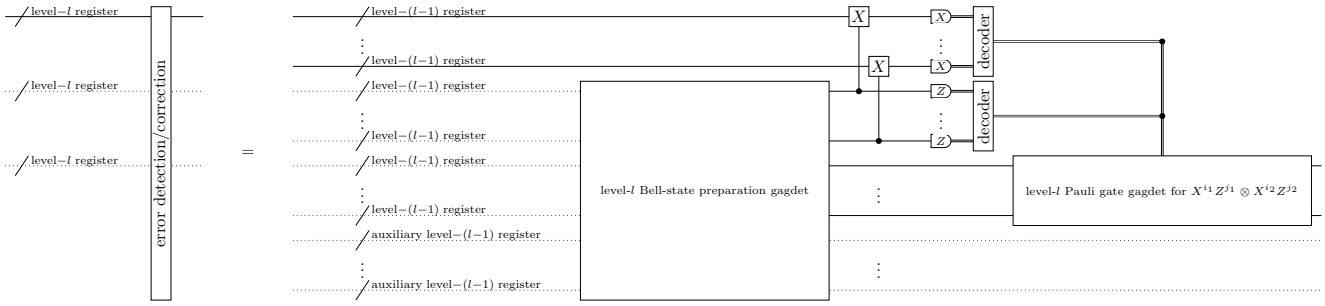
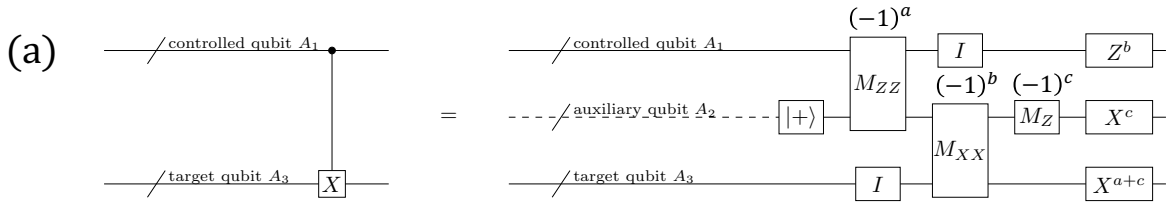


FIG. S7. Level-l error detection and error correction gadgets for the C_4/C_6 code using the level-$(l-1)$ gadgets.



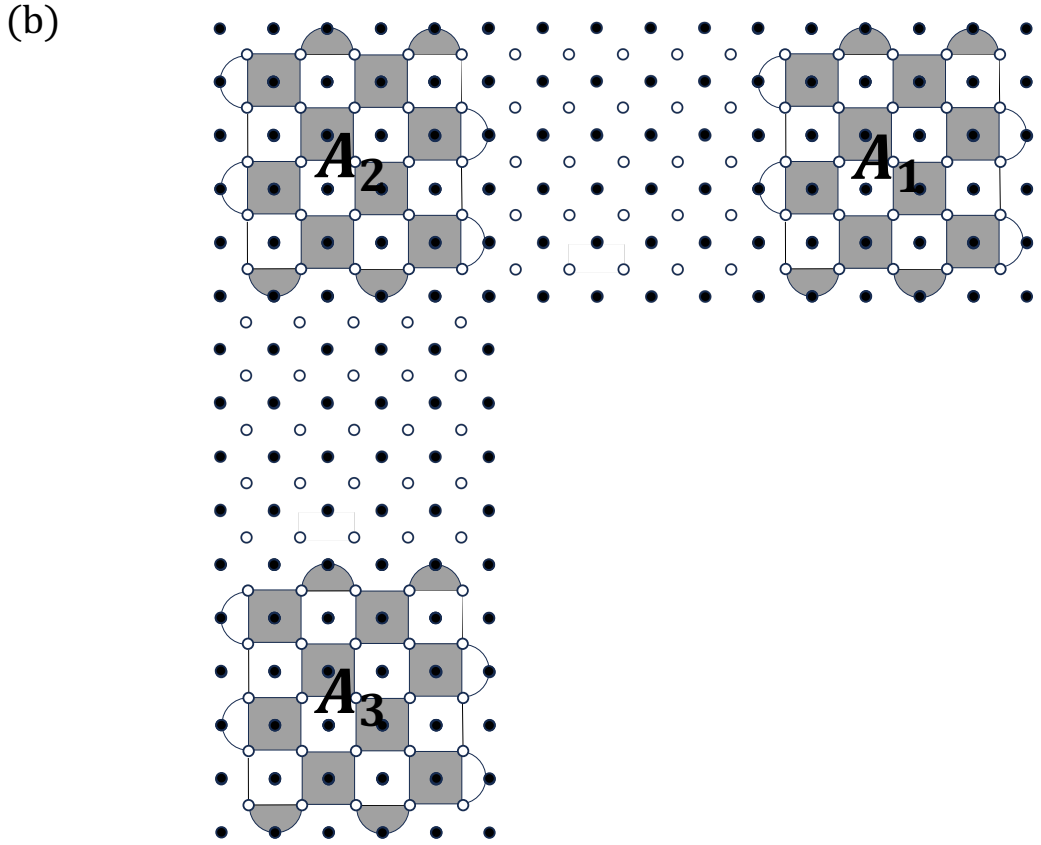


FIG. S8. (a) A quantum circuit for performing a CNOT gate. A measurement operation of a Pauli operator P, denoted by M_P, is represented by a box, with each measurement outcome displayed above it. (b) The layout of physical qubits for performing a logical CNOT gate between logical qubits encoded in a rotated surface code with the distance 5. Each circle represents a physical qubit. When defining surface codes on these physical qubits, the white circles serve as data physical qubits, and the black circles as auxiliary physical qubits for syndrome measurement. Each black (and white) region represents an $X(Z)$-type stabilizer generator of the surface code, acting on the data qubits within its region as Pauli $X(Z)$ operators, respectively.

For the M_{ZZ} operation in Fig. S8 (a) (and the M_{XX} operation as well), the measurement outcome of the logical $Z \otimes Z$ operator is determined by the product of measurement outcomes of Z-type stabilizer generators in the routing space. We estimate the probability $p_{\rm stab}$ of incorrectly reading the product of the logical measurement outcome by the stability experiment of the code block with size $d \times d$ with d rounds of syndrome measurements. The measurement outcome of the M_{ZZ} operation is flipped with the logical error rate $p^{\rm stab}_{M_{ZZ}}$. Along with measuring $Z \otimes Z$, the error correction is performed on the merged code block with size $d \times 3d$, where d is the code distance. We estimate the probability that the logical X error and Z error occur, denoted by p_X and p_Z, respectively, through the memory experiment of the merged code block with size $d \times 3d$ with d rounds of syndrome measurements. A logical X error during the error correction in implementing the logical M_{ZZ} operation leads to a logical $X \otimes X$ error acting on the control and auxiliary logical qubits at the logical error rate $p^X_{M_{ZZ}}$. In addition, a logical Z error during error correction in the M_{ZZ} operation leads to a Z error acting on the controlled logical qubit at the logical error rate is $p^Z_{M_{ZZ}}$. We numerically simulate these logical $X \otimes X$ and Z errors in addition to the errors in reading the logical measurement outcomes.

For the identity operation I in Fig. S8 (a), we estimate the probability of the logical X error and Z error, denoted by p^X_I and p^Z_I, respectively, through the memory experiment of the code block with size $d \times d$ with d rounds of syndrome measurements. Note that the logical identity operation is performed with d rounds of syndrome measurements here because the number of the time steps for performing the M_{ZZ} and M_{XX} operations is also d rounds. With the logical error rate $p^X_I\,(p^Z_I)$, the logical identity operation I suffers from the logical Pauli $X(Z)$ errors.

To estimate the logical error rate of the M_Z operation, we use the memory experiment by starting with a (noiseless) logical qubit in the logical state $|0\rangle$ and performing Z-basis measurements on data physical qubits. Subsequently, we calculate the Z-type stabilizer generators by multiplying the measurement outcomes of the data qubits, correcting errors, and deducing the logical measurement outcomes of the logical Z operator. The logical measurement outcome of the logical Z operator is flipped with the logical error rate p_{M_Z} in the M_Z operation.

As for the Pauli operations for correction operations, we can execute the logical Pauli operations classically by changing the Pauli frame [12]. We assume that they can be performed without noise, depending on the measurement outcomes of M_{ZZ}, M_{XX}, and M_Z operations.

In this way, for distance $d = 5, 7, 9, 11$ and various physical error rates p, we evaluate the logical CNOT error rate of the surface code.

c. *Concatenated Steane code*

We summarize the details of the protocol for the concatenated Steane code. The protocol for the concatenated Steane code can considered to be a special case of that for the concatenated quantum Hamming code in Ref. [4], which has been presented in Sec. A 1, but for completeness, we here present the details relevant to our analysis. A level-l register for $l \in \{1, 2, \cdots\}$ refers to the logical qubit of the concatenated Steane code (i.e., the $[[7^l, 1, 3^l]]$ code). To form a level-l register, we use seven level-$(l-1)$ registers (seven qubits) of the level-$(l-1)$ code to encode the level-l register as the logical qubit of the Steane code. The logical Pauli operators, denoted by $P^{(l)}$ for $P \in \{I, X, Y, Z\}$, are given by the level-$(l-1)$ logical Pauli operators acting on the nth code block, denoted by P_n for $P \in \{I, X, Y, Z\}$, as

$$\begin{aligned} X^{(l)} &= X_1^{(l-1)} \otimes X_2^{(l-1)} \otimes X_3^{(l-1)} \otimes I_4^{(l-1)} \otimes I_5^{(l-1)} \otimes I_6^{(l-1)} \otimes I_7^{(l-1)}, \\ Z^{(l)} &= Z_1^{(l-1)} \otimes Z_2^{(l-1)} \otimes Z_3^{(l-1)} \otimes I_4^{(l-1)} \otimes I_5^{(l-1)} \otimes I_6^{(l-1)} \otimes I_7^{(l-1)}. \end{aligned} \tag{A21}$$

For each concatenation level l, the level-l initial-state preparation gadget for the logical $|0\rangle$ ($|+\rangle$) state of the concatenated Steane code is recursively defined using the level-$(l-1)$ gadgets as shown in Fig. S9, as introduced in Ref. [21]. The measurement outcome of the auxiliary qubit in Fig. S9 is used for the verification; if it is non-zero, then the outcome state is discarded, and the initial-state preparation is rerun. Since the effect of the verification failure on the logical CNOT error rate is in a sub-leading order, we omit to include this effect in the numerical simulation.

The initial-state preparation gadget in Fig. S9 is designed to minimize the number of auxiliary qubits for the verification, compared to the conventional method shown in Fig. S10. To optimize the protocol, we numerically compare the performance of the two initial-state preparation gadgets by comparing the logical CNOT error rates $P^{(1)}_{\rm Steane}(p)$ for various physical error rates p in our error model with fitting by

$$P^{(1)}_{\rm Steane}(p) = a^{(1)}_{\rm Steane} p^2, \tag{A22}$$

as described in Methods. We present this numerical result in Fig. S11; since the method shown in Fig. S9 performs better than the conventional method as shown in Fig. S10 in our setting, we use the former method in our simulation. At the same time, we found through our numerical simulation that the conclusion as to which of the gadgets in

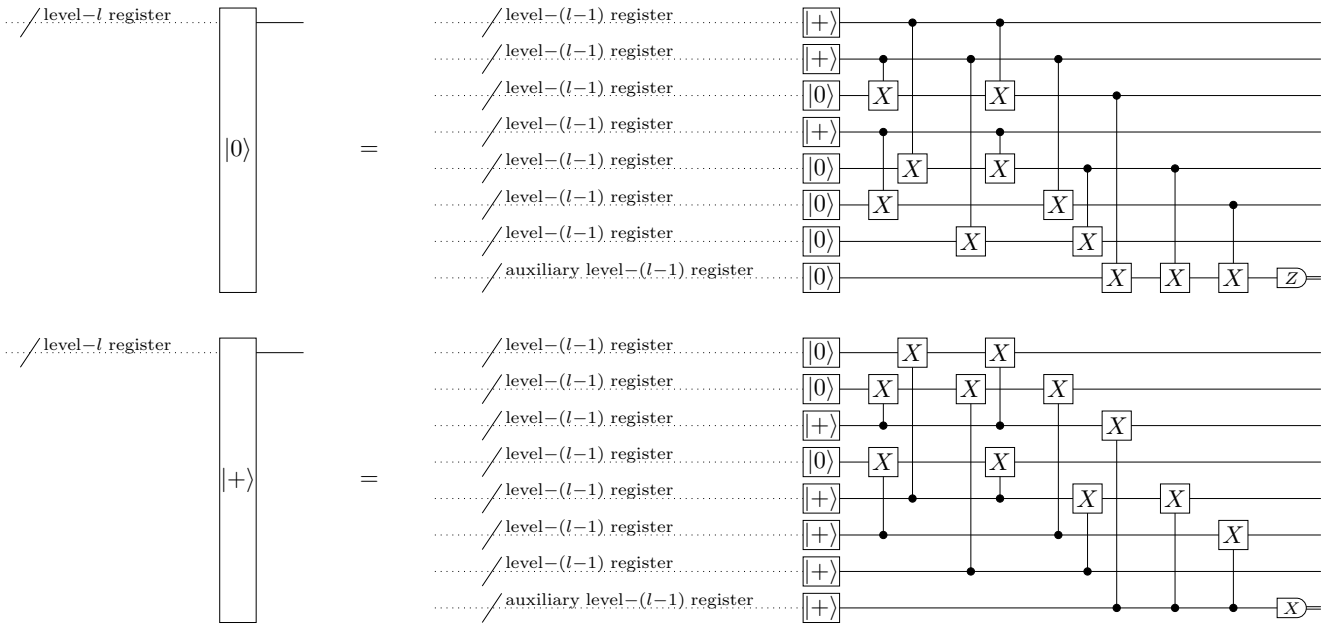


FIG. S9. A level-l initial-state preparation gadget for the concatenated Steane code proposed in Ref. [21]. It implements preparations of the logical $|0\rangle$ ($|+\rangle$) state. The auxiliary qubit is measured for verification. If the measurement outcome is not zero, the output quantum state is discarded and the initial-state preparation is rerun.

Figs. S9 and S10 achieves better logical error rates may change highly sensitively to the details of the error model and the simulation methods; thus, it may be generally inconclusive which of the preparation gadgets to use in a practical experimental platform while the gadget in Fig. S9 was slightly better in the particular setting of numerical simulation in Fig. S11.

Also, the level-l error correction gadget of the concatenated Steane code is recursively defined using the level-$(l-1)$ gadgets as shown in Fig. S12. This gadget is called Knill's error correction gadget [13]. Note that the protocol for the concatenated Steane code simulated here is different from a more optimized protocol for the concatenated Steane code simulated in Ref. [27], where the syndrome extraction for quantum error correction is repeated many times to improve the threshold. Apart from the point that we simulate the logical CNOT error rate while Ref. [27] the logical identity gate, the optimization of the repetition of the syndrome extraction should also be considered to be a reason that the estimated threshold for the concatenated Steane code in Ref. [27] is better than that estimated in this work; however, the contribution of this work is to provide the simulation results for the simple protocol as a baseline for further comparison with more optimized protocols.

d. C_4/Steane code

We summarize the details of the protocol for the C_4/Steane code. The protocol for the C_4/Steane code can be derived as a combination of the protocol for the C_4 code (i.e., a part of the protocol for the C_4/C_6 code) and the protocol for the concatenated Steane code, but for completeness, we here present the details relevant to our analysis. A level-1 register is the two logical qubits of the C_4 code (i.e., the $[[4,2,2]]$ code). The level-l register for $l \in \{2,3,\cdots\}$ refers to the two logical qubits of the C_4/Steane code. To form a level-l register, we use 7 level-$(l-1)$ registers (14 qubits); in particular, similar to the concatenated quantum Hamming code in Sec. A 1, the first (second) qubit from each of the 7 level-$(l-1)$ registers is picked up, and the first (second) qubit of the level-l register is encoded into these picked 7 qubits as the logical qubit of the $[[7,1,3]]$ Steane code. The logical Pauli operators of the level-1 register are the same as (A17). The logical Pauli operators acting on the ith logical qubit of the level-l register for $l \geq 2$, denoted by $P_i^{(l)}$ for $P \in \{I,X,Y,Z\}$, are given by the level-$(l-1)$ logical Pauli operators acting on the jth logical qubit of

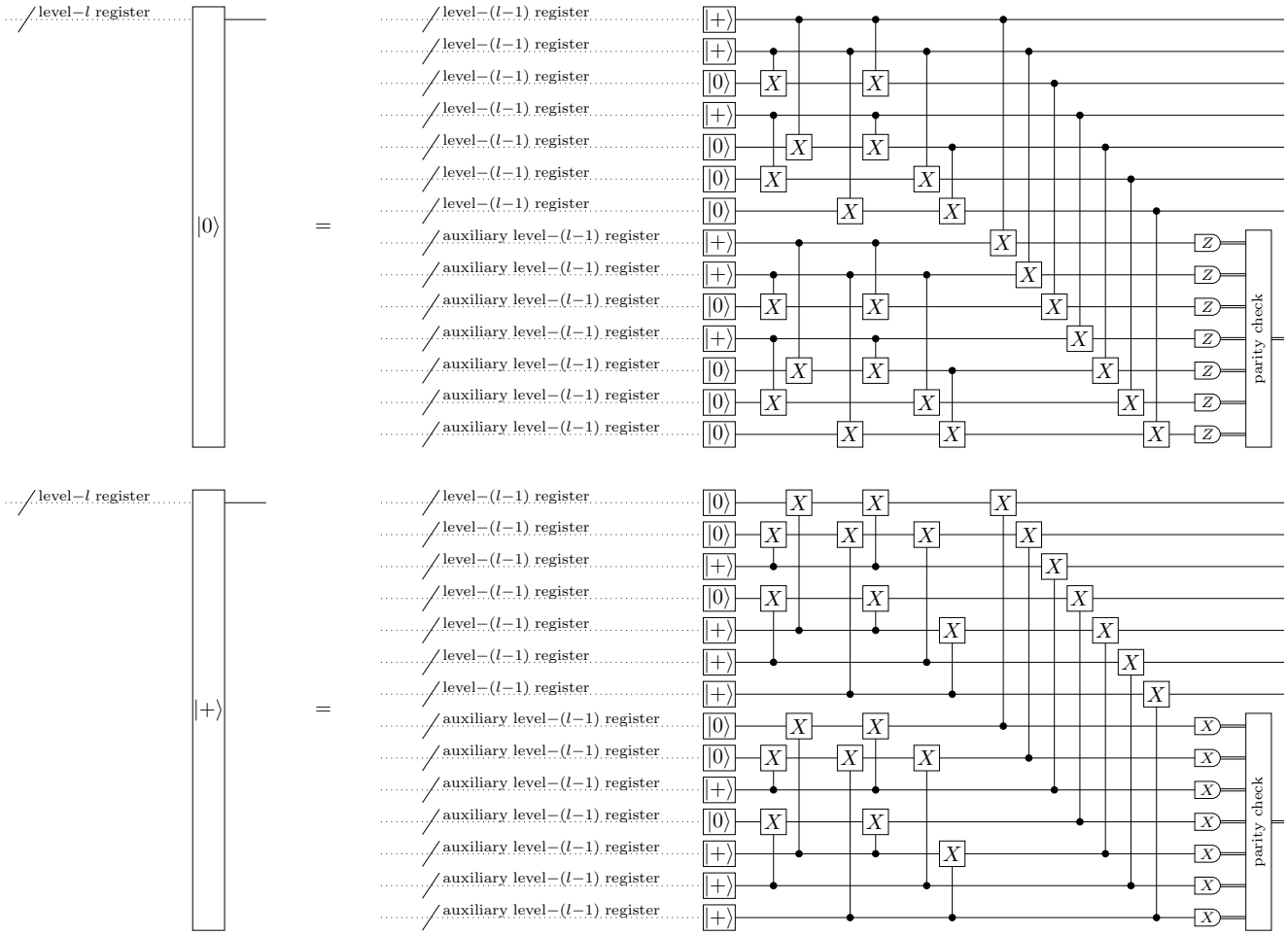


FIG. S10. A conventional method for a level-l initial-state preparation gadget for the concatenated Steane code using the level-$(l-1)$ gadgets. It implements preparation of the logical $|0\rangle$ ($|+\rangle$) state. The Z (X) stabilizer generators and the logical Z (X) operator are measured for verification from the measurement outcomes i_j of the $(j+7)$th qubits for $j \in \{1, \cdots, 7\}$. If $i_1 + i_3 + i_5 + i_7 \neq 0 \pmod 2$, $i_2 + i_3 + i_6 + i_7 \neq 0 \pmod 2$, or $i_1 + i_2 + i_3 \neq 0 \pmod 2$ hold, the output quantum state is discarded and the initial-state preparation is rerun.

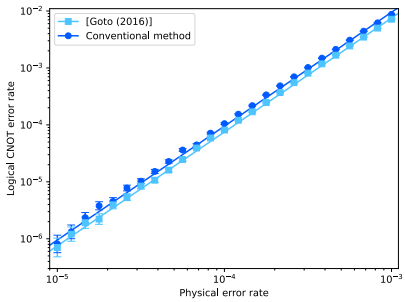


FIG. S11. Comparison of the logical CNOT error rate using the conventional initial-state preparation gadget (shown in Fig. S10) and that minimizing the number of auxiliary qubits for the verification proposed by Ref. [21] (shown in Fig. S9). Error bars in the plot represent the unbiased estimator of the standard deviation of $\log_{10} p_L$ for the logical CNOT error rates p_L. The lines in the plot are obtained from the fitting by (A22). In our setting, the gadget in Fig. S9 was slightly better than that in Fig. S10. At the same time, we found through this numerical simulation that the conclusion as to which of the gadgets achieves better logical error rates may change highly sensitively to the details of the error model and the simulation methods since the difference between these two gadgets is too subtle; thus, it may be generally inconclusive which of the preparation gadgets to use in a practical experimental platform.

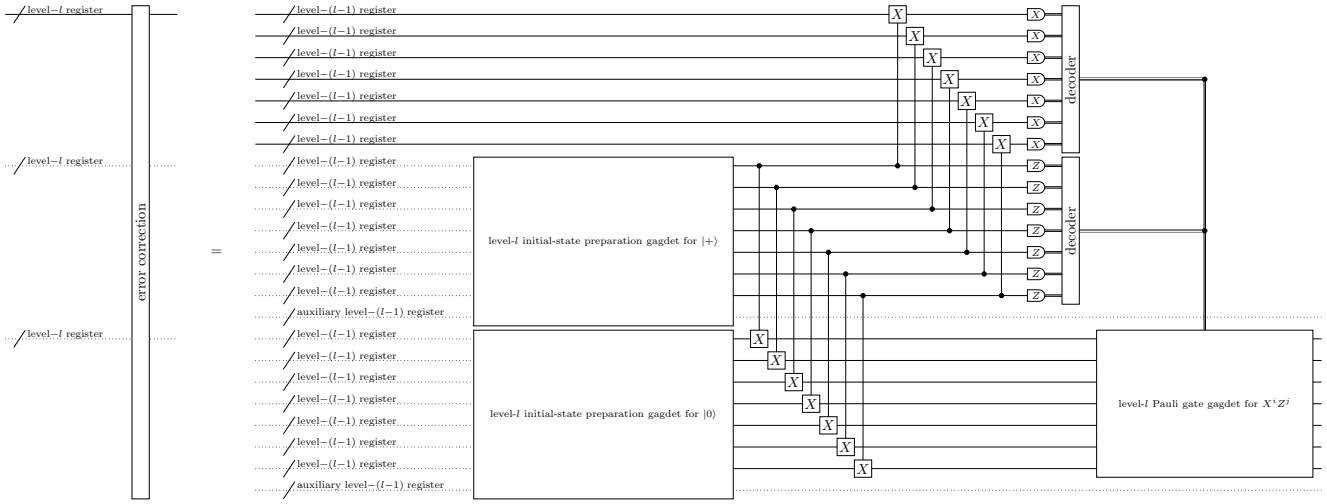


FIG. S12. A level-l error correction gadget for the concatenated Steane code is implemented by using the level-$(l-1)$ gadgets.

the nth level-$(l-1)$ register, denoted by $P_{n,j}^{(l-1)}$ for $P \in \{I, X, Y, Z\}$, as

$$\begin{aligned} X_i^{(l)} &= X_{i,1}^{(l-1)} \otimes X_{i,2}^{(l-1)} \otimes X_{i,3}^{(l-1)} \otimes I_{i,4}^{(l-1)} \otimes I_{i,5}^{(l-1)} \otimes I_{i,6}^{(l-1)} \otimes I_{i,7}^{(l-1)}, \\ Z_i^{(l)} &= Z_{i,1}^{(l-1)} \otimes Z_{i,2}^{(l-1)} \otimes Z_{i,3}^{(l-1)} \otimes I_{i,4}^{(l-1)} \otimes I_{i,5}^{(l-1)} \otimes I_{i,6}^{(l-1)} \otimes I_{i,7}^{(l-1)}. \end{aligned} \tag{A23}$$

The level-1 gadget of the C_4/Steane code is the same as the level-1 gadgets of the C_4/C_6 code, i.e., those for the $[[4, 2, 2]]$ code, shown in Figs. S3, S5, S6, and S7. The level-l gadget of the C_4/Steane code is recursively defined using the level-$(l-1)$ gadgets similarly to the concatenated Steane code shown in Figs. S10, S12, except that level-2 error correction gadget of the C_4/Steane code uses the level-2 Bell-state preparation gadget shown in Fig. S13. Since the effect of the verification failure on the logical CNOT error rate is in a sub-leading order, we omit to include this effect in the numerical simulation.

3. Decoder

We describe the decoding algorithms used in our numerical simulation for the concatenated Steane code, the C_4/C_6 code, the C_4/Steane code, and the concatenated quantum Hamming code. Note that for the surface code, we used the minimum-weight perfect matching algorithm for decoding implemented by PyMatching package [28].

The decoding algorithms used in our simulation for the concatenated Steane code, the C_4/C_6 code, the C_4/Steane code, and the concatenated quantum Hamming code are based on hard-decision decoders. Note that for the concatenated Steane code, the C_4/C_6 code, and the C_4/Steane code, a soft-decision decoder is also implementable within polynomial time [36, 62], which is expected to achieve higher threshold than the hard-decision decoders at the expense of computational time; in our numerical simulation, we use the hard-decision decoders to cover practical situations where the efficiency of implementing the decoder matters. It is unknown whether this construction of efficient soft-decision decoders for concatenated codes generalizes to the concatenated quantum Hamming code since the concatenated quantum Hamming code has a growing number of logical qubits.

For the concatenated Steane code, we use a hard-decision decoder shown in Ref. [4]. The measurement outcome of the level-l measurement gadget is given by a sequence of level-$(l-1)$ logical measurement outcomes $(m_1, \cdots, m_7)$. We check the parities $a_1 = m_1+m_3+m_5+m_7 \bmod 2$, $a_2 = m_2+m_3+m_6+m_7 \bmod 2$, and $a_3 = m_4+m_5+m_6+m_7 \bmod 2$, and if they are not all zeros, we identify the error location to be $i = a_1 + 2a_2 + 4a_3$. Then, we decode the level-l logical measurement outcome as

$$\bar{m} = \begin{cases} m_1 + m_2 + m_3 + 1 \bmod 2 & (i = 1, 2, 3) \\ m_1 + m_2 + m_3 \bmod 2 & (\text{otherwise}) \end{cases}. \tag{A24}$$

For the C_4/C_6 code, we use a hard-decision decoder shown in Ref. [36]. The measurement outcome of the level-1 measurement gadget is given by a sequence of measurement outcomes $(m_1^{(b)}, m_2^{(b)}, m_3^{(b)}, m_4^{(b)})$, where $b \in \{X, Z\}$

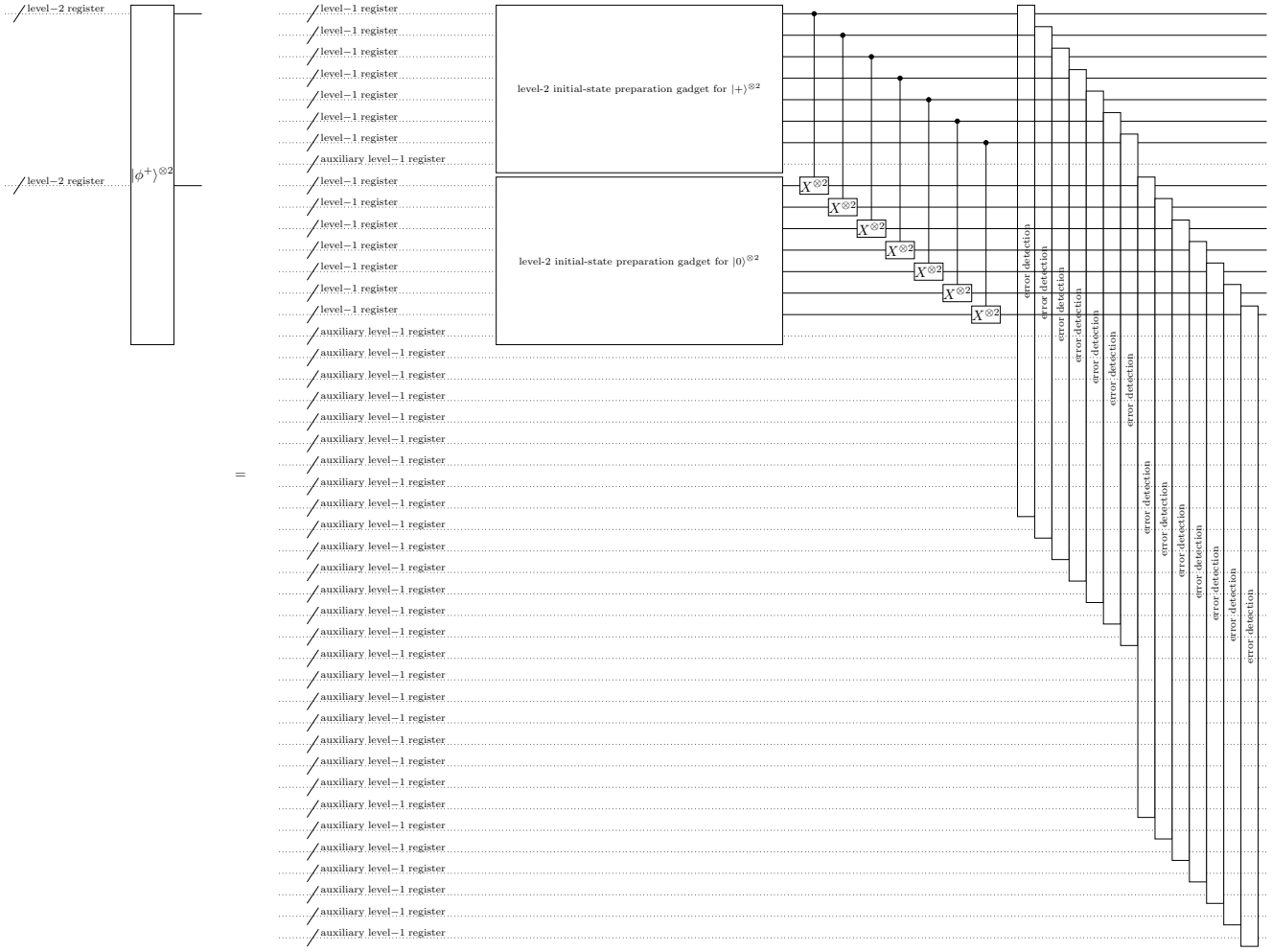


FIG. S13. A level-2 Bell-state preparation gadget for the C_4/Steane code implements preparation of the logical Bell state $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

represents the basis of the measurement. The parity of the measurement outcomes is checked to detect an error, and if $m_1^{(b)} + m_2^{(b)} + m_3^{(b)} + m_4^{(b)} = 0 \bmod 2$ holds, the measurement outcome is decoded as

$$(\bar{m}_1^{(Z)}, \bar{m}_2^{(Z)}) = (m_1^{(Z)} + m_2^{(Z)}, m_2^{(Z)} + m_4^{(Z)}) \bmod 2, \tag{A25}$$

$$(\bar{m}_1^{(X)}, \bar{m}_2^{(X)}) = (m_1^{(X)} + m_3^{(X)}, m_3^{(X)} + m_4^{(X)}) \bmod 2. \tag{A26}$$

Otherwise, we decode it as (E, E), where E represents that an error is detected. The measurement outcome of the level-l measurement gadget for $l \geq 2$ is given by a sequence of level-$(l-1)$ measurement outcomes $((m_1^{(b)}, m_2^{(b)}), (m_3^{(b)}, m_4^{(b)}), (m_5^{(b)}, m_6^{(b)}))$. If errors are detected in two or three out of three code blocks, we decode it as (E, E). If errors are detected in one code block, we decode it as

$$(\bar{m}_1^{(Z)}, \bar{m}_2^{(Z)}) = \begin{cases} (m_3^{(Z)} + m_4^{(Z)} + m_6^{(Z)}, m_4^{(Z)} + m_5^{(Z)}) \bmod 2 & ((m_1^{(Z)}, m_2^{(Z)}) = (E, E)) \\ (m_1^{(Z)} + m_2^{(Z)} + m_5^{(Z)}, m_2^{(Z)} + m_5^{(Z)} + m_6^{(Z)}) \bmod 2 & ((m_3^{(Z)}, m_4^{(Z)}) = (E, E)) \\ (m_2^{(Z)} + m_3^{(Z)}, m_1^{(Z)} + m_3^{(Z)} + m_4^{(Z)}) \bmod 2 & ((m_5^{(Z)}, m_6^{(Z)}) = (E, E)) \end{cases}, \tag{A27}$$

$$(\bar{m}_1^{(X)}, \bar{m}_2^{(X)}) = \begin{cases} (m_3^{(X)} + m_4^{(X)} + m_6^{(X)}, m_4^{(X)} + m_5^{(X)}) \bmod 2 & ((m_1^{(X)}, m_2^{(X)}) = (E, E)) \\ (m_1^{(X)} + m_2^{(X)} + m_5^{(X)}, m_2^{(X)} + m_5^{(X)} + m_6^{(X)}) \bmod 2 & ((m_3^{(X)}, m_4^{(X)}) = (E, E)) \\ (m_2^{(X)} + m_3^{(X)}, m_1^{(X)} + m_3^{(X)} + m_4^{(X)}) \bmod 2 & ((m_5^{(X)}, m_6^{(X)}) = (E, E)) \end{cases}. \tag{A28}$$

If no errors are detected, we check the parity of the measurement outcome to detect an error. If $m_1^{(b)} + m_3^{(b)} + m_5^{(b)} = 0 \bmod 2$ and $m_2^{(b)} + m_4^{(b)} + m_6^{(b)} = 0 \bmod 2$ hold, we decode it as

$$(\bar{m}_1^{(Z)}, \bar{m}_2^{(Z)}) = (m_2^{(Z)} + m_3^{(Z)}, m_1^{(Z)} + m_3^{(Z)} + m_4^{(Z)}) \bmod 2, \tag{A29}$$

$$(\bar{m}_1^{(X)}, \bar{m}_2^{(X)}) = (m_3^{(X)} + m_4^{(X)} + m_6^{(X)}, m_4^{(X)} + m_5^{(X)}) \bmod 2. \tag{A30}$$

Otherwise, we decode it as (E, E).

For the C_4/Steane code, we use the same decoder as the C_4/C_6 code for the level-1 protocol and as the concatenated Steane code for the level-l ($l \geq 3$) protocols. For the level-2 measurement gadget, the measurement outcome is given as a sequence of level-1 measurement outcomes $(m_1, m_2, m_3, m_4, m_5, m_6, m_7)$. If errors are detected in two code blocks, denoted by i and j, we search $(m'_1, m'_2, m'_3, m'_4, m'_5, m'_6, m'_7)$ such that $m'_k = m_k$ for $k \neq i, j$ and $m'_1 + m'_3 + m'_5 + m'_7 = m'_2 + m'_3 + m'_6 + m'_7 = m'_4 + m'_5 + m'_6 + m'_7 = 0 \bmod 2$. If such a sequence is found, we decode it as

$$\bar{m} = m'_1 + m'_2 + m'_3 \bmod 2. \tag{A31}$$

Otherwise, we use the same decoder as the concatenated Steane code.

For the concatenated quantum Hamming code, we use the decoder shown in Ref. [4], which is a straightforward generalization of (A24). See Ref. [4] for details.

Appendix B: Threshold analysis of the concatenated quantum Hamming code, the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code

In this section, we summarize the details of our numerical results on the threshold analysis.

We show the logical CNOT error rates of the quantum Hamming codes in Fig. S14 (a), from which we obtain the threshold of the original protocol in Ref. [4] based on the concatenated quantum Hamming code. This code is obtained by concatenating the quantum Hamming code $\mathcal{Q}_{l+2}$ on the concatenation level $l \in \{1, 2, \cdots\}$. We also show the threshold for a modification of this concatenated quantum Hamming code that is used in our protocol, which starts from $\mathcal{Q}_4$ by skipping $\mathcal{Q}_3$ (i.e., skipping the $[[7, 1, 3]]$ code). As described in Methods, the logical error rate $P_{r_l}(p)$ for the quantum Hamming code $\mathcal{Q}_r$ is approximated for $r_l \in \{3, 4, 5, 6, 7\}$ by the fitting curve

$$P_{r_l}(p) = a_{r_l} p^2, \tag{B1}$$

where the logical error rate of each data point is estimated using (A3). From our numerical results, we determine the fitting parameters by

$$a_3 = (1.603 \pm 0.013) \times 10^4, \tag{B2}$$

$$a_4 = (6.68 \pm 0.05) \times 10^4, \tag{B3}$$

$$a_5 = (5.09 \pm 0.04) \times 10^5, \tag{B4}$$

$$a_6 = (5.65 \pm 0.04) \times 10^6, \tag{B5}$$

$$a_7 = (5.59 \pm 0.05) \times 10^7. \tag{B6}$$

From these results, as described in Methods, we estimate the logical CNOT error rates for the concatenated quantum Hamming code in the original protocol starting from $\mathcal{Q}_3$ and that of our protocol starting from $\mathcal{Q}_4$ according to

$$P_{r_L} \circ \cdots \circ P_{r_2} \circ P_{r_1}(p), \tag{B7}$$

where $r_1, r_2, \ldots, r_L$ are the sequence of parameters of the quantum Hamming codes, and p is the physical error rate for $\mathcal{Q}_{r_1}$. The estimates of these logical error rates are shown in Figs. S14 (b) and (c). The threshold values of these two concatenated quantum Hamming codes are estimated as $\sim 10^{-5}$ and $\sim 3 \times 10^{-6}$, respectively. To achieve the logical error rate 10^{-24} using the one for our protocol starting from $\mathcal{Q}_4$, the physical error rate for $\mathcal{Q}_4$ should be less than $P_{\text{target}} = 2.2 \times 10^{-7}$, which is the logical error rate to be achieved by the underlying quantum code in the proposed protocol.

We also show the logical CNOT error rates of the C_4/C_6 code, the surface code, the Steane code, and the C_4/Steane code in Fig. S15 (a) and (b). Due to the limitation of the computational resources, for the numerical simulation of the level-2 concatenated Steane code and the level-2 C_4/Steane code, we simplified the quantum circuit shown in

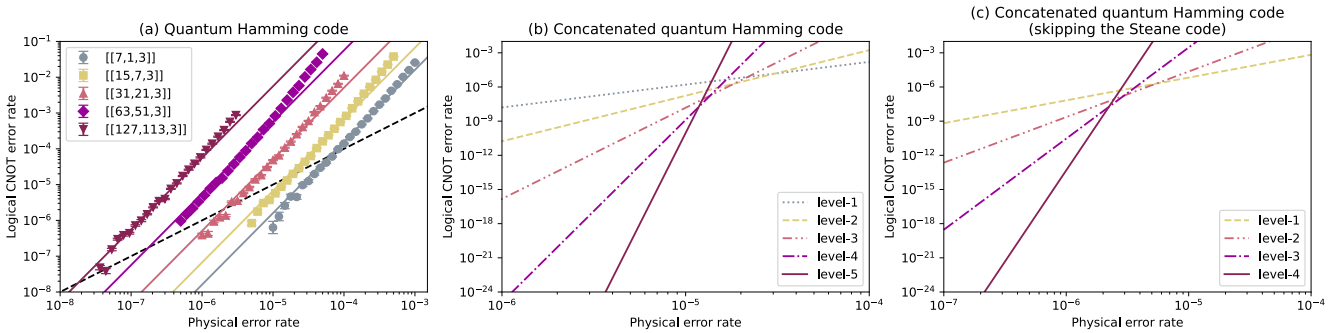


FIG. S14. (a) The logical CNOT error rates of the quantum Hamming codes $\mathcal{Q}_r$ for $r = 3$ ($[[7, 1, 3]]$), $r = 4$ ($[[15, 7, 3]]$), $r = 5$ ($[[31, 21, 3]]$), $r = 6$ ($[[63, 51, 3]]$) and $r = 7$ ($[[127, 113, 3]]$) for various physical error rates. Each point of the logical CNOT error rate in the plot is estimated using (A3) and (B1), where $P^{(0)}_{\text{CNOT}}$ in (A3) is given by an average over 10^6 simulation runs, and $P_{\text{verification}}$ and $P^{(i)}_{\text{CNOT}}$ in (A3) are given by averages over 10^4 simulation runs. The number of simulation runs counts all events including those in which the verification fails, which are discarded in the analysis. Error bars in the plot represent the unbiased estimator of the standard deviation of $\log_{10} p_L$ for the logical CNOT error rates p_L. The fitting yields the parameters in (B2)–(B6). The dashed line represents a line where the logical CNOT error rate equals the physical error rate. (b) The estimation of the logical CNOT error rate of the concatenated quantum Hamming code starting from $\mathcal{Q}_3$, obtained from the fitting results in (a) using (B7). (c) The estimation of the logical CNOT error rate of the modified concatenated quantum Hamming code starting from $\mathcal{Q}_4$ (skipping $\mathcal{Q}_3$), obtained in the same way as (b).

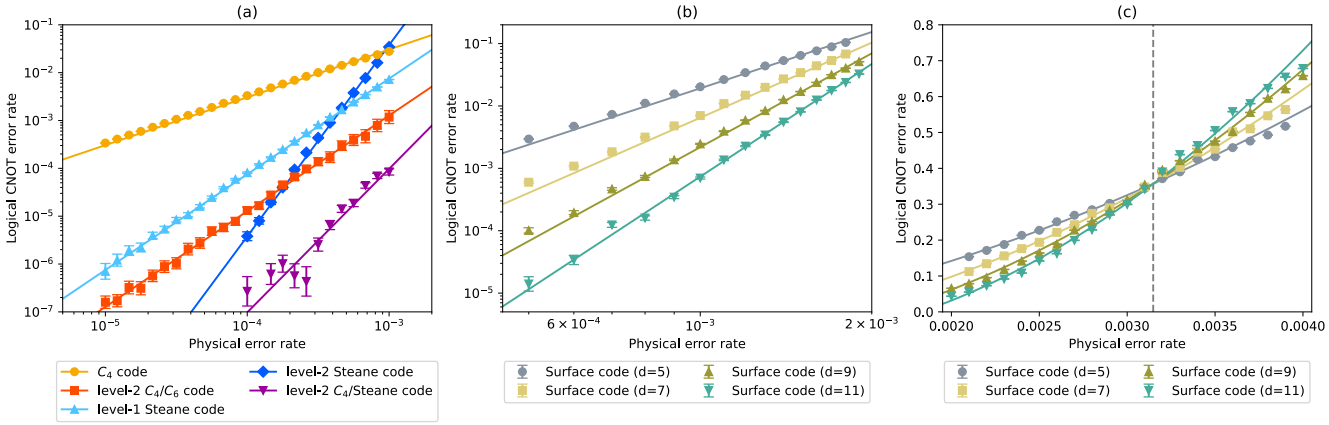


FIG. S15. The logical CNOT error rates of the C_4/C_6 code, the surface code, the concatenated Steane code, and the C_4/Steane code. Each point of the logical CNOT error rate in the plot is an average over 10^6 simulation runs (the C_4 code, the level-2 C_4/C_6 code, the level-1 Steane code, and the surface code) or 10^7 simulation runs (the level-2 concatenated Steane code and the level-2 C_4/Steane code). Similar to the quantum Hamming code in Fig. S14, the number of simulation runs for the C_4/C_6 code, the concatenated Steane code, and the C_4/Steane code counts all events including those in which the verification fails, which are discarded in the analysis. Error bars in the plot represent the unbiased estimator of the standard deviation of $\log_{10} p_L$ for the logical CNOT error rates p_L. In (a), we present the fitting of the logical CNOT error rates of the C_4/C_6 code, the concatenated Steane code, and the C_4/Steane code, and in (b), the surface code, which yields the parameters in (B13)–(B19). In (c), we present the fitting of the logical CNOT error rate of the surface code by (B20) when the physical error rate p is close to the threshold yields the parameters in (B21), where the vertical dashed line represents the threshold $p^{(\text{th})}_{\text{surface}}$ in (B21).

Fig. 3 of Methods in such a way that ten repetitions of the gate gadget of the logical CNOT$^{\otimes K}$ gate followed by the error correction in Fig. 3 of Methods are replaced with one gate gadget of the logical CNOT$^{\otimes K}$ gate followed by the error correction and the error-free logical CNOT$^{\otimes K}$ gate. As described in Methods, the fitting curves of the logical error rates $P^{(l)}_{C_4/C_6}$, $P^{(d)}_{\text{surface}}$, $P^{(l)}_{\text{Steane}}$, and $P^{(l)}_{C_4/\text{Steane}}$ for the level-l C_4/C_6 code, the distance-d surface code, the level-l concatenated Steane code, and the level-l C_4/Steane code, respectively, are given by

$$P^{(l)}_{C_4/C_6}(p) = A_{C_4/C_6}(B_{C_4/C_6}p)^{F_l}, \tag{B8}$$

$$P^{(d)}_{\text{surface}}(p) = A_{\text{surface}}(B_{\text{surface}}p)^{\frac{d+1}{2}}, \tag{B9}$$

$$P^{(l)}_{\text{Steane}}(p) = a^{(l)}_{\text{Steane}} p^{2^l}, \tag{B10}$$
$$P^{(1)}_{C_4/\text{Steane}}(p) = a^{(1)}_{C_4/\text{Steane}} p, \tag{B11}$$
$$P^{(2)}_{C_4/\text{Steane}}(p) = a^{(2)}_{C_4/\text{Steane}} p^3, \tag{B12}$$

where the notations are the same as the ones described in Methods. From our numerical results, we determine the fitting parameters for our results as

$$A_{C_4/C_6} = 0.73 \pm 0.03, \tag{B13}$$
$$B_{C_4/C_6} = 41.7 \pm 1.8, \tag{B14}$$
$$A_{\text{surface}} = 0.4998 \pm 0.0018, \tag{B15}$$
$$B_{\text{surface}} = 337.3 \pm 0.3, \tag{B16}$$
$$a^{(1)}_{\text{Steane}} = 7513 \pm 18, \tag{B17}$$
$$a^{(2)}_{\text{Steane}} = (3.78 \pm 0.04) \times 10^{10}, \tag{B18}$$
$$a^{(2)}_{C_4/\text{Steane}} = (9.8 \pm 0.6) \times 10^4. \tag{B19}$$

From this fitting, we observed that the level-3 C_4/Steane code for $p = 0.1\%$ has almost the same logical error rate as the level-2 C_4/Steane code; based on this observation, Fig. 2 of the main text excludes the data point corresponding to the level-3 C_4/Steane code for $p = 0.1\%$, presenting those at levels 1, 2, 4, and 5.

To obtain the threshold $p^{(\text{th})}_{\text{surface}}$ of the surface code in Fig. S15 (c), we fit the logical error rate of the surface code when the physical error rate p is close to the threshold by another fitting curve based on the critical exponent method of Ref. [49]. The fitting curve is given by

$$\begin{aligned} P'^{(d)}_{\text{surface}}(p) &= C_{\text{surface}} + D_{\text{surface}} x + E_{\text{surface}} x^2, \\ x &= (p - p^{(\text{th})}_{\text{surface}}) d^{1/\mu}, \end{aligned} \tag{B20}$$

where the estimated fitting parameters are

$$\begin{aligned} p^{(\text{th})}_{\text{surface}} &= (3.1480 \pm 0.0010) \times 10^{-3}, \\ \mu &= 1.471 \pm 0.003, \\ C_{\text{surface}} &= 0.3568 \pm 0.0003, \\ D_{\text{surface}} &= 72.7 \pm 0.2, \\ E_{\text{surface}} &= 2941 \pm 16. \end{aligned} \tag{B21}$$

Note that it consistently holds that $p^{(\text{th})}_{\text{surface}} \approx B^{-1}_{\text{surface}} \approx 0.3\%$.

[1] A. A. Kovalev and L. P. Pryadko, Fault tolerance of quantum low-density parity check codes with sublinear distance scaling, Phys. Rev. A **87**, 020304 (2013).
[2] D. Gottesman, Fault-tolerant quantum computation with constant overhead, Quantum Info. Comput. **14**, 1338–1372 (2014).
[3] 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)* (2018) pp. 743–754.
[4] H. Yamasaki and M. Koashi, Time-efficient constant-space-overhead fault-tolerant quantum computation, Nature Physics **20**, 247 (2024).
[5] A. Krishna and D. Poulin, Fault-tolerant gates on hypergraph product codes, Phys. Rev. X **11**, 011023 (2021).
[6] L. Z. Cohen, I. H. Kim, S. D. Bartlett, and B. J. Brown, Low-overhead fault-tolerant quantum computing using long-range connectivity, Science Advances **8**, eabn1717 (2022).
[7] M. A. Tremblay, N. Delfosse, and M. E. Beverland, Constant-overhead quantum error correction with thin planar connectivity, Phys. Rev. Lett. **129**, 050504 (2022).
[8] S. B. Bravyi and A. Y. Kitaev, Quantum codes on a lattice with boundary, arXiv:quant-ph/9811052 [quant-ph] (1998).
[9] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, Topological quantum memory, Journal of Mathematical Physics **43**, 4452 (2002).

[10] A. M. Steane, Simple quantum error-correcting codes, Phys. Rev. A **54**, 4741 (1996).
[11] R. W. Hamming, Error detecting and error correcting codes, The Bell system technical journal **29**, 147 (1950).
[12] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation, Phys. Rev. A **86**, 032324 (2012).
[13] E. Knill, Quantum computing with realistically noisy devices, Nature **434**, 39 (2005).
[14] 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.*, Logical quantum processor based on reconfigurable atom arrays, Nature **626**, 58 (2024).
[15] 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).
[16] L. Egan, D. M. Debroy, C. Noel, A. Risinger, D. Zhu, D. Biswas, M. Newman, M. Li, K. R. Brown, M. Cetina, *et al.*, Fault-tolerant control of an error-corrected qubit, Nature **598**, 281 (2021).
[17] 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, arXiv:2006.05416 [quant-ph] (2020).
[18] 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).
[19] D. Litinski and N. Nickerson, Active volume: An architecture for efficient fault-tolerant quantum computers with limited non-local connections, arXiv:2211.15465 [quant-ph] (2022).
[20] H. Goto, Step-by-step magic state encoding for efficient fault-tolerant quantum computation, Scientific Reports **4**, 7501 (2014).
[21] H. Goto, Minimizing resource overheads for fault-tolerant preparation of encoded states of the steane code, Scientific Reports **6**, 19578 (2016).
[22] B. Schumacher, Sending entanglement through noisy quantum channels, Phys. Rev. A **54**, 2614 (1996).
[23] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 124–134.
[24] C. Gidney and M. Ekerå, How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits, Quantum **5**, 433 (2021).
[25] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM **21**, 120 (1978).
[26] E. Barker and Q. Dang, Nist special publication 800-57 part 1, revision 4, NIST, Tech. Rep **16** (2016).
[27] A. M. Steane, Overhead and noise threshold of fault-tolerant quantum error correction, Phys. Rev. A **68**, 042322 (2003).
[28] O. Higgott, Pymatching: A python package for decoding quantum codes with minimum-weight perfect matching, arXiv:2105.13082 [quant-ph] (2021).
[29] O. Higgott and C. Gidney, Sparse blossom: correcting a million errors per core second with minimum-weight matching, arXiv:2303.15933 [quant-ph] (2023).
[30] D. Horsman, A. G. Fowler, S. Devitt, and R. Van Meter, Surface code quantum computing by lattice surgery, New Journal of Physics **14**, 123011 (2012).
[31] C. Vuillot, L. Lao, B. Criger, C. G. Almudéver, K. Bertels, and B. M. Terhal, Code deformation and lattice surgery are gauge fixing, New Journal of Physics **21**, 033028 (2019).
[32] C. Gidney, Stability Experiments: The Overlooked Dual of Memory Experiments, Quantum **6**, 786 (2022).
[33] C. Vuillot, L. Lao, B. Criger, C. García Almudéver, K. Bertels, and B. M. Terhal, Code deformation and lattice surgery are gauge fixing, New Journal of Physics **21**, 033028 (2019).
[34] A. W. Cross, D. P. Divincenzo, and B. M. Terhal, A comparative code study for quantum fault tolerance, Quantum Info. Comput. **9**, 541–572 (2009).
[35] C. Chamberland and P. Ronagh, Deep neural decoders for near term fault-tolerant experiments, Quantum Science and Technology **3**, 044002 (2018).
[36] H. Goto and H. Uchikawa, Fault-tolerant quantum computation with a soft-decision decoder for error correction and detection by teleportation, Scientific reports **3**, 2044 (2013).
[37] 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, arXiv:2308.08648 [quant-ph] (2023).
[38] M. Fellous-Asiani, J. H. Chai, Y. Thonnart, H. K. Ng, R. S. Whitney, and A. Auffèves, Optimizing resource efficiencies for scalable full-stack quantum computers, PRX Quantum **4**, 040319 (2023).
[39] C. A. Pattison, A. Krishna, and J. Preskill, Hierarchical memories: Simulating quantum ldpc codes with local gates, arXiv:2303.04798 [quant-ph] (2023).
[40] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, High-threshold and low-overhead fault-tolerant quantum memory, arXiv:2308.07915 [quant-ph] (2023).
[41] M. Christandl and A. Müller-Hermes, Fault-tolerant coding for quantum communication, IEEE Transactions on Information Theory **70**, 282 (2022).
[42] N. Baspin, O. Fawzi, and A. Shayeghi, A lower bound on the overhead of quantum error correction in low dimensions, arXiv:2302.04317 [quant-ph] (2023).
[43] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge university press, 2010).

[44] 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.
[45] J. Lee, D. W. Berry, C. Gidney, W. J. Huggins, J. R. McClean, N. Wiebe, and R. Babbush, Even more efficient quantum computations of chemistry through tensor hypercontraction, PRX Quantum **2**, 030305 (2021).
[46] N. Yoshioka, T. Okubo, Y. Suzuki, Y. Koizumi, and W. Mizukami, Hunting for quantum-classical crossover in condensed matter problems, arXiv:2210.14109 [quant-ph] (2023).
[47] C. Gidney, Stim: a fast stabilizer circuit simulator, Quantum **5**, 497 (2021).
[48] Specifications - supercomputer fugaku: Fujitsu global, `https://www.fujitsu.com/global/about/innovation/fugaku/specifications/` (2018).
[49] C. Wang, J. Harrington, and J. Preskill, Confinement-higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory, Annals of Physics **303**, 31–58 (2003).
[50] qpic, `https://github.com/qpic/qpic` (2016).
[51] D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology (1997).
[52] M. M. Wilde, Logical operators of quantum codes, Phys. Rev. A **79**, 062322 (2009).
[53] A. M. Steane, Fast fault-tolerant filtering of quantum codewords, arXiv:quant-ph/0202036 (2002).
[54] A. Paetznick and B. W. Reichardt, Fault-tolerant ancilla preparation and noise threshold lower bounds for the 23-qubit golay code, Quantum Inf. Comput. **12**, 1034 (2011).
[55] M. H. Freedman and D. A. Meyer, Projective plane and planar quantum codes, Foundations of Computational Mathematics **1**, 325 (2001).
[56] A. Y. Kitaev, Quantum error correction with imperfect gates, in *Quantum Communication, Computing, and Measurement*, edited by O. Hirota, A. S. Holevo, and C. M. Caves (Springer US, Boston, MA, 1997) pp. 181–188.
[57] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Annals of physics **303**, 2 (2003).
[58] H. Bombin and M. A. Martin-Delgado, Optimal resources for topological two-dimensional stabilizer codes: Comparative study, Physical Review A **76** (2007).
[59] C. Chamberland and E. T. Campbell, Universal quantum computing with twist-free and temporally encoded lattice surgery, PRX Quantum **3**, 010331 (2022).
[60] A. G. Fowler and C. Gidney, Low overhead quantum computation using lattice surgery, arXiv:1808.06709 [quant-ph] (2019).
[61] C. Gidney, Stability experiments: The overlooked dual of memory experiments, Quantum **6**, 786 (2022).
[62] D. Poulin, Optimal and efficient decoding of concatenated quantum block codes, Phys. Rev. A **74**, 052333 (2006).

Exponential quantum advantage for non-Hermitian eigenproblems

Xiao-Ming Zhang[1 2] Yukun Zhang[2] Wenhao He[3 4] Xiao Yuan[2 *]

[1] *School of Physics, South China Normal University, Guangzhou 510006, China*
[2] *Center on Frontiers of Computing Studies, Department of Computer Science, Peking University, Beijing, China*
[3] *Center for Computational Science and Engineering, Massachusetts Institute of Technology, Cambridge, USA*
[4] *School of Physics, Peking University, Beijing 100871, China*

Abstract. We present a family of quantum algorithms tailored for solving the eigenvalue problem for general matrices, encompassing scenarios with complex eigenvalues or even defective matrices. Our results find applications in diverse domains, including the *first* quantum algorithm estimating the relaxation time of Markov chains, solving Liouvillian gaps in open quantum systems, and verifying PT-symmetry broken/unbroken phases. These applications underscore the significance of our quantum eigensolvers for problems across various disciplines. By proofing the BQP-completeness, we also show that our quantum algorithm has in general an exponential speedup over classical methods.

Keywords: Quantum algorithms, Eigenvalues, non-Hermitian, open quantum systems, Markov chain

Eigensystem, a fundamental concept in linear algebra, represents key features of a matrix transformation. Formally, complex value λ_j and normalized vector $|v_j\rangle$ are called the eigenvalue and the corresponding eigenvector of a matrix A if

$$A|v_j\rangle = \lambda_j|v_j\rangle. \tag{1}$$

Eigensystem plays a central role in basically all fields of modern science and engineering. Nevertheless, for classical algorithms tackling Eq. (1), the cost generally grows formidably high for large matrices.

A potential solution is to make use of quantum computers. Many quantum algorithms have been proposed for such a purpose based on different techniques [3, 19, 28]. Yet, since quantum computing naturally favours Hermiticity, existing quantum algorithms have been mostly restricted to the special and simplified case of Hermitian matrices $A = A^\dagger$, where λ_j are real and $|v_j\rangle$ forms an orthonormal basis. For a general matrix, we could encounter complex and even defective eigenvalues and unorthogonal eigenvectors. The advantage of quantum computing in solving the general non-Hermitian eigenvalue problems remains an outstanding open question.

Here, we propose a family of efficient quantum eigensolver algorithms for general matrices. The algorithm is promised to have polylogarithmic runtime to the matrix dimension. For a diagonalizable matrix, the complexity of obtaining an arbitrary eigenvalue is $\tilde{O}(K^3\varepsilon^{-1}\gamma^{-1})$, and the complexity for obtaining the eigenvalue closest to a reference point or line is $\tilde{O}(K^3\varepsilon^{-2}\gamma^{-1})$, where K, ε and γ are the Jordan condition number, accuracy, and overlap between initial state and target state. The latter can be considered as the generalizations of ground energy and energy gap problems, whose decision version is shown to be BQP (bounded-error quantum polynomial time)-complete. In other words, the existence of exponential quantum advantage of our algorithm is expected, unless universal quantum computer can be efficiently simulated classically.

*xiaoyuan@pku.edu.cn

Our quantum eigensolver for general matrices would have profound applications in various modern tasks. A typical example is for open quantum systems, in which many novel phenomenon emerges, such as $\mathcal{PT}$-symmetry breaking [5, 6, 10, 16, 26], skin effects [36] and non-hermiticity driven topological phase transition [20, 27, 31]. While current studies on related topics have been restricted to few-body or analytically solvable cases, our algorithm can potentially provide exponential quantum speedup for general many-body open quantum systems. We provide examples on two of the most pivotal problems in non-Hermitian physics: Liouvillian gap estimation and the witness of spontaneous symmetry breaking. Besides, in the field of stochastic processes, our algorithm could also be applied to estimate the relaxation time of a Markov chain, a problem whose quantum advantages were unknown before.

Eigenvalue Problems. For a general matrix A, one can perform the Jordan decomposition as

$$A = P\Lambda P^{-1}, \tag{2}$$

where Λ is a matrix in the Jordan canonical form (JCF), whose diagonal elements correspond to the eigenvalues, and P is an invertible matrix. A is called *diagonalizable* if Λ is diagonal. Most generally, we have $\Lambda = \Lambda_1 \oplus \Lambda_2 \oplus \cdots \oplus \Lambda_M$, where,$\Lambda_j$ are Jordan blocks. In the case $M < N$, we call A a *defective* matrix. It is worth noting that eigenvalues are fundamentally different from singular values unless the matrix is normal with spectral decomposition. Therefore, the eigenvalue problem does not trivially fit into the framework of quantum singular value transformation [14, 23].

We define $m'_{\max} \equiv \max_j \dim(\Lambda_j)$ as the largest dimension of the Jordan blocks, and κ_P as the condition number of the matrix P or the Jordan condition number of A [22]. Regarding the nonuniqueness of Eq. (2), we define κ_P as the minimum value for all possible P. Without loss of generality, we assume that these two quantities are upper bounded by $m_{\max} \geqslant m'_{\max}$ and $K \geqslant \kappa_P$ for some known $m_{\max}$ and K. It turns out that the difficulty of

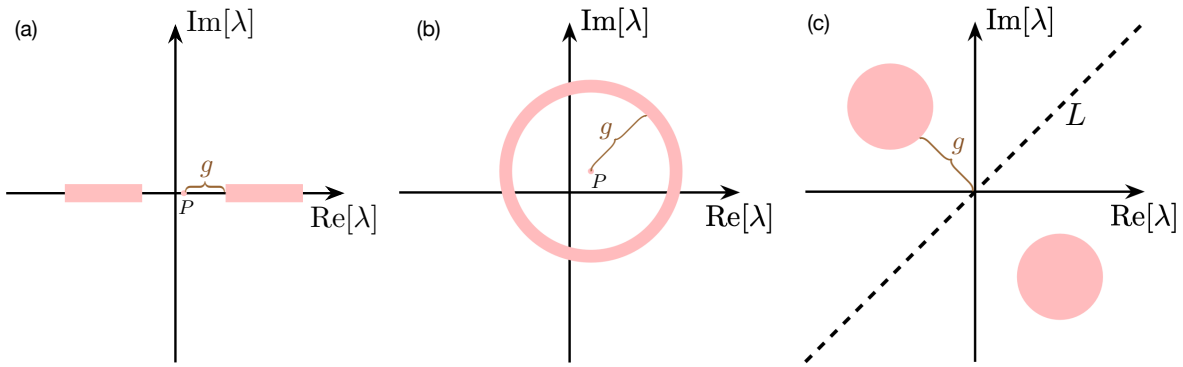


Figure 1: (a) Energy gap for Hermitian matrices with reference point P, (b) the point gap for non-Hermitian matrices with reference point P, and (c) the line gap for non-Hermitian matrices with reference line L.

the problem depends on both $m_{\max}$ and K.

The first problem we consider is to output an estimation of one eigenvalue without additional constraints, which is informally described as follows.

Problem 1 *Given a square matrix A with $\|A\| \leqslant 1$, output an eigenvalue up to accuracy $\varepsilon \in (0,1)$.*

Here, $\|\cdot\|$ refers to the spectral norm of a matrix. We also consider two generalization of ground energy (or energy gap) problems for Hermitian matrix to the non-Hermitian domains. These two problems are informally described as follows.

Problem 2 *Given a square matrix A satisfying $\|A\| \leqslant 1$, a reference point P. Up to an accuracy $\varepsilon \in (0,1)$, output an eigenvalue closest to P.*

Problem 3 *Given a square matrix A satisfying $\|A\| \leqslant 1$, a reference line L in the complex plain such that L. Up to an accuracy $\varepsilon \in (0,1)$, output an eigenvalue closest to L.*

In the case where P or L have no overlaps with eigenvalues, Problem 2 or 3 corresponds to finding an eigenvalue that is closest to the reference point P, or line L (up to an accuracy ε). Therefore, they can be considered as two different ways of the generalization of the ground energy problem for Hermitian matrices. On the other hand, when P or L overlaps with at least one of the eigenvalues, Problems 2 and 3 become *Point gap*, or *Line gap* problems [7, 8, 15]. In some cases, both point gaps and line gaps are non-vanishing. But there exists matrices with non-vanishing point gap, but zero line gap. Physics systems with Hamiltonian corresponding these two cases may emerge from different symmetries and topologies [7, 8, 15].

Results. We first discuss the assumptions of the algorithms. Given a general square matrix $A \in \mathbb{C}^{N\times N}$ with $N = 2^n$, we consider its block encoding that provides unitary access to the matrix. For a unitary $\mathscr{O}_A$, we say it is a block encoding of A if it encodes the desirable matrix A such that $A = (\langle 0^a| \otimes I)\, \mathscr{O}_A\, (|0^a\rangle \otimes I)$, with I the N-dimensional identity. Note that we have neglected a scaling factor compared to the conventional definition as it can be absorbed in matrix A. Block-encoding is a standard way of encoding the classical description of a matrix to quantum operations [9, 14, 21, 23, 35]. In practice, $\mathscr{O}_A$ may be constructed by sparse-access input model or linear combination of unitaries (LCU) [21], depending on the form of A being presented.

For Hermitian matrices, the eigenvalue problem is typically solved by assuming the existence of an initial state that can be prepared to have a reasonable lower-bounded overlap with the targeted eigenstate [3, 19]. Otherwise, the problems are in general QMA-compete [17]. Here, a similar assumption is also made. We introduce an oracle $\mathscr{P}_A$, which given an input μ satisfying $|\mu| \leqslant 1$, outputs a quantum state $|\psi_\mu^{\text{ini}}\rangle$ satisfying $|\langle\psi_\mu^{\text{ini}}|u_0(\mu)\rangle| \geqslant \gamma$. Here, $|u_0(\mu)\rangle$ is the right singular vector of the matrix $A - \mu I$ corresponding to its smallest singular value. $\mathscr{P}_A$ may be constructed quantumly, with methods like variational quantum algorithms [12, 32, 33] or adiabatic state preparation [3]. Alternatively, one may find an approximated model of A whose eigenvalue can be calculated efficiently on a classical computer. We also note that the state preparation assumption can be weaken to be just requiring the nontrivial overlap to the eigenvectors of the target eigenvalues.

Here and after, we assume that $\mathscr{O}_A$, $\mathscr{P}_A$ can be queried efficiently. For simplicity, we also count the query to $\mathscr{O}_A^\dagger$, controlled-$\mathscr{O}_A$ or controlled-$\mathscr{O}_A^\dagger$ as a single query to $\mathscr{O}_A$, and similar for $\mathscr{P}_A$. This is reasonable because unitaries $\mathscr{O}_A$ and $\mathscr{P}_A$ are typically constructed with elementary single- and two-qubit gates. Taking inverse and controlled operations only introduce constant gate overhead.

For Problem 1, we have the following result.

Theorem 1 *With success probability at least $1-\delta$ (for any $\delta \in (0,1)$), Problem 1 can be solved with*

$$\tilde{\mathcal{O}}\left(K^3 \varepsilon^{-3m_{\max}+2} \gamma^{-1}\right) \tag{3}$$

uses of the query to $\mathscr{O}_A$, $\mathscr{P}_A$, and extra single- and two-qubit gates.

Here $\tilde{\mathcal{O}}(\cdot)$ omits the polylogarithmic dependence on $1/\delta$, $1/\varepsilon$, K, and N. We also clarify that for n-qubit systems,

the extra single- and two-qubit gate number contains a dependency $O(n)$, which is neglected by $\tilde{O}$.

When $m_{\max} = 1$, i.e. A is diagonalizable, the complexity reduces to $\tilde{\mathcal{O}}\left(K^3\varepsilon^{-1}\gamma^{-1}\right)$, achieving a nearly-optimal dependency on ε, i.e., the Heisenberg limit. Furthermore, the dependency on K can be reduced to $\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1})$ if eigenvalues are promised to be real. We achieve the following result for Problems 2 and 3.

Theorem 2 *Given $g \geqslant \varepsilon$, with success probability at least $1-\delta$ (for any $\delta \in (0,1)$), Problem 2 and 3 can be solved with*

$$\tilde{O}(K^3\varepsilon^{-3m_{max}+1}\gamma^{-1}) \tag{4}$$

queries to $\mathscr{O}_A$, $\mathscr{P}_A$, and extra single- and two-qubit gates.

For diagonalizable matrices, the accuracy dependency is $\tilde{O}(\varepsilon^{-2})$. It is open whether the above theorem is optimal or not. Besides, if more restrictions exist on the eigenvalue distribution, the query complexity may be further reduced. For example, if we are promised that the eigenvalues are real, the complexity can be reduced to $\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1})$, achieving the nearly Heisenberg scaling again. We note that the Heisenberg scaling is also achieved in [30] with an independent method. Yet, methods in Ref [30] work only for matrices with real eigenvalues, while our algorithms are applicable for general complex eigenvalue spectrums.

Below, we briefly introduce the main idea of our algorithms achieving Theorem 1 and 2. Our algorithm is based on the following key observation.

$$\sigma_0(A-\mu I) = 0 \text{ if and only if } \mu \text{ is an eigenvalue.}$$

where $\sigma_0(\cdot)$ is the minimum singular value of a matrix. Specifically, eigenvalue problems can be transferred to the problem of searching for μ, such that $A-\mu I$ has zero singular values. In practice, however, we can only estimate the singular value up to a certain accuracy. We define a cost function $C(\mu) \equiv \sigma_0(A-\mu I)$. The distance from μ to an eigenvalue can be bounded by $C(\mu)$ in the following lemma.

Lemma 3 *When A is diagonalizable, we have $C(\mu) \leqslant \min_{\lambda_j}|\mu-\lambda_j| \leqslant KC(\mu)$. When A is defective, we have $C(\mu) \leqslant \min_{\lambda_j}|\mu-\lambda_j| \leqslant 3(KC(\mu))^{1/m_{\max}}$.*

It indicates that for diagonalizable matrix, it suffices to find μ satisfying $C(\mu) \leqslant \varepsilon K^{-1}$ to achieve accuracy $\min_{\lambda_j}|\mu-\lambda_j| \leqslant \varepsilon$, and similar for defective matrices.

The remaining task is to search for a μ with sufficiently small $C(\mu)$. Our searching method is based on a subroutine called the singular value threshold subroutine (SVTS) which output True (False) when $C(\mu)$ is smaller (larger) than a given value. We then develop different divide-and-conquer methods for eigenvalue searching for different problems, and achieve scaling claimed in Theorem 1, 2.

Now we discuss the applications of our results in three different subjects.

Liouvillian gap for open quantum systems. in open quantum system, Liouvillian gap (LG) is an important quantity charactering the decaying behaviour and phase transitions of open quantum systems [4, 24, 25, 29, 34, 37]. It is defined as the gap between the largest and second largest real part of the eigenvalues of a vectorized Liouvillian super operators. LG corresponds to a line gap problem with $L = \{ib, b \in \mathbb{R}\}$ and hence efficiently solvable based on Theorem 2, provided nontrivial initial state.

Witness of simultaneous PT-symmetry breaking. In non-Hermitian physics, whether a PT-symmetric matrix is simultaneously broken (unbroken) is determined by whether it has (does not have) complex eigenvalues. Our algorithm with mild modification, can be used to determine if there are complex eigenvalue or not, and hence serves as a quantum witness of the simultaneous PT-symmetry breaking. This can be a powerful tool for studying the many-body non-Hermitian physics and potentially provide exponential quantum speedup.

Relaxation time of Markov chains. The spectral gap of a stochastic matrix A, $g_{\mathrm{mar}} \equiv 1-\max_{\lambda_j \neq 1}|\lambda_j|$, determines the relaxation time $t_{\mathrm{rel}} \equiv 1/g_{\mathrm{mar}}$. It determines the time converging to the stationary distribution [18]. We can estimate the absolute spectral gap and hence the relaxation time. For example, if we assume that $\|A\| \leqslant 1$, and $m_{\max} = 1$ (i.e. diagonalizable), g_{mar} can then be estimated to accuracy ε with $O(K^3\varepsilon^{-2}\gamma^{-1})$ queries to $\mathscr{O}_A$, $\mathscr{P}_A$ and extra single- and two-qubit gates.

Quantum advantages. The exponential quantum advantage of Problem. 2, 3 can be obtained straightforwardly, because they covers all instances of the eigenvalue problems for *Hermitian* matrix. Combining Theorem. 2 (i.e. BQP) with Theorem 1.2 in [13] for BQP-hardness of Hermitian ground state problems, the decision version of Problem. 2, 3 are BQP-complete when $\varepsilon = \Omega(1/\mathrm{poly}(n))$ and nontrivial initial state exists.

We also study the BQP-completeness of LG and PT-symmetry breaking withness problems. These problems are more complicated, because they are special cases of eigenvalue problems. Our strategy contains two steps of mapping. Take the LG problem as an example, the first step is to map a polynomial-size quantum circuit to a guided ground state problems of $O(1)$-local Hamiltonian H. This can be achieved using the construction in [13], which adds the effect of guiding state to the Kitaev's construction of proofing QMA-completeness [17]. The second step is to map whether ground energy property of H to the property of a specific LG problem. Such a LG problem can be solved efficiently using our quantum algorithms, and hence BQP-complete. Because BQP$\neq$ BPP unless universal quantum computer can be efficiently simulated classically, our result can be summarized as follows.

Theorem 4 *There exist instances of Liouvillian gap and PT-symmetry breaking withness problems, such that quantum algorithm can provide exponential quantum speedup, unless universal quantum computer can be efficiently simulated classically.*

References

[1] For short, $\tilde{O}(\cdot)$ runtime refers to $\tilde{O}(\cdot)$ queries to $\mathscr{O}_A$, $\mathscr{P}_A$, and extra single- and two-qubit gates.

[2] See Supplemental Material which contains necessary details for understanding results in the main text.

[3] Tameem Albash and Daniel A Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, 2018.

[4] Leonardo Banchi, Daniel Burgarth, and Michael J Kastoryano. Driven quantum dynamics: Will it blend? *Physical Review X*, 7(4):041015, 2017.

[5] Carl M Bender and Stefan Boettcher. Real spectra in non-hermitian hamiltonians having p t symmetry. *Physical review letters*, 80(24):5243, 1998.

[6] Carl M Bender, Stefan Boettcher, and Peter N Meisinger. Pt-symmetric quantum mechanics. *Journal of Mathematical Physics*, 40(5):2201–2229, 1999.

[7] Emil J Bergholtz, Jan Carl Budich, and Flore K Kunst. Exceptional topology of non-hermitian systems. *Reviews of Modern Physics*, 93(1):015005, 2021.

[8] Dan S Borgnia, Alex Jura Kruchkov, and Robert-Jan Slager. Non-hermitian boundary modes and topology. *Physical review letters*, 124(5):056802, 2020.

[9] Shantanav Chakraborty, András Gilyén, and Stacey Jeffery. The power of block-encoded matrix powers: Improved regression techniques via faster hamiltonian simulation. *Leibniz international proceedings in informatics*, 132, 2019.

[10] Eric Delabaere and Duc Tai Trinh. Spectral analysis of the complex cubic oscillator. *Journal of Physics A: Mathematical and General*, 33(48):8771, 2000.

[11] 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. *PRX Quantum*, 3(4):040305, 2022.

[12] Suguru Endo, Jinzhao Sun, Ying Li, Simon C Benjamin, and Xiao Yuan. Variational quantum simulation of general processes. *Physical Review Letters*, 125(1):010501, 2020.

[13] Sevag Gharibian and François 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 Symposium on Theory of Computing*, pages 19–32, 2022.

[14] 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.

[15] Kohei Kawabata, Ken Shiozaki, Masahito Ueda, and Masatoshi Sato. Symmetry and topology in non-hermitian physics. *Physical Review X*, 9(4):041015, 2019.

[16] Avinash Khare and Bhabani Prasad Mandal. A pt-invariant potential with complex qes eigenvalues. *Physics Letters A*, 272(1-2):53–56, 2000.

[17] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*. Number 47. American Mathematical Soc., 2002.

[18] David A Levin and Yuval Peres. *Markov chains and mixing times*, volume 107. American Mathematical Soc., 2017.

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

[20] Stefano Longhi. Topological phase transition in non-hermitian quasicrystals. *Physical review letters*, 122 (23):237601, 2019.

[21] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019.

[22] Guang Hao Low and Yuan Su. Quantum eigenvalue processing. *arXiv:2401.06240*, 2024.

[23] John M Martyn, Zane M Rossi, Andrew K Tan, and Isaac L Chuang. Grand unification of quantum algorithms. *PRX Quantum*, 2(4):040203, 2021.

[24] Mariya V Medvedyeva, Fabian HL Essler, and Tomaž Prosen. Exact bethe ansatz spectrum of a tight-binding chain with dephasing noise. *Physical review letters*, 117(13):137202, 2016.

[25] Takashi Mori and Tatsuhiko Shirai. Resolving a discrepancy between liouvillian gap and relaxation time in boundary-dissipated quantum many-body systems. *Physical Review Letters*, 125(23):230604, 2020.

[26] Ali Mostafazadeh. Pseudo-hermiticity versus pt symmetry: the necessary condition for the reality of the spectrum of a non-hermitian hamiltonian. *Journal of Mathematical Physics*, 43(1):205–214, 2002.

[27] Nobuyuki Okuma and Masatoshi Sato. Topological phase transition driven by infinitesimal instability: Majorana fermions in non-hermitian spintronics. *Physical review letters*, 123(9):097701, 2019.

[28] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Alán Aspuru-Guzik, and Jeremy L O?brien. A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5(1):4213, 2014.

[29] Daniel A Rowlands and Austen Lamacraft. Noisy spins and the richardson-gaudin model. *Physical review letters*, 120(9):090401, 2018.

[30] Changpeng Shao. Computing eigenvalues of matrices in a quantum computer. *arXiv preprint arXiv:1912.08015*, 2019.

[31] Sebastian Weidemann, Mark Kremer, Stefano Longhi, and Alexander Szameit. Topological triple phase transition in non-hermitian floquet quasicrystals. *Nature*, 601(7893):354–359, 2022.

[32] Xu-Dan Xie, Zheng-Yuan Xue, and Dan-Bo Zhang. Variational quantum eigensolvers for the non-hermitian systems by variance minimization. *arXiv:2305.19807*, 2023.

[33] Nobuyuki Yoshioka, Yuya O Nakagawa, Kosuke Mitarai, and Keisuke Fujii. Variational quantum algorithm for nonequilibrium steady states. *Physical Review Research*, 2(4):043289, 2020.

[34] Dong Yuan, He-Ran Wang, Zhong Wang, and Dong-Ling Deng. Solving the liouvillian gap with artificial neural networks. *Physical Review Letters*, 126(16): 160401, 2021.

[35] Xiao-Ming Zhang and Xiao Yuan. On circuit complexity of quantum access models for encoding classical data. *arXiv:2311.11365*, 2023.

[36] Xiujuan Zhang, Tian Zhang, Ming-Hui Lu, and Yan-Feng Chen. A review on non-hermitian skin effect. *Advances in Physics: X*, 7(1):2109431, 2022.

[37] Bozhen Zhou, Xueliang Wang, and Shu Chen. Exponential size scaling of the liouvillian gap in boundary-dissipated systems with anderson localization. *Physical Review B*, 106(6):064203, 2022.

Quantum Eigensolver for General Matrices

Xiao-Ming Zhang,[1,2] Yukun Zhang,[2] Wenhao He,[3,4] and Xiao Yuan[2,*]

[1]School of Physics, South China Normal University, Guangzhou 510006, China
[2]Center on Frontiers of Computing Studies, School of Computer Science, Peking University, Beijing 100871, China
[3]Center for Computational Science and Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
[4]School of Physics, Peking University, Beijing 100871, China

The eigenvalue problem, a cornerstone in linear algebra, has profound significance in modern science for its wide applications in mathematics, physics, and information science. Quantum algorithms addressing this problem have hitherto been constrained to special normal matrices that admit spectral decomposition, leaving the extension to general matrices an open challenge. In this work, we present a family of quantum algorithms tailored for solving the eigenvalue problem for general matrices, encompassing scenarios with complex eigenvalues or even defective matrices. Our algorithms work for finding eigenvalues without additional constraints, or identifying eigenvalues that are closest to a specified point or line, extending the results for ground energy and energy gap problems for Hermitian matrices. Our results find applications in diverse domains, including estimating the relaxation time of Markov chains, solving Liouvillian gaps in open quantum systems, and verifying PT-symmetry broken/unbroken phases. Moreover, by proving the BQP-completeness of the generalized Liouvillian gap problems, we show that our quantum algorithm has in general an exponential speedup over classical methods. These results underscore the significance of our quantum eigensolvers for problems across various disciplines.

Eigensystem, a fundamental concept in linear algebra, represents key features of a matrix transformation. Formally, complex value λ_j and normalized vector $|v_j\rangle$ are called the eigenvalue and the corresponding eigenvector of a matrix A if

$$A|v_j\rangle = \lambda_j|v_j\rangle. \tag{1}$$

Eigensystem plays a central role in basically all fields of modern science and engineering. Nevertheless, for classical algorithms tackling Eq. (1), i.e. classical eigensolvers, the cost generally grows formidably high for large matrices, which would be inefficient for tackling large data or complex systems.

A potential solution is to make use of quantum computers to construct more efficient quantum eigensolvers. Many quantum algorithms have been proposed for such a purpose based on different techniques [1–3]. Yet, since quantum computing naturally favours Hermiticity, existing quantum algorithms have been mostly restricted to the special and simplified case of Hermitian matrices $A = A^\dagger$, where λ_j are real and $|v_j\rangle$ forms an orthonormal basis. For a general matrix, we could encounter complex and even defective eigenvalues and unorthogonal eigenvectors. Although there are variational quantum algorithms attempting to solve relative problems, their efficiency are not guaranteed. The advantage of quantum computing in solving the general non-Hermitian eigenvalue problems remains an outstanding question.

Here, we propose a family of efficient quantum eigensolver algorithms for general matrices. The algorithm is promised to have polylogarithmic runtime with respect to the matrix dimension, under the block-encoding and nontrivial initial state assumptions. These two assumptions are also standard treatment for Hermitian eigensystem problems [2, 3]. For diagonalizable matrix, the complexity of obtaining an arbitrary eigenvalue is $\tilde{O}(K^3\varepsilon^{-1}\gamma^{-1})$, and the complexity for the obtaining the eigenvalue closest to a reference point or line is $\tilde{O}(K^3\varepsilon^{-2}\gamma^{-1})$, where K, ε and γ are the Jordan condition number, accuracy and overlap between initial state and target state. The latter can be considered as the generalizations of ground energy and energy gap problems, and we show that their decision version are BQP-complete. In other words, existence of exponential quantum advantage is highly likely. Our algorithm also works for defective matrix with higher complexity, but but is still efficient. The algorithm is based on three techniques: the relationship between eigenvalues of matrix A and the minimum singular value of $A - \mu I$, quantum singular value threshold subroutine extended from quantum singular-value estimation, and problem-specific searching algorithms.

Our quantum eigensolver for general matrices would have profound applications in various modern tasks. A typical example is for open quantum systems, in which many novel phenomenon emerges, such as $\mathcal{PT}$-symmetry breaking [4–8], skin effects [9] and non-hermiticity driven topological phase transition [10–12]. While current studies on related topics has been restricted to few-body or analytically solvable cases, our algorithm can potentially provide exponential quantum speedup for general many-body open quantum systems. We provide examples on two of the most pivotal problems in non-Hermitian physics: Liouvillian gap estimation and the witness of spontaneous symmetry breaking. Besides, in the field of stochastic process, our algorithm could also be applied to estimate the relaxation time of Markov chain, a problem whose quantum advantages are unknown.

Eigenvalue Problems. In the main text, we focus on the eigenvalue problems. The eigenvector is closely related to the eigenvalue, and will be discussed in details in Sec. VI of [13].

One can perform Jordan decomposition of a general square matrix A as

$$A = P\Lambda P^{-1}, \tag{2}$$

where Λ is a matrix in the Jordan canonical form (JCF), whose

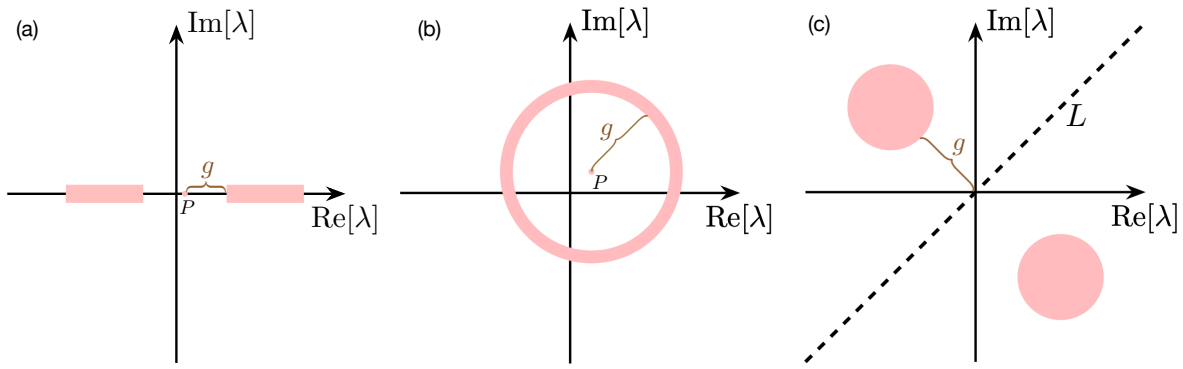


FIG. 1: Sketch of (a) the energy gap for Hermitian matrices with reference point $P = 0$, (b) the point gap for non-Hermitian matrices with reference point $P = 0$, and (c) the line gap for non-Hermitian matrices with reference line $L = \{ib, b \in \mathbb{R}\}$.

diagonal elements correspond to the eigenvalues, and P is an invertible matrix. A is called *diagonalizable* if Λ is diagonal. Most generally, Λ is a block-diagonal matrix *as close to a diagonal matrix as possible* $\Lambda = \Lambda_1 \oplus \Lambda_2 \oplus \cdots \oplus \Lambda_M$ with $M \leqslant N$. Each Jordan block Λ_j is in the form of

$$\Lambda_j = \begin{pmatrix} \lambda_j & 1 & & \\ & \lambda_j & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_j \end{pmatrix}. \tag{3}$$

In case $M < N$, we call A a *defective* matrix. It is worth noting that eigenvalues are fundamentally different from singular values unless the matrix is normal with spectral decomposition. Therefore, the eigenvalue problem does not trivially fit into the framework of quantum singular value transformation [14, 15].

We define $m'_{\max} \equiv \max_j \dim(\Lambda_j)$ as the largest dimension of Jordan blocks, and κ_P as the condition number of matrix P. κ_P can also be named as the Jordan condition number of A [16]. Regarding the nonuniqueness of Eq. (2), we define κ_P as the minimum value for all possible P. It turns out that the difficulty of the problem depends on both $m'_{\max}$ and κ_P. We are promised that two quantities above are upper bounded by $m_{\max} \geqslant m'_{\max}$ and $K \geqslant \kappa_P$ for some known $m_{\max}$ and K.

We first summarize the detailed definitions of the eigenvalue problems. The first problem we consider is to output an estimation of an eigenvalue defined as follows.

Problem 1. *Given a square matrix A with $\|A\| \leqslant 1$ and accuracy $\varepsilon \in (0, 1)$. The goal is to output the eigenvalue estimation λ', such that $\min_{\lambda_j} |\lambda' - \lambda_j| \leqslant \varepsilon$, where λ_j are eigenvalue solutions to Eq. (1).*

Here, $\|\cdot\|$ refers to the spectral norm of a matrix. Problem 1 has no restrictions on the eigenvalue. We may require that the eigenvalue to be estimated have certain properties. Take the Hermitian matrix as an example, there are two important questions related to eigenvalues. The first one is the lowest eigenvalue problem. For a quantum many-body system described by a Hermitian Hamiltonian, this corresponds to the ground-state energy of the system [1–3]. The second one is the eigenvalue gap problem, which plays a critical role in many-body physics phenomena, such as conductivity and superconductivity. Extending from Hermitian to non-Hermitian matrices with complex eigenvalues, the generalization of both questions are not unique [17, 18], which correspond to the eigenvalue searching problems under different restrictions. In particular, we consider the following two problems.

Problem 2. *Given a square matrix A satisfying $\|A\| \leqslant 1$, a reference point $P \in \mathcal{D}(0, 1)$ and accuracy $\varepsilon \in (0, 1)$. Let $g \equiv \min_{\lambda_j \neq P} |\lambda_j - P|$, $\mathcal{S} \equiv \{\lambda_j \big| |\lambda_j - P| \in [g, g + \varepsilon]\}$. The goal is to output gap estimation g' and eigenvalue estimation λ', such that $|g' - g| \leqslant \varepsilon$ and $|\lambda' - \lambda_j| \leqslant \varepsilon$ for some $\lambda_j \in \mathcal{S}$.*

Problem 3. *Given a square matrix A satisfying $\|A\| \leqslant 1$, a reference line L in the complex plain such that $L \bigcup \mathcal{D}(0, 1) \neq \varnothing$, and accuracy $\varepsilon \in (0, 1)$. Let $g = \min_{\lambda_j \notin L, p \in L} |\lambda_j - p|$, $\mathcal{S} \equiv \{\lambda_j \big| \min_{p \in L} |\lambda_j - p| \in [g, g + \varepsilon]\}$. The goal is to output the gap estimation g' and eigenvalue estimation λ', such that $|g' - g| \leqslant \varepsilon$ and $|\lambda' - \lambda_j| \leqslant \varepsilon$ for some $\lambda_j \in \mathcal{S}$.*

Here, we have defined the disk as $\mathcal{D}(\mu, r) \equiv \{x \big| |x - \mu| \leqslant r\}$. In case P or L have no overlap with eigenvalues, Problem 2 or 3 corresponds to finding an eigenvalue that is closest to the reference point P, or line L (up to an accuracy ε). Therefore, they can be considered as two different ways of the generalization of the ground energy problem for Hermitian matrices. On the other hand, when P or L overlaps with at least one of the eigenvalues, Problems 2 and 3 become *Point gap*, or *Line gap* problems [17–19]. As illustrated in Fig. 1, they can be considered as two different ways of the generalizations from the energy gap problem for Hermitian case. In some cases, both point gaps and line gaps are non-vanishing. But there exists matrices with non-vanishing point gap, but zero line gap. Physics systems with Hamiltonian corresponding these two cases may emerge from different symmetries and topologies [17–19].

Furthermore, we note that an accurate approximation to the eigenvector quantum state can be obtained based on an accurate estimation of eigenvalue as will be discussed in Sec. VI of [13].

Results. Here, we introduce our results for the three eigenvalue problems. We only summarize the results in the main text and refer to [13] for details.

We first discuss the assumptions of the algorithms. Given a general square matrix $A \in \mathbb{C}^{N\times N}$ with $N = 2^n$, we consider its block encoding that provides unitary access to the matrix. For a unitary $\mathcal{O}_A$, we say it is a block encoding of A if it encodes the desirable matrix A such that $A = (\langle 0^a| \otimes I)\, \mathcal{O}_A\, (|0^a\rangle \otimes I)$, with I the N-dimensional identity. Note that we have neglected a scaling factor compared to the conventional definition as it can be absorbed in matrix A. Block-encoding is a standard way of encoding the classical description of a matrix to quantum operations [14, 15, 20–22]. In practice, $\mathcal{O}_A$ may be constructed by sparse-access input model or linear combination of unitaries (LCU) [20], depending on the form of A being presented.

For Hermitian matrices, the eigenvalue problem is typically solved by assuming the existence of an initial state that can be prepared to have a reasonable lower-bounded overlap with the targeted eigenstate [2, 3]. Otherwise, the problems are in general QMA-compete [23]. Here, a similar assumption is also made. We introduce an oracle $\mathcal{P}_A$, which given an input μ satisfying $|\mu| \leqslant 1$, outputs a quantum state $|\psi_\mu^{\text{ini}}\rangle$ satisfying $|\langle\psi_\mu^{\text{ini}}|u_0(\mu)\rangle| \geqslant \gamma$. Here, $|u_0(\mu)\rangle$ is the right singular vector of the matrix $A - \mu I$ corresponding to its smallest singular value. $\mathcal{P}_A$ may be constructed quantumly, with methods like variational quantum algorithms [24–26] or adiabatic state preparation [2]. Alternatively, one may find an approximated model of A whose eigenvalue can be calculated efficiently on a classical computer. We also note that the state preparation assumption can be weaken to be just requiring the nontrivial overlap to the eigenvectors of the target eigenvalues, at the cost of a worse scaling with γ (see [13]).

Here and after, we assume that $\mathcal{O}_A$, $\mathcal{P}_A$ can be queried efficiently. For simplicity, we also count the query to $\mathcal{O}_A^\dagger$, controlled-$\mathcal{O}_A$ or controlled-$\mathcal{O}_A^\dagger$ as a single query to $\mathcal{O}_A$, and similar for $\mathcal{P}_A$. This is reasonable because unitaries $\mathcal{O}_A$ and $\mathcal{P}_A$ are typically constructed with elementary single- and two-qubit gates. Taking inverse and controlled operations only introduce constant gate overhead.

For Problem 1, we have the following result.

Theorem 1. *With success probability at least* $1-\delta$*, Problem 1 can be solved with*

$$\tilde{O}\left(K^3\varepsilon^{-3m_{\max}+2}\gamma^{-1}\right) \tag{4}$$

uses of the query to $\mathcal{O}_A$*,* $\mathcal{P}_A$*, and extra single- and two-qubit gates.*

Here $\tilde{O}(\cdot)$ omits the polylogarithmic dependence on $1/\delta$, $1/\varepsilon$, K, and N. We also clarify that for qubit systems, the extra single- and two-qubit gate number contains a dependency of qubit number $O(n)$, which is neglected by $\tilde{O}$.

When $m_{\max} = 1$, i.e. A is diagonalizable, Eq. (S-47) reduces to $\tilde{O}\left(K^3\varepsilon^{-1}\gamma^{-1}\right)$, achieving a nearly-optimal dependency on ε, which is also called the Heisenberg scaling. Besides, the dependency on K can be reduced to $\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1})$ if eigenvalues are promised to be real (see Sec. V A of [13]).

We achieve the following result for Problems 2 and 3.

Theorem 2. *Promised that* $g \geqslant \varepsilon$*. With success probability at least* $1-\delta$*, Problem 2 and 3 can be solved with*

$$\tilde{O}(K^3\varepsilon^{-3m_{max}+1}\gamma^{-1}) \tag{5}$$

queries to $\mathcal{O}_A$*,* $\mathcal{P}_A$*, and extra single- and two-qubit gates.*

For diagonalizable matrix, the accuracy dependency is $\tilde{O}(\varepsilon^{-2})$. It is open whether the above theorem is optimal or not. The complication is that different from Problem 1, we should exclude the possibility for eigenvalues with a gap smaller than g. Besides, if more restrictions exist on the eigenvalue distribution, the query complexity may be further reduced. For example, if we are promised that the eigenvalues are real, the complexity can be reduced to $\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1})$, achieving the nearly Heisenberg scaling (see Sec. V B of [13]). We note that the Heisenberg scaling is also achieved in [27] with an independent method. Yet, methods in Ref [27] works only for matrices with real eigenvalues, while our algorithms are applicable for general complex eigenvalue spectrums.

Below, we briefly introduce the main idea of our algorithms achieving Theorem 1 and 2 and refer to Sec. II, III of [13] for details. To begin with, we consider an equivalent form of Eq. (1) as

$$(A - \lambda_j I)|v_j\rangle = 0. \tag{6}$$

Our algorithm is based on the following key observation.

$\sigma_0(A-\mu I) = 0$ *if and only if* μ *is the solution to Eq. (6),*

where $\sigma_0(\cdot)$ is the minimum singular value of a matrix. Specifically, eigenvalue problems can be transferred to the problem of searching for μ, such that $A - \mu I$ has zero singular values. In practice, however, we can only estimate the singular value up to a certain accuracy. We define a cost function

$$C(\mu) \equiv \sigma_0(A - \mu I). \tag{7}$$

The distance from μ to an eigenvalue can be bounded by $C(\mu)$ in the following lemma (see Sec. I A of [13]).

Lemma 1. *When* A *is diagonalizable, we have* $C(\mu) \leqslant \min_{\lambda_j}|\mu-\lambda_j| \leqslant KC(\mu)$*. When* A *is defective, we have* $C(\mu) \leqslant \min_{\lambda_j}|\mu-\lambda_j| \leqslant 3(KC(\mu))^{1/m_{\max}}$.

Lemma. 1 indicates that for diagonalizable matrix, it suffices to find μ satisfying $C(\mu) \leqslant \varepsilon K^{-1}$ to achieve accuracy $\min_{\lambda_j}|\mu-\lambda_j| \leqslant \varepsilon$, and similar for defective matrices.

To solve Problem 1, the remaining task is to search for a μ with sufficiently small $C(\mu)$. Our searching method is based on a subroutine called the singular value threshold subroutine (SVTS), denoted as $O_C(\mu, \tilde{\varepsilon}, \delta)$. The inputs of SVTS are

center $\mu \in \mathcal{D}(0,1)$, threshold $\tilde{\varepsilon}$, and success probability $\delta \in (0,1)$ respectively. Informally speaking, the output of SVTS satisfies the following

$$\Pr\left[O_C(\mu,\tilde{\varepsilon},\delta) = \text{True} \middle| C(\mu) \leqslant \tilde{\varepsilon}/2\right] \geqslant 1-\delta \tag{8}$$

$$\Pr\left[O_C(\mu,\tilde{\varepsilon},\delta) = \text{False} \middle| C(\mu) \geqslant \tilde{\varepsilon}\right] \geqslant 1-\delta, \tag{9}$$

provided initial state with nontrivial overlap to the target eigenvectors. In Sec. I of [13], we show that SVTS can be constructed using quantum singular value transformation [14] with $\tilde{O}\left(\tilde{\varepsilon}^{-1}\gamma^{-1}\right)$ complexity [28]. We then develop a divide-and-conquer method for eigenvalue searching, which uses only $O(\text{polylog}(\varepsilon^{-1}))$ queries to SVTS, and achieve scaling claimed in Theorem 1.

Problem 2 and 3 are more challenging because we should output eigenvalues as close to the reference point (line) as possible. Take Problem 2 as an example, our strategy is as follows. Suppose we are promised that $g \in [R^{\min}, R^{\max}]$, and we define $\Delta = R^{\max} - R^{\min}$. We query a set of SVTSs with centers around

the complication is that to claim g' is a good estimation of g with accuracy ε, we should ensure that there is no eigenvalue in the region $\mathcal{D}(P, g'-\varepsilon)/\mathcal{D}(P,\varepsilon)$. Our iterative strategy is as follows. Suppose at the jth step, we are confidence that $g \in [R_j^{\min}, R_j^{\max}]$. Let $\Delta_j = R_j^{\max} - R_j^{\min}$, we reduce Δ_j by querying a set of SVTSs. The process is terminated until $\Delta_j \leqslant \varepsilon$. After that, we search for an eigenvalue near the circle with radius g'.

Now we discuss the applications of our results in different problems.

Liouvillian gap for open quantum systems. The Liouvillian gap (LG) is an important quantity characterizing the decaying behaviour and phase transitions of open quantum systems [29–34]. The dynamics of an open quantum system can be described by the Lindblad master equation $\dot{\rho} = \mathcal{L}(\rho)$, where $\mathcal{L}$ is a linear superoperator. One can perform vectorization on the master equation, which becomes $\dot{\tilde{\rho}} = \tilde{\mathcal{L}} \cdot \tilde{\rho}$, where $\tilde{\rho} = \sum_{m,n} \rho_{mn} |m\rangle \otimes |n\rangle$ and $\tilde{\mathcal{L}}$ is typically a non-Hermitian matrix. Let $\lambda_j(\tilde{\mathcal{L}})$ be the eigenvalues of $\tilde{\mathcal{L}}$ ordered according to the magnitude of the real part, i.e. $\text{Re}\lambda_0(\tilde{\mathcal{L}}) \geqslant \text{Re}\lambda_1(\tilde{\mathcal{L}}) \geqslant \cdots$. LG is formally defined as

$$g_{\text{L}} \equiv |\text{Re}\lambda_1(\tilde{\mathcal{L}})|. \tag{10}$$

g_{L} has a close relation to the relaxation behaviour of the open quantum system. In most cases, the relaxation time τ of an open quantum system satisfies $\tau \lesssim 1/g_{\text{L}}$ [32].

For many-body systems, analytic solutions to LG only exist for some special cases, while numerical calculation with classical computers suffers from the exponential increase of the Hilbert space. On the other hand, LG can potentially be solved with a quantum computer efficiently based on our quantum eigensolver. Compared to Problem 3, LG is a line gap problem with $L = \{ib, b \in \mathbb{R}\}$. So according to Theorem 2, if $\tilde{\mathcal{L}}$ is diagonalizable and $\|\tilde{\mathcal{L}}\| \leqslant 1$, LG can be efficiently estimated to accuracy ε with $\tilde{O}(K^3\varepsilon^{-2}\gamma^{-1})$ complexity [28].

In most open quantum system models, $\tilde{\mathcal{L}}$ can be decomposed into the linear combination of Pauli strings. So the block encoding of $\tilde{\mathcal{L}}$, up to a rescaling factor, can be efficiently constructed. Moreover, due to the BQP-completeness of the decision version of Problem 3 (i.e. Problem xx in []), our result also indicates that quantum algorithm can potentially provide exponential speedup in the LG problem.

Spontaneous-symmetry-breaking witness. In quantum systems described by non-Hermitian Hamiltonian, the eigenvalue does not necessarily to be complex. A typical example is the parity-time (PT) symmetry systems [4–8]. A matrix is called PT symmetry if it is invariant under simultaneous application of parity-reversal operator $\mathcal{P}$ and time-reversal operator $\mathcal{T}$. The eigenvalues of the PT-symmetry operator can either be real only or appear as complex conjugate pairs. The former possesses PT-symmetry and is therefore categorized as PT-unbroken phase when the matrix is diagonalizable [8, 35]. In the second case, PT-symmetry is spontaneously broken and therefore categorized as the PT-broken phase. The transition between these two phases is of broad interest with applications in quantum sensing [36, 37].

To verify whether the quantum system is in the PT-broken or PT-unbroken phase, it suffices to determine if it contains complex eigenvalues. In practice, we may allow a certain error ε. When all eigenvalues are at most ε distance away from the real axis, the matrix is categorized as PT-unbroken. With a mild modification of the algorithms for solving Problem 3, one can solve this problem with a similar complexity claimed in Theorem 2. For example, when A is promised to be diagonalizable and $\|A\| \leqslant 1$. With success probability $1-\delta$, one can verify whether A has eigenvalues satisfying $\left|\text{Im}[\lambda_j]\right| \geqslant \varepsilon$, or all eigenvalues are in the real axis, with $\tilde{O}(K^3\varepsilon^{-2}\gamma^{-1})$ complexities, and hence characterizing the PT-broken (-unbroken) phase.

Relaxation time of Markov chain. Markov chain has broad applications in both natural and social science [38–42]. Finite Markov chain can be described by non-Hermitian stochastic matrix A, whose largest eigenvalue is 1. Besides, the absolute spectral gap of A is $g_{\text{ag}} \equiv 1 - \max_{\lambda_j \neq 1} |\lambda_j|$, which determines the relaxation time $t_{\text{ag}} \equiv 1/g_{\text{ag}}$. In particular, for irreducible, time-reversible Markov chain, t_{ag} can be used to upper bound the mixing time, i.e. the time converging to the stationary distribution [42]. We note that t_{ag} is a global property, and different from the *hitting time* of a particular site [43].

With a similar strategy to solving Problem 2 and 3, we can estimate the absolute spectral gap and hence the relaxation time. For example, if $\|A\|$ is upper bounded by a constant and $m_{\max} = 1$ (i.e. diagonalizable), g_{ag} can then be estimated to accuracy ε with $O(K^3\varepsilon^{-2}\gamma^{-1})$ complexity [28].

Quantum advantages. The exponential quantum advantage of Problem. 2, 3 can be obtained straightforwardly, because they covers all instances of the eigenvalue problems for *Hermitian* matrix. Combining Theorem. 2 (i.e. BQP) with Theorem 1.2 in [44] for BQP-hardness of Hermitian ground state problems,

the decision version of Problem. 2, 3 are BQP-complete when $\varepsilon = \Omega(1/\mathrm{poly}(n))$ and nontrivial initial state exists.

We also study the BQP-completeness of LG problem. This problem is more complicated, because they are special cases of eigenvalue problems. Our strategy contains two steps of mapping. The first step is to map a polynomial-size quantum circuit to a guided ground state problems of $O(1)$-local Hamiltonian H. This can be achieved using the construction in [44], which adds the effect of guiding state to the Kitaev's construction of proofing QMA-completeness [23]. The second step is to map whether ground energy property of H to the property of a specific LG problem. Such a LG problem can be solved efficiently using our quantum algorithms, and hence BQP-complete. Because BQP$\neq$ BPP unless universal quantum computer can be efficiently simulated classically, our result can be summarized as follows.

Theorem 3. *There exist instances of Liouvillian gap problem, such that quantum algorithm can provide exponential quantum speedup, unless universal quantum computer can be efficiently simulated classically.*

Our strategy can also be used to analysis the quantum advantage of Spontaneous PT-symmetry-breaking witness, and other related problems.

Discussions. We have developed quantum algorithms for solving eigenvalue problems. The idea can also be generalized to the study of the properties related to eigenvectors. Future works include finding more applications in physics, data science, and other related fields.

Acknowledgement. We thank Seth Lloyd, Xiaogang Li and Dong Yuan for their helpful discussions. This work is supported by the National Natural Science Foundation of China (Grant No. 12175003, No. 12361161602, and No. 12247124), NSAF (Grant No. U2330201), and Project funded by China Postdoctoral Science Foundation (Grant No. 2023T160004)

Note-added. Another related work has appeared during the preparation of this work [16]. In Theorem 3 and Theorem 12 of Ref [16], eigenvalue estimation is discussed based on stronger assumptions that initial state with $O(\varepsilon)$ distance to the corresponding eigenvector can be prepared.

* Electronic address: xiaoyuan@pku.edu.cn

[1] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O?brien, A variational eigenvalue solver on a photonic quantum processor, Nature communications **5**, 4213 (2014).
[2] T. Albash and D. A. Lidar, Adiabatic quantum computation, Reviews of Modern Physics **90**, 015002 (2018).
[3] L. Lin and Y. Tong, Near-optimal ground state preparation, Quantum **4**, 372 (2020).
[4] C. M. Bender and S. Boettcher, Real spectra in non-hermitian hamiltonians having p t symmetry, Physical review letters **80**, 5243 (1998).
[5] C. M. Bender, S. Boettcher, and P. N. Meisinger, Pt-symmetric quantum mechanics, Journal of Mathematical Physics **40**, 2201 (1999).
[6] A. Khare and B. P. Mandal, A pt-invariant potential with complex qes eigenvalues, Physics Letters A **272**, 53 (2000).
[7] E. Delabaere and D. T. Trinh, Spectral analysis of the complex cubic oscillator, Journal of Physics A: Mathematical and General **33**, 8771 (2000).
[8] A. Mostafazadeh, Pseudo-hermiticity versus pt symmetry: the necessary condition for the reality of the spectrum of a non-hermitian hamiltonian, Journal of Mathematical Physics **43**, 205 (2002).
[9] X. Zhang, T. Zhang, M.-H. Lu, and Y.-F. Chen, A review on non-hermitian skin effect, Advances in Physics: X **7**, 2109431 (2022).
[10] N. Okuma and M. Sato, Topological phase transition driven by infinitesimal instability: Majorana fermions in non-hermitian spintronics, Physical review letters **123**, 097701 (2019).
[11] S. Longhi, Topological phase transition in non-hermitian quasicrystals, Physical review letters **122**, 237601 (2019).
[12] S. Weidemann, M. Kremer, S. Longhi, and A. Szameit, Topological triple phase transition in non-hermitian floquet quasicrystals, Nature **601**, 354 (2022).
[13] See Supplemental Material which contains necessary details for understanding results in the main text.
[14] 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.
[15] J. M. Martyn, Z. M. Rossi, A. K. Tan, and I. L. Chuang, Grand unification of quantum algorithms, PRX Quantum **2**, 040203 (2021).
[16] G. H. Low and Y. Su, Quantum eigenvalue processing, arXiv:2401.06240 (2024).
[17] K. Kawabata, K. Shiozaki, M. Ueda, and M. Sato, Symmetry and topology in non-hermitian physics, Physical Review X **9**, 041015 (2019).
[18] E. J. Bergholtz, J. C. Budich, and F. K. Kunst, Exceptional topology of non-hermitian systems, Reviews of Modern Physics **93**, 015005 (2021).
[19] D. S. Borgnia, A. J. Kruchkov, and R.-J. Slager, Non-hermitian boundary modes and topology, Physical review letters **124**, 056802 (2020).
[20] G. H. Low and I. L. Chuang, Hamiltonian simulation by qubitization, Quantum **3**, 163 (2019).
[21] S. Chakraborty, A. Gilyén, and S. Jeffery, The power of block-encoded matrix powers: Improved regression techniques via faster hamiltonian simulation, Leibniz international proceedings in informatics **132** (2019).
[22] X.-M. Zhang and X. Yuan, On circuit complexity of quantum access models for encoding classical data, arXiv:2311.11365 (2023).
[23] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and quantum computation*, 47 (American Mathematical Soc., 2002).
[24] S. Endo, J. Sun, Y. Li, S. C. Benjamin, and X. Yuan, Variational quantum simulation of general processes, Physical Review Letters **125**, 010501 (2020).
[25] N. Yoshioka, Y. O. Nakagawa, K. Mitarai, and K. Fujii, Variational quantum algorithm for nonequilibrium steady states, Physical Review Research **2**, 043289 (2020).
[26] X.-D. Xie, Z.-Y. Xue, and D.-B. Zhang, Variational quantum eigensolvers for the non-hermitian systems by variance minimization, arXiv:2305.19807 (2023).

[27] C. Shao, Computing eigenvalues of matrices in a quantum computer, arXiv preprint arXiv:1912.08015 (2019).

[28] For short, $\tilde{O}(\cdot)$ runtime refers to $\tilde{O}(\cdot)$ queries to $\mathcal{O}_A$, $\mathcal{P}_A$, and extra single- and two-qubit gates.

[29] M. V. Medvedyeva, F. H. Essler, and T. Prosen, Exact bethe ansatz spectrum of a tight-binding chain with dephasing noise, Physical review letters **117**, 137202 (2016).

[30] L. Banchi, D. Burgarth, and M. J. Kastoryano, Driven quantum dynamics: Will it blend? Physical Review X **7**, 041015 (2017).

[31] D. A. Rowlands and A. Lamacraft, Noisy spins and the richardson-gaudin model, Physical review letters **120**, 090401 (2018).

[32] T. Mori and T. Shirai, Resolving a discrepancy between liouvillian gap and relaxation time in boundary-dissipated quantum many-body systems, Physical Review Letters **125**, 230604 (2020).

[33] D. Yuan, H.-R. Wang, Z. Wang, and D.-L. Deng, Solving the liouvillian gap with artificial neural networks, Physical Review Letters **126**, 160401 (2021).

[34] B. Zhou, X. Wang, and S. Chen, Exponential size scaling of the liouvillian gap in boundary-dissipated systems with anderson localization, Physical Review B **106**, 064203 (2022).

[35] X. Li, C. Zheng, J. Gao, and G. Long, Dynamics simulation and numerical analysis of arbitrary time-dependent $\mathcal{PT}$-symmetric system based on density operators, (2022).

[36] S. Yu, Y. Meng, J.-S. Tang, X.-Y. Xu, Y.-T. Wang, P. Yin, Z.-J. Ke, W. Liu, Z.-P. Li, Y.-Z. Yang, *et al.*, Experimental investigation of quantum p t-enhanced sensor, Physical Review Letters **125**, 240506 (2020).

[37] J.-H. Park, A. Ndao, W. Cai, L. Hsu, A. Kodigala, T. Lepetit, Y.-H. Lo, and B. Kanté, Symmetry-breaking-induced plasmonic exceptional points and nanoscale sensing, Nature Physics **16**, 462 (2020).

[38] J. R. Norris, *Markov chains*, 2 (Cambridge university press, 1998).

[39] J. Odencrantz, Markov chains: Gibbs fields, monte carlo simulation, and queues, Technometrics **42**, 438 (2000).

[40] O. Ibe, *Markov processes for stochastic modeling* (Newnes, 2013).

[41] S. P. Meyn and R. L. Tweedie, *Markov chains and stochastic stability* (Springer Science & Business Media, 2012).

[42] D. A. Levin and Y. Peres, *Markov chains and mixing times*, Vol. 107 (American Mathematical Soc., 2017).

[43] A. N. Chowdhury and R. D. Somma, Quantum algorithms for gibbs sampling and hitting-time estimation, arXiv:1603.02940 (2016).

[44] 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 Symposium on Theory of Computing* (2022) pp. 19–32.

[45] Y. Dong, L. Lin, and Y. Tong, Ground-state preparation and energy estimation on early fault-tolerant quantum computers via quantum eigenvalue transformation of unitary matrices, PRX Quantum **3**, 040305 (2022).

[46] R. A. Horn and C. R. Johnson, *Topics in matrix analysis* (Cambridge university press, 1994).

[47] W. Kahan, B. Parlett, and E. Jiang, Residual bounds on approximate eigensystems of nonnormal matrices, SIAM Journal on Numerical Analysis **19**, 470 (1982).

[48] J. Erxiong, Bounds for the smallest singular value of a jordan block with an application to eigenvalue perturbation, Linear Algebra and its Applications **197**, 691 (1994).

[49] G. H. Low and I. L. Chuang, Optimal hamiltonian simulation by quantum signal processing, Phys. Rev. Lett. **118**, 010501 (2017).

[50] G. H. Low, T. J. Yoder, and I. L. Chuang, Methodology of resonant equiangular composite quantum gates, Physical Review X **6**, 041067 (2016).

Supplemental material

Contents

I. Singular value threshold subroutine

Our protocol of searching eigenvalue depends on the the SVTS oracle which output "True" when $C(\mu)$ is small (and hence μ is close to an eigenvalue due to Lemma. 1). More specifically, the SVTS is defined as follows.

Definition 1. *Let $\mu \in \mathcal{D}(0,1)$, $\tilde{\varepsilon}$, $\delta \in (0,1)$ be the center, threshold and success probability of the SVTS respectively. Let $C(\mu)$ be the minimum singular value of $A-\mu I$ (cf. Eq. (7)). We define $O_C(\mu,\tilde{\varepsilon},\delta)$ as the output of SVTS, which satisfies the following*

$$Pr\left[O_C(\mu,\tilde{\varepsilon},\delta)=True \middle| C(\mu)\leqslant \tilde{\varepsilon}/2\right]\geqslant 1-\delta, \tag{S-1a}$$

$$Pr\left[O_C(\mu,\tilde{\varepsilon},\delta)=False \middle| C(\mu)\geqslant \tilde{\varepsilon}\right]\geqslant 1-\delta. \tag{S-1b}$$

In this section, we show that the SVTS can be constructed efficiently. Our result is as follows.

Lemma 2 (SVTS)**.** *SVTS satisfying Eq. (S-1) can be constructed with $\tilde{O}\left(\tilde{\varepsilon}^{-1}\gamma^{-1}\right)$ uses of the query to $\mathcal{O}_A$, $\mathcal{P}_A$, and extra single- and two-qubit gates.*

Recall that $\mathcal{O}_A$ is the block encoding of A, i.e. an $(n+a)$ qubit satisfying $(\langle 0^a|\otimes I)\mathcal{O}_A(|0^a\rangle\otimes I)=A$. It is typically required that $a=O(\mathrm{poly}(n))$. $\mathcal{P}_A$ is state preparation unitary satisfying $\mathcal{P}_A|0\rangle^{\otimes n}=|\psi\rangle$, such that $|\langle u_0(\mu)|\psi\rangle|\geqslant\gamma$. Here, $|u_0(\mu)\rangle$ is the right singular vector of $A-\mu I$ corresponding to the minimum singular value. This is in analogy to the ground state for Hermitian matrix.

The aim of Lemma. 2 is to approximately determine where the targeted eigenvalue lies, a task similar to the fuzzy bisection scheme proposed in Ref. [45]. Yet, the main difference between our motivation and Dong *et al.* [45] is that to deal with complex eigenvalues, we take advantage of the relationship between eigendecomposition and singular value decomposition as given by Lemma. 1. That is given the construction of $A-\mu I$, if the shifted value μ is close enough to the targeted eigenvalue λ_j, $C(\mu)$ is then close to zero. Therefore, we can decide whether there is an eigenvalue λ_j that is close to the attempted shift μ by determining the existence of singular value signals close to zero by QSVT techniques [14].

The remaining of this section is organized as follows. In Sec. I A, we proof Lemma. 1. In Sec. I B, for an arbitrary matrix M satisfying $\|M\|\leqslant 1$, we show how to determine whether its minimum singular value is smaller than $\varepsilon/2$ or larger than ε, provided the block encoding of M. In Sec. I C, we show that the block encoding a rescaled matrix, $\tilde{A}=\frac{A-\mu I}{1+|\mu|}$, can be constructed with $O(1)$ querying to $\mathcal{O}_A$. In combination, we complete the proof of Lemma. 2.

A. Proof of Lemma. 1

$C(\mu)\leqslant \min_{\lambda_j}|\mu-\lambda_j|$ follows straightforwardly from Weyl's Theorem [46]. Below, we focus on the upper bound of $\min|\mu-\lambda_j|$. We begin with the diagonalizable matrix. We should proof that $\min_{\lambda_j}|\mu-\lambda_j|\leqslant\kappa_P C(\mu)$. Let $\|\cdot\|=\sigma_{\max}(\cdot)$ be the operator norm. According to definition, the cost function satisfies

$$C(\mu)=0 \qquad \mu=\lambda_j, \tag{S-2}$$

$$C(\mu)=\left\|(M-\mu I)^{-1}\right\|^{-1} \qquad \mu\neq\lambda_j. \tag{S-3}$$

When $\mu=\lambda_j$, Lemma. 1 holds obviously. We now consider the case when $\mu\neq\lambda_j$. Because $PP^{-1}=P^{-1}P=I$, we have

$$M-\mu I=P(\Lambda-\mu I)P^{-1}, \tag{S-4}$$

and

$$(M-\mu I)^{-1}=P(\Lambda-\mu I)^{-1}P^{-1}. \tag{S-5}$$

Therefore,

$$\begin{aligned}\|(M-\mu I)^{-1}\| &= \|P(\Lambda-\mu I)^{-1}P^{-1}\|\\ &\leqslant \|P\|\|(\Lambda-\mu I)^{-1}\|\|P^{-1}\|\\ &\leqslant \|P\|\|P^{-1}\|\|(\Lambda-\mu I)^{-1}\|\end{aligned} \tag{S-6}$$

By definition, we have $\kappa_P \equiv \sigma_{\max}(P)/\sigma_{\min}(P)$, where $\sigma_{\min}(P)$ is the minimum singular value of P. Because $1/\sigma_{\min}(P) = \sigma_{\max}(P^{-1})$, we have

$$\kappa_P = \sigma_{\max}(P)\sigma_{\max}(P^{-1}) = \|P\|\|P^{-1}\|. \tag{S-7}$$

Moreover, we have

$$\|(\Lambda - \mu I)^{-1}\| = \frac{1}{\min|\mu - \lambda_j|}. \tag{S-8}$$

Combining Eq. (S-6), (S-7) and (S-8), we have

$$C(\mu)^{-1} = \frac{\kappa_P}{\min|\mu - \lambda_j|}, \tag{S-9}$$

which is equivalent to Eq. (**??**).

We then consider the defective matrix case. We first consider the Jordan normal form of the matrix $M - \mu I$. It can be expressed as $M - \mu I = P\tilde{\Lambda}P^{-1}$, where $\tilde{\Lambda} \equiv \Lambda - \mu I \equiv \tilde{\Lambda}_1 \oplus \tilde{\Lambda}_2 \oplus \cdots \oplus \tilde{\Lambda}_M$ is a block-diagonal matrix, where each Jordan block is

$$\tilde{\Lambda}_j = \begin{pmatrix} \lambda_j - \mu & 1 & & \\ & \lambda_j - \mu & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_j - \mu \end{pmatrix}. \tag{S-10}$$

According to Eq. (S-3), we have

$$\begin{aligned} C(\mu) =& \left\|(M - \mu I)^{-1}\right\|^{-1} \\ =& \left\|P\mathrm{diag}\left(\tilde{\Lambda}_1^{-1}, \tilde{\Lambda}_2^{-1}, \cdots, \tilde{\Lambda}_N^{-1}\right)P^{-1}\right\|^{-1} \\ \geqslant& \kappa_P^{-1}\left\|\mathrm{diag}\left(\tilde{\Lambda}_1^{-1}, \tilde{\Lambda}_2^{-1}, \cdots, \tilde{\Lambda}_N^{-1}\right)\right\|^{-1} \\ \geqslant& \kappa_P^{-1}\left\|\tilde{\Lambda}_j^{-1}\right\|^{-1} \\ =& \frac{\sigma_{\min}(\tilde{\Lambda}_j)}{\kappa_P}. \end{aligned} \tag{S-11}$$

Note that Eq. (S-11) is applied for arbitrary j. According to Ref.[47] (see also Ref. [48]), let $\delta_j = |\lambda_j - \mu|$, we have

$$\sigma_{\min}(\tilde{\Lambda}_j) \geqslant \frac{\delta_j^{m_j}}{(1+\delta_j)^{m_j - 1}}. \tag{S-12}$$

Because the operator norm of A is bounded by $\|A\| \leqslant 1$, we also have $|\lambda_j| \leqslant 1$ for all eigenvalues. Our searching region is also restricted by $|\mu| \leqslant 1$, so we have $\delta_j \leqslant 2$. We can simplify Eq. (S-12) as

$$\sigma_{\min}(\tilde{\Lambda}_j) \geqslant \left(\frac{\delta_j}{1+\delta_j}\right)^{m_j}(1+\delta_j) \geqslant (\delta_j/3)^{m_j}. \tag{S-13}$$

Combining Eq. (S-11) with Eq. (S-13), we have

$$\kappa_P C(\mu) \geqslant (\delta_j/3)^{m_j}, \tag{S-14}$$

which gives

$$\delta_j \leqslant 3(\kappa_P C(\mu))^{1/m_j}. \tag{S-15}$$

Because $\min_j |\mu - \lambda_j| \leqslant \delta_j$, we have

$$\min_j |\mu - \lambda_j| \leqslant 3(\kappa_P C(\mu))^{1/m_j}. \tag{S-16}$$

When $C(\mu) \leqslant 1/\kappa_P$, we have $\kappa_P C(\mu) \leqslant 1$, and the right hand side of Eq. (S-16) increases monotonically with m_j. So $\min_j |\mu - \lambda_j| \leqslant 3(\kappa_P C(\mu))^{1/m_{\max}}$. When $C(\mu) > 1/\kappa_P$, we have $\kappa_P C(\mu) > 1$, so the right hand side of Eq. (S-16) is larger than 3. Because we always have $\min_j |\mu - \lambda_j| \leqslant 2$, we also have $\min_j |\mu - \lambda_j| \leqslant 3(\kappa_P C(\mu))^{1/m_{\max}}$, and the proof is of Lemma. 1 completed.

B. Singular value filtering

Given a general matrix $M \in \mathbb{C}^{N\times N}$ satisfying $\|M\| \leqslant 1$, we can perform singular value decomposition as follows

$$M = \sum_{j=0}^{N-1} \sigma_j |w_j\rangle\langle u_j| \tag{S-17}$$

for some singular value $0 \leqslant \sigma_0 \leqslant \sigma_1 \cdots$, orthonormal left singular vectors $\{|w_j\rangle\}$ and right singular vectors $\{|u_j\rangle\}$. Let $P(\cdot)$ be a real polynomial function, we define the singular value transformation of a matrix as

$$P^{(\mathrm{svt})}(M) = \begin{cases} P(\sigma_j)|w_j\rangle\langle u_j| & \text{if the degree of } P(\cdot) \text{ is odd} \\ P(\sigma_j)|u_j\rangle\langle u_j| & \text{if the degree of } P(\cdot) \text{ is even} \end{cases} \tag{S-18}$$

According to [14], QSVT can be effectively constructed with $\mathcal{O}_M$ and few extra elementary quantum gates, if $P(\cdot)$ satisfies some reasonable criteria. More specifically, we have the following.

Lemma 3 (QSVT for real polynomials with definite parity, adapted from Theorem 4 in [14])**.** *Let $P \in \mathbb{R}$ be a polynomial function satisfying (1) The degree of P is at most d; (2) P is either of even or odd parity; (3) For $\forall x \in [-1, 1], |P(x)| \leqslant 1$.*

Then there exists a block encoding of $P(M)$ using d queries of $\mathcal{O}_M$ and its inverse, one extra ancillary qubit, and $O(a + 1)d$ extra single- and two-qubit gates.

The next step is thus to approximate a shifted Heaviside function $H(x - \theta)$ with a polynomial function $P_H^{(\mathrm{svt})}(\cdot)$ using QSVT methods. The shifted Heaviside function is given by

$$H(x-\theta) = \begin{cases} 1, & x \leq \theta \\ 0, & x > \theta \end{cases} \tag{S-19}$$

Regarding the approximated block encoding, we say that a unitary U_M is the (α, a, η)-block encoding of $\tilde{A}$ if $\|\alpha(\langle 0^a| \otimes I)U_M(|0^a\rangle \otimes I) - M\| \leqslant \eta$. From [49], we have the following lemma.

Lemma 4. *Let $\Delta, \eta \in (0, 0.5)$. Given a matrix $\tilde{A}$ with its $(1, a, 0)$ block-encoding $\mathcal{O}_{\tilde{A}}$, we can construct a $(1, a + 1, \eta)$-block-encoding of $P_H^{svt}(\tilde{A})$ satisfying $|P_H(x) - 1| \leq \eta$ for $\forall x \in [-1, \Delta/2]$, and $|P_H(x)| \leq \eta$ for $\forall x \in [\Delta, 1]$ using $O\left(\frac{1}{\Delta}\log\left(\frac{1}{\eta}\right)\right)$ applications of $\mathcal{O}_{\tilde{A}}$ and $O\left(\frac{a}{\Delta}\log\left(\frac{1}{\eta}\right)\right)$ extra single- and two-qubit gates.*

Here, we have approximated the Heaviside function with a shift $\theta = 3\Delta/4$. It is worth noting that the function between interval $x \in [\Delta/2, \Delta]$ often takes values that smoothly interpolate the function value of the two endpoints of the interval. See Sec. V of Ref. [45] for an example. For simplicity, we will denote the $(1, a + 1, \eta)$-block encoding unitary of $P_H^{\mathrm{svt}}(M)$ as U_H.

For the sake of generality, we consider a slightly weaker state preparation assumption than the one used in Lemma. 2. We define $\mathscr{P}_M^{(\Delta)}$ as a state preparation unitary satisfying the following: Let $\mathscr{P}_M|0^n\rangle = |\psi\rangle$ with $\sum_j c_j|u_j\rangle$, if M has at least one singular value satisfying $\sigma_j \leqslant \varepsilon/2$, then $\|\Pi_{\Delta/2}|\psi\rangle\| \geqslant \gamma$, where $\Pi_{\Delta/2} = \sum_{j\in\{j'|\sigma_{j'}\leqslant\varepsilon/2\}} |u_j\rangle\langle u_j|$. In other words, $|\psi\rangle$ has nontrivial overlap to the subspace spanned by singular vectors, whose small singular values are small, if any. This weaker assumption is useful for solving Problem. 7 which is useful for the discussion of BQP-completeness.

Applying U_H to the join state of ancillary qubits at state $|+\rangle|0^{a+1}\rangle$ and data qubit at state $|\psi\rangle$, we obtain

$$U_H|+\rangle|0^{a+1}\rangle|\psi\rangle = |+\rangle|0^{a+1}\rangle \sum_j c_j P_H(\sigma_j)|u_j\rangle + |\text{garb}\rangle \tag{S-20}$$

for some $|c_0| \geqslant \gamma$, and

$$(\langle+|\langle 0^{a+1}| \otimes I)|\text{garb}\rangle = 0. \tag{S-21}$$

If we project the ancillary qubits to $|+\rangle|0^{a+1}\rangle$, the success probability of the projection is given by

$$p_{\text{suss}} \equiv \left\|(\langle+|\langle 0^{a+1}| \otimes I)U_H|+\rangle|0^{a+1}\rangle|\psi\rangle\right\| \tag{S-22}$$

$$= \sum_j |c_j|^2 |P_H(\sigma_j)|^2. \tag{S-23}$$

If the smallest singular value of A satisfies $\sigma_0 \leqslant \Delta/2$, we have

$$p_{\text{suss}} \geqslant |c_0|^2 |P_H(\sigma_0)|^2 \geqslant |c_0|^2 (1-\eta)^2 \geqslant \gamma/4. \tag{S-24}$$

If $\sigma_0(A) \geqslant \Delta$, we have

$$p_{\text{suss}} \leqslant \eta^2. \tag{S-25}$$

We note that η decays rapidly with order d for the polynomial function. For example, we may require that the probability in the second case is at most half of the probability in the first case, i.e.

$$\eta^2 \leqslant (\gamma/4)/2 = \gamma/8. \tag{S-26}$$

This can be achieved with $d = O\left(\frac{\log(1/\gamma)}{\Delta}\right)$. To distinguish whether Eq. (S-24) or Eq. (S-25) are satisfied, we can use the Monte Carlo method by performing the projection process many times. To achieve a constant correct probability, this method requires sampling size $O(\gamma^{-2})$, and each run of the quantum circuit requires a single query to U_H (Lemma 9 of Ref [45], see also Ref [3]). Alternatively, we can improve the dependency on γ to $O(\gamma^{-1})$ with the amplitude amplification method.

Lemma 5 (Lemma.12 in Ref [45]). *Given a unitary W applied at $n_w + 1$ qubits, and let*

$$\omega = \|(\langle 0| \otimes I_{2^{n_w}})W|0\rangle|0^{n_w}\rangle\|, \tag{S-27}$$

where $I_{2^{n_w}}$ is 2^{n_w}-dimensional identity. It is further promised that either $\omega \leqslant \gamma_1$ or $\omega \geqslant \gamma_2$ for some $0 \leqslant \gamma_1 < \gamma_2$. These two cases can be distinguished with success probability at least 1-δ with $O\left((\gamma_2 - \gamma_1)^{-1}\log(\delta^{-1})\right)$ queries to W and one additional ancilla qubit.

We define $\mathscr{P}'^{(\Delta)}_M = \left(I_2 \otimes \text{Hard} \otimes I_{2^{a+1}} \otimes \mathscr{P}^{(\Delta)}_M\right)$, where Hard is Hardamard gate. Following the definition in Eq. (S-20), it can be verified that

$$(I_2 \otimes U_H)\,\mathscr{P}'^{(\Delta)}_M|0\rangle|0^{n+a+2}\rangle \tag{S-28}$$

$$= |0\rangle|+\rangle|\psi\rangle \tag{S-29}$$

$$= |0\rangle\left(|+\rangle|0^{a+1}\rangle \sum_j c_j P_H(\sigma_j)|u_j\rangle + |\text{garb}\rangle\right). \tag{S-30}$$

We define $|\psi'\rangle = |+\rangle|0^{a+1}\rangle \sum_j c_j P_H(\sigma_j)|u_j\rangle$, and a controlled rotation $R_{|\psi'\rangle} \equiv I_2 \otimes |\psi'\rangle\langle\psi'| + X \otimes (I - |\psi'\rangle\langle\psi'|)$. According to Eq. (S-21), we have

$$p_{\text{suss}} = \|(\langle 0| \otimes I_{2^{a+2}}) R_{|\psi'\rangle} |0\rangle |0^{a+2}\rangle\|. \tag{S-31}$$

Here, p_{suss} is the success probability of projection defined in Eq. (S-22). According to Eq. (S-24) and Eq. (S-25), we can set two thresholds of projection success probabilities to be $\gamma_1 = \eta^2 \leqslant \gamma/8$ and $\gamma_2 = \gamma/4$ respectively. According to Lemma. 5, we can distinguish whether $p_{\text{suss}} \leqslant \gamma_1$ or $p_{\text{suss}} \geqslant \gamma_2$ with $O\left((\gamma_2 - \gamma_1)^{-1} \log(\delta^{-1})\right) = \tilde{O}\left(\gamma^{-1}\right)$ queries to $R_{|\psi'\rangle}$.

$R_{|\psi'\rangle}$ requires single query to U_H, $\mathscr{P}_M'^{(\Delta)}$ and $O(n)$ extra single- and two-qubit quantum gates. Summing up the complexities, we have

Lemma 6. *Let $\Delta, \eta \in (0, 0.5)$, for $M \in \mathbb{C}^{N\times N}$ satisfying $\|M\| \leqslant 1$, and promised that its minimum singular value as defined in Eq. (S-17) satisfies either $\sigma_0 \leqslant \Delta/2$ or $\sigma_0 \geqslant \Delta$. We can distinguish these two cases with probability at least $1 - \delta$ using $\tilde{O}(\Delta^{-1}\gamma^{-1})$ queries to $\mathcal{O}_M$, $\mathscr{P}_M^{(\Delta)}$ and their inverses, and extra single- and two-qubit gates.*

Note that $\tilde{O}(\cdot)$ has neglected the dependency on n. Lemma. 2 is related to Lemma. 6 with $M = \frac{A-\mu I}{1+|\mu|}$ and $\Delta = \varepsilon/(1 + |\mu|)$. In this case, it can be verified that $\mathscr{P}_A$ satisfies the criterial for $\mathscr{P}_M^{\Delta}$. Therefore, the remaining task of proofing Lemma. 2 is therefore to show that $\mathcal{O}_M$ can be block encoded with $O(1)$ query to $\mathcal{O}_A$.

C. Block encoding of shifted and rescaled matrix

For brevity, we simply denote $\mathcal{O}_{A,\mu}$ as the block encoding of matrix $(A - \mu I)/(1 + |\mu|)$. We have the following result about its construction.

Lemma 7. *Given a square matrix A satisfying $\|A\| \leqslant 1$ and μ satisfying $|\mu| \leqslant 1$, $\mathcal{O}_{A,\mu}$ can be constructed with one query of single-qubit controlled $\mathcal{O}_A$, single ancillary qubit, and a constant number of extra single- and two-qubit gates.*

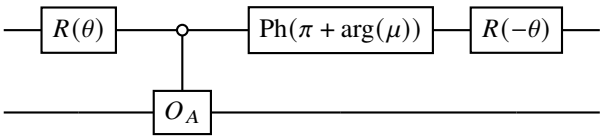
Proof. Let $\theta = \arccos\left(\sqrt{\frac{1}{1+|\mu|}}\right)$ and

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \text{Ph}(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}. \tag{S-32}$$

The block encoding unitary is constructed as

$$\mathcal{O}_{A,\mu} = (R(-\theta) \otimes I) \left(|0\rangle\langle 0| \otimes \mathcal{O}_A - |1\rangle\langle 1| \otimes e^{i\arg(\mu)} I\right) (R(\theta) \otimes I), \tag{S-33}$$

which is equivalent to the following quantum circuit



It can be verified that.

$$\begin{aligned} \langle 0^{a+1}|\mathcal{O}_{A,\mu}|0^{a+1}\rangle &= (\cos\theta\langle 0| + \sin\theta\langle 1|) \otimes I \left(|0\rangle\langle 0| \otimes \mathcal{O}_A - |1\rangle\langle 1| \otimes e^{i\arg(\mu)} I\right) (\cos\theta|0\rangle + \sin\theta|1\rangle) I \\ &= \cos^2\theta \mathcal{O}_A - \sin^2\theta e^{i\arg(\mu)} I \\ &= \frac{\mathcal{O}_A - \mu I}{1 + |\mu|}. \end{aligned} \tag{S-34}$$

□

Combining Lemma. 6 and 7, we achieve Lemma. 2 readily.

II. Solutions to Problem 1

In this section, we discuss the solution to Problem 1 for general matrices. The solution when eigenvalues are promised to be real is discussed in Sec. V. Our solution is summarized as a pseudo-code in Algorithm. 1. The protocol is based on the following lemma that can be straightforwardly verified from Lemma. 1 and the definition of O_C in Definition. 1.

Lemma 8. *For diagonalizable matrix, if* $\min_j |\mu - \lambda_j| \leqslant r/(2K)$*, with probability at least* $1-\delta$*, the output of* $O_C(\mu, r/K, \delta)$ *is True. If* $\min_j |\mu - \lambda_j| \geqslant r$*, with probability at least* $1-\delta$*, the output of* $O_C(\mu, r/K, \delta)$ *is False.*

For defective matrix, we define

$$\nu(r) = (r/3)^{m_{\max}} (2K)^{-1}. \tag{S-35}$$

if $\min_j |\mu-\lambda_j| \leqslant \nu(r)$*, with probability at least* $1-\delta$*, the output of* $O_C(\mu, 2\nu(r), \delta)$ *is True. If* $\min_j |\mu-\lambda_j| \geqslant r$*, with probability at least* $1-\delta$*, the output of* $O_C(\mu, 2\nu(r), \delta)$ *is False.*

Proof. We first consider the diagonalizable case. When $\min_j |\mu - \lambda_j| \leqslant r/(2K)$, by to Lemma. 1, we have $C(\mu) \leqslant r/(2K)$, and according to Definition. 1, Lemma. 8 holds true in this case. When $\min_j |\mu - \lambda_j| \geqslant r$, by to Lemma. 1, we have $C(\mu) \geqslant r/K$ and according to Definition. 1, the output of $O_C(\mu, r/K, \delta)$ is "False" with probability $1-\delta$. By taking the contraposition of the statement, Lemma. 8 holds true in this case.

For defective matrix case, the argument is similar except that $r/(2K)$ is replaced by $\nu(r)$. □

Lemma. 8 is also illustrated in Fig. S1a. Each SVTS (i.e. $O_C(\mu, r/K, \delta)$ for diagonalizable matrix or $O_C(\mu, 2\nu(\mu), \delta)$ for defective matrix) contains an inner region and outer region marked with yellow and green color respectively. If there is at least one eigenvalue in the inner (yellow) region, the output of SVTS is likely to be "True" (with probability at least $1-\delta$) . If the output of SVTS is True, it is likely that there are at least one eigenvalues in the outer (green) region (with probability at least $1-\delta$). The radius of inner region is $r/2K$ or $\nu(r)$ for diagonalizable and defective matrices, the radius of outer region is r.

Because $\|A\| \leqslant 1$, all eigenvalues are in $\mathcal{D}(0,1)$. Our strategy of solving Problem. 1 is to iteratively shrink the region in which there is at least one eigenvalue in it (with high probability). Our method contains $J = \lceil \log_2(1/\varepsilon) \rceil$ steps, and the process of each step is illustrated in Fig. S1b (see also Algorithm. 2). Suppose that before the jth step, we are confidence that there is at least one eigenvalue in the region $\mathcal{D}(\lambda_{\rm gss}, D)$. At this step, we shrink the radius of such confidence region from D to $D/2$. This is achieved by introducing a set of SVTSs, whose inner region covers $\mathcal{D}(\lambda_{\rm gss}, D)$. This ensures that at least one of the SVTS has output "True". Another restriction is that the outer region of each SVTS has a radius $D/2$. In this way, once we obtain an output "True", we are confidence that at least one eigenvalue is in the region $\mathcal{D}(\lambda'_{\rm gss}, D/2)$, where $\lambda'_{\rm gss}$ is the center of such SVTS with output "True".

Note that in Algorithm. 2, we have introduced a set of points $\mathcal{N}_{\rm net}(\lambda_{\rm gss}, D, m_{\max})$. It represents the centers of all SVTSs satisfying the criteria above. Equivalently, we have

$$\mathcal{D}(\lambda_{\rm gss}, D) \subset \bigcup_{\mu \in \mathcal{N}_{\rm net}(\lambda_{\rm gss}, D, 1)} \mathcal{D}(\mu, D/4K), \tag{S-36}$$

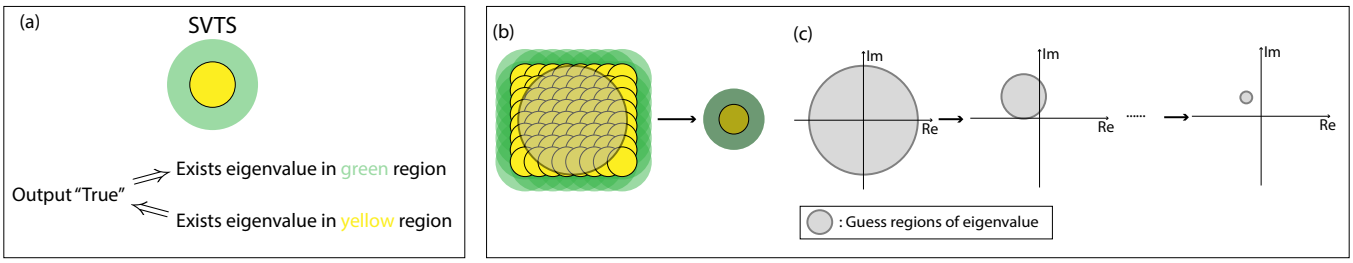
when $m_{\max} = 1$, or

$$\mathcal{D}(\lambda_{\rm gss}, D) \subset \bigcup_{\mu \in \mathcal{N}_{\rm net}(\lambda_{\rm gss}, D, m_{\max})} \mathcal{D}(\mu, \nu(D/2)). \tag{S-37}$$

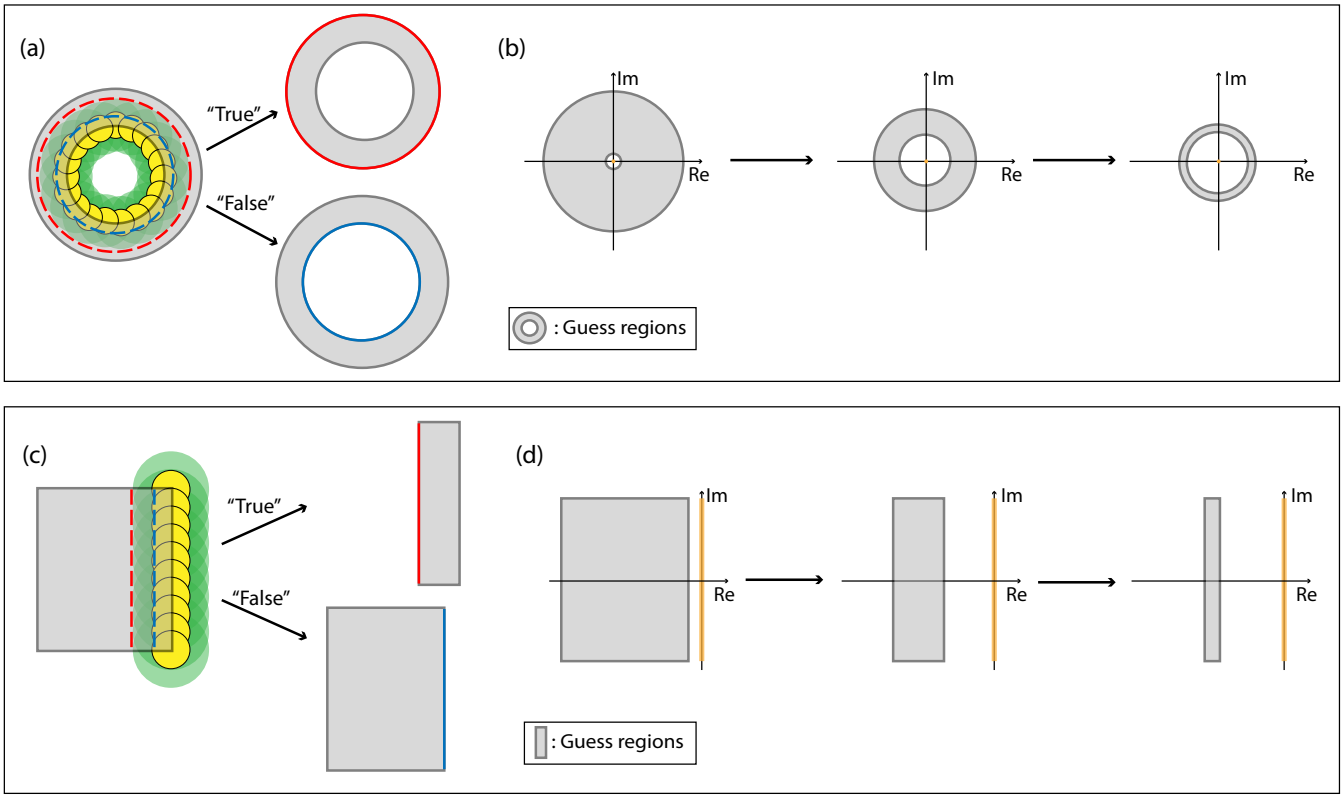
when $m_{\max} > 1$.

We first estimate the complexity of diagonalizable matrices. According to Lemma. 8, the query to each SVTS has complexity $\tilde{O}(KD^{-1}\gamma^{-1})$. Moreover, the area of $\mathcal{D}(\lambda_{\rm gss}, D)$ and the inner regions of SVTSs are πD^2 and $\pi D^2/(4K)^2$ respectively. So it suffices to use $O(K^2)$ number of SVTSs to cover $\mathcal{D}(\lambda_{\rm gss}, D)$. Therefore, the complexity at each step is $\tilde{O}(KD^{-1}\gamma^{-1}) \times O(K^2) = \tilde{O}(K^3 D^{-1}\gamma^{-1})$. In Algorithm. 1, the total algorithm contains $J = \lceil \log_2(1/\varepsilon) \rceil$ steps, and we have $D \geqslant \varepsilon$. So the total complexity is $\tilde{O}(K^3\varepsilon^{-1}\gamma^{-1})$.

For defective matrix, the threshold of each SVTS is $2\nu(D/2) = O(D^{m_{\max}}/K)$. The complexity of each query to SVTS is therefore $\tilde{O}(KD^{-m_{\max}}\gamma^{-1})$. The inner region of each SVTS has area $O(D^{2m_{\max}}/K^2)$, so totally $O(K^2 D^{-2m_{\max}+2})$ number of SVTSs is required to cover $\mathcal{D}(\lambda_{\rm gss}, D)$. Therefore, the complexity for each step is $\tilde{O}(K^3 D^{-3m_{\max}+2}\gamma^{-1})$, while the total complexity of Algorithm. 1 is $\tilde{O}(K^3\varepsilon^{-3m_{\max}+2}\gamma^{-1})$.



Supplementary Figure S1: (a) Sketch of SVTS. (b) Sketch of Algorithm. 2 for shrinking the range of eigenvalue searching (Problem 1). The initial and updated guess region is enclosed by grey circles. (c) Sketch of Algorithm. 4 for shrinking the range of point gap. The initial guess region is a ring enclosed by two grey circles (Problem 2). The updated guess region is a ring enclosed by a grey circle and red (one of the SVTS has output "True") or blue (all of the SVTS has output "False") circles.



Supplementary Figure S2: (a) and (b): Sketch of the process solving Problem. 2. (c) and (d): Sketch of the process solving Problem. 3.

Algorithm 1 Quantum eigenvalue searching for Problem 1.

$D \leftarrow 1, \delta' \leftarrow \delta/\lceil \log_2(D/\varepsilon) \rceil$
while $D > \varepsilon$:
  $\lambda_{\text{gss}} \leftarrow \mathscr{R}\left(\lambda_{\text{gss}}, D, \delta'\right)$
  $D \leftarrow D/2$:
end while
return λ_{gss}

Algorithm 2 $\mathscr{R}(\lambda_{\text{gss}}, D, \delta)$

$\delta' \leftarrow \delta/|\mathcal{N}_{\text{net}}(\lambda_{\text{gss}}, D, m_{\max})|$
for all $\mu \in \mathcal{N}_{\text{net}}(\lambda_{\text{gss}}, D, m_{\max})$:
  if $m_{\max} = 1$:
    $B \leftarrow O_C(\mu, D/4K, \delta')$
  else if: $m_{\max} > 1$:
    $B \leftarrow O_C(\mu, 2\nu(D/2), \delta')$
  end if
  if B = True:
    break for
  end if
end for
return μ

III. Solution to Problem. 2

In this section, we introduce our protocols for solving Problem 2. We specify the reference point as the original point, i.e. $P = 0$. The goal is then to find an eigenvalue that is closest to, but not equal to 0. In case $P \neq 0$, we can always define a new matrix $\tilde{A} = (A - PI)/(1 + |P|)$, and the problem then reduces to the point gap problem for $\tilde{A}$ with the original point as the reference point. Our algorithm contains two stages. In the first stage, the goal is to output an estimation of the point gap $g \equiv \min_{\lambda_j} |P - \lambda_j|$ to accuracy ε. In the second stage, we search an eigenvalue close to the circle with radius g.

A. Stage 1: estimating the point gap

The main idea of stage 1 is as follows. Initially, we have $g \in [\varepsilon, 1]$. We introduce an eigenvalue range shrinking subroutine (ERSS) in Sec. **??**, based on which the range of g shrinks iteratively.

According to definition in Problem 2, we initially have $g \in [R_0^{\min}, R_0^{\max}]$ with $R_0^{\min} = \varepsilon$ and $R_0^{\max} = 1$. Our strategy is to shrink the range of g iteratively. The full process is summarized in Algorithm. 3. Suppose at the jth step, we are confidence that

$$g \in [R_{j-1}^{\min}, R_{j-1}^{\max}]. \tag{S-38}$$

In this step, $R_{j-1}^{\min}$ or $R_{j-1}^{\max}$ is updated by querying the eigenvalue range shrinking subroutine (ERSS)

$$\mathcal{S}(R^{\min}, R^{\max}, r, \delta) \to (\tilde{R}^{\min}, \tilde{R}^{\max}) \tag{S-39}$$

defined in Algorithm. 4. The ERSS contains four input parameters. $R^{\min}$ and $R^{\max}$ are the recent confidence region in which the gap g is in. The third parameter $r > 0$ controls the step size of updating. It is required that $r \leqslant R^{\min}$ and $r \leqslant R^{\max} - R^{\min}$. The first requirement ensures that the output of ERSS will not be affected by eigenvalue at the original point, if any. The second requirement ensures that the current gap $\Delta_j \equiv R_j^{\max} - R_j^{\min}$ is non-increasing. The last parameter δ is the failure probability. The ERSS has the following property.

Lemma 9. *Let A be a square matrix satisfying $\|A\| \leqslant 1$. Let $(\tilde{R}_a, \tilde{R}_b)$ be the output of $\mathcal{S}(R_a, R_b, r, \delta)$ for some $0 < R_a < R_b \leqslant 1$, and $0 < r \leqslant \min(R_a, (R_b - R_a)/2)$, and $\delta \in (0, 1)$. Then, suppose the point gap satisfies $g \in [R_a, R_b]$, with probability at least $1 - \delta$, we have $g \in [\tilde{R}^{\min}, \tilde{R}^{\max}]$. Here, $\tilde{R}_a$ and $\tilde{R}_b$ are defined in Algorithm. 4.*

Moreover, the complexity of ERSS is given by the following.

Lemma 10. *$\mathcal{S}(R_a, R_b, r, \delta)$ defined in Algorithm. 4 can be realized with $\tilde{O}\left(K^2 R_a r^{-2m_{max}} \gamma^{-1}\right)$ queries to $\mathcal{O}_A$, $\mathcal{P}_A$ and there inverses, and single- and two-qubit gates.*

Base on Lemma 9, we are able to update the region of g by $\mathcal{S}\left(R_{j-1}^{\min}, R_{j-1}^{\max}, r, \delta'\right) \to (R_j^{\min}, R_j^{\max})$, where δ' is set as a sufficiently small value. From Algorithm. 4, it can also be verified that

$$|\Delta_{j-1} - \Delta_j| = \Omega(r^{m_{\max}}/K). \tag{S-40}$$

Stage 1 is separated into two substages. In substage 1, we set $r = R_{j-1}^{\min}$ at each step, and this substage terminates when $R_j^{\min} \geqslant R_j^{\max}/2$. The complexity of each step is $\tilde{O}\left(K^2 (R_j^{\min})^{-2m_{\max}+1} \gamma^{-1}\right)$. From Eq. (S-40), it can be verified that this substage terminates with at most $O(K\varepsilon^{-m_{\max}+1})$ steps. Because $R_j^{\min} \geqslant \varepsilon$, The total complexity for this substage is

$$\tilde{O}\left(K^2 \varepsilon^{-2m_{\max}+1} \gamma^{-1}\right) \times O(K\varepsilon^{-m_{\max}+1}) = \tilde{O}\left(K^3 \varepsilon^{-3m_{\max}+2} \gamma^{-1}\right). \tag{S-41}$$

In substage 2, we set $r = \left(R_{j-1}^{\max} - R_{j-1}^{\min}\right)/2$, and this substage terminates when $\Delta_j \leqslant \varepsilon$. In this substage, the complexity of each step is $\tilde{O}\left(K^2 \varepsilon^{-2m_{\max}} \gamma^{-1}\right)$. This substage contains $\tilde{O}(K\varepsilon^{-m_{\max}+1})$ steps as can be verified from Eq. (S-40). So the total complexity of substage 2 is

$$\tilde{O}\left(K^2 \varepsilon^{-2m_{\max}} \gamma^{-1}\right) \times O(K\varepsilon^{-m_{\max}+1}) = \tilde{O}\left(K^3 \varepsilon^{-3m_{\max}+1} \gamma^{-1}\right). \tag{S-42}$$

Combining Eq. (S-41) and Eq. (S-42), the total complexity of stage 1 is $\tilde{O}\left(K^3 \varepsilon^{-3m_{\max}+1} \gamma^{-1}\right)$.

Algorithm 3 Stage 1 for solving Problem 2

$R_0^{\min} \leftarrow \varepsilon$; $R_0^{\max} \leftarrow 1$; $j \leftarrow 1$
while $R_{j-1}^{\min} < R_{j-1}^{\max}/2$: # Substage 1
  $(R_j^{\min}, R_j^{\max}) \leftarrow \mathcal{S}(R_{j-1}^{\min}, R_{j-1}^{\max}, R_{j-1}^{\min}, \delta')$
  $j \leftarrow j + 1$
end while
while $R_{j-1}^{\max} - R_{j-1}^{\min} > \varepsilon$: # Substage 2
  $(R_j^{\min}, R_j^{\max}) \leftarrow \mathcal{S}\left(R_{j-1}^{\min}, R_{j-1}^{\max}, \left(R_{j-1}^{\max} - R_{j-1}^{\min}\right)/2, \delta'\right)$
  $j \leftarrow j + 1$
end while
return $\left(R_{j-1}^{\min}, R_{j-1}^{\max}\right)$

1. *Eigenvalue range shrinking subroutine*

Here, we give detailed construction of the ERSS. For compactness, we define

$$\tilde{\nu}(r) = \begin{cases} r/K & m_{\max} = 1 \\ (r/3)^{m_{\max}} (2K)^{-1} & m_{\max} > 1 \end{cases} \tag{S-43}$$

Algorithm 4 $\mathcal{S}(R_a, R_b, r, \delta)$ (Eigenvalue range shrinking subrutine)

$\delta' \leftarrow \delta/|\mathcal{N}_{\text{ring}}(R_a, \tilde{\nu}(r))|$
for all $t \in \mathcal{N}_{\text{ring}}(R_a, \tilde{\nu}(r))$:
  $B \leftarrow O_C(t, \tilde{\nu}(r), \delta')$
  if B = True:
    break for
  end if
end for
if B = True:
  $\tilde{R}_a \leftarrow R_a$
  $\tilde{R}_b \leftarrow R_a + r$
else if B = False:
  $\tilde{R}_a \leftarrow R_a + \tilde{\nu}(r)/4$
  $\tilde{R}_b \leftarrow R_b$
end if
return $(\tilde{R}_a, \tilde{R}_b)$

Here, we have also defined

$$\mathcal{N}_{\text{ring}}(R,s)=\left\{Re^{i2\pi m/M(R,s)}\middle|m\in\{1,2\cdots,M(R,s)\}\right\},\tag{S-44}$$

where

$$M(R,s)=\frac{2\pi}{\arctan(s/(2R))}.\tag{S-45}$$

$\mathcal{N}_{\text{ring}}(R,s)$ defines a set of points at the circle with radius R. The main idea of ERSS is illustrated in Fig. S1c. The yello (inner) region of all SVTSs covers the edge of the circle with radius $R^{\min}$. If either of the SVTS has output true, we have $B=$ True. In this case, with confidence at least $1-\delta$, there exists at least one eigenvalue in the region covered by the green disks. So $R^{\max}$ is updated. Otherwise, we have $B=$ False. In this case, with confidence at least $1-\delta$, all of the eigenvalues are outside the region covered by the yellow disks, so $R^{\min}$ is updated. The validity of Lemma. 9 can be verified straightforwardly based on Lemma. 8.

We then estimate the runtime of $\mathcal{S}$. Because $\tilde{\nu}(r)=O(r^{m_{\max}}/K)$, we have $|\mathcal{N}_{\text{ring}}(R_{\text{a}},\tilde{\nu}(r))|=\tilde{O}(R_aKr^{-m_{\max}})$, and each query to the SVTS has runtime $\tilde{O}(Kr^{-m_{\max}}\gamma^{-1})$. So the total runtime of $\mathcal{S}(R_a,R_b,r,\delta)$ is $\tilde{O}(Kr^{-m_{\max}})\times\tilde{O}(Kr^{-m_{\max}}\gamma^{-1})=\tilde{O}(R_aK^2r^{-2m_{\max}}\gamma^{-1})$

B. Stage 2: obtaining the eigenvalue

After stage 1, we are confidence that $g\in[R_J^{\min},R_J^{\max}]$ for some $R_J^{\max}-R_J^{\min}\leqslant\varepsilon$. In other words, we are confident that there exists at least one eigenvalue in the region $\tilde{\mathcal{D}}=\mathcal{D}(0,R_J^{\max})/\mathcal{D}(0,R_J^{\min})$, while there is no eigenvalue in the region $\mathcal{D}(0,R_J^{\min})/\mathcal{D}(0,\varepsilon)$.

The remaining task is then to find an eigenvalue estimation in $\tilde{\mathcal{D}}$. This is achievable with a similar strategy for Problem 1. We can introduce a set of SVTSs, whose outer region has radius ε, and the inner region covers $\tilde{D}$. Accordingly, the complexity of implementing each SVTS is $\tilde{O}(\nu(\varepsilon))=\tilde{O}(K\varepsilon^{-m_{\max}})$. The area of $\tilde{\mathcal{D}}$ is upper bounded by $2\pi\varepsilon$, while the area of inner region of each SVTS is $\nu(\varepsilon)=\tilde{O}(\varepsilon^{m_{\max}}/K)$. So it suffices to use totally $\tilde{O}(K\varepsilon^{-m_{\max}+1})$ number of SVTSs to cover $\tilde{\mathcal{D}}$. Therefore, the total complexity of this stage is $\tilde{O}(K\varepsilon^{-m_{\max}}\gamma^{-1})\times\tilde{O}(K\varepsilon^{-m_{\max}+1})=\tilde{O}(K^2\varepsilon^{-2m_{\max}+1})$.

Combining the complexity for stage 1 and stage 2, the total complexity for solving Problem 2 is $\tilde{O}\left(K^3\varepsilon^{-3m_{\max}+1}\gamma^{-1}\right)$.

IV. Solution to Problem. 3

We now discuss the solution to Problem 3. Similar to the point gap problem, we can assume that the reference line is the imaginary axis $L=\{ia|a\in\mathbb{R}\}$. The problem with other reference lines is equivalent to this one up to a simple transformation. For $L=\{e^{i\theta}a+b|a,b\in\mathbb{R}\}$, we can define a rescaled matrix up to a phase $\tilde{A}=\frac{e^{-i\theta}(A-bI)}{\sqrt{1+b^2}}$, and the problem reduces to the one with imaginary axis as reference line.

The protocol is similar to the one for point gap problem in the previous section. In stage 1, we obtain an estimation of g with Algorithm. 5. Comparing to Algorithm. 3, we have just replaced the ERSS of $\mathcal{S}$ by $\mathcal{S}_{\text{line}}$, which is defined in Algorithm. 6. Recall that for $\mathcal{S}$, we cover the circle $\{x||x|=R_a\}$ with the inner region of SVTSs. There centers are defined by $\mathcal{N}_{\text{ring}}$. For $\mathcal{S}_{\text{line}}$, we cover two segments $\{\pm a+ib|-1\leqslant b\leqslant 1\}$ instead, with $\mathcal{N}_{\text{ring}}$ is replaced by $\mathcal{N}_{\text{line}}$ as defined in (S-46).

$$\mathcal{N}_{\text{line}}(R,s)=\{\pm R-i,\pm R-i(1-s'),\pm R-i(1-2s'),\cdots,\pm R+i\},\tag{S-46}$$

with $s'=(\lceil 2/s\rceil)^{-1}$. See also Fig. S2(c), (d) for illustration. Following the same argument in Sec. III A, the complexity of stage 1 is $\tilde{O}\left(K^3\varepsilon^{-3m_{\max}+1}\gamma^{-1}\right)$.

After stage 1, we are confidence that there exists at least one eigenvalues in the region $\left\{\pm a+ib\middle|R_j^{\min}\leqslant a\leqslant R_j^{\max},-1\leqslant b\leqslant 1\right\}$ for some $R_j^{\max}-R_j^{\min}\leqslant\varepsilon$. The area of this region is therefore at most 2ε, which is at the same order to the area of guess region for point gap problem stage 2. Therefore, for line gap problem stage 2, we can obtain an estimation of expected eigenvalue with the same strategy in Sec. III B. The complexity is still $\tilde{O}(K^2\varepsilon^{-2m_{\max}+1})$.

Combining stages 1 and 2, the total complexity of solving Problem. 3 is also $\tilde{O}\left(K^3\varepsilon^{-3m_{\max}+1}\gamma^{-1}\right)$.

V. Real eigenvalue cases

If we are promised that all eigenvalues are real and non-defective (i.e. $m_{\max} = 1$), the search region of eigenvalue the becomes the segment $[-1, 1]$ in real axis. In this section, we discuss how solutions to Problem. 1-3 can be simplified in this case.

A. Real eigenvalue case for Problem. 1

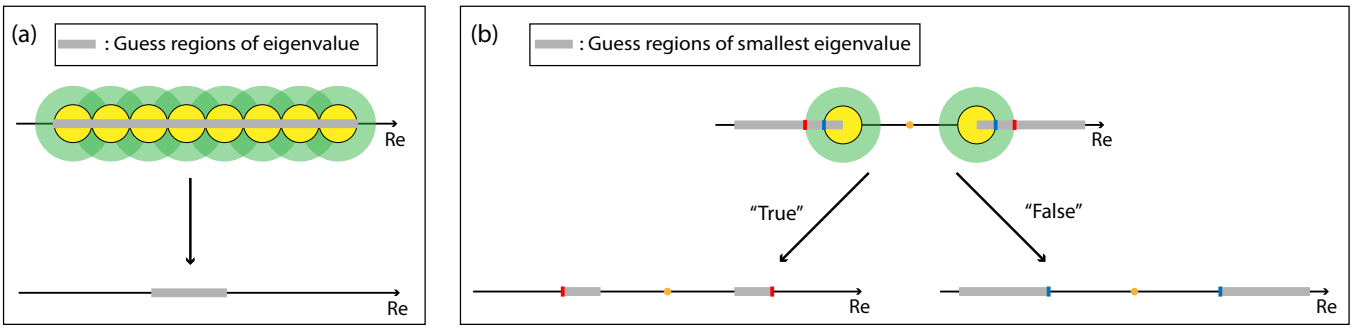
Similar to the general case in Sec. II, we use a divided-and-conquer strategy and the full algorithm is provided in Algorithm. 7. Before each iteration, the guess region is $[\lambda_{\text{gss}} - D, \lambda_{\text{gss}} + D]$ (initially, we have $\lambda_{\text{gss}} = 0$ and $D = 1$). After querying $\mathscr{R}_{\text{real}}(\lambda_{\text{gss}}, D, \delta)$ defined in Algorithm, 8, λ_{gss} is updated and $D \to D/2$. Compared to the $\mathscr{R}$ for general case, the main difference is that $\mathscr{R}_{\text{real}}$ only need to cover segment $[\lambda_{\text{gss}} - D, \lambda_{\text{gss}} + D]$ in real axis with the inner region of SVTS, instead of the entire disk $\mathcal{D}(\lambda_{\text{gss}}, D)$. See also Fig. S3 (a) for illustration.

In Algorithm. 7, $\mathscr{R}_{\text{real}}$ requires $O(K)$ queries to SVTS, and each query has complexity $\tilde{O}(KD^{-1}\gamma^{-1})$. So the total complexity of $\mathscr{R}_{\text{real}}$ is $\tilde{O}(K^2D^{-1}\gamma^{-1})$. Because $D \geqslant \varepsilon$, and Algorithm. 7 has totally $O(\log(\varepsilon^{-1}))$ queries to $\mathscr{R}_{\text{real}}$, the total complexity of the algorithm is $\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1})$. So we have the following result.

Theorem 4. *Promised that $\lambda_j \in \mathbb{R}$ for all eigenvalues λ_j and $m_{\max} = 1$, with success probability at least $1 - \delta$, Problem 1 can be solved with*

$$\tilde{O}\left(K^2\varepsilon^{-1}\gamma^{-1}\right) \tag{S-47}$$

uses of the query to $\mathcal{O}_A$, $\mathscr{P}_A$ and their inverses, and extra single- and two-qubit gates.



Supplementary Figure S3: Eigenvalue searching protocols with promised that eigenvalues are real. (a) Sketch of Algorithm. 8 for shrinking the range of eigenvalue searching for Problem 1. The initial and updated guess region is marked by grey lines. (b) Sketch of Algorithm. 10 for shrinking the range of eigenvalue for Problem 2, 3. The initial guess regions are two grey lines. The updated guess regions are two segments with one side marked by red (one of the SVTS has output "True") or blue (all of the SVTS has output "False") colors.

B. Real eigenvalue case for Problem. 2, 3

When eigenvalues are promised to be real and non-defective, both Problem. 2 and Problem. 3 reduce to the following.

Problem 4. *Given a diagonalizable matrix $\|A\| \leqslant 1$, promised that $\lambda_j \in \mathbb{R}$ and $|\lambda_j| < \varepsilon$ for all eigenvalues λ_j. Let $g \equiv \min_{\lambda_j \neq P} |\lambda_j - P|$ and $\mathcal{S} \equiv \{\lambda_j \big| |\lambda_j| \in [g, g + \varepsilon]\}$ for some accuracy $\varepsilon \in (0, 1)$. The goal is to output an eigenvalue estimation λ', such that $|\lambda' - \lambda_j| \leqslant \varepsilon$ for some $\lambda_j \in \mathcal{S}$.*

Note that similar to Section. III, we set the reference point as 0. Our solution to Problem. 4 is summarized in Algorithm. 9, where the variable $\delta' = \delta/J_{\max}$ is determined by $J_{\max}$, the maximal number of queries to SVTS as will be upper bounded later. The main ideal is similar to the general case. At each iteration, we are initially promised that $g \in [R_j^{\min}, R_j^{\max}]$ and we shrink this range by querying a subroutine $\mathcal{S}_{\text{real}}$ defined in Algorithm. 10. Different from $\mathcal{S}$, the subroutine $\mathcal{S}_{\text{real}}$ use only two queries to the SVTS because we only need to cover the corresponding segment in real axis. See Fig. S3(b) for illustration.

Algorithm. 9 contains two substages, in below, we analyze their complexities separately.

For substage 1, we begin with analysing the maximal number of iterations required, denoted as J. We consider the worst case when we always have $B = \text{False}$. In this case, we have $R_{j+1}^{\min} = R_j^{\min}(1 + 1/(2K))$, and therefore $R_j^{\min} = \varepsilon(1 + 1/(2K))^j$. Substage

1 terminates whenever $R_j^{\min} \leqslant 1/2$, so we have $\varepsilon(1+1/(2K))^J = \Theta(1)$. Accordingly, we have

$$J = O\left(\frac{\log((2\varepsilon)^{-1})}{\log(1+1/(2K))}\right) = O(K\log(\varepsilon^{-1})). \tag{S-48}$$

Each query to the SVTS has complexity $\tilde{O}((K/R_j^{\min})\gamma^{-1}\text{polylog}(\delta'^{-1})) = \tilde{O}(K\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta'^{-1}))$, so the total complexity of substage 1 is

$$J \times \tilde{O}(K\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta'^{-1})) = \tilde{O}(K^2\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta'^{-1})).$$

For substage 2, we first define $\Delta_j = R_j^{\max} - R_j^{\min}$. Again, we first analyse the the maximal number of iterations in this substage, denoted as J'. In the worst case, we always have B = False, which gives $\Delta_{j+1} = \Delta_j(1-1/(4K))$. Suppose substage 2 begins with $j = j'$ and we denote $\Delta = \Delta_{j'}$. Then, we have $\Delta_j = \Delta(1-1/(4K))^{j-j'}$. Substage 2 terminates whenever $\Delta_j \leqslant \varepsilon$, so we have $\Delta(1-1/(4K))^{J'} = \Theta(\varepsilon)$. Accordingly, we have

$$J' = O\left(\frac{\log(\varepsilon/\Delta)}{\log(1-1/(4K))}\right) = O(-K\log(\varepsilon/\Delta)) = O(K\log(\varepsilon^{-1})). \tag{S-49}$$

In substage 2, each query to the SVTS has complexity $\tilde{O}((K/\Delta_j)\gamma^{-1}\text{polylog}(\delta'^{-1})) = \tilde{O}(K\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta'^{-1}))$. So the total complexity is

$$J \times \tilde{O}(K\varepsilon^{-1}\gamma^{-1}) = \tilde{O}(K^2\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta'^{-1})). \tag{S-50}$$

Combining the complexity for substage 1 and 2, the total complexity of Algorithm. 10 (i.e. $\mathcal{S}_{\text{diag}}(\pm 1)$ in Algorithm. 9) is

$$\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta'^{-1})). \tag{S-51}$$

For each $\mathcal{S}_{\text{diag}}(\pm 1)$, the total number of queries to SVTS can be upper bounded by $J_{\max} = J + J' = \tilde{O}(K)$. Therefore, to achieve sucess probability $1-\delta$, it suffices to set $\delta' = \tilde{O}(\delta/K)$. Inserting into Eq. (S-51), the total complexity of Algorithm. 10 is

$$\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1}\text{polylog}(\delta/K^{-1})) = \tilde{O}(K^2\varepsilon^{-1}\gamma^{-1}). \tag{S-52}$$

Therefore, we have the following theorem.

Theorem 5. *With success probability at least* $1-\delta$*, Problem 4 can be solved with*

$$\tilde{O}(K^2\varepsilon^{-1}\gamma^{-1}) \tag{S-53}$$

queries to $\mathcal{O}_A$*,* $\mathcal{P}_A$ *and their inverses, and extra single- and two-qubit gates.*

VI. Eigenvector state preparation

A. main idea

In this section, we consider the problem of preparing eigenvector states. To facilitate the discussion, we first define the singular value decomposition of matrix $(A-\mu I)$ as

$$A - \mu I \equiv \sum_{k=0}^{N-1} s_k(\mu)|w_k(\mu)\rangle\langle u_k(\mu)|, \tag{S-54}$$

where $s_k(\mu) \leqslant s_{k+1}(\mu)$, and $\langle w_k(\mu)|w_{k'}(\mu)\rangle = \langle u_k(\mu)|u_{k'}(\mu)\rangle = \delta_{k,k'}$. We suppose λ and $|v\rangle$ is a pair of solution to the eigenfunction Eq. (1). Then, it can be verified that $s_0(\lambda) = 0$ and $|u_0(\lambda)\rangle = |v\rangle$. We can obtain an eigenvector with infidelity ε_{vec} in two stages:

- Stage.1: Obtain an estimation $\hat{\lambda}$ that is sufficiently close to λ, such that $1 - |\langle u_0(\lambda)|u_0(\hat{\lambda})\rangle|^2 \leqslant \varepsilon_{\text{vec}}/2$.
- Stage.2: Obtain a quantum state $|v'\rangle$ that is sufficiently close $|u_0(\hat{\lambda})\rangle$, such that $1 - |\langle u_0(\hat{\lambda})|v'\rangle|^2 \leqslant \varepsilon_{\text{vec}}/2$.

It can then be verified that the output quantum state satisfies $1 - |\langle v|v'\rangle|^2 \leqslant \varepsilon_{\text{vec}}$.

Accordingly, we will address two problems in this section. The first problem is the required accuracy of $\hat{\lambda}$. The complexity of stage 1 can then be obtained readily based on Theorem. 1 or 2, depending on the restrictions on the corresponding eigenvalues, if any. The second problem is the complexity of stage 2. The total complexity of eigenvector state preparation is then the combination of complexities of two stages.

B. Stage 1

We define $\Delta_{\text{sig}}(\lambda)$ as a lower bound of the gap between the first and second smallest singular value of $A - \mu I$, which satisfies $s_1(\lambda) - s_0(\lambda) \geqslant \Delta_{\text{sig}}(\lambda)$. For general matrices, we have the following result.

Theorem 6. *Let λ be one of the eigenvalues of square matrix A satisfying $\|A\| \leqslant 1$. To achieve vector accuracy $1 - |\langle u_0(\lambda)|u_0(\hat{\lambda})\rangle|^2 \leqslant \varepsilon_{vec}/2$ for arbitrary $\varepsilon_{vec} \in (0, 1)$, it suffices to have*

$$|\hat{\lambda} - \lambda| \leqslant \Delta_{sig}(\lambda)\sqrt{\varepsilon_{vec}/2}. \tag{S-55}$$

Proof. Suppose $|\hat{\lambda} - \lambda| \leqslant \varepsilon_{\text{val}}$, we have

$$\begin{aligned}\|(A - \hat{\lambda}I)|u_0(\lambda)\rangle\| &= \|((\lambda - \hat{\lambda})I + (A - \lambda I))|u_0(\lambda)\rangle\| \\ &\leqslant \|(\lambda - \hat{\lambda})I|u_0(\lambda)\rangle\| + \|(A - \lambda I)|u_0(\lambda)\rangle\| \\ &\leqslant \varepsilon_{\text{val}} + 0 \\ &= \varepsilon_{\text{val}}.\end{aligned} \tag{S-56}$$

We then decompose $|u_0(\hat{\lambda})\rangle$ with the right singular vectors of $(A - \lambda I)$ as $|u_0(\hat{\lambda})\rangle = \sum_{j=0}^{N-1} c_j|u_j(\lambda)\rangle$. Because $(A - \lambda I)|u_j(\lambda)\rangle = s_j(\lambda)|w_j(\lambda)\rangle$, Eq. (S-56) becomes

$$\left\| \sum_{j=0}^{N-1} c_j s_j(\lambda)|w_j(\lambda)\rangle \right\| \leqslant \varepsilon_{\text{val}}. \tag{S-57}$$

Because $|w_j(\lambda)\rangle$ are orthonormal, we have

$$\sum_{j=0}^{N-1} |c_j|^2 s_j(\lambda)^2 \leqslant \varepsilon_{\text{val}}^2. \tag{S-58}$$

Because $s_0(\lambda) = 0$ and $s_{j>0}(\lambda) \geqslant \Delta_{\text{sig}}(\lambda)$, we have

$$\Delta_{\text{sig}}(\hat{\lambda})^2 \sum_{j=1}^{N-1} |c_j|^2 \leqslant \varepsilon_{\text{val}}^2, \tag{S-59}$$

which gives

$$\sum_{j=1}^{N-1} |c_j|^2 \leqslant \varepsilon_{\text{val}}^2 \Delta_{\text{sig}}(\hat{\lambda})^{-2}. \tag{S-60}$$

The infidelity of $|u_0(\hat{\lambda})\rangle$ therefore satisfies

$$\begin{aligned}1 - |\langle u_0(\lambda)|u_0(\hat{\lambda})\rangle|^2 &= \sum_{j=1}^{N-1} |c_j|^2 \\ &\leqslant \varepsilon_{\text{val}}^2 \Delta_{\text{sig}}(\hat{\lambda})^{-2}.\end{aligned} \tag{S-61}$$

Therefore, to achieve infidelity $1 - |\langle u_0(\lambda)|u_0(\hat{\lambda})\rangle|^2 \leqslant \varepsilon_{\text{vec}}/2$, it suffices to have $\varepsilon_{\text{val}} = \Delta_{\text{sig}}(\lambda)\sqrt{\varepsilon_{\text{vec}}/2}$. □

For diagonalizable matrix, we may replace the gap of singular value by the gap of eigenvalues. Similarly, we assume that there exists an upper bound of the eigenvalue gap $\Delta_{\text{eig}}(\lambda)$, such that $\min_{\lambda_j\neq\lambda}|\lambda-\lambda_j| \geqslant \Delta_{\text{eig}}(\lambda)$. When the target accuracy ε_{vec} is sufficiently small, we have the following result.

Theorem 7. *Let λ be one of the eigenvalues of the square and diagonalizable matrix A which satisfies $\|A\| \leqslant 1$. To achieve vector accuracy $1-|\langle u_0(\lambda)|u_0(\hat{\lambda})\rangle|^2 \leqslant \varepsilon_{vec}/2$ for $\varepsilon_{vec} \in (0, K^{-1}\Delta_{eig}(\lambda))$, it suffices to have*

$$|\hat{\lambda}-\lambda| \leqslant (K^{-1}\Delta_{eig}(\lambda)-\varepsilon_{vec})\sqrt{\varepsilon_{vec}/2}. \tag{S-62}$$

Proof. Given an arbitrary pair of matrices M_1, M_2, we have the following relation

$$\sigma_j(M_1M_2) \geqslant \sigma_0(M_1)\sigma_j(M_2), \tag{S-63}$$

where $\sigma_j(\cdot)$ is the jth singular value of a matrix with nondecreasing order. According to the eigenvalue decomposition $A-\lambda I = P(\Lambda-\lambda I)P^{-1}$, we have

$$\begin{aligned}\sigma_1(A-\lambda I) &\geqslant \sigma_0(P)\sigma_1((\Lambda-\lambda I)P^{-1})\\ &\geqslant \sigma_0(P)\sigma_1(\Lambda-\lambda I)\sigma_0(P^{-1})\\ &\geqslant K^{-1}\sigma_1(\Lambda-\lambda I)\\ &= K^{-1}\Delta_{\text{eig}}(\lambda).\end{aligned} \tag{S-64}$$

Because $\sigma_0(\Lambda-\lambda I)=0$, we have $\Delta_{\text{sig}}(\lambda) \geqslant K^{-1}\Delta_{\text{eig}}(\lambda)$. Combining with Theorem. 6, we can achieve the result claimed in Theorem. 7.

□

With Theorem. 6 or Theorem. 7, the complexity of stage 1 can be determined based on Theorem. 1 or Theorem. 2 (depending on whether we have restrictions on the corresponding eigenvalue) by replacing the accuracy of eigenvalue ε by Eq. (S-55) or Eq. (S-62).

C. Stage 2

We then discuss the complexity of stage.2. Preparing $|u_0(\hat{\lambda})\rangle$ can be considered as the generalization of ground state preparation for Hermitian matrices. Using the QSVT technique together with amplitude amplification [3], we can achieve the following [14].

Theorem 8. *A quantum state $|v'\rangle$ satisfying $1-|\langle u_0(\hat{\lambda})|v'\rangle|^2 \leqslant \varepsilon_{vec}/2$, for some $\varepsilon_{vec} \in (0,1)$, can be prepared using $\tilde{O}(\Delta_{sig}(\hat{\lambda})^{-1}\gamma^{-1})$ queries to $\mathcal{O}_A$, $\mathcal{P}_A$, and extra single- and two-qubit gates.*

Again, we may replace the singular value gap by eigenvalue gap when A is diagonalizable.

Theorem 9. *When A is diagonalizable, a quantum state $|v'\rangle$ satisfying $1-|\langle u_0(\hat{\lambda})|v'\rangle|^2 \leqslant \varepsilon_{vec}/2$, for some $\varepsilon_{vec} \in \left(0, \frac{1}{2}K^{-1}\Delta_{eig}\right)$, can be prepared using $\tilde{O}(K\Delta_{eig}(\lambda)^{-1}\gamma^{-1})$ queries to $\mathcal{O}_A$, $\mathcal{P}_A$, and extra single- and two-qubit gates.*

Proof. According to the perturbation theorem of Weyl, we have $|\Delta_{\text{sig}}(\lambda)-\Delta_{\text{sig}}(\hat{\lambda})| \leqslant |\sigma_1(\lambda)-\sigma_1(\hat{\lambda})|+|\sigma_0(\lambda)-\sigma_0(\hat{\lambda})| \leqslant 2|\lambda-\hat{\lambda}| \leqslant \varepsilon_{\text{vec}}$. So $\Delta_{\text{sig}}(\hat{\lambda}) \geqslant \Delta_{\text{sig}}(\lambda)-\varepsilon_{\text{vec}}$. Because $\Delta_{\text{sig}}(\lambda) \geqslant K^{-1}\Delta_{\text{eig}}(\lambda)$, when $\varepsilon_{\text{vec}} \leqslant \frac{1}{2}K^{-1}\Delta_{\text{eig}}(\lambda)$, we have $\Delta_{\text{sig}}(\hat{\lambda}) \leqslant \frac{1}{2}K^{-1}\Delta_{\text{eig}}(\lambda)$. Combining with Theorem. 8, we achieve Theorem. 9. □

Note that in Theorem. 9, the prefactor $\frac{1}{2}$ for the upper bound of ε_{vec} can be replaced by any constant within $(0,1)$.

The total complexity of eigenvector state preparation can be obtained by combining Theorem. 1 or 2 for stage 1 with Theorem. 8 or Theorem. 9 for stage 2.

VII. Applications

A. Dissipation of open quantum system: Liouvillian gap

The dynamics of a close quantum system is described by Schrodinger's equation with an Hermitian Hamiltonian. When the system to be studied has interactions with its environment, however, the evolution goes beyond Hermiticity. This type of open

quantum system can be modeled by the Lindblad master equation. Under Markov approximation, the evolution of a quantum state described by density matrix ρ can be generally expressed as

$$\dot{\rho} = \mathcal{L}(\rho) \equiv -i[H,\rho] + \sum_{\mu}\left(-\frac{1}{2}L_\mu^\dagger L_\mu \rho - \frac{1}{2}\rho L_\mu^\dagger L_\mu + L_\mu \rho L_\mu^\dagger\right) \tag{S-65}$$

for some Hermitian Hamiltonian H and dissipators L_μ which are not necessarily to be non-Hermitian.

1. *Vectorization and Block-encoding of Liouvillian*

$$\dot{\rho} = -i[H,\rho] + \sum_{\mu}\left(L_\mu \rho L_\mu^\dagger - \frac{1}{2}\left\{L_\mu^\dagger L_\mu, \rho\right\}\right) \equiv \mathcal{L}(\rho) \tag{S-66}$$

for some Hermitian Hamiltonian H and non-Hermitian dissipators L_μ that can be decomposed in the form of

$$H = \sum_j \alpha_j V_{0,j}, \tag{S-67}$$

$$L_\mu = \sum_j \sqrt{\alpha_{\mu,j}} V_{\mu,j}, \tag{S-68}$$

where $\alpha_j, \beta_{j,\mu} > 0$. The "square' in Eq. (S-68) is to ensure that the Hermitian and non-Hermitian terms in Eq. (S-66) have the same units. V_j, $V_{k,\mu}$ are unitaries that can be implemented efficiently on quantum devices. Here, as an example, we only focus on qubit system. By abuse of notations, we let I, X, Y, Z be the single-qubit identity and Pauli operators in this section. We assume that $V_{\mu,j} \in \mathbb{P}^{\otimes n}$ is n-qubit Pauli string up to a phase, with $\mathbb{P} = \{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\}$. With abuse of notations, Several examples of the dissipation terms are provided in Table. S-I. Accordingly, we define a normalization factor $C = \sum_{\mu=0}\sum_j \alpha_{\mu,j}$ and assume that $C = \text{poly}(n)$.

By performing vectorization, Eq. (S-66) is equivalent to $\dot{\tilde{\rho}} = \tilde{\mathcal{L}} \cdot \tilde{\rho}$, where

$$\tilde{\rho} = \sum_{m,n} \rho_{mn} |m\rangle \otimes |n\rangle \tag{S-69}$$

and

$$\tilde{\mathcal{L}} = \sum_{\mu=0} \tilde{\mathcal{L}}_\mu, \tag{S-70}$$

$$\tilde{\mathcal{L}}_0 = -iH \otimes I^{\otimes n} + iI^{\otimes n} \otimes H^T, \tag{S-71}$$

$$\tilde{\mathcal{L}}_{\mu\geqslant 1} = \left(L_\mu \otimes L_\mu^* - \frac{1}{2}L_\mu^\dagger L_\mu \otimes I^{\otimes n} - \frac{1}{2} I^{\otimes n} \otimes L_\mu^T L_\mu^*\right). \tag{S-72}$$

Accordingly, we have

$$\tilde{\mathcal{L}}_0 = \sum_j \alpha_0 (V_j \otimes I^{\otimes n}) + i\alpha_j (I^{\otimes n} \otimes V_j^T), \tag{S-73}$$

$$\tilde{\mathcal{L}}_{\mu\geqslant 1} = \sum_{j,k} \sqrt{\alpha_{\mu,j}\alpha_{\mu,k}}\left(V_{\mu,j} \otimes V_{\mu,k}\right) - \frac{1}{2}\sqrt{\alpha_{\mu,j}\alpha_{\mu,k}}\left(V_{\mu,j}^\dagger V_{\mu,k} \otimes I^{\otimes n}\right) - \frac{1}{2}\sqrt{\alpha_{\mu,j}\alpha_{\mu,k}}\left(I^{\otimes n} \otimes V_{\mu,j}^T V_{\mu,k}^*\right). \tag{S-74}$$

Due to the following relations,

$$I^* = I, X^* = X, Y^* = -Y, Z^* = Z, \tag{S-75}$$

$$I^T = I, X^T = X, Y^T = -Y, Z^T = Z, \tag{S-76}$$

$\tilde{\mathcal{L}}$ is also a linear combination of Pauli strings with normalization factor

$$\tilde{C} = 2\left(\sum_j \alpha_j + \sum_\mu \sum_{j,k} \sqrt{\alpha_{\mu,j}\alpha_{\mu,k}}\right) \tag{S-77}$$

$$\leqslant 2\left(\sum_j \alpha_j + \sum_\mu \sum_j \alpha_{\mu,j}\right) \tag{S-78}$$

$$= 2C. \tag{S-79}$$

In other words, we can express the vectorized Liouvillian in the form of

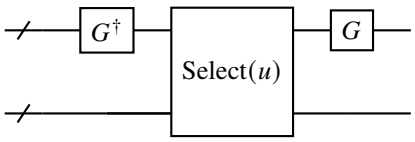
$$\tilde{\mathcal{L}}/\tilde{C} = \sum_{j=0}^{J} \beta_j u(j) \tag{S-80}$$

for some $\sum_j \beta_j = 1$, $J = \mathrm{poly}(n)$, $u_j \in \mathbb{P}^{\otimes n}$ and $\tilde{C} = 2C$.

We then show how to perform block-encoding of Eq. (S-80) based on the linear combination of unitaries [20]. Let $G|0\rangle = \sum_j \sqrt{\beta_j}|j\rangle$ and $\mathrm{Select}(u) = \sum_j |j\rangle\langle j| \otimes u(j)$, it can be verified that

$$\left(\langle 0| \otimes I^{\otimes n}\right)\left(G^\dagger \otimes I^{\otimes n}\right)\mathrm{Select}(u)\left(G \otimes I^{\otimes n}\right)\left(|0\rangle \otimes I^{\otimes n}\right) = \tilde{L}/\tilde{C}. \tag{S-81}$$

So the following circuit is the block-encoding of $\tilde{\mathcal{L}}/\tilde{C}$, which can be constructed with $O(n)$ qubits and $O(J\mathrm{polylog}(n))$ circuit depth.



Supplementary Table S-I:

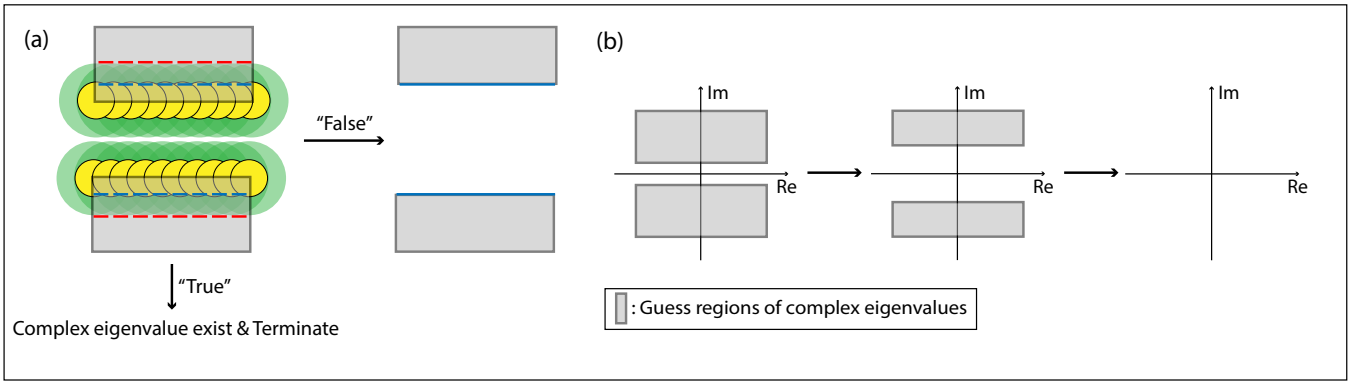
Dissipation type	Lindbladian term	$\tilde{\mathcal{L}}_\mu$
Dephasing	$\eta(Z\rho Z - \rho)$	$\eta(Z\otimes Z - I\otimes I)$
Depolarization	$\frac{\eta}{3}(X\rho X + Y\rho Y + Z\rho Z - 3\rho)$	$\frac{\eta}{3}(X\otimes X + Y\otimes Y + Z\otimes Z - 3I\otimes I)$
Damping	$\eta(\sigma^-\rho\sigma^+ - \sigma^+\sigma^-\rho - \rho\sigma^+\sigma^-)$	$\frac{\eta}{4}(X\otimes(X+iY) + Y\otimes(iX-Y) - Z\otimes I - I\otimes(Z+2I))$

2. *Liouvillian gap (LG)*

As mentioned in the main text, LG is defined as the smallest distance between the distance between imaginary axis and the eigenvalues excluding those in the imaginary axis. So the LG of $\tilde{\mathcal{L}}/\tilde{C}$ is equivalent to the line gap problem (Problem. 3) with L the imaginary axis. To achieve accuracy ε of $\tilde{\mathcal{L}}$, we should achieve accuracy $\varepsilon/\tilde{C}$ of $\tilde{\mathcal{L}}/\tilde{C}$. So we have the following result.

Theorem 10. *Given a Lindblad master equation described by Eq.* (S-66)- (S-68)*, and promised that the corresponding LG is larger than ε, the LG can be estimated to accuracy ε with $\tilde{O}(K^3(\varepsilon/C)^{-3m_{\max}+2}\gamma^{-1})$ queries to $\tilde{\mathcal{P}}_{\tilde{\mathcal{L}}}$ and extra circuit depth, and $O(n)$ ancillary qubits. Here, K is the Jordan condition number of $\tilde{\mathcal{L}}$, and $m_{\max}$ is the largest dimension of the Jordan block for $\tilde{\mathcal{L}}$.*

In Sec. VIII, we will further introduce a decision version of the LG problems, and show that it is BQP-complete.



Supplementary Figure S4: Solution to Problem. 5. (a) Sketch of each iterations in searching complex eigenvalues. If one of the SVTSs has output true, we terminate the algorithm and conclude the witness of complex eigenvalues. If all SVTSs has output "False", we shrink the search region. (b) If no complex eigenvalues are witnessed, the search region is updated iteratively until it vanishes.

B. non-Hermitian Hamiltonian: symmetry breaking witness

1. *Shrodinger equation with non-Hermitian Hamiltonian*

Effective non-Hermitian Hamiltonian has been widely used in studying open quantum physics, which may emerge from different backgrounds. In below, we introduce one of the most typical derivations from the short-time limit of Lindblad master equation, although its applicability is much broader.

The dissipation terms of the Lindblad master equation, i.e. Eq. (S-66), can be separated into two parts. The first part $\mathcal{L}_{\text{con}}(\rho) = \sum_\mu -\frac{1}{2}L_\mu^\dagger L_\mu \rho - \frac{1}{2}\rho L_\mu^\dagger L_\mu$ is called *continuous* dissipation terms, and the second part $\mathcal{L}_{\text{jump}}(\rho) = \sum_\mu L_\mu \rho L_\mu^\dagger$ is called *quantum jump* terms. When the evolution time τ is relatively small, for example $\tau < \|L_\mu L_\mu^\dagger\|$, the jump term can be neglected and the evolution reduces to

$$\dot{\rho} = -i[H,\rho] + \sum_\mu \left(-\frac{1}{2}L_\mu^\dagger L_\mu \rho - \frac{1}{2}\rho L_\mu^\dagger L_\mu\right). \tag{S-82}$$

We define

$$H_{\text{eff}} = H - \frac{1}{2}iL_\mu^\dagger L_\mu. \tag{S-83}$$

It can be verified that Eq. (S-82) is equivalent to

$$\dot{\rho} = -i[\rho H_{\text{eff}} - \rho H_{\text{eff}}^\dagger]. \tag{S-84}$$

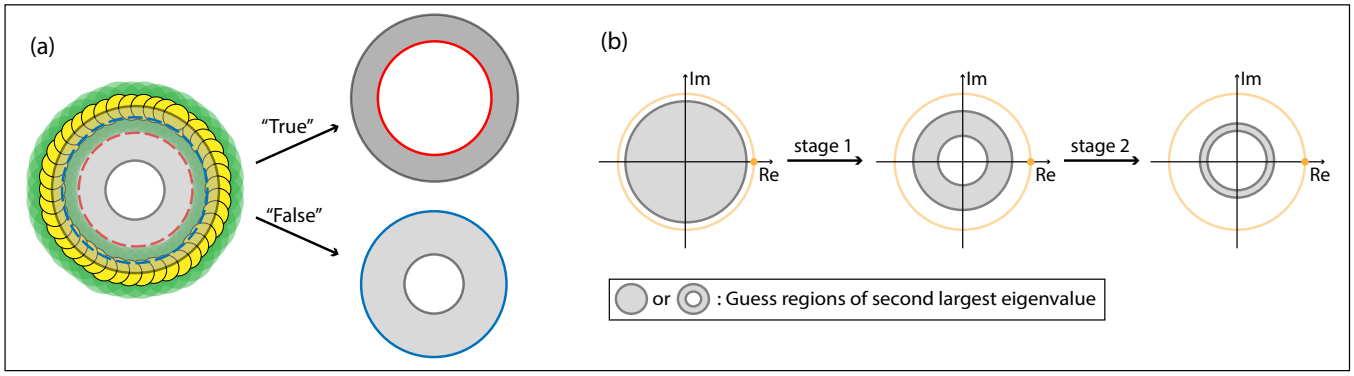
Instead of density matrix, we may characterize the quantum state with an *unnormalized* wavefunction $|\psi\rangle$. It can be verified that when $\rho = |\psi\rangle\langle\psi|$, Eq. (S-82) is equivalent to the following non-Hermitian Shrodinger equation

$$|\dot{\psi}\rangle = -iH_{\text{eff}}|\psi\rangle. \tag{S-85}$$

So the system can be characterized by the effective Hamiltonian H_{eff}, which is in general non-Hermitian.

2. *Spectrum reality and spontaneous symmetry breaking*

Following the conventions in [4–6], we let $\mathcal{T}$ be the antilinear complex-conjugation operator which act as the time-reversal operator, i.e. $\mathcal{T}|\psi\rangle = |\psi\rangle^*$. Note that Because $\mathcal{T}^2 = I$, we have $\mathcal{T}^{-1} = \mathcal{T}$. Here, we consider a slightly more general cases than the parity-time symmetry. More specifically, we let S be an arbitrary invertible matrix, and say that a matrix H has $S\mathcal{T}$-symmetry if



Supplementary Figure S5: Solution to Problem. 6. (a) Sketch of each iterations in estimating the absolute gap of eigenvalues. (b) The guess region of $\lambda'_{\max}$, the second largest absolute value of eigenvalues, is updated iteratively.

$$H = S\mathcal{T}H(S\mathcal{T})^{-1}. \tag{S-86}$$

Suppose $H|v\rangle = \lambda|v\rangle$, we have

$$HS\mathcal{T}|v\rangle = S\mathcal{T}H\mathcal{T}^{-1}S^{-1}(S\mathcal{T}|v\rangle) = S\mathcal{T}H|v\rangle = S(\lambda^*|v\rangle^*) = \lambda^* S|v\rangle^* = \lambda^* S\mathcal{T}|v\rangle. \tag{S-87}$$

So $S\mathcal{T}|v\rangle$ is also an eigenvector of H with eigenvalue λ^*. If λ is real, $S\mathcal{T}|v\rangle$ and $|v\rangle$ are linearly dependent, and hence $|v\rangle$ is invariant under the transformation of $S\mathcal{T}$, i.e. preserves the $S\mathcal{T}$-symmetry. One the other hand, whenever λ is a complex value, $S\mathcal{T}|v\rangle$ and $|v\rangle$ have different eigenvalues and hence linearly independent. So for $|v\rangle$, the $S\mathcal{T}$-symmetry is spontaneously broken.

Therefore, the complex eigenvalue serves as a witness for $S\mathcal{T}$-symmetry breaking. In the next section, we discuss the search for complex eigenvalue with quantum computing.

3. *Quantum computing witness of spontaneous symmetry breaking*

As mentioned above, the complex eigenvalue for an $S\mathcal{T}$-symmetry matrix serves as a witness of the spontaneous $S\mathcal{T}$-symmetry breaking. We therefore consider the following problem.

Problem 5. *Given a square and diagonalizable matrix A with $\|A\| \leqslant 1$. Output "True" if there exist eigenvalue λ_j satisfying $Im(\lambda_j) > \varepsilon$; Output "False" if all eigenvalues are real. For other scenarios, output either "True" or "False".*

For simplicity, we have assumed that A is diagonalizable here, although the generalization to defective case is straightforward. Our solution to Problem. 5 is given in Algorithm. 5. As sketched in Fig. S4, at each iteration, we are confidence that there are no eigenvalues with imaginary part $\mathrm{Im}(\lambda_j) \in [\varepsilon, b]$. We update b iteratively by querying a set of SVTSs. The algorithm is terminates whenever an SVTS has output true. In this case, we witness a complex eigenvalue. On the other hand, if b increases consistently until $b \geqslant 1$ (notice that we always have $|\lambda_j| \leqslant 1$), we judge that no complex eigenvalues are witnessed, and terminate the algorithm.

The success probability can achieve a constant level for sufficiently small δ', and the runtime of Algorithm. 5 is similar to Algorithm. 3 and Algorithm. 5 for point gap and line gap estimations. So we have the following theorem.

Theorem 11. *With success probability at least $1-\delta$, Problem. 5 can be solved with*

$$\tilde{O}(K^3\varepsilon^{-2}\gamma^{-1}) \tag{S-88}$$

queries to $\mathcal{Q}_A$, $\mathcal{P}_A$, and extra single- and two-qubit gates.

C. Markov process: absolute gap and relaxation time

We formalize the absolute gap problem can be formalized as follows.

Problem 6. *Let A be a stochastic matrix describing a Markov process. We further assume that A is diagonalizable, and $\|A\| \leqslant C$ for some constant C. Let $g_{ab} = \lambda_{\max} - \max_{\lambda_j \neq \lambda_{\max}} |\lambda_j|$ be the absolute gap with promise that $g_{ab} \geqslant \Delta$ for some $\Delta > \varepsilon$. Output an estimation g'_{ab} of the absolute gap with accuracy $|g'_{ab} - g_{ab}| \leqslant \varepsilon$.*

Here, we have restricted our discussion to diagonalizable case, although the generalization to defective case is possible with a similar process to Sec. III, IV.

For stochastic matrix, we always have $\|A\| \geqslant 1$, so we should consider the block-encoding of a rescaled A instead. More specifically, we consider $\tilde{A} = A/C$ for some constant $C \geqslant \|A\|$, and let $\mathcal{O}_{\tilde{A}}$ be the block-encoding of $\tilde{A}$. The maximal eigenvalue of $\tilde{A}$ is $1/C$. In below we study the estimation of the absolute gap of $\tilde{A}$ instead, which is related to the absolute gap of A by a factor of $1/C$.

With a slight abuse of notation, we let $\lambda'_{\max}$ be the second largest absolute value of the eigenvalues of $\tilde{A}$. We initially have $\lambda'_{\max} \in [0, (1-\Delta)/C]$. In our algorithm (provided in Algorithm. 12), $\lambda'_{\max}$ is updated iteratively. We suppose that the guess region of $\lambda'_{\max}$ before each iteration is $\lambda'_{\max} \in [R^{\min}, R^{\max}]$. As illustrated in Fig. S5, we query a set of SVTSs with centers $\mu \in \mathcal{N}_{\text{ring}}(R^{\max}, (1-R^{\max})/K)$. The inner regions of these SVTSs covers the circle with radius $R^{\max}$. If all SVTS has output "False", $R^{\max}$ is updated; if either of the SVTS has output "True", we update the $R^{\min}$. This process is encapsulated as an eigenvalue range shrinking subroutine, $\mathcal{S}_{\text{ag}}$, defined in Algorithm. 13. The update process contains separated into two stages. In stage 1, the radius of the outer region of each SVTS is $1 - R^{\max}$. In stage 2, the radius is $(R^{\max} - R^{\min})/2$ instead.

The complexity of the Algorithm. 12 is similar to Algorithm. 3 for solving Problem. 2, with ε replaced by ε/C, i.e. $\tilde{O}(K^3(\varepsilon/C)^{-2}\gamma^{-1})$. So we have the following result.

Theorem 12. *Let $\mathcal{O}_{\tilde{A}}$ be the block encoding of matrix $\tilde{A} \equiv A/C$ for some $C \geqslant \|A\|$. Problem. 6 can be solved with $\tilde{O}(C^2K^3\varepsilon^{-2}\gamma^{-1})$ queries to $\mathcal{O}_{\tilde{A}}$ and $\mathcal{P}_A$.*

Moreover, we can estimate the relaxation time based on Theorem. 12. The relaxation time of the Markov process is defined as $\tau_{\text{rel}} \equiv 1/g_{\text{ab}}$, and its absolute accuracy is $\varepsilon_{\text{rel}} = \Delta\tau_{\text{rel}}/\tau_{\text{rel}}$. We can define $\tau_{\text{bnd}} = 1/\Delta$ as the promised upper bound of τ_{rel}, which gives $\varepsilon_{\text{rel}} \sim \tau^2_{\text{bnd}}\varepsilon$. Accordingly, we can be estimate the relaxation time with complexity $\tilde{O}(\tau^2_{\text{bnd}}C^2K^3\varepsilon^{-2}_{\text{rel}}\gamma^{-1})$. While this represents the first efficient query complexity result for the relaxation time, we believe there is still much room for improvement.

VIII. Quantum advantage analysis

In this section, we discuss the quantum advantage of our algorithms. We take the Liouvillian gap problem as an example, while the method can be applied to other related problems, such as the witness of PT-symmetry breaking.

To facilitate our discussion, we first formally define a decision version of the Liouvillian gap problem as follows.

Problem 7 (decision version of the Liouvillian gap problem)**.**
Input:

(1) Constants $\gamma, a, b \in (0, 1]$ such that $\Delta = b - a > 0$.

(2) An n-qubit Liouvillian operator $\mathcal{L}$, and block encoding unitary of its rescaled vectorized form $\mathcal{O}_{\tilde{\mathcal{L}}}$.

(3) State preparation unitary $\mathcal{P}^{eig}_{\mathcal{L}}$ satisfying $\mathcal{P}^{eig}_{\mathcal{L}}|0\rangle = |\psi^{ini}\rangle$.

Let g be the Liouvillian gap of $\tilde{\mathcal{L}}$, we are promised that:

(i) $\mathcal{O}_{\tilde{\mathcal{L}}}$ can be constructed with polynomial-size quantum circuit;

(ii) $\tilde{\mathcal{L}}$ is diagonalizable, and the Jordan condition number of $\tilde{\mathcal{L}}$ is upper bounded by $K = O(poly(n))$;

(iii) $\mathcal{P}^{eig}_{\mathcal{L}}$ can be constructed with polynomial-size quantum circuit. Let λ be an eigenvalue of $\tilde{\mathcal{L}}$ satisfying $|Re(\lambda) + g| \leqslant \Delta\gamma/K$. Let Π_λ be the projection onto the subspace spanned by eigenvectors of $\tilde{\mathcal{L}}$, whose corresponding eigenvalues λ_j satisfies $|\lambda - \lambda_j| \leqslant \Delta$. We have $\left\|\Pi_{\tilde{\mathcal{L}}}|\psi_{ini}\rangle\right\| = \gamma$;

(iv) Either $g \leqslant a$ or $g \geqslant b$ are satisfied;

Output "True" when $g \leqslant a$ and output "False" when $g \geqslant b$.

We will show that Problem. 7 is BQP-complete and hence provides exponential quantum speedup, unless universal quantum circuit can be efficiently simulated on a classical computer.

We note that (i) indicates that $\|\tilde{\mathcal{L}}\| \leqslant 1$. In practice, this can be satisfied by performing rescaling. We also note that the state preparation assumption here is weaker than the one used in the main text. It can be satisfied by an initial state with nontrivial overlap to the eigenvectors, whose corresponding eigenvalues are close to the line defined by the Liouvillian gap. This revision is important for the Hamiltonian-to-Liouvillian mapping in order to proof the BQP-hardness (Sec. VIII B). Moreover, with this weaker assumption, we can still solve the Liouvillian gap problem efficiently (Sec. VIII A).

A. BQP of Problem. 7

In this section, we assume that $\tilde{\mathcal{L}}$ is diagonalizable and $\|\tilde{\mathcal{L}}\| \leqslant 1$ as suggested by Problem. 7. We denote the eigenvector associated to λ [i.e. the one satisfying $|\mathrm{Re}(\lambda) + g| \leqslant \Delta\gamma/K$ defined in promise (iii)] as $|v\rangle$. We also denote $\{(\lambda_j, |v_j\rangle)\}$ as the set containing all pairs of eigenvalues and eigenvectors.

In the first step, we construct a quantum circuit filtering small singular values of a matrix

$$\tilde{\mathcal{L}}' = \frac{\tilde{\mathcal{L}} - \mu I}{1 + |\mu|} \tag{S-89}$$

for some $|\mu| \leqslant 1$. To facilitate the discussion, we consider the singular value decomposition in the form of Eq. (S-54). Because μ is fixed in most cases of our discussion, we use the abbreviation $\tilde{\mathcal{L}}' = \sum_j s_j |w_j\rangle\langle u_j|$ for simplicity. We then introduce a projection operator

$$\Pi_{\varepsilon/2}^{(\mathrm{sig})} \equiv \sum_{j \in \{j' | s_{j'} \leqslant \varepsilon/2\}} |u_j\rangle\langle u_j|, \tag{S-90}$$

which projects the state into the subspace spanned by right singular vectors corresponding to $s_j \leqslant \varepsilon/2$, and we have the following result.

Lemma 11. *For arbitrary quantum state $|\psi\rangle$, suppose $|\langle v|\psi\rangle| \geqslant \gamma$ and $|\mu - \lambda| \leqslant \varepsilon\gamma/4$, we have $\|\Pi_{\varepsilon/2}^{(sig)}|\psi\rangle\| \geqslant \gamma/2$.*

Proof. We decompose $|v\rangle$ and $|\psi\rangle$ using the right singular vector of $\tilde{\mathcal{L}}'$ (see Eq. (S-89)) as follows

$$|v\rangle = \sum_j \alpha_j(v)|u_j\rangle, \qquad |\psi\rangle = \sum_j \alpha_j(\psi)|u_j\rangle, \tag{S-91}$$

which satisfies $\left|\sum_j \alpha_j(v)\alpha_j(\psi)\right| \geqslant \gamma$. According to the triangular inequality, we also have

$$\sum_j \left|\alpha_j(v)\alpha_j(\psi)\right| \geqslant \left|\sum_j \alpha_j(v)\alpha_j(\psi)\right| \geqslant \gamma. \tag{S-92}$$

Because $|\mu - \lambda| \leqslant \varepsilon\gamma/4$, we have $\|\tilde{\mathcal{L}}'|v\rangle\| \leqslant \left\|\frac{M-\mu I}{1+|\mu|}|v\rangle\right\| \leqslant \varepsilon\gamma/4$, which is equivalent to $\sqrt{\sum_j s_j^2 \alpha_j(v)^2} \leqslant \varepsilon\gamma/4$. Therefore,

$$\sqrt{\sum_{j \in \{j' | s_{j'} > \varepsilon/2\}} \alpha_j(v)^2} \leqslant (\varepsilon/2)^{-1} \sqrt{\sum_{j \in \{j' | s_{j'} > \varepsilon/2\}} s_j^2 \alpha_j(v)^2} \leqslant \gamma/2. \tag{S-93}$$

Using Cauchy-Schwarz inequality and notice that $\sqrt{\sum_{j \in \{j' | s_{j'} > \varepsilon/2\}} \alpha_j(\psi)^2} \leqslant 1$, we have

$$\sum_{j \in \{j' | s_{j'} > \varepsilon/2\}} |\alpha_j(v)\alpha_j(\psi)| \leqslant \gamma/2. \tag{S-94}$$

Combining with Eq. (S-92), we have

$$\sum_{j\in\{j'|s_{j'}\leqslant\varepsilon/2\}}\left|\alpha_j(v)\alpha_j(\psi)\right| \geqslant \gamma - \sum_{j\in\{j'|s_{j'}>\varepsilon/2\}}\left|\alpha_j(v)\alpha_j(\psi)\right| \geqslant \gamma/2. \tag{S-95}$$

Using Cauchy-Schwarz inequality again, we have

$$\begin{aligned}\sum_{j\in\{j'|s_{j'}\leqslant\varepsilon/2\}}\left|\alpha_j(v)\alpha_j(\psi)\right| &\leqslant \sqrt{\left(\sum_{j\in\{j'|s_{j'}\leqslant\varepsilon/2\}}\left|\alpha_j(v)\right|^2\right)\left(\sum_{j\in\{j'|s_{j'}\leqslant\varepsilon/2\}}\left|\alpha_j(\psi)\right|^2\right)}\\ &\leqslant \sqrt{\left(\sum_{j\in\{j'|s_{j'}\leqslant\varepsilon/2\}}\left|\alpha_j(\psi)\right|^2\right)}\\ &= \left\|\Pi^{(\mathrm{sig})}_{\varepsilon/2}|\psi\rangle\right\|.\end{aligned} \tag{S-96}$$

Combining Eq. (S-95) with Eq. (S-96), we have

$$\left\|\Pi^{(\mathrm{sig})}_{\varepsilon/2}|\psi\rangle\right\| \geqslant \gamma/2. \tag{S-97}$$

□

We can generalize the argument of Lemma. 11 to the case when the *projection* to a subspace spanned by $|v-j\rangle$, whose eigenvalues are close to λ. More specifically, it is straightforward to obtain the following result from Lemma. 11.

Lemma 12. *Let $\Pi^{eig}_{\lambda,\varepsilon\gamma/4}$ be the projection onto the subspace spanned by $|v_j\rangle$, whose corresponding eigenvalues satisfy $|\lambda_j-\lambda|\leqslant\varepsilon\gamma/4$. Then, we have $\|\Pi^{(sig)}_{\varepsilon/2}|\psi\rangle\|\geqslant\gamma/2$.*

Using the same technique in Sec. I for constructing SVTS, and combine with Lemma. 12, we can also construct a singular value threshold subroutine, which verifies whether we are close to an eigenvalue of matrix $\mathcal{L}$ (i.e. λ) or not.

Lemma 13. *We consider a subroutine $O'_C(\mu,\varepsilon,\delta)$ with output either "True" or "False", which satisfying the following*
(1) If $|\mu-\lambda|\leqslant\varepsilon\gamma/4K$, output "True" with probability at least $1-\delta$;
(2) If the output of $O'_C(\mu,\varepsilon,\delta)$ is "True", $\min_{\lambda_j}|\mu-\lambda_j|\leqslant\varepsilon$ with probability at least $1-\delta$.
Then, $O'_C(\mu,\varepsilon,\delta)$ can be constructed with $\tilde{O}(K\varepsilon^{-1}\gamma^{-2})$ queries to $\mathcal{O}_{\mathcal{L}}$ and $\mathcal{P}^{eig}_{\mathcal{L}}$, and extra single- and two-qubit gates.

Details of the proof will be provided in the future version of the manuscript.

O'_C determines two disks with center μ. The small disk has radius $\varepsilon\gamma/4K$. If λ is in this disk, the output of $O'_C(\mu,\varepsilon,\delta)$ is "True". We can introduce multiple oracles, such that the small disks covers the region $\mathcal{D}(0,1)$. In this way, there exist at least one oracle, such that the output is "True" (with high probability). In practice, we require at most $O(\mathrm{poly}(K,\varepsilon^{-1},\gamma^{-1}))$ number of oracles. The algorithm for solving Problem. 7 works as follows. We record the center of oracles that has largest real part, denoted as μ'. If $\mathrm{Re}(\mu')\leqslant(a+b)/2$, we output "True"; if $\mathrm{Re}(\mu')>(a+b)/2$ we output "False". To ensure that the correctness of the output, it suffices to set $\varepsilon=O(\Delta)$, where $\Delta=b-a$. Therefore, the total number of oracles, and hence the total runtime is upper bounded by $O(\mathrm{poly}(K,\Delta^{-1},\gamma^{-1}))$. In other words, we have the following result.

Theorem 13. *For arbitrary $K,\Delta^{-1},\gamma^{-1}=O(poly(n))$, with success probability $2/3$, Problem. 7 can be solved with polynomial-size quantum circuit.*

Note that the success probability may be replace by arbitrary constant in $(0.5,1)$.

B. BQP-hardness of problem. 7

Our strategy of proofing BQP-hardness is as follows. First, we consider a type of ground state problems of local guided Hermitian matrix problems that are known to be BQP-hard. Second, we construct a mapping from these ground state problems to specific instances of Problem. 7. This establishes the BQP-hardness of Problem. 7.

We begin with the BQP-hardness result of local Hermitian matrices.

Problem 8 (GLH(k, a, b, γ))**.** *Given a k-local Hermitian matrix*

$$H = \sum_{p=1}^{P} \alpha_p u_p \tag{S-98}$$

acting on n qubits. Promised that:

(1) $P = O(poly(n))$, $\sum_p |\alpha_p| = O(poly(n))$, and $\|H\| \leqslant 1$.

(2) Either $\lambda_H \leqslant a_H$ or $\lambda_H \geqslant b_H$ holds.

(3) We can prepare a classical description of $O(1)$-sparse quantum state $|\psi_H\rangle$. Let Π_H be the projection operator onto the vector space spanned by the ground states of H, we have $\|\Pi_H|\psi_H\rangle\| \geqslant \gamma_H$

(4) We can efficiently prepare another quantum state $|\psi_H^{\perp}\rangle$such that $\|\Pi_{H,b_H}|\psi_H^{\perp}\rangle\| = \Omega(1)$, where Π_{H,b_H} is the projection of operator onto the vector space spanned by eigenvectors, whose corresponding eigenvalue is larger than b_H;

The goal is to output "False" when $\lambda_H \leqslant a_H$, and output "True" when $\lambda_H \geqslant b_H$.

Problem. 8 is almost the same as the guided local Hamiltonian problem defined in [44]. The only difference is that we have introduced promise (2), which is useful for our mapping from H to the Liouvillian gap problem. We note that with the Hamiltonian construction in [44] for proving its BQP-hardness, promise (2) can be easily achieved with some trivial initial states, such as all qubits at state $|0\rangle$ except that register A is at a product state orthogonal to the $|x\rangle$, i.e. the input state of the corresponding circuit to be mapped. So BQP-hardness is still applied, and we have the following result.

Lemma 14 (Adapted from Theorem 1.2 of [44])**.** *There exists parameters $\gamma_H, a_H, b_H \in [0, 1]$ with $b_H - a_H = \Omega(1/poly(n))$, such that GLH$(6, a_H, b_H, \gamma_H)$ is BQP-hard.*

We then consider the mapping of Problem. 8 to Problem. 7. To begin with, we consider a polynomial approximation of the sign function.

Lemma 15 (Adapted from [50])**.** *For arbitrary $a, b \in [-1, 1]$ satisfying $\Delta \equiv b - a = \Omega(1/poly(n))$ and $\varepsilon \in (0, 1]$, there exists a d-degree polynomial $f_{sgn,a,b,\varepsilon}(x) = \sum_{j=0}^{d} \alpha_j x^j$ for some $d = \tilde{O}(\Delta)$, which satisfies*

$$\min_{x\in[-1,a]\cup[b,1]} |f_{sign,a,b,\varepsilon}(x) - sign(x - (a + b)/2)| \leqslant \varepsilon, \tag{S-99}$$

and $\sum_j |\alpha_j| = O(poly(n))$.

The main idea of our construction is as follows. Based on Lemma. 15, we define a polynomial of matrix as $A = f_{\text{sgn},a_H,b_H,\varepsilon}(H) = \sum_{j=0}^{d} \alpha_j H^j$. It can be verified that when the minimum eigenvalue of H satisfies $\lambda_{\min}(H) \leqslant a_H$, we have $\lambda_{\min}(A) \leqslant -1 + \varepsilon$, and when $\lambda_{\min}(H) \geqslant b_H$, we have $\lambda_{\min}(A) \geqslant 1 - \varepsilon$. Based on A, the Liouvillian operator is constructed as $\dot{\rho} = \mathcal{L}(\rho) = A\rho A^\dagger - \frac{1}{2}A^\dagger A\rho - \frac{1}{2}\rho A^\dagger A$. It can be verified that in the former case, $\mathcal{L}$ has a large Liouvillian gap, and in the later case, the Liouvillian gap is small. Based on this property, we achieve the following result.

Lemma 16. *Given an arbitrary 6-local Hermitian matrix H in the form of Eq. (S-98). Promised that (1)-(4) in Problem. 8 are satisfied, and $\gamma_H, a_H, b_H \in [0, 1]$ with $b_H - a_H = \Omega(1/poly(n))$. Then, there exists $\varepsilon = \Omega(1/poly(n))$ and $C = O(poly(n))$ satisfying the following. Let*

$$A = f_{sgn,a_H,b_H,\varepsilon}(H) = \frac{1}{C}\sum_{j=0}^{d} \alpha_j H^j, \tag{S-100}$$

and

$$\mathcal{L}(\rho) = A\rho A^\dagger - \frac{1}{2}A^\dagger A\rho - \frac{1}{2}\rho A^\dagger A. \tag{S-101}$$

The vectorized Liouvillian operator $\tilde{\mathcal{L}}$ of $\mathcal{L}(\rho)$ satisfies all promise (i)-(iv) in Problem. 7 with $a = \varepsilon/2C^2$, $b = (1 - 2\varepsilon)/2C^2$ and some $\gamma = \Omega(1)$. Moreover, the Liouvillian gap of $\tilde{\mathcal{L}}$ satisfies $g \geqslant b$ when $\lambda_{\min}(H) \leqslant a_H$, and $g \leqslant a$ when $\lambda_{\min}(H) \geqslant b_H$.

Proof. The vectorized Liouvillian operator is

$$\tilde{\mathcal{L}} = A \otimes A^* - \frac{1}{2}\left(A^\dagger A \otimes I^{\otimes n} + I^{\otimes n} \otimes (A^\dagger A)^*\right) \tag{S-102}$$

$$= A \otimes A^* - \frac{1}{2}\left(A^2 \otimes I^{\otimes n} + I^{\otimes n} \otimes (A^2)^*\right). \tag{S-103}$$

According to Lemma. 15, the block-encoding of $\tilde{\mathcal{L}}$ can be efficiently constructed for some appropriate $C = \mathrm{poly}(n)$. The block encoding of A^* is similar, and the block encoding of $\tilde{\mathcal{L}}$ can be constructed using linear combination of unitaries of $A \otimes A^*$, $A^2 \otimes I^{\otimes n}$ and $I^{\otimes n} \otimes (A^2)^*$. So promise (i) is satisfied. Moreover, because $\tilde{\mathcal{L}}$ is an Hermitian matrix, promise (ii) is also satisfied.

We then consider promise (iii), (iv) and the correctness of the Liouvillian gap. We construct the nontrivial initial state preparation as

$$\mathscr{P}^{\mathrm{eig}}_{\mathcal{L}}|0\rangle = |\psi_H\rangle|\psi_H^{\perp *}\rangle, \tag{S-104}$$

where $|\psi_H\rangle$ and $|\psi_H^\perp\rangle$ are some quantum states satisfying criteria (3), (4) in Problem. 8 respectively. By definition, $\mathscr{P}^{\mathrm{eig}}_{\mathcal{L}}$ can be construct by polynomial-size quantum circuits.

We suppose $H = \sum_j \lambda_j |v_j\rangle\langle v_j|$. Then, we have $A = \sum_j \tilde{\lambda}_j |v_j\rangle\langle v_j|$, where $\tilde{\lambda}_j = f_{\mathrm{sgn},a_H,b_H,\varepsilon}(\lambda_j)$. Eq. (S-102) can be expressed as

$$\tilde{\mathcal{L}} = \sum_{j,k}\left(\tilde{\lambda}_j\tilde{\lambda}_k - \frac{1}{2}\tilde{\lambda}_j^2 - \frac{1}{2}\tilde{\lambda}_k^2\right)|v_j^*\rangle\langle v_j^*| \otimes |v_k\rangle\langle v_k| \tag{S-105}$$

$$= -\frac{1}{2}\sum_{j,k}(\tilde{\lambda}_j - \tilde{\lambda}_k)^2 |v_j\rangle\langle v_j| \otimes |v_k^*\rangle\langle v_k^*|. \tag{S-106}$$

Accordingly, the Liouvillian gap of $\tilde{\mathcal{L}}$ is

$$g = \frac{1}{2C^2}\min_{\tilde{\lambda}_j \neq \tilde{\lambda}_k} |\tilde{\lambda}_j - \tilde{\lambda}_k|^2. \tag{S-107}$$

In below, we discuss the cases $\lambda_{\min}(H) \leqslant a_H$ and $\lambda_{\min}(H) \geqslant b_H$ separately.

When $\lambda_{\min}(H) \geqslant b_H$, it can be verified that $\tilde{\lambda}_j \geqslant (1-\varepsilon)/C^2$ for all eigenvalues of A, and hence $g \leqslant \varepsilon/2C^2$. It can be verified that (iii) and (iv) can be satisfied for polynomially small ε.

The case $\lambda_{\min}(H) \leqslant a_H$ is more involved. In this case, there exists $\tilde{\lambda}_j$ such that $\tilde{\lambda}_j \leqslant \varepsilon/C^2$, so $g \geqslant (1-2\varepsilon)/2C^2$, and promised (iv) is satisfied. Let

$$\Pi_{\tilde{\mathcal{L}}} = \sum_{\lambda_j < a_H, \lambda_k < b_H} |v_j\rangle\langle v_j| \otimes |v_k^*\rangle\langle v_k^*| + |v_k\rangle\langle v_k| \otimes |v_j^*\rangle\langle v_j^*|. \tag{S-108}$$

It can be verified that $\Pi_{\tilde{\mathcal{L}}}$ is just the projection onto the subspace spanned by eigenvectors of $\tilde{\mathcal{L}}$, whose eigenvalues are smaller than a_H. Moreover, because γ_H is assumed to be a constant, it can be verified from Eq. (S-108) and criteria (3), (4) in Problem. 8 that

$$\left\|\Pi_{\tilde{\mathcal{L}}}|\psi_H\rangle|\psi_H^{\perp *}\rangle\right\| = \Omega(\gamma_H/C^2) = \Omega(1/\mathrm{poly}(n)). \tag{S-109}$$

Therefore, promise (iii) is also satisfied, which complete the proof. □

Combining Lemma. 14 with Lemma. 16, we have the following result.

Theorem 14. *There exists $K, \gamma^{-1}, \Delta^{-1} = O(poly(n))$, such that Problem. 7 is BQP-hard.*

Combining Theorem. 13 with Theorem. 14, we arrive at the following result.

Theorem 15. *There exists $K, \gamma^{-1}, \Delta^{-1} = O(poly(n))$, such that Problem. 7 is BQP-hard.*

IX. More pseudo codes

A. pseudo code for stage 1 of Problem. 3

Algorithm 5 Stage 1 for solving Problem 3

$R_0^{\min} \leftarrow \varepsilon$; $R_0^{\max} \leftarrow 1$; $j \leftarrow 1$
while $R_{j-1}^{\min} < R_{j-1}^{\max}/2$: # Substage 1
  $(R_j^{\min}, R_j^{\max}) \leftarrow \mathcal{S}_{\text{line}}(R_{j-1}^{\min}, R_{j-1}^{\max}, R_{j-1}^{\min}, \delta')$
  $j \leftarrow j+1$
end while
while $R_{j-1}^{\max} - R_{j-1}^{\min} > \varepsilon$: # Substage 2
  $(R_j^{\min}, R_j^{\max}) \leftarrow \mathcal{S}_{\text{line}}\left(R_{j-1}^{\min}, R_{j-1}^{\max}, \left(R_{j-1}^{\max} - R_{j-1}^{\min}\right)/2, \delta'\right)$
  $j \leftarrow j+1$
end while
return $\left(R_{j-1}^{\min}, R_{j-1}^{\max}\right)$

Algorithm 6 $\mathcal{S}_{\text{line}}(R_{\text{a}}, R_{\text{b}}, r, \delta)$ (Eigenvalue range shrinking subroutine for line gap problem)

$\delta' \leftarrow \delta/|\mathcal{N}_{\text{line}}(R_{\text{a}}, \tilde{\nu}(r))|$
for all $t \in \mathcal{N}_{\text{line}}(R_{\text{a}}, \tilde{\nu}(r))$:
  $B \leftarrow O_C(t, \tilde{\nu}(r), \delta')$
  if B = True:
    break for
  end if
end for
if B = True:
  $\tilde{R}_{\text{a}} \leftarrow R_{\text{a}}$
  $\tilde{R}_{\text{b}} \leftarrow R_{\text{a}} + r$
else if B = False:
  $\tilde{R}_{\text{a}} \leftarrow R_{\text{a}} + \tilde{\nu}(r)/4$
  $\tilde{R}_{\text{b}} \leftarrow R_{\text{b}}$
end if
return $\left(\tilde{R}_{\text{a}}, \tilde{R}_{\text{b}}\right)$

B. pseudo code for solving Problem. 1 in real and diagonalizable case

Algorithm 7 Eigenvalue searching for Problem 1 in real and diagonalizable case.

$D \leftarrow 1$, $\delta' \leftarrow \delta/\lceil \log_2(D/\varepsilon) \rceil$
while $D > \varepsilon$:
  $\lambda_{\text{gss}} \leftarrow \mathscr{R}_{\text{real}}\left(\lambda_{\text{gss}}, D, \delta'\right)$
  $D \leftarrow D/2$:
end while
return λ_{gss}

Algorithm 8 $\mathscr{R}_{\text{real}}(\lambda_{\text{gss}}, D, \delta)$

$\delta' \leftarrow \delta/(2 \times \lceil 2K \rceil + 1)$
for all $\mu \in \left\{ nD/2K \middle| n = 0, \pm 1, \pm 2, \cdots, \pm \lceil 2K \rceil \right\}$:
  $B \leftarrow O_C\left(\mu, D/4K, \delta'\right)$
  if B = True:
    break for
  end if
end for
return μ

C. pseudo code for solving Problem. 4 (eigenvalue gap problem in real and diagonalizable case)

Algorithm 9 Solutions to Problem. 4

$R_0^{\min} \leftarrow \varepsilon$; $R_0^{\max} \leftarrow 1$; $j \leftarrow 1$
while $R_{j-1}^{\max} - R_{j-1}^{\min} > R_{j-1}^{\min}$: # substage 1
  $\left(R_j^{\min}, R_j^{\max}, S\right) \leftarrow \mathscr{S}_{\text{real}}\left(R_{j-1}^{\min}, R_{j-1}^{\max}, R_{j-1}^{\min}\right)$
end while
while $R_{j-1}^{\max} - R_{j-1}^{\min} > \varepsilon$ **and** $S \neq 0$: # substage 2
  $\left(R_j^{\min}, R_j^{\max}, S\right) \leftarrow \mathscr{S}_{\text{real}}\left(R_{j-1}^{\min}, R_{j-1}^{\max}, (R_{j-1}^{\max} - R_{j-1}^{\min})/(2K)\right)$
end while
return $S \times (R_j^{\max} + R_j^{\min})/2$

Algorithm 10 $\mathscr{S}_{\text{real}}\left(R_a, R_b, r\right)$

$B_+ \leftarrow O_C(R_a, r/K, \delta')$
$B_- \leftarrow O_C(-R_a, r/K, \delta')$
$B = B_+ \vee B_-$
if B = False:
  $S = 0$
else if B_+ = True:
  $S = 1$
else if B_- = True:
  $S = -1$
end if
if B = True:
  $\tilde{R}_a \leftarrow R_a$
  $\tilde{R}_b \leftarrow R_b + r$
else:
  $\tilde{R}_a \leftarrow R_a(1 + 1/(2K))$
  $\tilde{R}_b \leftarrow R_b$
end if
return (R_a, R_b, S)

D. pseudo code for solving Problem. 5 (complex eigenvalue witness)

Algorithm 11 Algorithm solving Problem 5

$b \leftarrow \varepsilon$
while $b < 1$:
$\Delta a \leftarrow \lfloor b/(4K) \rfloor$
  for $a \in \{-1, -1 + \Delta a, -1 + 2\Delta a, \cdots, 1\}$:
    query $B_+ = O_C(a + ib, 2b/\Delta a, \delta')$
    query $B_- = O_C(a - ib, 2b/\Delta a, \delta')$
    if B_- = True or B_+ = True:
      Output True and **Terminate**
    end if
  end for
  $b \leftarrow b(1 + 1/(4K))$
end while
Output False

E. pseudo code for solving Problem. 6 (eigenvalue absolute gap estimation)

Algorithm 12 Solution to Problem 6

$R_0^{\min} \leftarrow 0$; $R_0^{\max} \leftarrow (1 - \Delta)/C$; $j \leftarrow 1$
while $(1 - R_{j-1}^{\max})/2 < 1 - R_{j-1}^{\min}$: # Stage 1
  $(R_j^{\max}, R_j^{\min}) \leftarrow \mathcal{S}(R_{j-1}^{\max}, R_{j-1}^{\min}, 1 - R_{j-1}^{\max}, \delta')$
  $j \leftarrow j + 1$
end while
while $R_{j-1}^{\max} - R_{j-1}^{\min} > \varepsilon/C$: # Stage 2
  $(R_j^{\max}, R_j^{\min}) \leftarrow \mathcal{S}\left(R_{j-1}^{\max}, R_{j-1}^{\min}, \left(R_{j-1}^{\max} - R_{j-1}^{\min}\right)/2, \delta'\right)$
  $j \leftarrow j + 1$
end while
return $1 - \left(\left(R_{j-1}^{\min} + R_{j-1}^{\max}\right)/2\right)$

Algorithm 13 $\mathcal{S}_{\text{ag}}(R_{\text{a}}, R_{\text{b}}, r, \delta)$

$\delta' \leftarrow \delta/|\mathcal{N}_{\text{ring}}(R_{\text{a}}, r/K)|$
for all $t \in \mathcal{N}_{\text{ring}}(R_{\text{a}}, r/K)$:
  $B \leftarrow O_C(t, r/K, \delta')$ # O_C works for the rescaled matrix $\tilde{A} = A/C$
  if B = True:
    break for
  end if
end for
if B = True:
  $\tilde{R}_{\text{a}} \leftarrow R_{\text{a}}$
  $\tilde{R}_{\text{b}} \leftarrow R_{\text{a}} - r$
else if B = False:
  $\tilde{R}_{\text{a}} \leftarrow R_{\text{a}} - r/(4K)$
  $\tilde{R}_{\text{b}} \leftarrow R_{\text{b}}$
end if
return $(\tilde{R}_{\text{a}}, \tilde{R}_{\text{b}})$

Optimal Ternary Signal Constellation and A Priori Probabilities Maximizing Capacity under Energy Constraints

Shion Kitamura[1] * Tiancheng Wang[1 2] † Souichi Takahira[3] ‡
Tsuyoshi Sasaki Usuda[1] §

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, Aichi, Japan.*
[2] *Faculty of Informatics, Kanagawa University, Kanagawa, Japan.*
[3] *Faculty of Information Engineering, Meijo University, Aichi, Japan.*

Abstract. For the efficient use of energy in quantum communication, it is better to use discrete signals that approach the classical capacity achieved by a continuous input of coherent states. The analytical treatment of the classical communication channel requires discretization. The class of BPSK coherent-state signals has been proven to be optimal in the case of binary discretization; however, for multiary discretization, the optimal signals is unknown. In this study, we consider the case of ternary discretization. We calculate the channel capacity for various signals. Our numerical calculation suggests that the optimal signal constellation is 3PSK signals.

Keywords: Quantum communication, Quantum channel capacity, Ternary discretization

1 Introduction

In quantum communication [1, 2], it is important to increase the channel capacity as much as possible within limited resources. The classical capacity of a (lossy) quantum channel is attained by continuous inputs of coherent states [3]. In particular, the capacity is asymptotically achieved by binary coherent-state signals when the average number of photons is very small, and it has been analytically proven that the optimal signal constellation in this case is the BPSK signals [4]. Ishida *et al.* applied up to 16-ary signals and showed that the energy constraint to attain the capacity widened [5]. Recently, by applying the results of [6], we showed that the calculation can be simplified [7], and by computing the capacity with discrete-valued input for a large number of signals, we found that the results of [5] can be extended [8, 9]. Furthermore, we demonstrated how the capacity with discrete-valued input changes depending on a specific digital modulation scheme or signal constellations in which the number of signals is the same [10].

However, the optimal signal constellation for coherent states when only the number of signals M is limited under the energy constraint has only been determined for $M = 2$ [4]. In this study, we consider the case of $M = 3$ and numerically determine the optimal signal constellation for coherent states.

*im233003@cis.aichi-pu.ac.jp
†wang@kanagawa-u.ac.jp
‡takahira@meijo-u.ac.jp
§usuda@ist.aichi-pu.ac.jp

2 Preliminaries

For a Hilbert space $\mathcal{H}$ of a quantum system, a set of M-ary quantum-state signals is defined as follows

$$\mathcal{S} = \{|\psi_i\rangle \in \mathcal{H} \mid i = 1, 2, \ldots, M, \langle\psi_i|\psi_i\rangle = 1\}. \quad (1)$$

Let ξ_i be the *a priori* probability of $|\psi_i\rangle$ and $\xi = \{\xi_i \mid i = 1, 2, \ldots, M\}$. Then $(\mathcal{S}, \xi)$ is often referred to as the quantum information source and

$$\hat{\rho} = \sum_{i=1}^{M} \xi_i |\psi_i\rangle\langle\psi_i| \quad (2)$$

is the so-called density operator of $(\mathcal{S}, \xi)$. We introduce the weighted Gram matrix with *a priori* probabilities G, that is, an M-by-M matrix whose (i, j) component is $\langle\tilde{\psi}_i|\tilde{\psi}_j\rangle$, where $|\tilde{\psi}_i\rangle = \sqrt{\xi_i}|\psi_i\rangle$.

Because

$$G \cong \hat{\rho}, \quad (3)$$

the eigenvalues of $\hat{\rho}$ can be obtained by calculating those of G.

The von Neumann entropy is defined as

$$H(\mathcal{S}, \xi) = -\mathrm{Tr}(\hat{\rho} \log_2 \hat{\rho}), \quad (4)$$

and the classical capacity of a quantum channel is defined as $H(\mathcal{S}, \xi)$ maximized with respect to *a priori* probabilities:

$$C = \max_{\xi} H(\mathcal{S}, \xi). \quad (5)$$

From (3), $H(\mathcal{S}, \xi)$ can be calculated as

$$H(\mathcal{S}, \xi) = -\mathrm{Tr}\,(G \log_2 G) = -\sum_j \lambda_j \log_2 \lambda_j, \quad (6)$$

where λ_j are the eigenvalues of G.

3 Discretization problem for quantum continuous channels

3.1 Energy constraint

The input to the quantum communication channel is a coherent state of various amplitudes $|\alpha\rangle$, which imposes an energy constraint:

$$\int |\alpha|^2 P(d^2\alpha) \leq m, \tag{7}$$

where m is the average number of photons and $P(\alpha)$ is the probability distribution of the coherent-state set. The quantum continuous channel capacity for m is then given by

$$C_{\text{full}} = g(m) = (m+1)\log_2(m+1) - m\log_2 m. \tag{8}$$

3.2 Ternary discretization

In the ternary discretization problem, we consider the case in which only three coherent states are available. These coherent states are $|\alpha\rangle, |\beta\rangle, |\gamma\rangle$ with *a priori* probabilities $p_1, p_2, p_3 (= 1 - p_1 - p_2)$ respectively. We address the problem of locating the capacity of ternary channel

$$C_3 = \sup_{\{|\alpha\rangle,|\beta\rangle,|\gamma\rangle\}} \sup_{\{p_1,p_2,p_3\}} H(\{|\alpha\rangle,|\beta\rangle,|\gamma\rangle\},\{p_1,p_2,p_3\}) \tag{9}$$

with the energy constrained to

$$p_1|\alpha|^2 + p_2|\beta|^2 + p_3|\gamma|^2 \leq m. \tag{10}$$

4 Main results

4.1 One-dimensional constraint

Because the optimal solution for binary discretization is BPSK signals [4], we first add another signal $|\beta\rangle$ to the BPSK signals $\{|\alpha\rangle, |-\alpha\rangle\}$ to examine whether entropy H increases. Without loss of generality, we assume that α is a non-negative real number. We also assume that $\beta \in \mathbb{R}$ $(\beta \geq 0)$. This assumes that all three signals exist on the real axis of the phase plane, which is equivalent to considering the case of a one-dimensional constraint. Let $\beta = a\alpha$ $(a \geq 0)$. Given that we are adding another signal to BPSK signals $\{|\alpha\rangle, |-\alpha\rangle\}$, which have equal probabilities, and that the average number of photons of $|\alpha\rangle$ and $|-\alpha\rangle$ are the same, let q be the *a priori* probability of $|\beta\rangle$, and let the *a priori* probabilities of $|\alpha\rangle$ and $|-\alpha\rangle$ be equal to probability $\frac{1-q}{2}$.

We examine the $q = P(\beta)$-dependence of the entropy for various values of a. As a result, the best case is found when $a = 0$, that is, when $|\beta\rangle$ is the vacuum state $|0\rangle$; that is, the 3ASK signal constellation is optimal when the additional signal is constrained to be on the real axis. Additionally, we examine the properties of the optimal value of probability q when β is set to 0; the optimal value approaches $q = \frac{2}{3}$ for $m \to 0$ and $q = \frac{1}{3}$ for $m \to \infty$. The latter is trivial because the upper limit of the entropy of ternary signals is $\log_2 3$.

We also demonstrate the numerical feature of C_3 when constrained to one dimension.

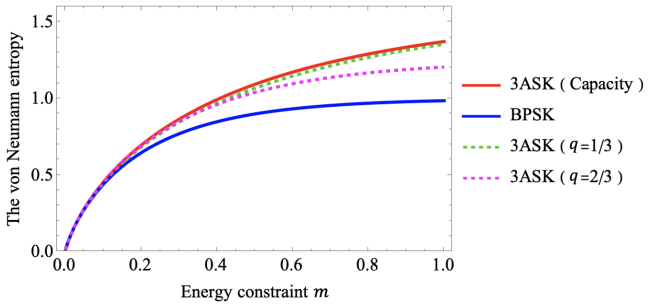


Figure 1: C_3 with one-dimensional constraint.

Figure 1 shows the von Neumann entropy using the optimal probabilities for each m. The figure shows that, although probability q must be optimized to achieve C_3, the maximum entropy values for $q = \frac{2}{3}$ and $q = \frac{1}{3}$ are fairly close to the channel capacity.

4.2 Adding a signal on the imaginary axis

The set of amplitudes of the ternary signals that we consider is $\{-\alpha, \mathbf{i}\beta, \alpha\}$. Based on the same considerations as those in the previous section, there is no loss of generality if $\beta \geq 0$. We also assume that $\beta = b\alpha$ $(b \geq 0)$. Regarding the probabilities, the *a priori* probability of $|\mathbf{i}\beta\rangle$ is q, and the *a priori* probabilities of $|\alpha\rangle$ and $|-\alpha\rangle$ are equal to $\frac{1-q}{2}$ each, by the same considerations as those in the previous section.

We examine the $q = P(\beta)$-dependence of entropy for various values of b. The results demonstrate that $b = 0$ is not the maximum for any m, and that adding an imaginary component increases the entropy. This is true even when m varies; however, the optimal value of b differs depending on m.

Figure 2 plots the optimal relative amplitude b versus the energy constraint m. Large amplitude values are optimal when m is small, and as m increases, the amplitude becomes small and then converges to a constant value. For all m, $b > 1.5$, which indicates that the three signal points are located at the vertices of an isosceles triangle with a rather short base.

Additionally, the optimal amplitude value is large when the energy constraint m is small. By contrast,

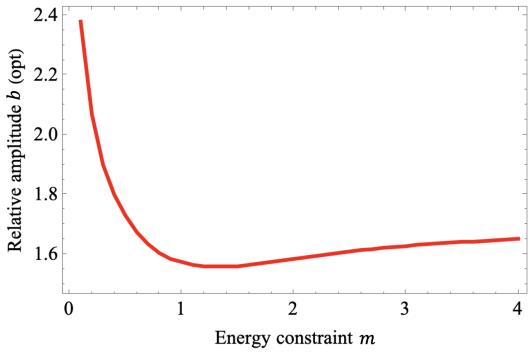


Figure 2: Optimal relative amplitude value b with respect to energy constraint m.

because the energy constraint is satisfied, the probability is small. As m increases, the probability of $|\mathbf{i}\beta\rangle$ asymptotically approaches $\frac{1}{3}$, which corresponds to a uniform probability distribution.

Because the entropy is determined only by the relative positions of the signal points, translating the entire signal does not change the entropy. The average number of photons in the above signal is

$$N_{\mathrm{S}}(0) = (1-q)\alpha^2 + q\beta^2, \tag{11}$$

but the signal amplitudes are $\{-\alpha - \mathbf{i}c, \mathbf{i}(\beta - c), \alpha - \mathbf{i}c\}$, where the entire signal is translated by c (≥ 0) in the negative direction of the imaginary axis. The average number of photons is

$$\begin{aligned} N_{\mathrm{S}}(c) &= (1-q)(\alpha^2 + c^2) + q(\beta - c)^2 \\ &= N_{\mathrm{S}}(0) + c^2 - 2q\beta c \\ &= N_{\mathrm{S}}(0) + (c - q\beta)^2 - q^2\beta^2, \end{aligned} \tag{12}$$

which is smaller than $N_{\mathrm{S}}(0)$. In particular, $N_{\mathrm{S}}(c)$ has the minimum value at $c = q\beta$ because

$$N_{\mathrm{S}}^{(\min)} = N_{\mathrm{S}}(0) - q^2\beta^2 < N_{\mathrm{S}}(0). \tag{13}$$

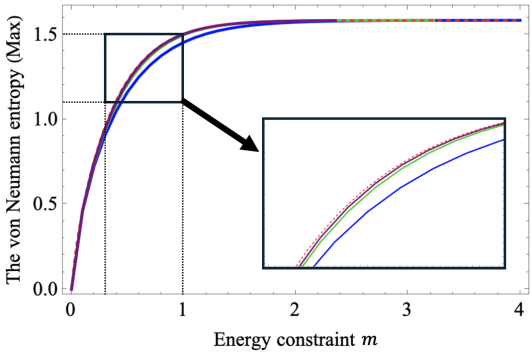


Figure 3: The von Neumann entropy with respect to energy constraint m.

Figure 3 shows the von Neumann entropy for energy constraint m. Note that there are four lines. The blue line shows the entropy of the ternary signals obtained by adding the signal on the imaginary axis to the BPSK signals, as shown in the previous subsection. The green line shows the entropy improved by shifting the blue line by $q\beta$ in the negative direction of the imaginary axis, as previously shown. The purple line shows the optimized *a priori* probability of the additional signal for the green line, which is almost the same as the green line, but slightly improved. For comparison, the red dotted line shows the capacity of the 3PSK signals, which is slightly higher than the purple line. Furthermore, the *a priori* probability distribution of the signals is closer to uniform after optimization.

4.3 Optimal signal constellation

For the *a priori* probability of the signal state $\mathbf{i}(\beta - q\beta)$ in signal $\{-\alpha - \mathbf{i}q\beta, \mathbf{i}(\beta - q\beta), \alpha - \mathbf{i}q\beta\}$ in the previous subsection, the energy is minimal in the same signal class with the same relative position of signals when we set q, but changing the *a priori* probability again provides room for optimization. When the relative positions of the signals are slightly changed, the signal constellation, which is an isosceles triangle with a slightly short base, approaches an equilateral triangle and the *a priori* probability distribution approaches uniform; that is, if we gradually improve the signal by removing signal constraints in this manner, we naturally obtain 3PSK signals. Furthermore, we generated a large number of random signals, examined their entropy values, and found that none exceeded the 3PSK channel capacity.

From the above, we can conclude that the optimal signal constellation for ternary discretization is 3PSK signals based on numerical considerations.

5 Conclusion

In this study, we addressed the problem of the ternary discretization of continuous communication channels and numerically demonstrated that the class of 3ASK signals is optimal when the signal is limited to coherent states on the real axis of the phase plane. Furthermore, the degrees of freedom of the signal constellation are gradually increased in two dimensions. As a result, we finally showed numerically that the optimal signal constellation is 3PSK signals, that is, we achieved C_3.

Acknowledgments: This work has been supported in part by JSPS KAKENHI Grant Number JP20K20397, JP20H00581, JP21K04064, and the Hibi Science Foundation. We thank MG and Liam Exelby from Edanz (https://jp.edanz.com/ac) for editing a draft of this manuscript.

References

[1] C. W. Helstrom: *Quantum detection and estimation theory*, Academic Press, New York, (1976).

[2] O. Hirota: *The foundation of quantum information science*, Morikita Publishing, Japan, (2002). (in Japanese)

[3] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen: "Classical capacity of the lossy bosonic channel: the exact solution," Phys. Rev. Lett. **90**, 027902, (2004).

[4] M. Sohma and O. Hirota: "Binary discretization for quantum continuous channels," Phys. Rev. **A62**, 052312, (2000).

[5] Y. Ishida, K. Kato, and T. S. Usuda: "Capacity of attenuated channel with discrete-valued input," Proc. of the 8th International Conference on Quantum Communication, Measurement and Computing (QCMC), (2006).

[6] T. Wang, R. Miyazaki, S. Takahira, and T. S. Usuda: "Simplification of the Gram matrix eigenvalue problem for quantum signals formed by rotating signal points in a circular sector region," IEEJ Trans. on Electronics, Information and Systems **142**, pp.74-87, (2022). (in Japanese)

[7] S. Kitamura, T. Wang, S. Takahira, and T. S. Usuda: "Simplification of the generalized Gram matrix eigenvalue problem for asymmetric M-ary coherent-state signals," Proc. of 2022 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, E1-1, (2022). (in Japanese)

[8] S. Kitamura, T. Wang, S. Takahira, and T. S. Usuda: "Simplification of the eigenvalue problem for density operators representing asymmetric quantum signals and its application to capacity calculations," Proc. of the 45th Symposium on Information Theory and its Applications (SITA), pp.169-174, (2022). (in Japanese)

[9] S. Kitamura, T. Wang, S. Takahira, and T. S. Usuda: "Calculation of capacity with discrete-valued inputs using efficiently obtained eigenvalues," Proc. 23rd Asian Quantum Information Science Conference (AQIS2023), pp.267-270, (2023).

[10] S. Kitamura, T. Wang, S. Takahira, and T. S. Usuda: "Signal constellations and a priori probabilities achieving 99% capacity of quantum channel," Proc. of the 46th Symposium on Information Theory and its Applications (SITA), pp.510-515, (2023). (in Japanese)

[11] K. Kato, M. Osaki, and O. Hirota: "Derivation of classical capacity of quantum channel for discrete information source," Phys. Lett. **A251**, pp.157-163, (1999).

[12] C. E. Shannon: "A mathematical theory of communication," The Bell System Technical Journal **27**, pp.379-423, (1948).

[13] R. A. Horn and C. R. Jonson: *Matrix analysis*, Cambridge University Press, (1985).

Error interference in quantum simulation

Boyang Chen[1] Jue Xu[2] Xiao Yuan [*3 4] Qi Zhao[2 †]

[1] *Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*
[2] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[3] *Center on Frontiers of Computing Studies, Peking University, Beijing 100871, China*
[4] *School of Computer Science, Peking University, Beijing 100871, China*

Abstract. Understanding algorithmic error accumulation in quantum simulation is an important topic, both for fundamental interest and practical improvement in quantum computing tasks. In this paper, we investigate error interference, a phenomenon where errors in different segments can destructively interfere, leading to non-linear error accumulation. We establish a general framework for algorithmic error interference and provide sufficient and necessary conditions for its occurrence. Additionally, we present an approximate version of error interference that yields tighter error bounds than previous approaches. Our findings extend the understanding of error interference phenomena beyond the two-term Hamiltonian case, including higher-order Trotter formulas and more complex Hamiltonians with speed-ups in implementing Hamiltonian simulation and digital adiabatic algorithms. These results have practical implications for Hamiltonian simulation implementation and may inspire more algorithm designs to exploit error interference for reducing total error in quantum simulations and related tasks.

Keywords: Trotter error, Hamiltonian simulation, error interference

1 Introduction

Simulating quantum dynamics is a central application of quantum computation [1, 2]. Efficient quantum algorithms have been proposed for simulating the Schrodinger equation of a general quantum system [3–6], a notoriously difficult task for classical computers. Quantum simulation has wide applications in quantum chemistry [7–9] and quantum field theories [10], and also serves as an indispensable subroutine for other fundamental quantum algorithms, such as quantum phase estimation [11] and the HHL algorithm [12] for solving linear systems.

Since the first digital quantum dynamics simulation algorithm based on the product formula for k-local Hamiltonians proposed by Lloyd [3], novel techniques such as truncated Taylor series (LCU) [13, 14] and Quantum Signal Processing (QSP) [15–17] have been developed, and the algorithms have been improved to optimal or nearly optimal complexity with respect to several key parameters [15–21]. Nevertheless, variants of the product formula are still promising candidates for near-term quantum devices to achieve practical quantum advantages [22] due to their simplicity, mild hardware requirements, and decent performance in practice.

For a given Hamiltonian $H = \sum_{l=1}^{L} H_l$, implementing product formula (PF), also known as Trotter-Suzuki formula, requires dividing the long-time evolution $e^{-\mathrm{i}Ht}$ into several segments r and approximating the short-time evolution $e^{-\mathrm{i}Ht/r}$ using the pth-order product formula $\mathscr{U}_p(t)$ [23], e.g., $\mathscr{U}_1(t) := e^{-\mathrm{i}H_1 t}e^{-\mathrm{i}H_2 t}\cdots e^{-\mathrm{i}H_L t}$, with an error term $\epsilon = \|\mathscr{U}_1(t/r) - e^{-\mathrm{i}Ht/r}\|$. The total error called Trotter error can be upper-bounded by $r\epsilon$ via the triangle inequality. Increasing r results in a smaller Trotter error. Before implementation, it is necessary to estimate the total error and choose an appropriate r to suppress the total error under a predetermined threshold. Thus, understanding the performance of Trotter errors is an important topic. A tighter analysis can help save gate costs in both Hamiltonian simulation [24, 25] and other product formula related tasks, such as imaginary time evolution [26], quantum Monte Carlo [27, 28], quantum adiabatic algorithms [29], and quantum phase estimation [30]. Although a few attempts have been made in this direction [31–37], there still exists a gap between empirical results and theoretical analysis, even for the simple case like simulating power-law decaying interactions Hamiltonians with the first-order product formula.

Recently, it has been found that for the first-order product formula (PF1) with $H = A + B$, errors in different segments can have destructive error interference, and the total error may not increase linearly with the number of segments r [36]. This error interference phenomenon can be explained from a second-order product formula perspective [38] and can also result in speed-up in various applications, e.g., quantum adiabatic algorithms [29], and quantum phase estimation [30]. However, we still lack systematic proof and understanding of this error interference phenomenon. Currently, error interference only exists in the two-term case $H = A + B$ with PF1, which can not explain the error interference phenomenon in the three-term cases $H = A + B + C$ with PF1 [33]. Many questions remain, such as when we will have error interference, whether we can go beyond the two-term case and observe error interference in higher-order product formulas, whether there are approximate interference cases, and how to utilize this interference in algorithm design.

In this work, we establish a general framework for algorithmic error interference in product formula quantum simulation methods and provide sufficient and necessary conditions for error interference. Next, we give a gen-

*xiaoyuan@pku.edu.cn
†zhaoqi@cs.hku.hk

eral theoretical lower bound for algorithmic error accumulation, which in various cases excludes the possibility of error interference, e.g., when considering quantum signal processing algorithms. As applications, we provide more examples with (approximate) error interference phenomena beyond the $H = A + B$ case, including $H = A + B + C$ cases in the Heisenberg model, Fermi-Hubbard model, and power-law interaction models. For example, for power-law interaction Hamiltonians, we can use our result to have improved error bounds. The approximate error interference also exists in higher-order product formula approximation of perturbative evolution and can lead to speed-ups in some regions of implementing digital adiabatic algorithms. Our results are fundamentally interesting, furthering our understanding of the product formula theory, and practically useful, directly applicable to the implementation of Hamiltonian simulation using realist quantum hardware. Leveraging our error interference bounds, our results may also inspire better algorithm designs to reduce the total error [37].

2 Interference theory

2.1 Asymptotic error interference of product formulas

For a given Hamiltonian $H = \sum_{l=1}^{L} H_l$ of L terms, the first-order product formula (PF1), also known as the Trotter-Suzuki formula [23, 39], can approximate the quantum dynamics $e^{-\mathrm{i}\delta t H}$ by the product of the dynamics of each term, that is

$$\mathscr{U}_1(\delta t) := e^{-\mathrm{i}H_1\delta t} e^{-\mathrm{i}H_2\delta t} \cdots e^{-\mathrm{i}H_L\delta t} = \prod_{l}^{\longrightarrow} e^{-\mathrm{i}H_l\delta t}. \quad (1)$$

As the Hamiltonian terms H_l are not commutative to each other in general, the introduced approximation error (we will call it Trotter error throughout the paper) is upper bounded $\left\|\mathscr{U}_1(\delta t) - e^{-\mathrm{i}H\delta t}\right\| = \mathcal{O}(\alpha_{comm}\delta t^2)$ where $\|\cdot\|$ is the spectral norm and $\alpha_{comm} = \sum_{l_1,l_2=1}^{L} \|[H_{l_2}, H_{l_1}]\|$. For a long time evolution $e^{-\mathrm{i}tH}$, we can divide the whole evolution into several segments r and repeatedly apply the product formula for $\delta t = t/r$, i.e., $\mathscr{U}_1^r(t/r)$. To suppress the algorithmic error, the second-order product formula can be defined as $\mathscr{U}_2(\delta t) := \prod_l^{\rightarrow} e^{-\mathrm{i}H_l\delta t/2} \prod_l^{\leftarrow} e^{-\mathrm{i}H_l\delta t/2}$, where $\prod_l^{\leftarrow}$ denotes a product in reverse order. More generally, a p-th order Suzuki product formula (PFp) $\mathscr{U}_p(\delta t)$ can be defined recursively. In most error analyses, a triangle inequality is applied and the total error is bounded

$$\left\|\mathscr{U}_p^r(t/r) - e^{-\mathrm{i}tH}\right\| \le r \left\|\mathscr{U}_p(t/r) - e^{-\mathrm{i}Ht/r}\right\| \quad (2)$$

In some cases, the error in each segment may have the interference and the triangle inequality error bound is pessimistic, e.g., a two-term Hamiltonian $H = A + B$ [40, 41], and Hamiltonians with a power-law rapidly decaying interactions [33].

2.2 Asymptotic error interference of product formulas

In this section, we study the accumulation of error in the product formula and give general criteria on when the error would exhibit a feature of *interference*, and prove the error interference property of the error rigorously.

Definition 1 (Interference, informal)**.** *For a pth-order product formula $\mathscr{U}(t/r)$ approximating $e^{-\mathrm{i}Ht/r}$, if the total error grows sublinearly to the sum of error of each timestep, i.e.,*

$$\left\|\mathscr{U}_p^r(t/r) - e^{-\mathrm{i}Ht}\right\| = o\Big(r \left\|\mathscr{U}_p(t/r) - e^{-\mathrm{i}H(t/r)}\right\|\Big), \quad (3)$$

where $\|\cdot\|$ denotes the spectral norm and when t and r/t are both large enough, then we say that the Trotter error interferes.

The requirement in the definition that t and r/t needs to tend to infinity simultaneously might seem weird at the first glance, but it is the correct way to define interference in an asymptotic way: say, take the result in [40] as an example, they show that the trotter error of two-term PF1 for lattice Hamiltonians can be bounded by $\mathcal{O}\Big(n\frac{t}{r} + n\frac{t^3}{r^2}\Big)$, while the bound by accumulation is $\mathcal{O}\Big(n\frac{t^2}{r}\Big)$. The interference bound would be better than the accumulation bound asymptotically only if both t and $r/t = 1/\delta t$ tends to infinity.

To explore the error accumulation, we apply a new error analysis which directly estimates the error for a long time evolution. We can express the approximated evolution by an effective Hamiltonian H_{eff} with $\exp(-\mathrm{i}\delta t H_{\text{eff}}) = \exp(-\mathrm{i}\delta t(H + H_{\text{error}}))$ where H_{error} is the exponentiated error term. Suppose the Hermitian H has spectral decomposition $H = P\Lambda P^*$ where $P \in SU(d)$ and Λ is diagonal. Diagonal elements of Λ are exactly the eigenvalues of H, and their corresponding eigenstates are exactly the columns of P. Thus, the ideal evolution can rewritten as $\exp(-\mathrm{i}\delta t H) = P\exp(-\mathrm{i}\delta t(\Lambda))P^*$. The approximated evolution $\exp(-\mathrm{i}\delta t H_{\text{eff}})$ can also be spectral decomposed as $\exp(-\mathrm{i}\delta t H_{\text{eff}}) = (P+\delta P)\exp(-\mathrm{i}\delta t(\Lambda+\delta\Lambda))(P+\delta P)^\dagger$ where δP and $\delta\Lambda$ are the deviations in eigenvectors and eigenvalues, respectively. For a long time evolution, the approximated evolution is repeated r times, $\exp(-\mathrm{i}r\delta t H_{\text{eff}}) = (P+\delta P)\exp(-\mathrm{i}r\delta t(\Lambda+\delta\Lambda))(P+\delta P)^\dagger$. The error in eigenvectors remains δP, regardless of r, while the error in eigenvalues will accumulate $r\delta t\delta\Lambda$. As a result, the total error is roughly $\delta P + r\delta t\delta\Lambda$. Considering that δP is independent of total time t and the number of segments, the accumulation of error mainly stems from the second term, $r\delta t\delta\Lambda$. If $r\delta t\delta\Lambda$ is much smaller than δP, the total error will show a sublinear accumulation phenomenon.

Hereafter, we mainly focus on product formula methods. For PFp, the exponentiated error term H_{error} is $\mathcal{O}(\delta t^p)$. We can rewrite this error as $H_{\text{error}} = R\delta t^p + R_{re}$, where R is the leading-order terms in Trotter error and R_{re} is the high-order remainder with $\|R_{re}\| = \mathcal{O}(\delta t^{p+1})$.

In general, δP and $\delta\Lambda$ are both $\mathcal{O}(\|R\|\delta t^p)$ and the Trotter error in one segment is $\|\mathscr{U}(\delta t) - e^{-\mathrm{i}\delta t H}\| = \mathcal{O}(\delta t(\delta\Lambda + \delta P)) = \mathcal{O}(\|R\|\delta t^{p+1})$. For a long time evolution with a total error $\delta P + t\delta\Lambda$, the second term $t\delta\Lambda$ will dominate, leading to a $\mathcal{O}(\|R\|t^{p+2}/r^{p+1})$ total error. Interestingly, when a specific condition is satisfied, $\delta\Lambda$ will be surprising small the growth of total error will not accumulate linearly with the number of Trotter steps and appear the phenomenon of error interference. We express this result in the following theorem.

Definition 2 (Orthogonality condition)**.** *Consider a given Hamiltonian evolution $e^{-i\delta t H}$ and its approximation $e^{-\mathrm{i}\delta t H_{eff}}$. If the leading-order term R of $H_{error} = H - H_{eff}$ satisfies that*

$$\langle\psi_i|R|\psi_i\rangle = 0 \tag{4}$$

for all eigenstates $|\psi_i\rangle$ of H. We say this approximation $e^{-\mathrm{i}\delta t H_{eff}}$ satisfies an orthogonality condition

Theorem 3 (Neccesary and sufficient condition for error interference)**.** *The orthogonality condition is a necessary and sufficient condition for error interference. Suppose that $H_{error} \approx Rt^p/r^p$, the total error can be bounded by*

$$\left\|e^{-\mathrm{i}H_{eff}t} - e^{-\mathrm{i}Ht}\right\| = \mathcal{O}\left(\|R\|\left(\frac{t^p}{r^p} + \|R\|\frac{t^{2p+1}}{r^{2p}}\right)\right). \tag{5}$$

If $e^{-\mathrm{i}\delta t H_{eff}}$ do not satisfy the orthogonality condition, then the error term would be

$$\left\|e^{-\mathrm{i}H_{eff}t} - e^{-\mathrm{i}Ht}\right\| = \Omega\left(\frac{t^{p+1}}{r^p}\max_i\langle\psi_i|R|\psi_i\rangle\right). \tag{6}$$

The orthogonality requirement $\langle\psi_i|R|\psi_i\rangle = 0$ is equivalent to that there exsits a matrix M such that $[H, M] = R$. The condition also has a necessary criteria

$$\mathrm{Tr}\big(RH^k\big) = 0, \forall k \geq 1. \tag{7}$$

As a corollary of Theorem 3, we get immediately a sufficient condition that when the error would accumulate linearly.

Corollary 4 (Error lower bound)**.** *For a formula $\mathscr{U}(t)$ approximating $e^{-\mathrm{i}Ht}$ and its leading error is R in the sense that $\mathscr{U}(t) = e^{-\mathrm{i}Ht + Rt^{p+1}/r^{p+1} + o(t^{p+1}/r^{p+1})}$, and if $\mathrm{Tr}(RH^n) \neq 0$ for some $n \in \mathbb{N}$, then $\left\|\mathscr{U}^r(t/r) - e^{-\mathrm{i}Ht}\right\| = \Omega(\frac{t^{p+1}}{r^p})$ as t and r/t tends to infinity.*

Theorem 3 is a general bound for error of any product formula, but it is most useful only for the product formulas. For other types of simulation algorithms like LCU or QSP, the error would just accumulate linearly. This is because the unitary generated by, say LCU algorithm, is a polynomial in the desired dynamics H. Thus the error of the algorithm would have the same eigenbasis with H, so the error does not interfere. Error of QSP simulation is fourier coefficients of the Hamiltonian, which does not interfere either.

Corollary 4 can be used to estimate the long-term error. If we find that the error does not interfere, then we can estimate the total error by just summing up the (empirical) error in each timestep, which could save a lot of computational resources.

2.3 Approximated interference of Trotter errors

In Theorem 3, we give the criteria of when the error would self-cancel exactly. But sometimes the error might not self-cancel exactly but instead only a major part of the error would "interfere". We will develop the theory of approximation of approximated interference of Trotter errors in this section. First we will derive the approximation formula of the error.

Lemma 5. *Assume that we hope to simulate H, with error term $R = R_1 + R_2$, where R_1, R_2 are some Hermitian matrices, then we have*

$$\begin{aligned}&\left\|e^{-\mathrm{i}(H + t^p/r^p R)t} - e^{-\mathrm{i}Ht}\right\| \\ &\leq \|R_2\|\frac{t^{p+1}}{r^p} + \left\|e^{-\mathrm{i}(H + t^p/r^p R_1)t} - e^{-\mathrm{i}Ht}\right\|\end{aligned}$$

Lemma 5 can be used to prove the error self-canceling of higher-order PFs when one of them is overwhelmingly large compared to other terms. Take 2-term PF2 $\mathscr{U}_2(t) = e^{-\mathrm{i}H_1 t/2}e^{-\mathrm{i}H_2 t}e^{-\mathrm{i}H_1 t/2}$ for example. The leading term of the error is $\mathrm{i}Rt^3$, where $R = [H_1, [H_1, H_2]] - [H_2, [H_1, H_2]]$. When $\|H_1\|$ is much larger than $\|H_2\|$, we can rewrite R as $R = [H_1 + H_2, [H_1, H_2]] - [2H_2, [H_1, H_2]]$, where the first term satisfies the orthogonal condition, while the second term is much smaller than the first term. Theoretical and numerical evidences are provided in the technical version.

2.4 Exact error interference bound for the first-order product formula

In Theorem 3, we work with large $\mathcal{O}$ factors, ignoring the hidden constant in the convergence rate. We also hope to calculate the explicit constant factors when we want to give an explicit bound on the error. So here we will prove a theorem with explicit constant factors. The following theorem is a more explicit form of Theorem 3 in the case of PF1. In the case of PF1, we can show rigorously that the errors would interfere and grow sublinearly. Here we provide the statement for tight bound in the general case. The statement of tight bound for PF1 will be shown in the technical version.

Theorem 6 (Tight upper bound for general error interference)**.** *Let H and R be Hermitians, let h be any real parameter. Let $\{|\psi_i\rangle\}$ and $\{|\psi_i'\rangle\}$ be the eigenvectors of H and $H + hR$ respectively and let $\{\lambda_i\}, \{\lambda_i'\}$ be the corresponding eigenvalues. Then R can be decomposed as $R = \sum b_{jk}|\psi_j\rangle\langle\psi_k'|$. For any $\epsilon > 0$, let $\Delta_H^\epsilon(R) = \sum_{0 \leq \lambda_j - \lambda_k' < \epsilon} b_{jk}|\psi_j\rangle\langle\psi_k'|$, for $\epsilon < 0$, define $\Delta_H^\epsilon(R) = \sum_{\epsilon < \lambda_j - \lambda_k' \leq 0} b_{jk}|\psi_j\rangle\langle\psi_k'|$, and $\mathcal{R}_H^\epsilon(R) = \sum_{|\lambda_j - \lambda_k'| \geq \epsilon} \frac{1}{\lambda_j - \lambda_k'} b_{jk}|\psi_j\rangle\langle\psi_k'|$. Then we have*

$$\begin{aligned}&\|\exp(-\mathrm{i}(H + hR)t) - \exp(-\mathrm{i}Ht)\| &(8)\\ &\leq 4h\max_{|\epsilon'| \leq \epsilon}\left\|\Delta_H^{\epsilon'}(R)\right\|t + 2h\left\|\mathcal{R}_H^\epsilon(R)\right\| &(9)\end{aligned}$$

References

[1] Richard P. Feynman. Simulating physics with computers. *Int J Theor Phys*, 21(6):467–488, June 1982.

[2] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge ; New York, 10th anniversary ed edition, 2010.

[3] Seth Lloyd. Universal Quantum Simulators. *Science*, 273(5278):1073–1078, August 1996.

[4] S. P. Jordan, K. S. M. Lee, and J. Preskill. Quantum Algorithms for Quantum Field Theories. *Science*, 336(6085):1130–1133, June 2012.

[5] Sam McArdle, Suguru Endo, Alan Aspuru-Guzik, Simon C Benjamin, and Xiao Yuan. Quantum computational chemistry, 2020.

[6] Andrew M. Childs, Yuan Su, Minh C. Tran, Nathan Wiebe, and Shuchen Zhu. Theory of Trotter Error with Commutator Scaling. *Phys. Rev. X*, 11(1):011020, February 2021.

[7] Dave Wecker, Bela Bauer, Bryan K. Clark, Matthew B. Hastings, and Matthias Troyer. Gate-count estimates for performing quantum chemistry on small quantum computers. *Phys. Rev. A*, 90:022305, Aug 2014.

[8] Ryan Babbush, Jarrod McClean, Dave Wecker, Alán Aspuru-Guzik, and Nathan Wiebe. Chemical basis of trotter-suzuki errors in quantum chemistry simulation. *Phys. Rev. A*, 91:022311, Feb 2015.

[9] Ryan Babbush, Peter J Love, and Alán Aspuru-Guzik. Adiabatic quantum simulation of quantum chemistry. *Scientific Reports*, 4:6603, 2014.

[10] Stephen P Jordan, Keith SM Lee, and John Preskill. Quantum algorithms for quantum field theories. *Science*, 336(6085):1130–1133, 2012.

[11] A. Yu Kitaev. Quantum measurements and the Abelian Stabilizer Problem, November 1995.

[12] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for solving linear systems of equations. *Phys. Rev. Lett.*, 103(15):150502, October 2009.

[13] Andrew M. Childs and Nathan Wiebe. Hamiltonian Simulation Using Linear Combinations of Unitary Operations. *QIC*, 12(11&12), 2012.

[14] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating hamiltonian dynamics with a truncated taylor series. *Phys. Rev. Lett.*, 114:090502, Mar 2015.

[15] Guang Hao Low and Isaac L. Chuang. Optimal hamiltonian simulation by quantum signal processing. *Phys. Rev. Lett.*, 118:010501, Jan 2017.

[16] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019.

[17] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics. *Proc. 51st Annu. ACM SIGACT Symp. Theory Comput.*, pages 193–204, June 2019.

[18] Dominic W. Berry, Graeme Ahokas, Richard Cleve, and Barry C. Sanders. Efficient quantum algorithms for simulating sparse Hamiltonians. *Commun. Math. Phys.*, 270(2):359–371, March 2007.

[19] Dominic W. Berry, Andrew M. Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *2015 IEEE 56th Annu. Symp. Found. Comput. Sci.*, pages 792–809, October 2015.

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

[21] Guang Hao Low. Hamiltonian simulation with nearly optimal dependence on spectral norm. In *51st Annual ACM Symposium on Theory of Computing*, pages 491–502, 2019.

[22] Youngseok Kim, Andrew Eddins, Sajant Anand, Ken Xuan Wei, Ewout van den Berg, Sami Rosenblatt, Hasan Nayfeh, Yantao Wu, Michael Zaletel, Kristan Temme, and Abhinav Kandala. Evidence for the utility of quantum computing before fault tolerance. *Nature*, 618(7965):500–505, June 2023.

[23] Masuo Suzuki. General theory of fractal path integrals with applications to many-body theories and statistical physics. *J. Math. Phys.*, 32(2):400–407, 1991.

[24] Andrew M. Childs, Yuan Su, Minh C. Tran, Nathan Wiebe, and Shuchen Zhu. Theory of Trotter Error with Commutator Scaling. *Phys. Rev. X*, 11(1):011020, February 2021.

[25] Andrew M Childs, Dmitri Maslov, Yunseong Nam, Neil J Ross, and Yuan Su. Toward the first quantum simulation with quantum speedup. *Proc. Natl. Acad. Sci. U.S.A.*, 115(38):9456–9461, 2018.

[26] Mario Motta, Chong Sun, Adrian TK Tan, Matthew J O'Rourke, Erika Ye, Austin J Minnich, Fernando GSL Brandão, and Garnet Kin-Lic Chan. Determining eigenstates and thermal states on a quantum computer using quantum imaginary time evolution. *Nature Physics*, 16(2):205–210, 2020.

[27] Sergey Bravyi. Monte carlo simulation of stoquastic hamiltonians. *Quantum Info. Comput.*, 15(13–14):1122–1140, October 2015.

[28] Sergey Bravyi and David Gosset. Polynomial-time classical simulation of quantum ferromagnets. *Phys. Rev. Lett.*, 119:100503, Sep 2017.

[29] Lucas K. Kovalsky, Fernando A. Calderon-Vargas, Matthew D. Grace, Alicia B. Magann, James B. Larsen, Andrew D. Baczewski, and Mohan Sarovar. Self-healing of Trotter error in digital adiabatic state preparation. *Phys. Rev. Lett.*, 131(6):060602, August 2023.

[30] Changhao Yi and Elizabeth Crosson. Spectral analysis of product formulas for quantum simulation. *npj Quantum Information*, 8(1):37, 2022.

[31] Yuan Su, Hsin-Yuan Huang, and Earl T Campbell. Nearly tight trotterization of interacting electrons. *Quantum*, 5:495, 2021.

[32] Burak Şahinoğlu and Rolando D. Somma. Hamiltonian simulation in the low-energy subspace. *npj Quantum Inf*, 7(1):119, July 2021.

[33] 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.

[34] Qi Zhao and Xiao Yuan. Exploiting anticommutation in Hamiltonian simulation. *Quantum*, 5:534, August 2021.

[35] Markus Heyl, Philipp Hauke, and Peter Zoller. Quantum localization bounds trotter errors in digital quantum simulation. *Science Advances*, 5(4):eaau8342, 2019.

[36] Minh C. Tran, Su-Kuan Chu, Yuan Su, Andrew M. Childs, and Alexey V. Gorshkov. Destructive Error Interference in Product-Formula Lattice Simulation. *Phys. Rev. Lett.*, 124(22):220502, June 2020.

[37] Minh C. Tran, Yuan Su, Daniel Carney, and Jacob M. Taylor. Faster digital quantum simulation by symmetry protection. *PRX Quantum*, 2:010323, Feb 2021.

[38] David Layden. First-Order Trotter Error from a Second-Order Perspective. *Phys. Rev. Lett.*, 128(21):210501, May 2022.

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

[40] Minh C. Tran, Su-Kuan Chu, Yuan Su, Andrew M. Childs, and Alexey V. Gorshkov. Destructive Error Interference in Product-Formula Lattice Simulation. *Phys. Rev. Lett.*, 124(22):220502, June 2020.

[41] David Layden. First-Order Trotter Error from a Second-Order Perspective. *Phys. Rev. Lett.*, 128(21):210501, May 2022.

Error interference in quantum simulation

Boyang Chen,[1] Jue Xu,[2] Xiao Yuan,[3,4,*] and Qi Zhao[2,†]

[1] *Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[2] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[3] *Center on Frontiers of Computing Studies, Peking University, Beijing 100871, China*
[4] *School of Computer Science, Peking University, Beijing 100871, China*

(Dated: May 21, 2024)

Understanding algorithmic error accumulation in quantum simulation is an important topic, both for fundamental interest and practical improvement in quantum computing tasks. In this paper, we investigate error interference, a phenomenon where errors in different segments can destructively interfere, leading to non-linear error accumulation. We establish a general framework for algorithmic error interference and provide sufficient and necessary conditions for its occurrence. Additionally, we present an approximate version of error interference that yields tighter error bounds than previous approaches. Our findings extend the understanding of error interference phenomena beyond the two-term Hamiltonian case, including higher-order Trotter formulas and more complex Hamiltonians with speed-ups in implementing Hamiltonian simulation and digital adiabatic algorithms. These results have practical implications for Hamiltonian simulation implementation and may inspire more algorithm designs to exploit error interference for reducing total error in quantum simulations and related tasks.

I. INTRODUCTION

Simulating quantum dynamics is a central application of quantum computation [1, 2]. Efficient quantum algorithms have been proposed for simulating the Schrodinger equation of a general quantum system [3–6], a notoriously difficult task for classical computers. Quantum simulation has wide applications in quantum chemistry [7–9] and quantum field theories [10], and also serves as an indispensable subroutine for other fundamental quantum algorithms, such as quantum phase estimation [11] and the HHL algorithm [12] for solving linear systems.

Since the first digital quantum dynamics simulation algorithm based on the product formula for k-local Hamiltonians proposed by Lloyd [3], novel techniques such as truncated Taylor series (LCU) [13, 14] and Quantum Signal Processing (QSP) [15–17] have been developed, and the algorithms have been improved to optimal or nearly optimal complexity with respect to several key parameters [15–21]. Nevertheless, variants of the product formula are still promising candidates for near-term quantum devices to achieve practical quantum advantages [22] due to their simplicity, mild hardware requirements, and decent performance in practice.

For a given Hamiltonian $H = \sum_{l=1}^{L} H_l$, implementing product formula (PF), also known as Trotter-Suzuki formula, requires dividing the long-time evolution $e^{-\mathrm{i}Ht}$ into several segments r and approximating the short-time evolution $e^{-\mathrm{i}Ht/r}$ using the pth-order product formula $\mathscr{U}_p(t)$ [23], e.g., $\mathscr{U}_1(t) := e^{-\mathrm{i}H_1 t}e^{-\mathrm{i}H_2 t}\cdots e^{-\mathrm{i}H_L t}$, with an error term $\epsilon = \|\mathscr{U}_1(t/r) - e^{-\mathrm{i}Ht/r}\|$. The total error called Trotter error can be upper-bounded by $r\epsilon$ via the triangle inequality. Increasing r results in a smaller Trotter error. Before implementation, it is necessary to estimate the total error and choose an appropriate r to suppress the total error under a predetermined threshold. Thus, understanding the performance of Trotter errors is an important topic. A tighter analysis can help save gate costs in both Hamiltonian simulation [24, 25] and other product formula related tasks, such as imaginary time evolution [26], quantum Monte Carlo [27, 28], quantum adiabatic algorithms [29], and quantum phase estimation [30]. Although a few attempts have been made in this direction [31–37], there still exists a gap between empirical results and theoretical analysis, even for the simple case like simulating power-law decaying interactions Hamiltonians with the first-order product formula.

Recently, it has been found that for the first-order product formula (PF1) with $H = A + B$, errors in different segments can have destructive error interference, and the total error may not increase linearly with the number of segments r [36]. This error interference phenomenon can be explained from a second-order product formula perspective [38] and can also result in speed-up in various applications, e.g., quantum adiabatic algorithms [29], and quantum phase estimation [30]. However, we still lack systematic proof and understanding of this error interference phenomenon. Currently, error interference only exists in the two-term case $H = A + B$ with PF1, which can not explain the error interference phenomenon in the three-term cases $H = A + B + C$ with PF1 [33]. Many questions remain, such as when we will have error interference, whether we can go beyond the two-term case and observe error interference in higher-order product formulas, whether there are approximate interference cases, and how to utilize this interference in algorithm design.

In this work, we establish a general framework for algorithmic error interference in product formula quantum simulation methods and provide sufficient and necessary conditions for error interference. Next, we give a general theoretical lower bound for algorithmic error accumulation, which in various cases excludes the possibility of error interference, e.g., when considering quantum signal processing algorithms. As applications, we provide more examples with (approximate) error interference phenomena beyond the $H = A + B$ case, including $H = A + B + C$ cases in the Heisenberg model, Fermi-Hubbard model, and power-law interaction models. For example, for power-law interaction Hamiltonians, we can use our result to have improved error bounds. The approximate error interference also exists in higher-order product formula approximation of perturbative evolution and can lead to speed-ups in some regions of implementing digital adiabatic algorithms. Our results are fundamentally interesting, furthering our understanding of the product formula theory, and practically useful, directly applicable to the implementation of Hamiltonian simulation using realist quantum hardware. Leveraging our error interference bounds, our results may also inspire better algorithm designs to reduce the total error [37].

II. INTERFERENCE THEORY

A. Asymptotic error interference of product formulas

For a given Hamiltonian $H = \sum_{l=1}^{L} H_l$ of L terms, the first-order product formula (PF1), also known as the Trotter-Suzuki formula [23, 39], can approximate the quantum dynamics $e^{-\mathrm{i}\delta t H}$ by the product of the dynamics of each term, that is

$$\mathscr{U}_1(\delta t) := e^{-\mathrm{i}H_1\delta t} e^{-\mathrm{i}H_2\delta t} \cdots e^{-\mathrm{i}H_L\delta t} = \overrightarrow{\prod_l} e^{-\mathrm{i}H_l\delta t}. \tag{1}$$

As the Hamiltonian terms H_l are not commutative to each other in general, the introduced approximation error (we will call it Trotter error throughout the paper) is upper bounded $\left\|\mathscr{U}_1(\delta t) - e^{-\mathrm{i}H\delta t}\right\| = \mathcal{O}(\alpha_{comm}\delta t^2)$ where $\|\cdot\|$ is the spectral norm and $\alpha_{comm} = \sum_{l_1,l_2=1}^{L} \|[H_{l_2}, H_{l_1}]\|$. For a long time evolution $e^{-\mathrm{i}tH}$, we can divide the whole evolution into several segments r and repeatedly apply the product formula for $\delta t = t/r$, i.e., $\mathscr{U}_1^r(t/r)$. To suppress the algorithmic error, the second-order product formula can be defined as $\mathscr{U}_2(\delta t) := \prod_l^{\rightarrow} e^{-\mathrm{i}H_l\delta t/2} \prod_l^{\leftarrow} e^{-\mathrm{i}H_l\delta t/2}$, where $\prod_l^{\leftarrow}$ denotes a product in reverse order. More generally, a p-th order Suzuki product formula (PFp) $\mathscr{U}_p(\delta t)$ can be defined recursively. In most error analyses, a triangle inequality is applied and the total error is bounded

$$\left\|\mathscr{U}_p^r(t/r) - e^{-\mathrm{i}tH}\right\| \leq r \left\|\mathscr{U}_p(t/r) - e^{-\mathrm{i}Ht/r}\right\| \tag{2}$$

In some cases, the error in each segment may have the interference and the triangle inequality error bound is pessimistic, e.g., a two-term Hamiltonian $H = A + B$ [40, 41], and Hamiltonians with a power-law rapidly decaying interactions [33].

B. Asymptotic error interference of product formulas

In this section, we study the accumulation of error in the product formula and give general criteria on when the error would exhibit a feature of *interference*, and prove the error interference property of the error rigorously.

Definition 1 (Interference, informal)**.** For a pth-order product formula $\mathscr{U}(t/r)$ approximating $e^{-\mathrm{i}Ht/r}$, if the total error grows sublinearly to the sum of error of each timestep, i.e.,

$$\left\|\mathscr{U}_p^r(t/r) - e^{-\mathrm{i}Ht}\right\| = o\Big(r \left\|\mathscr{U}_p(t/r) - e^{-\mathrm{i}H(t/r)}\right\|\Big), \tag{3}$$

where $\|\cdot\|$ denotes the spectral norm and when t and r/t are both large enough, then we say that the Trotter error *interferes*.

The requirement in the definition that t and r/t needs to tend to infinity simultaneously might seem weird at the first glance, but it is the correct way to define interference in an asymptotic way: say, take the result in [40] as an example, they show that the trotter error of two-term PF1 for lattice Hamiltonians can be bounded by $\mathcal{O}\Big(n\frac{t}{r} + n\frac{t^3}{r^2}\Big)$,

while the bound by accumulation is $\mathcal{O}\left(n\frac{t^2}{r}\right)$. The interference bound would be better than the accumulation bound asymptotically only if both t and $r/t = 1/\delta t$ tends to infinity.

To explore the error accumulation, we apply a new error analysis which directly estimates the error for a long time evolution. We can express the approximated evolution by an effective Hamiltonian H_{eff} with $\exp(-\mathrm{i}\delta t H_{\text{eff}}) = \exp(-\mathrm{i}\delta t(H + H_{\text{error}}))$ where H_{error} is the exponentiated error term. Suppose the Hermitian H has spectral decomposition $H = P\Lambda P^*$ where $P \in SU(d)$ and Λ is diagonal. Diagonal elements of Λ are exactly the eigenvalues of H, and their corresponding eigenstates are exactly the columns of P. Thus, the ideal evolution can rewritten as $\exp(-\mathrm{i}\delta t H) = P\exp(-\mathrm{i}\delta t(\Lambda))P^*$. The approximated evolution $\exp(-\mathrm{i}\delta t H_{\text{eff}})$ can also be spectral decomposed as $\exp(-\mathrm{i}\delta t H_{\text{eff}}) = (P + \delta P)\exp(-\mathrm{i}\delta t(\Lambda + \delta\Lambda))(P + \delta P)^\dagger$ where δP and $\delta\Lambda$ are the deviations in eigenvectors and eigenvalues, respectively. For a long time evolution, the approximated evolution is repeated r times, $\exp(-\mathrm{i}r\delta t H_{\text{eff}}) = (P+\delta P)\exp(-\mathrm{i}r\delta t(\Lambda + \delta\Lambda))(P+\delta P)^\dagger$. The error in eigenvectors remains δP, regardless of r, while the error in eigenvalues will accumulate $r\delta t\delta\Lambda$. As a result, the total error is roughly $\delta P + r\delta t\delta\Lambda$. Considering that δP is independent of total time t and the number of segments, the accumulation of error mainly stems from the second term, $r\delta t\delta\Lambda$. If $r\delta t\delta\Lambda$ is much smaller than δP, the total error will show a sublinear accumulation phenomenon.

Hereafter, we mainly focus on product formula methods. For PFp, the exponentiated error term H_{error} is $\mathcal{O}(\delta t^p)$. We can rewrite this error as $H_{\text{error}} = R\delta t^p + R_{re}$, where R is the leading-order terms in Trotter error and R_{re} is the high-order remainder with $\|R_{re}\| = \mathcal{O}(\delta t^{p+1})$. In general, δP and $\delta\Lambda$ are both $\mathcal{O}(\|R\|\delta t^p)$ and the Trotter error in one segment is $\|\mathscr{U}(\delta t) - e^{-\mathrm{i}\delta t H}\| = \mathcal{O}(\delta t(\delta\Lambda + \delta P)) = \mathcal{O}(\|R\|\delta t^{p+1})$. For a long time evolution with a total error $\delta P + t\delta\Lambda$, the second term $t\delta\Lambda$ will dominate, leading to a $\mathcal{O}(\|R\|t^{p+2}/r^{p+1})$ total error. Interestingly, when a specific condition is satisfied, $\delta\Lambda$ will be surprising small the growth of total error will not accumulate linearly with the number of Trotter steps and appear the phenomenon of error interference. We express this result in the following theorem.

Definition 2 (Orthogonality condition)**.** Consider a given Hamiltonian evolution $e^{-i\delta t H}$ and its approximation $e^{-\mathrm{i}\delta t H_{\text{eff}}}$. If the leading-order term R of $H_{\text{error}} = H - H_{\text{eff}}$ satisfies that

$$\langle\psi_i|R|\psi_i\rangle = 0 \tag{4}$$

for all eigenstates $|\psi_i\rangle$ of H. We say this approximation $e^{-\mathrm{i}\delta t H_{\text{eff}}}$ satisfies an orthogonality condition

Theorem 1 (Neccesary and sufficient condition for error interference)**.** *The orthogonality condition is a necessary and sufficient condition for error interference. Suppose that $H_{error} \approx Rt^p/r^p$, the total error can be bounded by*

$$\left\|e^{-\mathrm{i}H_{eff}t} - e^{-\mathrm{i}Ht}\right\| = \mathcal{O}\left(\|R\|\left(\frac{t^p}{r^p} + \|R\|\frac{t^{2p+1}}{r^{2p}}\right)\right). \tag{5}$$

If $e^{-\mathrm{i}\delta t H_{eff}}$ do not satisfy the orthogonality condition, then the error term would be

$$\left\|e^{-\mathrm{i}H_{eff}t} - e^{-\mathrm{i}Ht}\right\| = \Omega\left(\frac{t^{p+1}}{r^p}\max_i\langle\psi_i|R|\psi_i\rangle\right). \tag{6}$$

The orthogonality requirement $\langle\psi_i|R|\psi_i\rangle = 0$ is equivalent to that there exsits a matrix M such that $[H, M] = R$. The condition also has a necessary criteria

$$\mathrm{Tr}\left(RH^k\right) = 0, \forall k \geq 1. \tag{7}$$

We can recover the results in [36] and [38] from Theorem 1. For a two-term Hamiltonian $H = H_1 + H_2$, the first-order trotter error behaves like $\mathscr{U}_1(\delta t) = \exp\left(-\mathrm{i}\delta t H + \delta t^2 R + o(\delta t^2)\right)$, where $R = [H_1, H_2] = [H_1 + H_2, H_2]$, thus the error term satisfies the orthogonal requirement. So, we can conclude that the error of first-order product formula would interfere and grow sublinearly.

There are more examples of dynamics exhibiting error interference. We will postpone the examples after Theorem 7. As a corollary of Theorem 1, we get immediately a sufficient condition that when the error would accumulate linearly.

Corollary 1 (Error lower bound)**.** *For a formula $\mathscr{U}(t)$ approximating $e^{-\mathrm{i}Ht}$ and its leading error is R in the sense that $\mathscr{U}(t) = e^{-\mathrm{i}Ht + Rt^{p+1}/r^{p+1} + o(t^{p+1}/r^{p+1})}$, and if $\mathrm{Tr}(RH^n) \neq 0$ for some $n \in \mathbb{N}$, then $\left\|\mathscr{U}^r(t/r) - e^{-\mathrm{i}Ht}\right\| = \Omega(\frac{t^{p+1}}{r^p})$ as t and r/t tends to infinity.*

As a direct corollary, we find that for many physical dynamics, the error of second order trotter formula does not interfere. Consider the toy model: one-dimensional lattice nearest neighbor Ising model $H = \sum_{j=1}^{n-1} X_j X_{j+1} +$

$\sum_{j=1}^{n} Z_j \coloneqq A + B$, the error of PF2 with time δt takes the form $H_{\text{eff}} - H = \frac{\delta t^3}{12} R = \frac{\delta t^3}{12}[A - B, [A, B]]$. It can be confirmed easily that $\text{Tr}(HR) \neq 0$, thus the error does not interfere. Theorem 1 is a general bound for error of any product formula, but it is most useful only for the product formulas. For other types of simulation algorithms like LCU or QSP, the error would just accumulate linearly. This is because the unitary generated by, say LCU algorithm, is a polynomial in the desired dynamics H. Thus the error of the algorithm would have the same eigenbasis with H, so the error does not interfere. Error of QSP simulation is fourier coefficients of the Hamiltonian, which does not interfere either.

Corollary 1 can be used to estimate the long-term error. If we find that the error does not interfere, then we can estimate the total error by just summing up the (empirical) error in each timestep, which could save a lot of computational resources.

C. Approximated interference of Trotter errors

In Theorem 1, we give the criteria of when the error would self-cancel exactly. But sometimes the error might not self-cancel exactly but instead only a major part of the error would "interfere". We will develop the theory of approximation of approximated interference of Trotter errors in this section. First we will derive the approximation formula of the error.

Lemma 2. *Assume that we hope to simulate H, with error term $R = R_1 + R_2$, where R_1, R_2 are some Hermitian matrices, then we have*

$$\left\| e^{-\mathrm{i}(H + t^p/r^p R)t} - e^{-\mathrm{i}Ht} \right\| \leq \|R_2\| \frac{t^{p+1}}{r^p} + \left\| e^{-\mathrm{i}(H + t^p/r^p R_1)t} - e^{-\mathrm{i}Ht} \right\| \tag{8}$$

Thus we can conclude from Lemma 2 that if H has error term R, H and R does not satisfy the condition in Theorem 1, but "a large fraction" of H and "a large fraction" of R satisfies the requirement in Theorem 1, then the error would also accumulate slower than the bound obtained by triangle inequality. This is formalized in the following lemma.

Theorem 3. *Assume that we hope to simulate H, with error term $R = R_1 + R_2$, assume that H is orthogonal respective to R_1, i.e., for any eigenstate $|\psi_i\rangle$ of H, $\langle\psi_i|R_1|\psi_i\rangle = 0$, then we have*

$$\left\| e^{-\mathrm{i}(H + t^p/r^p R)t} - e^{-\mathrm{i}Ht} \right\| = \mathcal{O}\left(\|R_2\| ht + \|R_1\| \left(\frac{t^p}{r^p} + \|R_1\| \frac{t^{2p+1}}{r^{p+1}} \right) \right) \tag{9}$$

In Theorem 3, we can see that when R_2 is small enough, namely both the target dynamics and the error is close to interference dynamics, then a large part of the error would not accumulate linearly.

Thus we can conclude that for any dynamics $H = H_1 + H_2$, and if error of product formula simulating H_1 would interfere, and $\|H_2\|$ is relatively small, then product formula simulating H would also have a relatively small error. We will formalize this in the following theorem.

Theorem 4. *Assume that $H = H_1 + H_2$, and each consists of terms $H_1 = \sum_l H_{1,l}, H_2 = \sum_j H_{2,j}$. Let $R_{12} = [H_1, H_2], R_1 = \sum_{l_1 < l_2} [H_{1,l_1}, H_{1,l_2}], R_2 = \sum_{l_1 < l_2} [H_{2.l_1}, H_{2,l_2}]$, and H is orthogonal to R_1, assume that r is some positive integer, then we have*

$$\begin{aligned} \left(\prod_l e^{-\mathrm{i}t/r H_{1,l}} \prod_j e^{-\mathrm{i}t/r H_{2,j}} \right)^r =& e^{-\mathrm{i}tH} + \mathcal{O}\Big(\frac{t^2}{r} (\|R_2\| + \|R_1\| \, \|H_2\| \, t) + \\ & \frac{t}{r} \|R_1\| \, \|H_1\| + \frac{t^3}{r^2} (\|R_{12}\| \, \|H\| + \|R_{12}\| \, \|R_1\| + \|R_1\| \, \|H\|) \Big) \end{aligned} \tag{10}$$

We can apply Theorem 3 to lattice Hamiltonians with power law interactions. More specifically, consider a Heisenberg dynamics with power-law interactions $H_{\text{pow}_\alpha} = \sum_{1 \leq j < k \leq n} \frac{1}{|j-k|^\alpha} (X_j X_k + Y_j Y_k + Z_j Z_k) + \sum_{j=1}^{n} h_j Z_j$ can be divided as $H_{\text{pow}_\alpha} = H_{\text{nn}} + H_{\text{li}}$, where H_{nn} refers to the terms acted on single site or nearest neighbors, and H_{li} refers to the long interactions. Then H_{li} would be small when α is large. Our theory could bound the error as $O(\frac{nt^2}{(\alpha-1)r} + \frac{nt}{r})$, while triangle inequality could bound the error as $O(\frac{nt^2}{r})$.

For higher order PF, we can show the error would interfere when one of H_i is much larger than all others. We show only rigorously for two-terms PF2, but similar techniques can be applied to higher order PF with more terms.

Theorem 5 (Approximate error interference of PF2 of two terms when one term is the major term). *For $H = H_1+H_2$, then the error of PF2 formula $\mathscr{U}_2(\tau) = e^{-\mathrm{i}H_1\tau/2}e^{-\mathrm{i}H_2\tau}e^{-\mathrm{i}H_1\tau/2}$ can be bounded as*

$$\left\|\mathscr{U}_2(t/r)^r - e^{-\mathrm{i}Ht}\right\| \leq \frac{1}{6}\left\|[H_1,H_2]\right\|\frac{t^3}{r^3} + \frac{1}{6}\left\|[H_2,[H_1,H_2]]\right\|\frac{t^3}{r^2} + \mathcal{O}\left(\|T\|\frac{t^4}{r^3}\right) \tag{11}$$

where $T = [H_1,[H_2,[H_1,H_2]]]$

Remark. This theorem shows that the error of 2 term PF2 would interfere when H_1 is much larger than H_2. Say in the case that both H_1 and H_2 are lattice Hamiltonian, and H_2 has a small norm, say $\|H_2\| \leq a$. Then the bound obtained by triangle inequality is $O(an\frac{t^3}{r^2})$. Theorem 5 could give a bound $O(a^2n\frac{t^3}{r^2} + an\frac{t^3}{r^3})$. The result can be generalized to higher order PF with more terms in a straightforward manner. As long as there is a leading term H_i much larger than all other H_j, then the error would interfere.

D. Exact error interference bound for the first-order product formula

In Theorem 1, we work with large $\mathcal{O}$ factors, ignoring the hidden constant in the convergence rate. We also hope to calculate the explicit constant factors when we want to give an explicit bound on the error. So here we will prove a theorem with explicit constant factors. The following theorem is a more explicit form of Theorem 1 in the case of PF1. In the case of PF1, we can show rigorously that the errors would interfere and grow sublinearly.

Theorem 6 (Tight upper bound for general error interference). *Let H and R be Hermitians, let h be any real parameter. Let $\{|\psi_i\rangle\}$ and $\{|\psi_i'\rangle\}$ be the eigenvectors of H and $H+hR$ respectively and let $\{\lambda_i\},\{\lambda_i'\}$ be the corresponding eigenvalues. Then R can be decomposed as $R = \sum b_{jk}|\psi_j\rangle\langle\psi_k'|$. For any $\epsilon > 0$, let $\Delta_H^\epsilon(R) = \sum_{0\leq\lambda_j-\lambda_k'<\epsilon} b_{jk}|\psi_j\rangle\langle\psi_k'|$, for $\epsilon < 0$, define $\Delta_H^\epsilon(R) = \sum_{\epsilon<\lambda_j-\lambda_k'\leq 0} b_{jk}|\psi_j\rangle\langle\psi_k'|$, and $\mathcal{R}_H^\epsilon(R) = \sum_{|\lambda_j-\lambda_k'|\geq\epsilon}\frac{1}{\lambda_j-\lambda_k'}b_{jk}|\psi_j\rangle\langle\psi_k'|$. Then we have*

$$\|\exp(-\mathrm{i}(H+hR)t) - \exp(-\mathrm{i}Ht)\| \leq 4h\max_{|\epsilon'|\leq\epsilon}\left\|\Delta_H^{\epsilon'}(R)\right\|t + 2h\left\|\mathcal{R}_H^\epsilon(R)\right\| \tag{12}$$

Theorem 7 (Tight upper bound for PF1). *Assume H_i to be Hermitian. Let $\mathscr{U}_1(\delta t) = \prod_l^{\rightarrow} e^{-\mathrm{i}\delta t H_l}$ be the first-order product formula. Assume $\mathscr{U}_1(\delta t)$ is acted r times and $T = r\delta t$. Define $R := \sum_{j<k}[H_j,H_k]$. Define $|\psi_i\rangle$ and $|\psi_i'\rangle$ to be the eigenvectors of H and $H+\frac{\delta t}{2\mathrm{i}}R$, and the corresponding eigenvectors are λ_i and λ_i'. Define $R := \sum_{j<k}[H_j,H_k]$ and it can be decomposed as $R = \sum b_{jk}|\psi_j\rangle\langle\psi_k'|$. For any ϵ, define $\Delta_H^\epsilon(R)$ and $\mathcal{R}_H^\epsilon(R)$ similarly to the definition in Theorem 6. Then we have that*

$$\|\mathscr{U}_1(\delta t)^r - \exp(-\mathrm{i}HT)\| \leq \|L_1(H)\|\frac{T^3}{r^2} + \|\Delta_H^\epsilon(R)\|\frac{T^2}{r} + \|\mathcal{R}_H\|\frac{T}{r} + \|L_2(H)\|\frac{T^4}{r^3} \tag{13}$$

where

$$L_1(H) = \frac{1}{2}\sum_i\left\|\sum_{i<l<k}[H_i,[H_l,H_k]]\right\| + \frac{1}{6}\sum_i\left\|\sum_{l>i}[H_i,[H_i,H_l]]\right\|$$

$$L_2(H) = \frac{1}{12}\sum_i\left\|\sum_{i<l<k}[H_i,[H_i,[H_l,H_k]]]\right\|$$

Remark. In Eq. (12) and Eq. (13), the leading term of the error is controlled by the norm of $\Delta_H^\epsilon(R)$ and $\mathcal{R}_H(R)$. $\Delta_H^\epsilon(R)$ can be viewed as the (almost) diagonal terms of R in the eigenbasis of H, while $\mathcal{R}_H^\epsilon(R)$ represents the off-diagonal terms of R in the eigenbasis of H. When $\Delta_H^0(R) = 0$, which is exactly the condition of Theorem 1, the error would behave as PF2 as long as r tends to infinity. But if $\mathcal{R}_H^\epsilon(R)$ is too large, then the error would grow as PF1 until r is large enough. In the real world, we observe that $\mathcal{R}(H)$ is generally of reasonable scale so we can say that the existence of interference is equivalent to $\Delta_H^0(R) = 0$

Remark. As a concrete example, PF2 would have a large $\Delta_H(R)$, meaning the error does not "interfere" and would accumulate linearly according to the triangle inequality.

III. APPLICATIONS

In this section, we present applications of our results, including numerical evidence to support our theory and better error analysis of certain algorithm.

A. Heisenberg model

The Heisenberg model is a typical quantum lattice many-body and its dynamics shows the feature of interference when the system size is small. In Fig. 1, we compare the empirical error and theoretical error bounds of the nearest-neighbor Heisenberg model

$$H_{\mathrm{nn}} = H_X + H_Y + H_Z \tag{14}$$

$$= J_x \sum_{j=1}^{n-1} X_j X_{j+1} + J_y \sum_{j=1}^{n-1} Y_j Y_{j+1} + \sum_{j=1}^{n-1} (J_z Z_j Z_{j+1} + h Z_j) \tag{15}$$

implemented by PF1 with tri-group (XYZ)

$$\mathscr{U}_1(\delta t) = e^{-\mathrm{i}\delta t H_X} e^{-\mathrm{i}\delta t H_Y} e^{-\mathrm{i}\delta t H_Z}. \tag{16}$$

The interference bound is obtained by the estimation as in Eq. (13). We can find that our bound matches the empirical error better than the triangle bound.

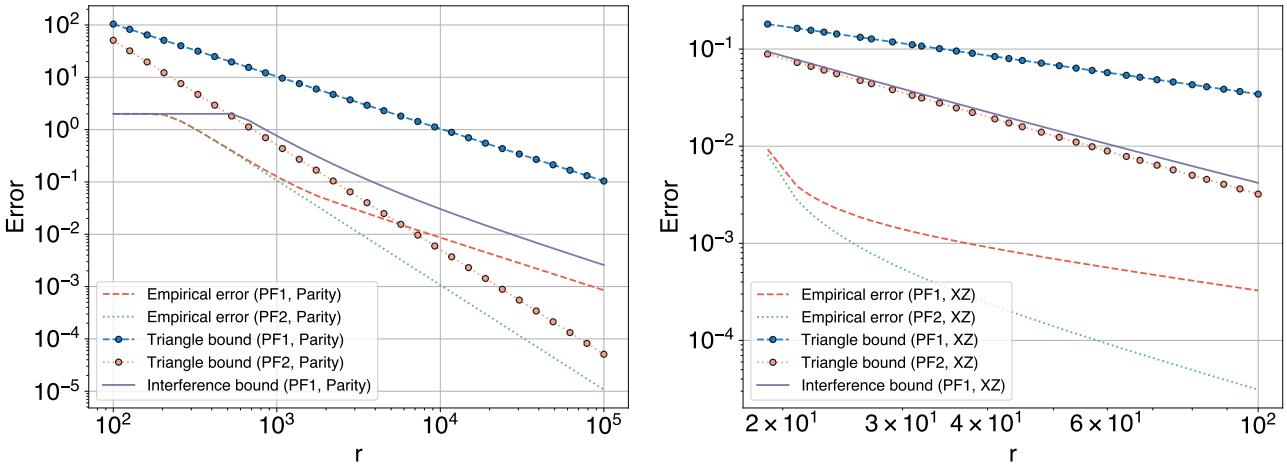


FIG. 1: (Left) Empirical Trotter error and theoretical error bounds of 8 qubits one-dimensional nearest-neighbor Heisenberg model ($J_x = J_y = J_z = 2$, $h = 0.5$). The green starred line is the empirical error of PF1 with tri-group (XYZ), while the purple dash line is its triangle bound, and the pink solid line is the interference bound for bi-group $L = 2$. We can see that the interference bound gives a much better estimation of the error scaling. On the other hand, the red dotted line represents the empirical error of PF1 with bi-group (Parity), while the orange dashed line is the error bound given by the triangle bound. We can find that triangle bound is almost tight, so the triangle bound gives the tight estimation of the error. We also plot the empirical error and the triangle bound of PF2 with bi-group for reference. (Right) We observe the interference of Trotter error for both PF1 and PF2 with XZ grouping when the Heisenberg model has the parameters ($J_x = 2$, $J_y = J_z = 0$, $h = 0.001$).

In contrast, we notice that fully connected Heisenberg model $H_{\mathrm{all}} = H'_X + H'_Y + H'_Z$ where $H'_X = \sum_{j<k} X_j X_k$, $H'_Y = \sum_{j<k} Y_j Y_k$, and $H'_Z = \sum_{j<k} Z_j Z_k + \sum_j Z_j$. With the similar tri-group (XYZ) to Eq. (15), the Trotter error of $\mathscr{U}_1(\delta t) = e^{-\mathrm{i}\delta t H'_X} e^{-\mathrm{i}\delta t H'_Y} e^{-\mathrm{i}\delta t H'_Z}$ does not interfere.

For the fully-connected Heisenberg model with power-law (decaying) interactions

$$H_{\mathrm{pow}_\alpha} = \sum_{j=1}^{n-1} \sum_{k=j+1}^{n} \frac{1}{|j-k|^\alpha} (X_j X_k + Y_j Y_k + Z_j Z_k) + \sum_{j=1}^{n} h Z_j,$$

where $\alpha > 0$ is the decaying coefficient, the error would decrease along with the the increase of α. In Section III A, we depict the Trotter error of PF1 with 6-qubit H_{pow_α}. The triangle bound and our bound are of the same origin as Fig. 1. We can find that our bound matches the error better when α is large, supportng the result in Lemma 2.

We can analyze asymptotically the error bound of α when error of PF1 of H_{nn} interferes. In such case, we can write $H_{\text{pow}_\alpha} = H_{\text{nn}} + H_{\text{li}}$, where H_{li} refers to the long interaction. Then the error of H_{nn} interferes, thus the error is $\mathcal{O}(n\frac{t^3}{r^2} + n\frac{t}{r})$. According to Lemma 2, the error scale of PF1 of H can be bounded by $\mathcal{O}(n\frac{t^3}{r^2} + n\frac{t}{r} + \alpha n^2\frac{t^2}{r})$, which tends to interfere when α is large. Our theoretical bound is an indicator of when approximate interference would happen as self healing of error does appear when α is large as we show numerically.

Our analysis also gives a better bound on the number of timesteps needed for reaching certain precision, therefore a better bound on the number of total gates required for the simulation. In Section III A, we show the numerical estimation of required timesteps r, both (numerically) empirically and theoretically. The empirical error of the simulation grows as $\mathcal{O}(n^{2.75})$. The bound by triangle inequalities could bound the number of required r as $\mathcal{O}(n^{3.39})$. Our bound could bound the required time step to $\mathcal{O}(n^{2.86})$, which is a better estimation of r.

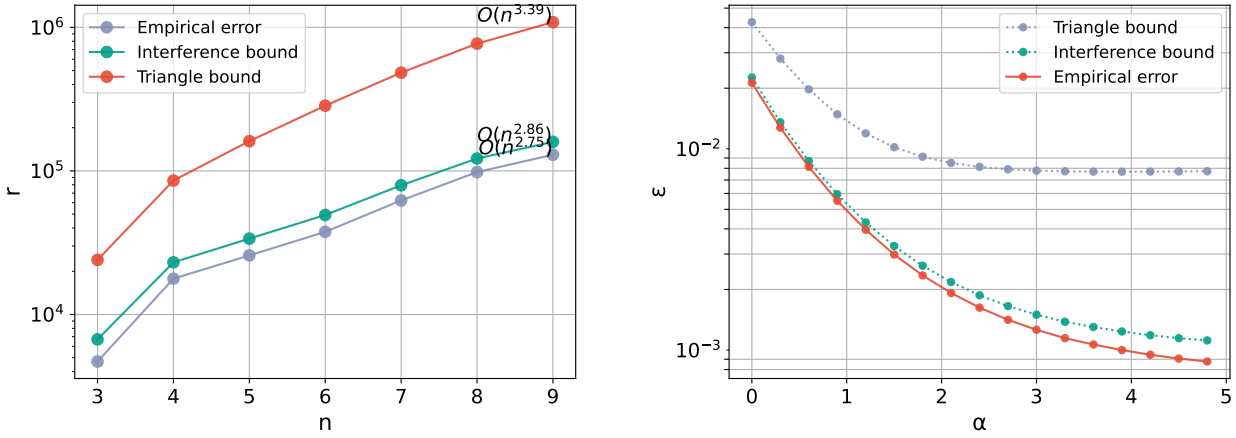


FIG. 2: (left) Numerical evaluation of number of timesteps r needed to achieve the fixed error threshold (here the threshold is the spectral norm of error not exceeding 0.01) and the estimations of r given by different bounds. The dynamics is 1-D lattice power-law Heisenberg model and the decaying coefficient $\alpha = 4$. The numerical evidence needs $O(n^{2.75})$ timesteps. The estimation from triangle inequality could bound the required timesteps as $O(n^{3.39})$ while our results could bound r as $O(n^{2.86})$. Here n refers to the system size, and r refers to the number of trotter steps required. (right) Numerical evaluation of error for the first-order product formula (PF1) of 1D power-law Heisenberg model on 8 qubits. The purple line is the empirical error, the red line is the interference bound, and the green line is the bound obtained by triangle inequality. We can find that the interference bound gives a nice estimation of the error. Here α refers to the decaying coefficient of the dynamics, and ε is the trotter error.

Generally, the second-order formula (PF2) does not interfere. Thus, the bound by the triangle inequality is tight for most cases of PF2. For example, even for simple models like bi-group of 1D nearest-neighbor Heisenberg model, consider the partition according to the parity (even-odd) of the site index of each Hamiltonian term $H = H_{\text{even}} + H_{\text{odd}}$ with

$$H_{\text{even}} = \sum_{j=1}^{\lfloor L/2 \rfloor} (X_{2j-1}X_{2j} + Y_{2j-1}Y_{2j} + Z_{2j-1}Z_{2j} + hZ_{2j-1})$$

$$H_{\text{odd}} = \sum_{j=1}^{\lceil L/2 \rceil - 1} (X_{2j}X_{2j+1} + Y_{2j}Y_{2j+1} + Z_{2j}Z_{2j+1} + hZ_{2j})$$

where all the summands in H_{even} (and H_{odd}) commute with each other. In Fig. 1, the numerical simulation shows that the error of PF2 follows exactly the bound of the triangle inequality (cf. [6, Eq. (152)]).

Notice that for PF1 with tri-group of 1D Heisenberg Hamiltonian where the terms are partitioned according to the type of Pauli operators. We can find that the dynamics satisfies $\Delta_H(R) = 0$ when n is small (Theorem 7). Namely, the evolution of the error "interferes".

B. Fermi-Hubbard model

The Fermi-Hubbard model on one-dimensional lattice of L sites is described by the Hamiltonian $H_{\text{FH}} = H_{\text{even}} + H_{\text{odd}} + H_{\text{int}}$ with three groups

$$H_{\text{even}} = v \sum_{j=1}^{\lfloor L/2 \rfloor} \sum_{\sigma \in \{\uparrow,\downarrow\}} a^\dagger_{2j-1,\sigma} a_{2j,\sigma} + a^\dagger_{2j,\sigma} a_{2j-1,\sigma},$$

$$H_{\text{odd}} = v \sum_{j=1}^{\lceil L/2 \rceil - 1} \sum_{\sigma \in \{\uparrow,\downarrow\}} a^\dagger_{2j,\sigma} a_{2j+1,\sigma} + a^\dagger_{2j+1,\sigma} a_{2j,\sigma},$$

$$H_{\text{int}} = u \sum_{j}^{L} n_{j,\uparrow} n_{j,\downarrow}$$

where j refer to neighboring lattice sites in the first sum, $v \in R$ is the kinetic hopping coefficient, and $u > 0$ the on-site interaction strength. $a^\dagger_{j,\sigma}$, $a_{j,\sigma}$ and $n_{j,\sigma} = a^\dagger_{j,\sigma} a_{j,\sigma}$ are the fermionic creation, annihilation and number operators, respectively, acting on site j and spin $\sigma \in \{\uparrow,\downarrow\}$. It can be observed in Fig. 3 that the interference is weaker when the norm of the interaction term H_{int} is stronger compared to the hopping terms.

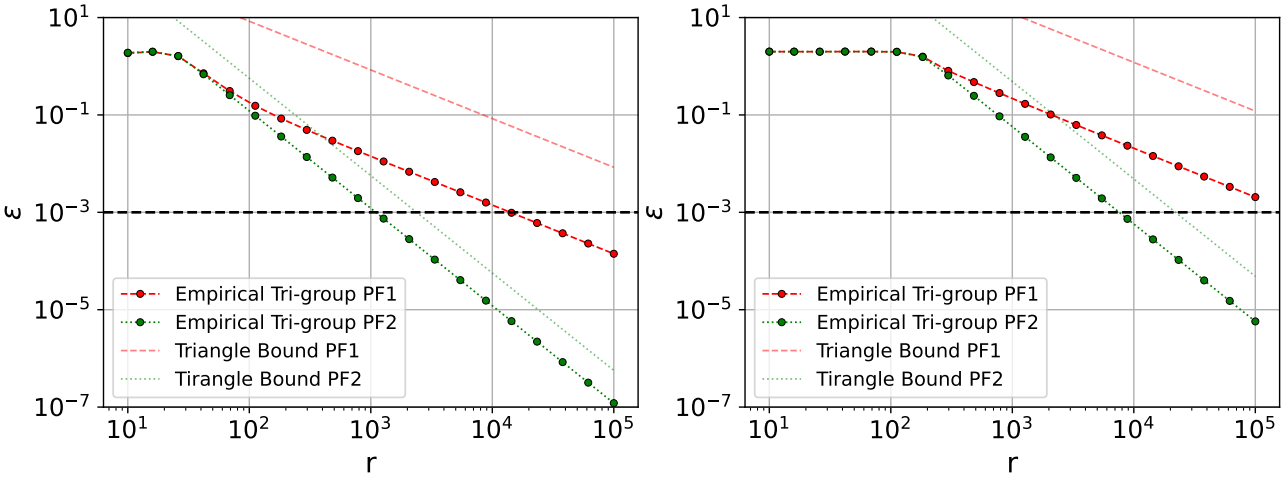


FIG. 3: Empirical Trotter error and bounds of PF1 and PF2 for tri-group 1D Fermi-Hubbard model with 4 sites (8 qubits). The interaction strength u is $0.1v$ for the left figure and $10v$ for the right one.

C. Adiabatic evolution and perturbation theory

Our bound would also give a better analysis of a product formula than the triangle bound if one of the terms in the product formula is significantly larger than all the other terms.

We'll take two-term PF2 as an illustrative example. For a two-term Hamiltonian $H = H_1 + H_2$, according to Corollary 1, interference of the error has a necessary criteria $\operatorname{tr} RH = 0$. For two-term PF2, we have $R = [H_1 - H_2, [H_1, H_2]]$. We can verify that for multi-partite physical systems such as Heisenberg model or Fermi-Hubbard model, so the errors does not interfere exactly.

However, when one of the H_i is relatively small, the error would approximately interfere. For example, assume $H = H_1 + \alpha H_2$, where α is a small constant. Then the leading error term R of PF2 can be expressed as $R = [H_1 - \alpha H_2, [H_1, \alpha H_2]] = [H_1 + \alpha H_2, [H_1, \alpha H_2]] - 2[\alpha H_2, [H_1, \alpha H_2]]$. Notice that the first term is of the form $[H, M]$, so this part of the error would interfere. So the linearly accumulated error is of the scaling $O(\alpha^2 t)$ while the triangle inequality would bound the error growth as $O(\alpha t)$.

The assumption that one of the H_i is relatively small makes sense in the start and end of adiabatic evolution, also applies to the simulation of perturbation dynamics. Recall that for adiabatic evolution implements a Hamiltonian

with two terms, $H[u(\tau)] = (1-u(\tau))H_1 + u(\tau)H_2$, and u is a continuous function satisfying the requirement $u(0) = 0, u(t) = 1$. In [29], they show that error of PF1 of adiabatic evolution has the self-healing property. Our results could show that the error interferes when τ is close to 0 or t even for higher order PF. Also one of H_i to be small is naturally the setting that the simulation of a perturbation dynamics. A perturbation dynamics typically contains of two dynamics $H = H_0 + H_1$, where H_0 is large and time-independent and H_1 is small. Thus our theory could also show the existence of error interference in the perturbation model.

Q.Z. acknowledges funding from HKU Seed Fund for Basic Research for New Staff via Project 2201100596, Guangdong Natural Science Fund—General Programme via Project 2023A1515012185, National Natural Science Foundation of China (NSFC) Young Scientists Fund via Project 12305030, 27300823, Hong Kong Research Grant Council (RGC) via No. 27300823, and NSFC/RGC Joint Research Scheme via Project N_HKU718/23.

* xiaoyuan@pku.edu.cn
† zhaoqi@cs.hku.hk

[1] R. P. Feynman, Int J Theor Phys **21**, 467 (1982).
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, Cambridge ; New York, 2010).
[3] S. Lloyd, Science **273**, 1073 (1996).
[4] S. P. Jordan, K. S. M. Lee, and J. Preskill, Science **336**, 1130 (2012), arxiv:1111.3633.
[5] S. McArdle, S. Endo, A. Aspuru-Guzik, S. C. Benjamin, and X. Yuan, Quantum computational chemistry (2020), arxiv:1808.10402.
[6] A. M. Childs, Y. Su, M. C. Tran, N. Wiebe, and S. Zhu, Phys. Rev. X **11**, 011020 (2021), arxiv:1912.08854.
[7] D. Wecker, B. Bauer, B. K. Clark, M. B. Hastings, and M. Troyer, Phys. Rev. A **90**, 022305 (2014).
[8] R. Babbush, J. McClean, D. Wecker, A. Aspuru-Guzik, and N. Wiebe, Phys. Rev. A **91**, 022311 (2015).
[9] R. Babbush, P. J. Love, and A. Aspuru-Guzik, Scientific Reports **4**, 6603 (2014).
[10] S. P. Jordan, K. S. Lee, and J. Preskill, Science **336**, 1130 (2012).
[11] A. Y. Kitaev, Quantum measurements and the Abelian Stabilizer Problem (1995), arxiv:quant-ph/9511026.
[12] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009), arxiv:0811.3171 [quant-ph].
[13] A. M. Childs and N. Wiebe, QIC **12**, 10.26421/QIC12.11-12 (2012), arxiv:1202.5822.
[14] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma, Phys. Rev. Lett. **114**, 090502 (2015).
[15] G. H. Low and I. L. Chuang, Phys. Rev. Lett. **118**, 010501 (2017).
[16] G. H. Low and I. L. Chuang, Quantum **3**, 163 (2019).
[17] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, Proc. 51st Annu. ACM SIGACT Symp. Theory Comput. , 193 (2019), arxiv:1806.01838.
[18] D. W. Berry, G. Ahokas, R. Cleve, and B. C. Sanders, Commun. Math. Phys. **270**, 359 (2007), arxiv:quant-ph/0508139.
[19] D. W. Berry, A. M. Childs, and R. Kothari, in *2015 IEEE 56th Annu. Symp. Found. Comput. Sci.* (2015) pp. 792–809, arxiv:1501.01715 [quant-ph].
[20] A. M. Childs and Y. Su, Phys. Rev. Lett. **123**, 050503 (2019).
[21] G. H. Low, in *51st Annual ACM Symposium on Theory of Computing* (2019) pp. 491–502.
[22] 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, Nature **618**, 500 (2023).
[23] M. Suzuki, J. Math. Phys. **32**, 400 (1991).
[24] A. M. Childs, Y. Su, M. C. Tran, N. Wiebe, and S. Zhu, Phys. Rev. X **11**, 011020 (2021), arxiv:1912.08854.
[25] A. M. Childs, D. Maslov, Y. Nam, N. J. Ross, and Y. Su, Proc. Natl. Acad. Sci. U.S.A. **115**, 9456 (2018).
[26] M. Motta, C. Sun, A. T. Tan, M. J. O'Rourke, E. Ye, A. J. Minnich, F. G. Brandão, and G. K.-L. Chan, Nature Physics **16**, 205 (2020).
[27] S. Bravyi, Quantum Info. Comput. **15**, 1122–1140 (2015).
[28] S. Bravyi and D. Gosset, Phys. Rev. Lett. **119**, 100503 (2017).
[29] L. K. Kovalsky, F. A. Calderon-Vargas, M. D. Grace, A. B. Magann, J. B. Larsen, A. D. Baczewski, and M. Sarovar, Phys. Rev. Lett. **131**, 060602 (2023), arxiv:2209.06242 [quant-ph].
[30] C. Yi and E. Crosson, npj Quantum Information **8**, 37 (2022).
[31] Y. Su, H.-Y. Huang, and E. T. Campbell, Quantum **5**, 495 (2021).
[32] B. Şahinoğlu and R. D. Somma, npj Quantum Inf **7**, 119 (2021), arxiv:2006.02660 [quant-ph].
[33] Q. Zhao, Y. Zhou, A. F. Shaw, T. Li, and A. M. Childs, Phys. Rev. Lett. **129**, 270502 (2022).
[34] Q. Zhao and X. Yuan, Quantum **5**, 534 (2021), arxiv:2103.07988.
[35] M. Heyl, P. Hauke, and P. Zoller, Science Advances **5**, eaau8342 (2019).
[36] M. C. Tran, S.-K. Chu, Y. Su, A. M. Childs, and A. V. Gorshkov, Phys. Rev. Lett. **124**, 220502 (2020), arxiv:1912.11047 [quant-ph].
[37] M. C. Tran, Y. Su, D. Carney, and J. M. Taylor, PRX Quantum **2**, 010323 (2021).
[38] D. Layden, Phys. Rev. Lett. **128**, 210501 (2022), arxiv:2107.08032 [quant-ph].

[39] S. Lloyd, Science **273**, 1073 (1996).
[40] M. C. Tran, S.-K. Chu, Y. Su, A. M. Childs, and A. V. Gorshkov, Phys. Rev. Lett. **124**, 220502 (2020), arxiv:1912.11047.
[41] D. Layden, Phys. Rev. Lett. **128**, 210501 (2022), arxiv:2107.08032.

Improved recursive QAOA for solving MAX-CUT on bipartite graphs

Eunok Bae[1] * Hyukjoon Kwon[1] V Vijendran[2 3] Soojoon Lee[4 1] †

[1] *School of Computational Sciences, Korea Institute for Advanced Study (KIAS), Seoul 02455, Korea*
[2] *Centre for Quantum Computation and Communication Technologies (CQC2T), Department of Quantum Science, Research School of Physics and Engineering, Australian National University, Acton 2601, Australia*
[3] *A*STAR Quantum Innovation Center (Q.InC), Institute of Materials Research and Engineering (IMRE), Agency for Science, Technology and Research (A*STAR), 2 Fusionopolis Way, Innovis #08-03, Singapore 138634, Republic of Singapore*
[4] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 02447, Korea*

Abstract. Recursive QAOA (RQAOA) is the variant of QAOA to overcome obstacles of low-level QAOA. RQAOA iteratively applies QAOA while progressively reducing the problem size through a recursive process. There are several instances in which RQAOA can get a better solution than QAOA or even get the optimal solution. In this work, we first analytically prove the limitation of the level-1 QAOA for solving MAX-CUT problem on bipartite graphs. Moreover, we observe that RQAOA outperforms QAOA, but it cannot guarantee the optimal solution when the number of nodes increases by numerical simulation. To improve the performance of RQAOA, we propose a modified RQAOA which reduces the region of optimization in QAOA subroutine, and we prove that our modified RQAOA can perfectly solve MAX-CUT on bipartite graphs.

Keywords: Quantum algorithm, QAOA, Recursive QAOA, MAX-CUT, bipartite graph

1 Introduction

Although Quantum Approximate Optimization Algorithm (QAOA) aiming to solve combinatorial optimization problems is considered a promising candidate for quantum advantage in the NISQ era, it has been known the performance limitations of low-level QAOA for certain instances [3, 4, 5, 7, 8]. There have been various modified QAOA to enhance its performance [11].

Recursive QAOA (RQAOA) is one of the variants of QAOA to overcome the obstacle of QAOA [4]. There are only a few results on RQAOA [4, 6, 9, 12, 10]. Moreover, while it was analytically proved in one of them that the level-1 RQAOA performs better than any constant level QAOA for solving MAX-CUT problem on cycle graphs [4] and complete graphs [12], the others have given only numerical evidences to claim similar arguments for finding the largest energy of Ising Hamiltonian [6] and for graph coloring problem [9].

From most of the results on RQAOA, it seems like RQAOA performs well for finding the optimal solution for combinatorial optimization problems. Recently, there has been known the instance in which RQAOA performs worse [10]. In this work, we give another example, bipartite graphs, that both RQAOA and QAOA cannot solve properly even though the solution for this instance is so intuitively easy to get. Furthermore, we propose a better strategy for solving MAX-CUT problem on bipartite graphs using RQAOA and prove that our modified RQAOA can solve it perfectly.

*eobae@kias.re.kr
†level@khu.ac.kr

2 Preliminaries

2.1 MAX-CUT problem

Let $G = (V, E)$ be a (undirected) graph with the set of vertices $V = \{1, 2, \ldots, n\}$ and the set of edges $E = \{ij : i, j \in V\}$. The MAX-CUT problem is a well-known combinatorial optimization problem that aims to split V into two disjoint subsets such that the number of edges spanning the two subsets is maximized. The MAX-CUT problem can be formulated by maximizing the cost function

$$C(\mathbf{x}) = \frac{1}{2} \sum_{ij \in E} (1 - x_i x_j)$$

for $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \{-1, 1\}^n$.

2.2 QAOA

QAOA can be viewed as a discrete version of Adiabatic Quantum Computing. The design of QAOA involves constructing a parameterized quantum circuit that alternates between applying the problem Hamiltonian (which encodes the optimization problem) and the driving Hamiltonian (which ensures broad exploration of the solution space). Here, we only focus on MAX-CUT problem which can be converted to the following problem Hamiltonian.

$$H_C = \frac{1}{2} \sum_{ij \in E} (I - Z_i Z_j),$$

where Z_i is the Pauli operator Z acting on the i-th qubit. The level-p QAOA, denoted by QAOA_p, can be described as the following algorithm.

Algorithm 1 ($\mathbf{QAOA}_p$ [1]) *The $QAOA_p$ is as follows.*

1. *Prepare the initial state $|+\rangle^{\otimes n}$.*

2. *Generate a variational wave function*

$$|\psi_p(\beta,\gamma)\rangle = \prod_{j=1}^{p} e^{-i\beta_j H_B} e^{-i\gamma_j H_C} |+\rangle^{\otimes n},$$

where $\beta = (\beta_1, \ldots, \beta_p)$, $\gamma = (\gamma_1, \ldots, \gamma_p)$, H_C is a problem Hamiltonian, $H_B = \sum_{i=1}^{n} X_i$ is a driving Hamiltonian, and X_i is the Pauli operator X acting on the i-th qubit.

3. *Compute the expectation value*

$$F_p(\beta,\gamma) = \langle\psi_p(\beta,\gamma)| H_C |\psi_p(\beta,\gamma)\rangle$$

by performing the measurement in the computational basis.

4. *Find the optimal parameters*

$$(\beta^*,\gamma^*) = \text{argmax}_{\beta,\gamma} F_p(\beta,\gamma)$$

using a classical optimization algorithm.

The approximation ratio α of QAOA$_p$ is defined as

$$\alpha_p = \frac{F_p(\beta^*,\gamma^*)}{C_{\max}},$$

where $C_{\max} = \max_{\mathbf{x}\in\{-1,1\}^n} C(\mathbf{x})$.

2.3 Recursive QAOA

RQAOA was introduced to address the limitations of the original QAOA by incorporating a recursive problem reduction strategy [4].

Algorithm 2 (RQAOA$_p$ [4]) *The RQAOA$_p$ is as follows.*

1. *Apply the original QAOA$_p$ to find the optimal parameters (β^*,γ^*) to maximize $F_p(\beta,\gamma)$.*

2. *Compute the edge expectation values*

$$M_{ij} = \langle\psi_p(\beta^*,\gamma^*)| Z_i Z_j |\psi_p(\beta^*,\gamma^*)\rangle$$

for every edges $ij \in E$.

3. *Pick the edge $kl = \text{argmax}_{ij\in E} M_{ij}$*

4. *By imposing the constraint $Z_k = sgn(M_{kl}) Z_l$, replace it with H_n to obtain*

$$H'_n = sgn(M_{kl}) \left[\sum_{ik\in E} J_{ik} Z_i Z_l\right] + \sum_{i,j\neq k} J_{ij} Z_i Z_j$$

5. *Call the QAOA recursively to maximize the expected value of a new Ising Hamiltonian H_{n-1} depending on $n-1$ variables:*

$$H_{n-1} = \sum_{il\in E'_0} J'_{ij} Z_i Z_l + \sum_{ij\in E'_1} J'_{ij} Z_i Z_j,$$

where

$$E'_0 = \{il : ik \in E\}, E'_1 = \{ij : i,j \neq k\},$$

and

$$J'_{ij} = \begin{cases} \text{sgn}(M_{kl}) J_{ik} & \text{if } il \in E'_0, \\ J_{ij} & \text{if } ij \in E'_1. \end{cases}$$

6. *The recursion stops when the number of variables reaches some threshold value $n_c \ll n$, and find $\mathbf{x}^* = \text{argmax}_{\mathbf{x}\in\{-1,1\}^{n_c}} \langle\mathbf{x}| H_{n_c} |\mathbf{x}\rangle$ by a classical algorithm.*

7. *Reconstruct the original (approximate) solution $\tilde{\mathbf{x}} \in \{-1,1\}^n$ from $\mathbf{x}^*$ using the constraints.*

3 Limitation of QAOA$_1$ and RQAOA$_1$

Let G be a bipartite graph and let α be the approximation ratio of the level-1 QAOA for solving MAX-CUT problem on G. Since bipartite graphs are triangle-free, we use the simpler analytic form of $F_1(\beta,\gamma)$ in Ref. [2] to get

$$\begin{aligned}\langle H_C\rangle &= \langle\psi_1(\beta,\gamma)| H_C |\psi_1(\beta,\gamma)\rangle \\ &= \sum_{ij\in E} \left[\frac{1}{2} + \frac{1}{4}\sin(4\beta)\sin\gamma\left(\cos^{\sigma_i-1}\gamma + \cos^{\sigma_j-1}\gamma\right)\right],\end{aligned}$$

where σ_i is the degree of the vertex i. For this case, we know that the optimal cut is the number of all edges. Furthermore, we can rewrite the expectation value of the MAX-CUT Hamiltonian of the level-1 QAOA in terms of the vertex degrees instead of the edges, and thus the approximation ratio is

$$\begin{aligned}\alpha_1 &= \max_{\beta,\gamma} \langle H_C\rangle / C_{\max} \\ &= \max_{\gamma} \left[\frac{1}{2} + \frac{1}{2}\sum_{d=1}^{d_{\max}} \frac{d|D_d|}{2|E|} \sin\gamma\cos^{d-1}\gamma\right],\end{aligned}$$

where $|D_d|$ is the number of vertices with degree d.

We get the bound of α_1 especially related to the average vertex degree which is the one of important properties of graphs as follows [13].

Theorem 3 (Bipartite graph) *Let (G,V) be a bipartite graph with two disjoint vertex sets V_1 and V_2. Then*

$$\begin{aligned}\alpha_1 &\leq \frac{1}{2} + \sum_{d=1}^{d_{\max}} \frac{d|D_d|}{2|E|} \left[\frac{1}{2\sqrt{d}}\left(\frac{\sqrt{d-1}}{\sqrt{d}}\right)^{d-1}\right] \\ &\leq \frac{1}{2} + \frac{1}{2\sqrt{e}}\left(\frac{1}{\sqrt{d_{ave}}} + \frac{\sqrt{e}-1}{d_{ave}}\right),\end{aligned}$$

where d_{ave} denotes the average vertex degree of the graph which can be defined as $\frac{\sum_{v\in V} d_v}{|V|}$, or equivalently, $\frac{2|E|}{|V|}$.

When we focus on complete bipartite graphs, we can show that the first bound in Theorem 3 is tight.

Corollary 4 (Complete bipartite graph) *Let $K_{n,n}$ be a complete bipartite graph with n nodes. Then*

$$\alpha_1 \leq \frac{1}{2} + \frac{1}{2\sqrt{n}}\left(1 - \frac{1}{n}\right)^{\frac{n-1}{2}}$$

Remark 5 *As we expect, we numerically observe that RQAOA$_1$ can have better solutions than QAOA$_1$ for MAX-CUT problem on complete bipartite graphs. However, we also figured out that there are some instances which are complete bipartite graphs $K_{n,n}$ in which RQAOA$_1$ can fail to find the exact solution especially when n increases.*

4 Our strategy for RQAOA

Complete bipartite graphs are well-structured and easy to find the exact solution intuitively. Surprisingly, both QAOA and RQAOA have limitations in solving the MAX CUT problem even for instances like complete bipartite graphs.

To overcome these limitations, we introduce an improved RQAOA with a novel parameter targeting strategy and prove that this algorithm can always find the optimal MAX-CUT solution on complete bipartite graphs, and even for bipartite graphs. Normally, if we reduce the region to find the optimal parameters (β, γ) to maximize the expectation value $F_p(\beta, \gamma)$ in QAOA, the maximum value we can obtain from QAOA will be also decreasing. Interestingly, we figured out that in the QAOA subroutine, reducing the optimization domain improves the performance of RQAOA in solving Max-Cut problem on bipartite graphs, even if QAOA does not find the true optimal parameters.

Algorithm 6 (Modified RQAOA$_1$) *We only modify the first step of RQAOA and the rest part is the same with the original RQAOA.*

1. *Apply the original QAOA to find the optimal parameters* (β^*, γ^*) *in the restricted domain where* $|\gamma| \leq \frac{\pi}{2w_{ij}^*}$ *with* $w_{ij}^* = \max_{ij \in E} w_{ij}$ *to maximize* $F_1(\beta, \gamma)$.

Let $K_{n,m}^w$ be a graph with two partitioned subsets V_1 and V_2 of vertices with $|V_1| = n$ and $|V_2| = m$, and the weight w_e of each edge e have the following properties:

- Weight of the edge consisting of vertices belonging to the same vertex set is always negative, that is, for the edge $e = ij$, if $i, j \in V_1$ or $i, j \in V_2$, then $w_e \leq 0$.
- Weight of the edge consisting of vertices belonging to the different vertex sets is always positive, that is, for the edge $e = ij$, if $(i, j) \in V_1 \times V_2$, then $w_e \geq 0$.

Now, we can prove our algorithm can always find the optimal MAX-CUT solution on bipartite graphs [13].

Theorem 7 *Our modified RQAOA for solving MAX-CUT problem on bipartite graphs can achieve the approximation ratio* 1.

To prove the main theorem, we first show that if $\gamma^* \leq \frac{\pi}{2w_{ij}^*}$ with $w_{ij}^* = \max_{ij \in E} w_{ij}$ in the QAOA$_1$ subroutine for solving MAX-CUT problem on bipartite graphs, all reduced graphs from our modified RQAOA$_1$ iterations can be well-partitioned graphs like $K_{n',m'}^w$ with the above properties. Second, we prove that RQAOA$_1$ can find the optimal solution for solving MAX-CUT problem on $K_{n,m}^w$ (which also includes all bipartite graphs) for any n and m if all reduced graphs from each iteration remain to be well-partitioned with the above properties.

5 Discussion

Although there have been not many results on RQAOA, almost all results show us that RQAOA outperforms the original QAOA or even best known classical algorithm for certain instances. It seems like RQAOA has more potential than QAOA for demonstrating quantum advantage in the NISQ era. However, we found that the counter-example that RQAOA can be worse than the best-known classical algorithm for some instances with a large enough number of nodes.

There would be several reasons that can explain why RQAOA performs worse such as the limitation of QAOA to optimize the parameters and the recursion step to fix variables on the eliminated edges. To analyze the performance of RQAOA for more general instances from this point of view remains to be opened for now.

We figured out that the bad optimization of QAOA would not be the only reason to explain the limitation of RQAOA by showing that RQAOA performs better even if we reduce the optimization domain for QAOA to solve MAX-CUT problem on bipartite graphs. Furthermore, we proposed the improved RQAOA to handle this problem for bipartite graphs. For future works, we will see if this argument could fit into more general instances such as d-regular graphs.

References

[1] E. Farhi, J. Goldstone, and S. Gutmann. A Quantum Approximate Optimization Algorithm. arXiv:1411.4028, 2014.

[2] Z. Wang, S. Hadfield, Z. Jiang, and E. G. Rieffel. Quantum approximate optimization algorithm for MaxCut: A fermionic view. Physical Review A, pages 022304, 2018.

[3] M. B. Hastings. Classical and quantum bounded depth approximation algorithms. arXiv:1905.07047, 2019.

[4] S. Bravyi, A. Kliesch, R. König, and E. Tang. Obstacles to State Preparation and Variational Optimization from Symmetry Protection. Physical Review Letters, pages 260504, 2019.

[5] E. Farhi, J. Goldstone, and S. Gutmann. The Quantum Approximate Optimization Algorithm Needs to See the Whole Graph: A Typical Case. arXiv:2004.09002, 2020.

[6] S. Bravyi, D. Gosset, D. Grier, and L. Schaeffer. Classical algorithms for Forrelation. arXiv:2102.06963, 2021.

[7] K. Marwaha. Local classical max-cut algorithm outperforms $p = 2$ QAOA on high-girth regular graphs. Quantum, pages 437, 2021.

[8] B. Barak and K. Marwaha. Classical algorithms and quantum limitations for maximum cut on high-girth graphs. arXiv:2106.05900, 2021.

[9] S. Bravyi, A. Kliesch, R. König, and E. Tang. Hybrid quantum-classical algorithms for approximate graph coloring. Quantum, pages 678, 2022.

[10] Y. J. Patel, S. Jerbi, T. Bäck, and V. Dunjko. Reinforcement Learning Assisted Recursive QAOA. Quantum Technol., pages 6, 2024.

[11] S. Bravyi, A. Kliesch, R. König, and E. Tang. Hybrid quantum-classical algorithms for approximate graph coloring. Quantum, pages 678, 2022.

[12] E. Bae and S. Lee. Recursive QAOA outperforms the original QAOA for the MAX-CUT problem on complete graphs. Quantum Inf Process, pages 78, 2024.

[13] E. Bae, H. Kwon, V. Vijendran, and S. Lee. In preparation.

Quantum-inspired algorithms for approximating matrix functions

Youngrong Lim[1] * Changhun Oh[2] †

[1] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*
[2] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*

Abstract. Computing matrix functions, such as the permanent and the hafnian, is one of the fundamental problems in the computational complexity community. In this work, we adopt quasiprobability distribution, a basic quantum optics tool, to tackle this problem. As a result, we have developed various classical algorithms that outperform the best-known ones. Remarkably, in some cases, we obtain multiplicative-error estimating algorithms for these matrix functions, where we exploit a symmetry of linear-optical circuits in the phase space to make the quasiprobability distributions log-concave functions.

Keywords: Gaussian boson sampling, permanent, hafnian, quasiprobability distributions

1 Introduction

Computing the permanent and hafnian of a given matrix is an intractable problem in general (#P-hard), even allowing a multiplicative-error. For a matrix having nonnegative entries, however, a fully polynomial randomized approximation scheme (FPRAS) of the permanent exists [1]. Then our question is to seek FPRAS for other classes of matrices. One of the key techniques is finding various representations of the matrix functions. For example, if we find an exotic integral representation of a matrix function, we can have a chance to approximate it more effectively.

Meanwhile, the outcome probabilities of a linear-optical circuit are connected to matrix functions, which lie at the heart of the hardness of boson sampling [2]. From the phase-space formalism of quantum physics, we can express the outcome probabilities as integrals using quasiprobability distributions. This means we have a quantum-inspired representation for the matrix function. Here, we fully exploit the advantages of this quasiprobability representation, far more generalizing an existing result of an additive-error approximating scheme for the permanent of a positive-semidefinite matrix [3]. Our technical contributions are two-fold. Firstly, we use Monte Carlo sampling to handle the negativity of quasiprobability [4]. Secondly, we manipulate the shape of quasiprobability distributions by exploiting the symmetry of linear-optical circuits in the phase space, resulting in better precision. Remarkably, we obtain multiplicative-error approximating schemes for some cases by making quasiprobability distributions log-concave functions. Consequently, we have FPRASs for the hafnian and Torontonian of some structured matrices. This also can reproduce an FPRAS for a positive definite matrix [5].

2 Results

Proofs of theorems and technical details are in Ref. [6].

Theorem 1 *(Estimating hafnian) For an $M \times M$ complex symmetric matrix R, one can approximate $|Haf(R)|^2$ with a success probability $1-\delta$ using the number of samples $O(\log \delta^{-1}/\epsilon^2)$ within the additive-error*

$$\epsilon \left(\frac{\lambda_{\max}}{\sqrt{1-2W(1/e)}} \right)^M \simeq \epsilon (1.502 \lambda_{\max})^M, \tag{1}$$

where $W(x)$ is Lambert W function and $\lambda_{\max}$ is the largest singular value of R.

Theorem 2 *(FPRAS for hafnian) Suppose we have a block matrix $A = \begin{pmatrix} R & B \\ B^T & R^* \end{pmatrix}$ with an $M \times M$ complex symmetric matrix R and an $M \times M$ HPSD matrix B, which have decompositions by a unitary matrix U as UDU^T and $UD'U^\dagger$, respectively, with*

$$D = \bigoplus_{i=1}^{M} \frac{(1+2n)\sinh 2r_i}{1+2n(1+n)+(1+2n)\cosh 2r_i}, \tag{2}$$

$$D' = \bigoplus_{i=1}^{M} \frac{2n(1+n)}{1+2n(1+n)+(1+2n)\cosh 2r_i}, \tag{3}$$

where $n = n_i$ for all i and $n, r_i \geq 0$. Then $Haf(A)$ can be approximated by FPRAS when the parameters satisfy a condition as

$$n \geq \frac{1}{4}\left(6\sinh(2r_{\max}) + \sqrt{18\cosh(4r_{\max})-14} - 2\right), \tag{4}$$

where $r_{\max} = \max_i r_i$.

References

[1] M. Jerrum, A. Sinclair, and E. Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. J. ACM, 51, 671–697, 2004.

[2] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. 43rd ACM Symp. Theory Comput. (STOC), 333–342, 2011.

[3] L. Chakhmakhchyan, N. J. Cerf, and R. Garcia-Patron. Quantum-inspired algorithm for estimating the permanent of positive semidefinite matrices. Phys. Rev. A, **96**, 022329, 2017.

*sshaep@gmail.com
†changhun0218@kaist.ac.kr

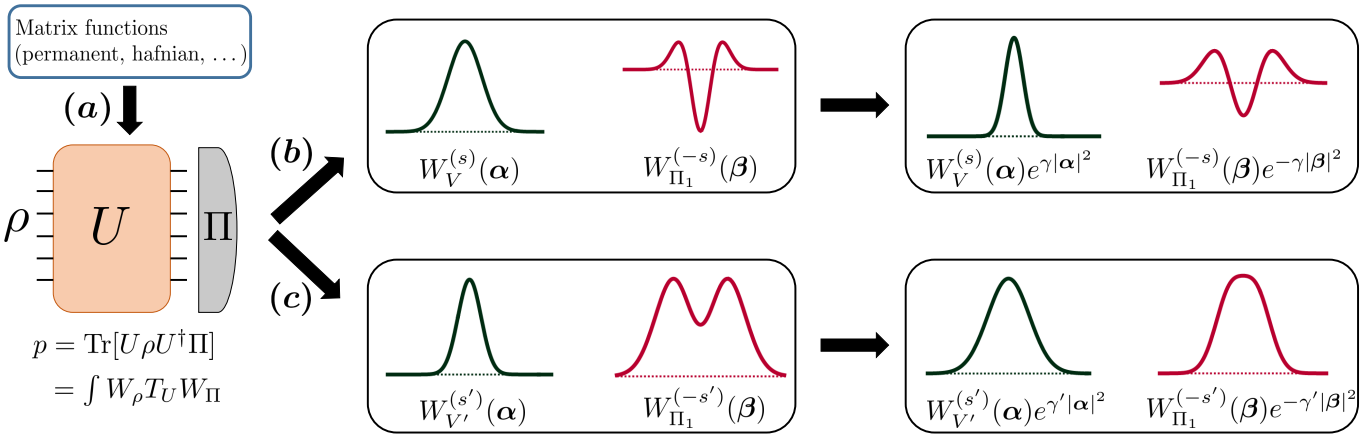


Figure 1: Schematic diagram of quantum-inspired classical algorithms for approximating matrix functions. For a given matrix function, (a) find an embedding of the matrix function onto an outcome probability of a quantum circuit (ρ, U, Π) and choose a quasiprobability representation of the probability. (b) We depict an example of a linear optical circuit, for the approximation scheme with additive-error. Using s-PQDs for the linear optical circuit, one can significantly reduce the negativity bound by appropriately choosing $\gamma < 0$. (c) Approximation scheme with multiplicative-error. When the classicality of the input state is large, one can make the s-PQDs of the measurement operator a log-concave function by choosing a suitable $\gamma' > 0$.

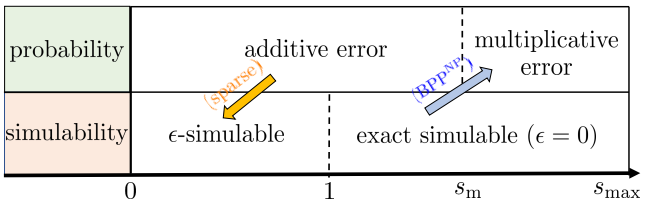


Figure 2: Regime of efficient classical algorithms for approximating outcome probabilities and the simulation of a GBS circuit with threshold detectors via the classicality $s_{\max}$. When the output distribution is poly-sparse, an approximate simulation is possible by estimating the probabilities within 1/poly additive-error (orange arrow) [7]. On the other hand, a multiplicative-error approximation of probability in $\mathrm{BPP}^{\mathrm{NP}}$ is possible by using exact simulation with classical input state $s_{\max} \geq 1$ (blue arrow) [8].

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

[5] A. Barvinok. A remark on approximating permanents of positive definite matrices. Linear Algebra Appl. 608, 399–406, 2021.

[6] Y. Lim and C. Oh. Approximating outcome probabilities of linear optical circuits npj Quant. Inf. **9**, 124, 2023.

[7] M. Schwarz and M. Van den. Nest. Simulating quantum circuits with sparse output distributions. Preprint at https://arxiv.org/abs/1310.6749, 2013.

[8] Rahimi-Keshari, L. Saleh, P. Austin, and T. C. Ralph. What can quantum optics say about computational complexity theory? Phys. Rev. Lett. **114**, 060501, 2015.

Strategic Code: A Unified Spatio-Temporal Framework for Quantum Error-Correction

Andrew Tanggara,[1,2,*] Mile Gu,[2,1,†] and 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.*

(Dated: May 29, 2024)

Quantum error-correcting code (QECC) is the central ingredient in fault-tolerant quantum information processing. An emerging paradigm of dynamical QECC shows that one can robustly encode logical quantum information both temporally and spatially in a more resource-efficient manner than traditional QECCs. Nevertheless, an overarching theory of how dynamical QECCs achieve fault-tolerance is lacking. In this work, we bridge this gap by proposing a unified spatio-temporal QECC framework called the "strategic code" built around an "interrogator" device which sequentially measures and evolves the spatial QECC in an adaptive manner based on the "quantum combs" formalism, a generalization of the channel-state duality. The strategic code covers all existing dynamical and static QECC, as well as all physically plausible QECCs to be discovered in the future, including those that involve adaptivity in its operational dynamics. Within this framework, we show an algebraic and an information-theoretic necessary and sufficient error-correction conditions for a strategic code, which consider spatially and temporally correlated errors. These conditions include the analogous known static QECC conditions as a special case. Lastly, we also propose an optimization-theoretic approach to obtain an approximate strategic code adapting to a correlated error.

The susceptibility of quantum systems to noise has been a major obstacle in achieving the advantages offered by quantum information processing tasks over their classical counterparts. A quantum error-correcting code (QECC) overcomes this problem by redundantly encoding quantum information in a noise-robust manner. However conventional QECCs involve operations on many-body quantum system to encode and decode logical information, which are notoriously resource-intensive. The novel paradigm of dynamical QECC offers a promising solution by utilizing the temporal dimension to encode and decode logical information, thus easing this demanding requirement. Many dynamical QECC has been proposed, with the most popular being the Floquet codes [1–13] which measurement sequence is performed periodically, although other non-periodic codes have also been explored [14–22].

Despite the remarkable progress in dynamical QECC research, an overarching theory of error-correction for QECCs considering both spatial and temporal encoding that is analogous to its static counterpart [23–29], has been largely unexplored. In order to analyze the error-correction capability of a QECC with respect to resources that it uses, both spatially and temporally, such theory is imperative. In this work we bridge this gap by proposing a QECC framework called the "strategic code" which unifies all existing dynamical and static QECCs, as well as all physically plausible QECCs to be discovered. The novelty of the strategic code lies in the "interrogator" device which captures any set of operations performed both spatially and temporally between the encoding and decoding stage, completing the conceptual gap operationally between static and dynamical QECC paradigms. The strategic code framework also generalize existing QECC paradigms by accommodating temporal operational adaptivity of the code and the effect of the most general class of noise with both spatial and temporal (non-Markovian) correlations [30–38].

Within the strategic code framework for QECCs with an interrogator that maintains a classical memory and for general error models (which may exhibit correlations), we show necessary and sufficient error-correction conditions, as well as formulate a multi-convex optimization problem to obtain an approximate code. Our conditions are presented in two equivalent forms: algebraically (Theorem 1) and an information-theoretically (Theorem 2). Due the generality of our framework, algebraic and information-theoretic necessary and sufficient conditions for static QECC [23–26] are included as special cases. Since strategic code subsumes notable QECC frameworks, such as the sequential Pauli measurements framework [20], ZX calculus framework [21], and anyon condensation framework [22], these conditions serve as a guide in a code construction within these frameworks.

I. GENERAL QECC SCENARIO

Error-correcting code scenario can always be described as interactions between a code and some noise changing the state of a physical system where logical information

* andrew.tanggara@gmail.com
† mgu@quantumcomplexity.org
‡ kishor.bharti1@gmail.com

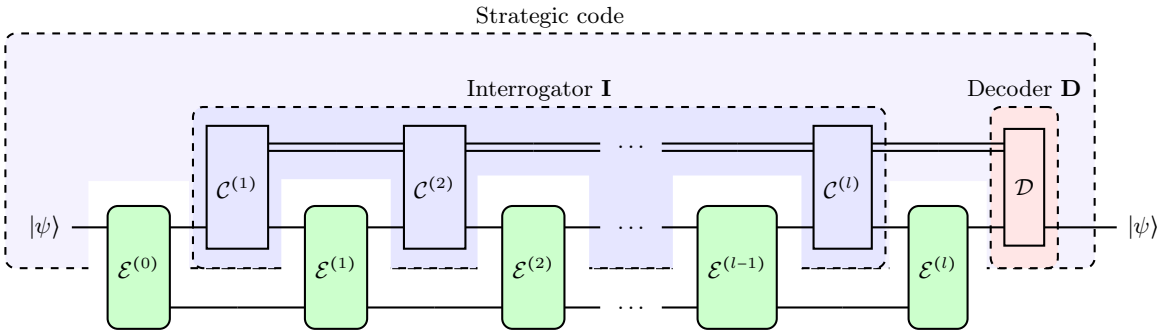


FIG. 1. General QECC Scenario. At round 0, error $\mathcal{E}^{(0)}$ is inflicted to code state $|\psi\rangle$ that belongs to the initial code space $\mathscr{S}_{Q_0}$, evolving it to error-inflicted subspace $\mathscr{S}_{Q_0'}$. Then an interrogator device **I** is applied to the code, performing quantum operations on the code l times in sequence. At each round $r \in \{1,\ldots,l\}$, evolution on the code is performed by a quantum operation $\mathcal{C}^{(r)}$, giving a new code space $\mathscr{S}_{Q_r}$ followed by error map $\mathcal{E}^{(r)}$ further evolving the code space $\mathscr{S}_{Q_r}$ to error-inflicted subspace $\mathscr{S}_{Q_r'}$. The interrogator maintains a classical memory (illustrated by double-wires) which keeps information about previous events (e.g. measurement outcome) and determines the choice of quantum operation performed at each round. At the start of round r, if the interrogator's memory state is m_{r-1} then it performs quantum operation $\mathcal{C}^{(r)}_{m_{r-1}}$. After performing the operation, it the updates the state of the classical memory register $m_{r-1} \mapsto m_r$ where m_r is the updated memory state that determines the subsequent operations. After the final round l, decoding **D** is performed based on the final memory state m_l, where channel $\mathcal{D}_{m_l}$ is applied to the code system to restore the initial code state $|\psi\rangle$.

is encoded in. Conventionally, the essential two ingredients of a code are: (1) an operation encoding the logical information into a physical system and (2) an operation that recovers logical information from any error caused by noise that occurs in between. In a quantum error-correcting code (QECC) scenario, further interplay between the code and noise can take place between encoding and decoding, allowing more interesting implications on the error-correction process due to inherent quantum-mechanical effects.

In general, a QECC scenario consists of three stages: The first stage being the encoding stage, the final stage being the decoding stage, and between them, any set of operations performed by the code, interacting with the noise (see Fig. 1). We simplify this by starting with an initial codespace $\mathscr{S}_{Q_0}$ instead of an encoding map (as an encoding map uniquely defines the initial codespace). Then a set of operations **I**, called the *interrogator*, is performed by the code in between encoding and decoding. The interrogator performs $l \geq 0$ rounds of *check operations* where the check operation $\mathcal{C}^{(r)}$ at round r may be chosen (from a set of allowed operations) *adaptively* based on events happened in the previous rounds stored in a classical memory register. When the classical memory register is in a *memory state* m_{r-1}, then a check operation $\mathcal{C}^{(r)}_{m_{r-1}}$ is performed. Between encoding and decoding, we also have errors **E** being inflicted on the code right after the encoding stage and after each round of operation. Errors can generally have spatial correlations within each round and temporal (non-Markovian) correlations across rounds. Lastly in the decoding stage, the decoding procedure **D** consists of multiple decoders that the coder can choose from based on the information stored in the classical memory m_l after the last round of operation. A successful QECC procedure recovers logical information encoded in the initial codespace as codestate $|\psi\rangle$.

Although here we focus on an interrogator where only classical memory storage is allowed, one can easily generalize this to an interrogator where quantum memory is involved. Such interrogator could model a scenario where a small-size quantum system can be used reliably to store some information about the code across time alongside classical memory to be used in the decoding stage. Particularly, this generalization reduces to the entanglement-assisted QECC (EAQECC) [39–41] when we set the number of rounds $l = 0$, see Appendix B 1 for details.

More formally, the entirety of an l-round QECC scenario is defined by the following objects:

1. A sequence of codespaces $\mathscr{S}_{Q_0}, \mathscr{S}_{Q_0'}, \ldots, \mathscr{S}_{Q_l}, \mathscr{S}_{Q_l'}$ which are a subspace of d dimensional complex vector space $\mathbb{C}^d$ and spaces of bounded linear operators from $\mathbb{C}^d$ to $\mathbb{C}^d$, $\mathscr{H}_{Q_0}, \mathscr{H}_{Q_0'}, \ldots, \mathscr{H}_{Q_l}, \mathscr{H}_{Q_l'}, \mathscr{H}_D$. The codespaces and operator spaces depends on operations performed in the two stages defined below, while the initial codespace $\mathscr{S}_{Q_0}$ is defined independent of them.

2. An interrogator **I** consists of a sequence of *check instruments* $\mathcal{C}^{(1)}, \mathcal{C}^{(2)} := \{\mathcal{C}^{(2)}_{m_1}\}_{m_1}, \ldots, \mathcal{C}^{(l)} := \{\mathcal{C}^{(l)}_{m_{l-1}}\}_{m_{l-1}}$ where $\mathcal{C}^{(r)}_{m_{r-1}} := \{\mathcal{C}^{(r)}_{m_r|m_{r-1}}\}_{m_r}$ and $\mathcal{C}^{(1)} := \{\mathcal{C}^{(1)}_{m_1}\}_{m_1}$ are a check instrument for round $r > 1$ and round $r = 1$, respectively. Each $\mathcal{C}^{(r)}_{m_r|m_{r-1}} : \mathscr{H}_{Q_{r-1}'} \to \mathscr{H}_{Q_r}$ is a completely-positive (CP) map

such that $\sum_{m_r} \mathcal{C}^{(r)}_{m_r|m_{r-1}}$ is trace preserving (TP). Check instrument $\mathcal{C}^{(r)}_{m_{r-1}}$ may perform a deterministic operation on the code (e.g. a unitary) in which $\mathcal{C}^{(r)}_{m_{r-1}}$ consist of only one element, or a probabilistic operation where each of its element maps an initial codestate to a post-measurement codestate.

3. Decoder $\mathbf{D} = \{\mathcal{D}_{m_l}\}_{m_l}$ where *decoding channel* $\mathcal{D}_{m_l} : \mathscr{H}_{Q'_l} \to \mathscr{H}_D$ is a CPTP map that given classical information m_l in the classical memory register recovers the initial code state $|\psi\rangle_{Q_0}$ (what this precisely means will be defined shortly in Definition 2).

4. Error $\mathbf{E}$ consists of a sequence of *error maps* $\mathcal{E}^{(0)}, \mathcal{E}^{(1)}, \ldots, \mathcal{E}^{(l)}$ where $\mathcal{E}^{(r)} : \mathscr{H}_{Q_r} \otimes \mathscr{H}_{E_{r-1}} \to \mathscr{H}_{Q'_r} \otimes \mathscr{H}_{E_r}$ is a CP trace non-increasing map defined by $\mathcal{E}^{(r)}(\rho) = \sum_{e_r} E_{e_r} \rho E^\dagger_{e_r}$ where bounded linear operator $E_{e_r} : \mathscr{S}_{Q_r} \otimes \mathscr{S}_{E_{r-1}} \to \mathscr{S}_{Q'_r} \otimes \mathscr{S}_{E_r}$ being a Kraus operator for $\mathcal{E}^{(r)}$ for $r \geq 1$ and $E^{(0)} : \mathscr{S}_{Q_0} \to \mathscr{S}_{Q'_0} \otimes \mathscr{S}_{E_0}$. Spaces labeled by E_{r-1} and E_r are the systems storing any temporal correlations in the noise environment from round $r-1$ to round r and from round r to round $r+1$, respectively. In the case of uncorrelated error sequence we simply have $\mathcal{E}^{(r)} : \mathscr{H}_{Q_r} \to \mathscr{H}_{Q'_r}$, with Kraus operators of the form $E_{e_r} : \mathscr{S}_{Q_r} \to \mathscr{S}_{Q'_r}$.

We remark that in the description above it is assumed that the dimension d of the quantum system where the code lives is always the same at all rounds. However, this assumption is only for convenience and is not assumed in our proofs thus can be relaxed to round-dependent dimensions. Namely, code spaces $\mathscr{S}_{Q_r}, \mathscr{S}_{Q'_r}$ being a subspace of $\mathbb{C}^{d_r}$ and $\mathscr{H}_{Q_r}, \mathscr{H}_{Q'_r}$ being spaces of bounded linear operators from $\mathbb{C}^{d_r}$ to $\mathbb{C}^{d_r}$.

Completely positive map $\mathcal{C}^{(r)}_{m_r|m_{r-1}}$ corresponds to mapping multiple measurement outcomes arising from measurement setting defined by memory state m_{r-1}. This can be formally described as POVM $\{M_{o_r|m_{r-1}}\}_{o_r}$ defined by the Kraus operators $C^{(r)}_{o_r|m_{r-1}}$ of CPTP map $\mathcal{C}^{(r)}_{m_{r-1}} = \sum_{m_r} \mathcal{C}^{(r)}_{m_r|m_{r-1}}$ defined by the instrument $\{\mathcal{C}^{(r)}_{m_r|m_{r-1}}\}_{m_r}$. Namely, $M_{o_r|m_{r-1}} = C^{(r)\dagger}_{o_r|m_{r-1}} C^{(r)}_{o_r|m_{r-1}}$ and $\mathcal{C}^{(r)}_{m_r|m_{r-1}}(\rho) = \sum_{o_r} C^{(r)}_{o_r|m_{r-1}} \rho C^{(r)\dagger}_{o_r|m_{r-1}}$. The memory state m_r is defined by some *memory update function* f_r that maps the measurement outcomes o_r and memory state m_{r-1} to memory state m_r, namely $\mathcal{C}^{(r)}_{m_{r-1}} = \sum_{m_r} \sum_{o_r : f_r(o_r, m_{r-1}) = m_r} \mathcal{C}^{(r)}_{o_r|m_{r-1}}$ where $\mathcal{C}^{(r)}_{o_r|m_{r-1}}(\rho) = C^{(r)}_{o_r|m_{r-1}} \rho C^{(r)\dagger}_{o_r|m_{r-1}}$. Thus, $\mathcal{C}_{m_r|m_{r-1}} = \sum_{o_r : f_r(o_r, m_{r-1}) = m_r} \mathcal{C}^{(r)}_{o_r|m_{r-1}}$. Note that here we consider time dependent memory update functions $f_1, \ldots, f_l$, for full generality, but of course one can instead consider a time-independent function f used in every round. Both measurement outcome o_r and measurement setting m_{r-1} should give spatial and temporal information about error occurrence. The memory state m_{r-1} at the start of round $r \in \{2, \ldots, l\}$ determines the choice of instrument $\mathcal{C}^{(r)}_{m_{r-1}}$ applied in that round, whereas memory state m_l at final round l is used to choose which decoder $\{\mathcal{D}_{m_l}\}_{m_l}$ is used to recover the initial codestate. Each final memory state m_l corresponds to a unique set O_{m_l} (defined by memory update functions $f_1, \ldots, f_l$) containing all check measurement outcome sequence $o = o_1, o_2, \ldots, o_l$ where there exists a sequence of memory states $m_1, \ldots, m_{l-1}$ such that $m_l = f_l(o_l, m_{l-1})$ and $m_{l-1} = f_{l-1}(o_{l-1}, m_{l-2})$, ..., $m_1 = f_1(o_1)$. Hence we can define a function f^* as $f^*_l(o) = f_l(o_l, f_{l-1}(o_{l-1}, \ldots f(o_1)\ldots))$ which maps an outcome sequence o to a final memory state. So we can express in symbols, $O_{m_l} = \{o : f^*_l(o) = m_l\}$.

Note that codespace $\mathscr{S}_{Q_r}$ at round r is determined by the choice of check instrument $\mathcal{C}^{(r)}_{m_{r-1}}$ and the outcome o_r from the measurement defined by it. Namely, $\mathcal{C}^{(r)}_{o_r|m_{r-1}}$ maps the state of the codespace $\mathscr{S}_{Q'_{r-1}}$ (the codespace after error map $\mathcal{E}^{(r-1)}$ at the previous round) to codespace $\mathscr{S}_{Q_r}$. Also, both codespaces $\mathscr{S}_{Q_r}$ and $\mathscr{S}_{Q'_{r-1}}$ may depend on the check instruments and error maps in the previous rounds.[1]

Interrogator $\mathbf{I}$, error $\mathbf{E}$, and decoder $\mathbf{D}$ in a QECC scenario can be represented by the quantum combs formalism [31, 42–47][2]. It has the advantage of compactly representing temporally-correlated sequence of dynamics on a quantum system as a positive semidefinite operator by generalizing the Choi-Jamiołkowski isomorphism [48–50] which holds the complete information about the temporal dynamics. Quantum combs has found many applications such as quantum causal inference [51, 52], metrology [53, 54], interactive quantum games [46], open quantum systems [55], quantum cryptography [56], and quantum communication [57]. However, to our knowledge no application of quantum combs has been made in the context of QECC before. In the following we describe the quantum combs representation for the QECC scenario. More technical details of the quantum combs representation can be found in Appendix B.

A. Strategic code and quantum combs representation

In an l-round QECC scenario, the entirety of how logical information is preserved can be described by the initial codespace $\mathscr{S}_{Q_0}$ and the sequence of check instruments $\mathcal{C}^{(1)}, \mathcal{C}^{(2)}, \ldots, \mathcal{C}^{(l)}$. These two objects made up the strategic code, defined formally in the following.

Definition 1. An l-round *strategic code* is defined by a tuple $(\mathscr{S}_{Q_0}, \mathbf{I})$ where $\mathscr{S}_{Q_0}$ is the *initial codespace*

[1] For Floquet codes this corresponds to the instantaneous stabilizer groups, which is a stabilizer group at a particular round r defined by the check measurement outcome at that round and as well as the outcomes and errors occurring up to that round.

[2] Also known as process tensor in [45] or quantum strategy in [46], and more generally, process matrix in [47] where exotic causal ordering can be exhibited.

which is a subspace of $\mathbb{C}^d$, and $\mathbf{I} = \{\mathbf{I}_{m_l}\}_{m_l}$ is a collection of positive semidefinite operators in $\mathscr{H}_{Q'_0} \otimes (\bigotimes_{r=1}^{l} \mathscr{H}_{Q'_{r-1}} \otimes \mathscr{H}_{Q_r})$ called the *interrogator*. Interrogator $\mathbf{I}$ describes all possible sequences of check instruments $\{\mathcal{C}^{(1)}, \mathcal{C}^{(2)}_{m_1}, \ldots, \mathcal{C}^{(l)}_{m_{l-1}}\}_{m_1,\ldots,m_{l-1}}$ along their with temporal dependence defined by functions $f_1, \ldots, f_l$. An element $\mathbf{I}_{m_l}$ of an interrogator is called an *interrogator operator*, which is a quantum comb describing the sequences of CP maps $\mathcal{C}^{(1)}_{m_1}, \mathcal{C}^{(2)}_{m_2|m_1}, \ldots, \mathcal{C}^{(l)}_{m_l|m_{l-1}}$ that ends in final memory state m_l. An interrogator operator $\mathbf{I}_{m_l}$ takes the form of

$$\mathbf{I}_{m_l} = \sum_{o \in O_{m_l}} |C_{m_l,o}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \tag{1}$$

where O_{m_l} is the set of check measurement outcome sequences $o = o_1, \ldots, o_l$ resulting in final memory state m_l. Here $|C_{m_l,o}\rangle\!\rangle = |C^{(l)}_{o_l|m_{l-1}}\rangle\!\rangle \otimes \cdots \otimes |C^{(1)}_{o_1}\rangle\!\rangle$ (with $m_r = f_r(o_r, m_{r-1})$) is an eigenvector of interrogator operator $\mathbf{I}_{m_l}$, and $|C^{(r)}_{o_r|m_{r-1}}\rangle\!\rangle$ is the vectorized representation of the Kraus operator $C^{(r)}_{o_r|m_{r-1}}$.

Note that $\mathscr{H}_{Q'_0} \otimes (\bigotimes_{r=1}^{l} \mathscr{H}_{Q'_{r-1}} \otimes \mathscr{H}_{Q_r})$ is the tensor product of bounded linear operator space of the inputs and outputs of the sequence of CP maps of the check instruments. An interrogator describes all possible "trajectories" of how the code evolves according to the sequence of check measurement outcomes and operations performed based on previously obtained outcomes. As an example, if the initial codestate is ρ^{Q_0} (round $r = 0$) and in round $r = 1$ a measurement is performed, an outcome 0 will result in post-measurement codestate $\rho_0^{Q_1}$ while an outcome $m_1 \neq 0$ codestate $\rho_{m_1}^{Q_1}$ which is generally is not equal to $\rho_0^{Q_1}$. Outcome m_1 also determines which operation is performed in the next round ($r = 2$). So if a measurement at $r = 2$ depending on outcome m_1 gives an outcome m_2, then we obtain codestate $\rho^{Q_2}_{m_2|m_1}$, where the label $m_2|m_1$ describes the "trajectory". If decoding is performed on $\rho^{Q_2}_{m_2|m_1}$, then the decoder will use m_2 to recover the initial state. For a diagram illustrating the trajectories of the code induced by the operations performed by the interrogator, see Fig. 2.

Now we turn to how decoding and errors are described in an l-round QECC scenario. Decoding channel $\mathcal{D}_{m_l}$ is described by each of its Choi-Jamiolkowski representation $\mathbf{D}_{m_l}$, which is a positive semidefinite operator in $\mathscr{H}_{Q'_l} \otimes \mathscr{H}_D$. Similarly, we can also represent the sequence of error CP maps $\mathcal{E}^{(0)}, \ldots, \mathcal{E}^{(l)}$ as positive semidefinite operator

$$\mathbf{E} = \sum_e |E_e\rangle\!\rangle\langle\!\langle E_e| \tag{2}$$

where $e = e_0, e_1, \ldots, e_l$ indicates an error sequence. Here $|E_e\rangle\!\rangle$ is the vectorized representation of the sequence of Kraus operators $E_{e_0}, \ldots, E_{e_l}$ of the error maps.

The entire interaction between an interrogator operator ending in final memory state m_l and the error

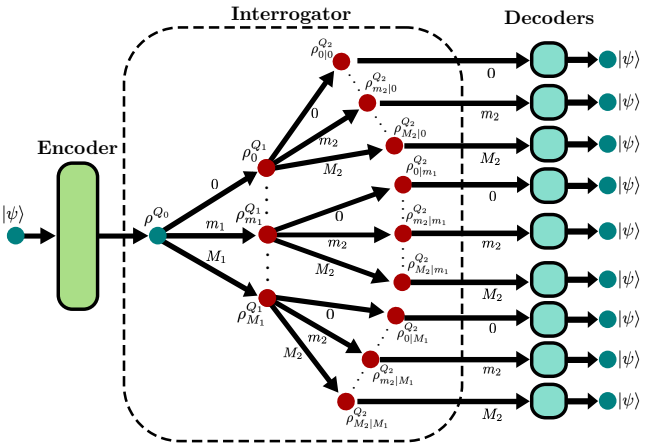


FIG. 2. Trajectories of the code evolution in an interrogator.

maps can be described as $\mathbf{E} * \mathbf{I}_{m_l}$ where "$*$" is an associative dyadic operation between two linear operators $A \in \mathscr{H}_A \otimes \mathscr{H}_C$ and $B \in \mathscr{H}_C \otimes \mathscr{H}_B$ known as the *link product* [42], which can be thought of as a generalization of the Hilbert-Schmidt inner product. The link product is defined as $A * B := \mathrm{Tr}_C((A^{\top_C} \otimes I_B)(I_A \otimes B))$ where Tr_C is partial trace over operator space $\mathscr{H}_C$, $\cdot^{\top_C}$ is the partial transpose over $\mathscr{H}_C$, and I_A, I_B are identity operators of $\mathscr{H}_A$ and $\mathscr{H}_B$, respectively. Note that if the operator space $\mathscr{H}_C$ has trivial dimension then $A * B = A \otimes B$, and if $\mathscr{H}_A, \mathscr{H}_B$ have a trivial dimension then $A * B = \mathrm{Tr}(A^\top B)$.

Some of our results are expressed in term of the explicit error sequence e described by $|E_e\rangle\!\rangle\langle\!\langle E_e|$ instead of $\mathbf{E}$. Hence at times we will describe the sequence of error maps as the collection of the rank-1 operators describing the error sequences, $\mathfrak{E} := \{|E_e\rangle\!\rangle\langle\!\langle E_e|\}_e$. In both the link product form and the rank-1 vector form, we can express the complete interaction between the an interrogator operator and an error sequence e as

$$\begin{aligned} \mathbf{E} * \mathbf{I}_{m_l} &= \sum_e |E_e\rangle\!\rangle\langle\!\langle E_e| * \mathbf{I}_{m_l} \\ &= \sum_e \sum_{o \in O_{m_l}} |K_{e,m_l,o}\rangle\!\rangle\langle\!\langle K_{e,m_l,o}|\,, \end{aligned} \tag{3}$$

where $|K_{e,m_l,o}\rangle\!\rangle$ is the vectorized form of Kraus operator $K_{e,m_l,o}$ defined by the Kraus operators of the check instruments and error maps $E_{e_l}, C^{(l)}_{o_l|m_{l-1}}, \ldots, C^{(1)}_{o_1}, E_{e_0}$ (where the check instrument $\mathcal{C}^{(r)}_{o_r|m_{r-1}}$ in round r implicitly performs an identity map on the environment $\mathscr{H}_{E_{r-1}}$, for explicit definition see Appendix B).

B. Interrogator in existing codes

A sequence of quantum operations that temporally evolve the spatial encoding of logical information while also extracting error syndromes is the central ingredient in dynamical QECCs such as spacetime codes [14–16],

Floquet codes [1–13], and dynamical code [20]. The notion of interrogator captures This sequence of operations in these codes can be formulated as an interrogator.

In an n-qubit spacetime code, generally a round of operation performed by the interrogator consists of Clifford gates and Pauli measurements on disjoint subsets of the n-qubits. Since the operations are not adapting to events in preceding rounds (measurements, etc.), here the interrogator simply stores all measurement outcomes o to be used at the decoding round. For more detailed discussions on interrogator formulation of spacetime code see Appendix C.

On the other hand in a Floquet code and a dynamical code, generally a round of operation by the interrogator consists of commuting Pauli measurements. Similar to the spacetime code, the sequence of operations performed on the code is predetermined and the interrogator simply stores all measurement outcomes o to be used at the decoding round. In Floquet code, however, Pauli measurements are performed in cycles. For example in the Hastings-Haah honeycomb code [1, 2], one performs a 3-cycle of Pauli X, followed by Pauli Y, then Pauli Z, which in principle can be performed cyclically indefinitely. However in the finite time window where measurement syndromes can be revealed from the measurements, error-correction analysis using an interrogator consisting of measurements in this time window can be useful. For more detailed discussion on the Hastings-Haah honeycomb code in the interrogator form, see Appendix D.

II. GENERAL ERROR-CORRECTION CONDITIONS

We now formalize the notion of correctability of an error $\mathbf{E}$ by a strategic code $(\mathscr{S}_{Q_0}, \mathbf{I} = \{\mathbf{I}_{m_l}\}_{m_l})$.

Definition 2. Strategic code $(\mathscr{S}_{Q_0}, \mathbf{I})$ corrects error $\mathbf{E}$ if there exists decoding channels $\{\mathcal{D}_{m_l}\}_{m_l}$ such that for all $|\psi\rangle \in \mathscr{S}_{Q_0}$,

$$\mathcal{D}_{m_l}(\mathbf{E} * \mathbf{I}_{m_l} * |\psi\rangle\langle\psi|) = \lambda_{m_l}|\psi\rangle\langle\psi| \tag{4}$$

for some constant $\lambda_{m_l} \in \mathbb{R}$.

We note that how recovery of the initial codestate $|\psi\rangle$ is being defined to be up to a constant independent of $|\psi\rangle$ is an artifact from the fact that the error $\mathbf{E}$ and the interrogator operator $\mathbf{I}_{m_l}$ are not necessarily trace preserving. Namely when there is only one reachable final memory state m_l with probability one given error $\mathbf{E}$ and initial codestate $|\psi\rangle$ then the constant is independent of m_l. Additionally when all error maps $\mathcal{E}^{(0)}, \ldots, \mathcal{E}^{(l)}$ are trace preserving then we have $\lambda_{m_l} = 1$. Now given a precise definition of a successful recovery for error-correction, in the following we give two equivalent necessary and sufficient conditions in an algebraic form and in an information-theoretic form.

A. Algebraic error-correction condition

Now we state the algebraic necessary and sufficient error-correction condition for a strategic code. For notational simplicity, below we suppress the identity operators for operator multiplications to match the dimensions, e.g. for operators $M \in \mathscr{H}_A \otimes \mathscr{H}_C$ and $N \in \mathscr{H}_C \otimes \mathscr{H}_B$ we write MN when we mean $(M \otimes I_B)(I_A \otimes N)$.

Theorem 1. *A strategic code $(\mathscr{S}_{Q_0}, \mathbf{I})$ corrects $\mathfrak{E}$ if and only if*

$$\langle\!\langle E_{e'}|\big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |j\rangle\langle i|\big)|E_e\rangle\!\rangle = \lambda_{e',e,m_l,o}\delta_{j,i} \tag{5}$$

for a constant $\lambda_{e',e,m_l,o} \in \mathbb{C}$, and for all m_l, all check measurement outcome sequence $o \in O_{m_l}$, all pairs of error sequences e, e', and all i, j.

Here $|C_{m_l}\rangle\!\rangle = \sum_{o\in O_{m_l}} |C_{m_l,o}\rangle\!\rangle$ and $|C_{m_l,o}\rangle\!\rangle$ is an eigenvector of interrogator operator $\mathbf{I}_{m_l}$ as defined in eqn. (1). Vectors $|i\rangle, |j\rangle$ are orthonormal basis vectors of initial codespace $\mathscr{S}_{Q_0}$.

Proof. First assume that strategic code $(\mathscr{S}_{Q_0}, \mathbf{I})$ corrects $\mathfrak{E}$, hence there is a set of decoding channels $\{\mathcal{D}_{m_l}\}_{m_l}$ such that (4) is satisfied. First note that we can express eqn. (4) in Kraus representation and use $\Pi_{Q_0}|\psi\rangle = |\psi\rangle$ where Π_{Q_0} is a projector to initial codespace $\mathscr{S}_{Q_0}$ to obtain

$$\begin{aligned}
&\mathcal{D}_{m_l}(\mathbf{E} * \mathbf{I}_{m_l} * |\psi\rangle\langle\psi|) \\
&= \sum_{e,o} \mathcal{D}_{m_l}(K_{e,m_l,o}\Pi_{Q_0}|\psi\rangle\langle\psi|\Pi_{Q_0}K_{e,m_l,o}^\dagger) \\
&= \sum_{e,o,k} D_{k|m_l}K_{e,m_l,o}\Pi_{Q_0}|\psi\rangle\langle\psi|\Pi_{Q_0}K_{e,m_l,o}^\dagger D_{k|m_l}^\dagger \\
&= \lambda_{m_l}\Pi_{Q_0}|\psi\rangle\langle\psi|\Pi_{Q_0} \ ,
\end{aligned} \tag{6}$$

where $\{D_{k|m_l}\}_k$ are the Kraus operators of decoding channel $\mathcal{D}_{m_l}$. By the non-uninqueness of Kraus representation (see e.g. [58]), both $D_{k|m_l}K_{e,m_l,o}$ and $\sqrt{\lambda_{m_l}}\Pi_{Q_0}$ can be thought of as Kraus representations of the composition of maps $\mathcal{D}_{m_l} \circ (\mathbf{E} * \mathbf{I}_{m_l} * (\cdot))$, where the latter Kraus representation consists of only one operator. Thus there must exist some complex number $\gamma_{k,e,o}^{(m_l)}$ such that $D_{k|m_l}K_{e,m_l,o}\Pi_{Q_0} = \gamma_{k,e,o}^{(m_l)}\Pi_{Q_0}$ for all e, o, k. Thus we have

$$\begin{aligned}
&\langle\!\langle E_{e'}|\big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |j\rangle\langle i|\big)|E_e\rangle\!\rangle \\
&= \sum_{o',k} (\langle\!\langle K_{e',m_l,o'}|j\rangle)D_{k|m_l}^\dagger D_{k|m_l}(\langle i|K_{e,m_l,o}\rangle\!\rangle) \\
&= \sum_{o',k} \langle j|\Pi_{Q_0}K_{e',m_l,o'}^\dagger D_{k|m_l}^\dagger D_{k|m_l}K_{e,m_l,o}\Pi_{Q_0}|i\rangle \\
&= \sum_{o',k} \gamma_{k,e',o'}^{(m_l)*}\gamma_{k,e,o}^{(m_l)}\langle j|i\rangle \\
&= \Big(\sum_k \big(\sum_{o'} \gamma_{k,e',o'}^{(m_l)*}\big)\gamma_{k,e,o}^{(m_l)}\Big)\delta_{j,i} \\
&= \lambda_{e',e,m_l,o}\delta_{j,i} \ ,
\end{aligned} \tag{7}$$

where the second equality is obtained by $\sum_k D^\dagger_{k|m_l} D_{k|m_l} = I_{Q'_l}$ and by $|K_{e,m_l,o}\rangle\!\rangle = \langle\!\langle C_{m_l,o}|E_e\rangle\!\rangle$, the third equality by $\langle i|K_{e,m_l,o}\rangle\!\rangle = K_{e,m_l,o}|i\rangle$, and the fourth equality by the non-unique Kraus representation relation $D_{k|m_l} K_{e,m_l,o} \Pi_{Q_0} = \gamma^{(m_l)}_{k,e,o} \Pi_{Q_0}$. Thus we show the necessity of condition in Theorem 1.

Now assume that eqn. (5) holds and consider $\lambda_{e',e,m_l} = \sum_o \lambda_{e',e,m_l,o}$. Note that $\Lambda_{m_l} = [\lambda_{e',e,m_l}]_{e',e}$ is a Hermitian matrix since by eqn. (5)

$$\begin{aligned}
\lambda^*_{e',e,m_l} &= \sum_o \lambda^*_{e',e,m_l,o} \\
&= \sum_{o',o} (\langle\!\langle E_{e'}|(|C_{m_l,o'}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |i\rangle\langle i|)|E_e\rangle\!\rangle)^* \\
&= \sum_{o',o} \langle\!\langle E_e|(|C_{m_l,o}\rangle\!\rangle\langle\!\langle C_{m_l,o'}| \otimes |i\rangle\langle i|)|E_{e'}\rangle\!\rangle \\
&= \sum_{o'} \lambda^*_{e',e,m_l,o'} \\
&= \lambda_{e,e',m_l} \ .
\end{aligned} \tag{8}$$

Since matrix Λ_{m_l} is Hermitian, it can be diagonalized to a diagonal matrix $[d_{e',e,m_l}]_{e',e}$ where $d_{e',e,m_l} = 0$ if $e' \neq e$ as

$$d_{e',e,m_l} = \sum_{\tilde{e},\bar{e}} u^*_{e',\tilde{e}} u_{\bar{e},e} \lambda_{\tilde{e},\bar{e},m_l} \tag{9}$$

where $U = [u_{e',e}]_{e',e}$ is a unitary matrix.

Now consider $|F_e\rangle\!\rangle = \sum_{\bar{e}} u_{\bar{e},e} |E_{\bar{e}}\rangle\!\rangle$ so that

$$\begin{aligned}
\sum_e \langle g|F_e\rangle\!\rangle\langle\!\langle F_e|g'\rangle &= \sum_{e,\tilde{e},\bar{e}} u^*_{e,\tilde{e}} u_{\bar{e},e} \langle g|E_{\bar{e}}\rangle\!\rangle\langle\!\langle E_{\tilde{e}}|g'\rangle \\
&= \sum_{\tilde{e},\bar{e}} \delta_{\tilde{e},\bar{e}} \langle g|E_{\bar{e}}\rangle\!\rangle\langle\!\langle E_{\tilde{e}}|g'\rangle \\
&= \sum_e \langle g|E_e\rangle\!\rangle\langle\!\langle E_e|g'\rangle
\end{aligned} \tag{10}$$

for any $|g\rangle, |g'\rangle \in (\bigotimes_{r=0}^{l-1} \mathscr{S}_{Q_r} \otimes \mathscr{S}_{Q'_r}) \otimes \mathscr{S}_{Q_l}$. Therefore

$$\begin{aligned}
\mathbf{E} * \mathbf{I}_{m_l} * |i\rangle\langle j| &= \sum_e |E_e\rangle\!\rangle\langle\!\langle E_e| * \mathbf{I}_{m_l} * |i\rangle\langle j| \\
&= \sum_e |F_e\rangle\!\rangle\langle\!\langle F_e| * \mathbf{I}_{m_l} * |i\rangle\langle j| \ ,
\end{aligned} \tag{11}$$

and also

$$\begin{aligned}
&\langle\!\langle F_{e'}|\Big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |j\rangle\langle i|\Big)|F_e\rangle\!\rangle \\
&= \sum_{\tilde{e},\bar{e}} u^*_{e',\tilde{e}} u_{\bar{e},e} \langle\!\langle E_{\tilde{e}}|\Big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |j\rangle\langle i|\Big)|E_{\bar{e}}\rangle\!\rangle \\
&= \sum_{\tilde{e},\bar{e}} u^*_{e',\tilde{e}} u_{\bar{e},e} \lambda_{\tilde{e},\bar{e},m_l,o} \delta_{j,i} =: \tilde{\lambda}_{e',e,m_l,o} \delta_{j,i} \ ,
\end{aligned} \tag{12}$$

for some constant $\tilde{\lambda}_{e',e,m_l,o} \in \mathbb{C}$.

For each error sequence e', consider an operator defined by $D_{e'|m_l} = \frac{1}{\sqrt{d_{e',e'}}} \langle\!\langle F_{e'}|(|C_{m_l}\rangle\!\rangle|\Pi_{Q_0}\rangle\!\rangle)$. Thus by using eqn. (5) and eqn. (12) the action of $D_{e'|m_l}$ on the codestate at the start of the decoding round is

$$\begin{aligned}
&D_{e'|m_l}(\langle\!\langle C_{m_l,o}|\langle\psi|)|F_e\rangle\!\rangle \\
&= \sum_{i,j} |j\rangle\, \psi_i \langle\!\langle F_{e'}|(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |j\rangle\langle i|)|F_e\rangle\!\rangle \\
&= \sum_{i,j,} |j\rangle\, \psi_i \tilde{\lambda}_{e',e,m_l,o} \delta_{j,i} = \tilde{\lambda}_{e',e,m_l,o}|\psi\rangle \ .
\end{aligned} \tag{13}$$

Therefore the overall action of a linear map $\mathcal{D}_{m_l}(\rho) = \sum_e D_{e|m_l} \rho D^\dagger_{e|m_l}$ on the density operator of the code at the start of the decoding round is

$$\begin{aligned}
&\sum_e \mathcal{D}_{m_l}(|F_e\rangle\!\rangle\langle\!\langle F_e| * \mathbf{I}_{m_l} * |\psi\rangle\langle\psi|) \\
&= \sum_{e,e',o} D_{e'|m_l}(\langle\!\langle C_{m_l,o}|\langle\psi|)|F_e\rangle\!\rangle\langle\!\langle F_e|(|C_{m_l,o}\rangle\!\rangle|\psi\rangle) D^\dagger_{e'|m_l} \\
&= \sum_{e,e',o} \tilde{\lambda}_{e',e,m_l,o} \tilde{\lambda}^*_{e',e,m_l,o} |\psi\rangle\langle\psi| = \lambda_{m_l} |\psi\rangle\langle\psi|
\end{aligned} \tag{14}$$

which recovers the initial state $|\psi\rangle$ as in (4).

Since $\mathcal{D}_{m_l}$ is a completely positive map, we now show that we can add another operator to make it trace-preserving. Consider polar decomposition

$$\begin{aligned}
&(\langle\!\langle C_{m_l}|\langle\!\langle \Pi_{Q_0}|)|F_e\rangle\!\rangle \\
&= U_{e,m_l} \sqrt{\langle\!\langle F_e|\big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l}| \otimes |\Pi_{Q_0}\rangle\!\rangle\langle\!\langle \Pi_{Q_0}|\big)|F_e\rangle\!\rangle} \\
&= U_{e,m_l} \Pi_{Q_0} \sqrt{d_{e,e,m_l}}
\end{aligned} \tag{15}$$

where the last equality is due to eqn. (9). Then can define projector $\Pi_{e,m_l} = U_{e,m_l} \Pi_{Q_0} U^\dagger_{e,m_l} = \frac{1}{\sqrt{d_{e,e,m_l}}} (\langle\!\langle C_{m_l}|\langle\!\langle \Pi_{Q_0}|)|F_e\rangle\!\rangle U^\dagger_{e,m_l}$, satisfying orthogonality

$$\begin{aligned}
&\Pi^\dagger_{e',m_l} \Pi_{e,m_l} \\
&= \frac{U_{e',m_l} \langle\!\langle F_{e'}|(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l}| \otimes |\Pi_{Q_0}\rangle\!\rangle\langle\!\langle \Pi_{Q_0}|)|F_e\rangle\!\rangle U^\dagger_{e,m_l}}{\sqrt{d_{e',e',m_l} d_{e,e,m_l}}} \\
&= \frac{d_{e',e,m_l} U_{e',m_l} \Pi_{Q_0} U^\dagger_{e,m_l}}{\sqrt{d_{e',e',m_l} d_{e,e,m_l}}} \ ,
\end{aligned} \tag{16}$$

since $d_{e',e,m_l} = 0$ for all $e \neq e'$. Therefore for each e we have

$$\begin{aligned}
D^\dagger_{e|m_l} D_{e|m_l} &= \frac{(\langle\!\langle C_{m_l}|\langle\!\langle \Pi_{Q_0}|)|F_e\rangle\!\rangle\langle\!\langle F_e|(|C_{m_l}\rangle\!\rangle|\Pi_{Q_0}\rangle\!\rangle)}{d_{e,e,m_l}} \\
&= U_{e,m_l} \Pi_{Q_0} U^\dagger_{e,m_l} = \Pi_{e,m_l} \ .
\end{aligned} \tag{17}$$

Then by adding projector $\Pi^\perp$ onto a space orthogonal to $\{\Pi_{e,m_l}\}_e$ to the set of operators $\{D_{e|m_l}\}_e$ defining $\mathcal{D}_{m_l}$ we have $\Pi^\perp + \sum_e D^\dagger_{e|m_l} D_{e|m_l} = I$, hence $\mathcal{D}_{m_l}$ is trace-preserving. □

As noted in the proof and by using the Kraus operators in eqn. (3), we can equivalently express eqn. (5) as

$$\begin{aligned}
&\langle\!\langle E_{e'}|\Big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \otimes |j\rangle\langle i|\Big)|E_e\rangle\!\rangle \\
&= \mathrm{Tr}(|K_{e',m_l}\rangle\!\rangle\langle\!\langle K_{e,m_l,o}| * |j\rangle\langle i|) \\
&= \langle j|K^\dagger_{e',m_l} K_{e,m_l,o}|i\rangle = \delta_{j,i} \lambda_{e',e,m_l,o} \ ,
\end{aligned} \tag{18}$$

where $K_{e',m_l} = \sum_o K_{e',m_l,o}$. This expression tells us for a final memory state m_l of a strategic code correcting $\mathfrak{E}$, the sequence of check measurement outcomes in O_{m_l} forms orthogonal an subspace $\mathscr{V}_{i,m_l}$ for each eigenbasis $\{|i\rangle_{Q_0}\}_i$ spanning initial codestate $\mathscr{S}_{Q_0}$, regardless of sequence of error. Namely subspace $\mathscr{V}_{i,m_l}$ is spanned by $\{\langle\!\langle C_{m_l,o}|\langle i|E_e\rangle\!\rangle\}_{e,o}$. Moreover, the independence of constant $\lambda_{e',e,m_l,o}$ from the initial codestate also indicates that the code state at the start of the decoding round is *uncorrelated* with the noise environment, although it generally depends on the final memory state m_l. Due to this independence between the noise environment and the code state, it is sufficient for the decoder to have the information about m_l to recover the initial state, i.e. to construct a projective measurement $\{\Pi_{e,m_l}\}_e$ used in the proof to project the noisy codestate onto subspace $\mathscr{V}_{i,m_l}$ and perform recovery unitary operator U_{e,m_l} according to outcome e to obtain the initial codestate.

For the special case when all check measurement outcomes are stored in the classical memory, i.e. there is a bijection between each memory state m_r and sequence of check measurement outcomes $o_1,\ldots,o_r$ for all r, the condition in Theorem 1 can be stated in a more symmetric manner as $\mathbf{I}_{m_l} = |C_{m_l,o}\rangle\!\rangle\langle\!\langle C_{m_l,o}|$. Since each final memory state m_l and each sequence of check measurement outcomes $o = o_1,\ldots,o_l$ have a one-to-one correspondence, we can simply write $|C_{m_l}\rangle\!\rangle := |C_{m_l,o}\rangle\!\rangle$.

Corollary 1. *A strategic code $(\mathscr{S}_{Q_0},\mathbf{I})$ storing all check measurement outcomes in its memory corrects error $\mathfrak{E}$ if and only if*

$$\langle\!\langle E_{e'}|\big(|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l}|\otimes|j\rangle\langle i|\big)|E_e\rangle\!\rangle = \lambda_{e',e,m_l}\delta_{j,i} \tag{19}$$

where $\lambda_{e',e,m_l}\in\mathbb{C}$ is some constant for all final memory state m_l and all pairs of error sequences e,e'.

B. Static quantum error-correction condition as a special case

From Theorem 1, we can recover the Knill-Laflamme necessary and sufficient error-correction condition for static QECC [23] (see also Appendix A), which is

$$\langle j|E_{e'}^\dagger E_e|i\rangle = \lambda_{e',e}\delta_{j,i} \tag{20}$$

where $|i\rangle,|j\rangle$ is an arbitrary pair of orthonormal vectors spanning codespace $\mathscr{S}_Q$ and $E_e,E_{e'}$ are a pair of Kraus operators of error map $\mathcal{E}(\rho_Q) = \sum_e E_e\rho_Q E_e^\dagger$. The static QECC scenario is obtained by setting the number of rounds to $l=0$ in a general QECC scenario, i.e. there is no sequence check instruments. The operator $|C_{m_l}\rangle\!\rangle\langle\!\langle C_{m_l,o}|$ in eqn. (5)simply becomes identity and vectorized error operators are of the form $|E_e\rangle\!\rangle = \sum_j E_e|j\rangle|j\rangle$ and constant is simply $\lambda_{e',e}$ as there is no dependence on the check measurement outcomes. Thus eqn. (5) becomes

$$\lambda_{e',e}\delta_{j,i} = \langle\!\langle E_{e'}|j\rangle\!\rangle\langle\!\langle i|E_e\rangle\!\rangle = \langle j|E_{e'}^\dagger E_e|i\rangle \tag{21}$$

giving us the Knill-Laflamme static QECC condition.

Lastly we note that without changing the strategic code framework, how strategic code error-correction is defined in Definition 2 can be generalized as follows. Instead of requiring the decoder output to be a state proportional to the initial codestate, we can instead introduce additional redundancy by encoding logical information in a subsystem of $\mathscr{S}_{Q_0}$ and requiring the decoder only to recover logical information stored in that subsystem. Namely, given initial codestate $\rho\otimes\sigma$ we want to recover $\rho\otimes\sigma_{m_l}$ given final memory state m_l. This is the generalization of the subsystem code [27, 29, 59, 60] to the strategic code framework. Corresponding to this definition, however, one needs a different necessary and sufficient condition than Theorem 1 and Theorem 2, which is left for future work. For more details on the subsystem code generalization to strategic code see Appendix B 2.

C. Information-theoretic error-correction condition

For a static QECC (special case of a strategic code with $l=0$), it was shown in [25] that a necessary and sufficient condition for a completely-positive, trace non-decreasing error map $\mathcal{E}:\mathscr{H}_Q\to\mathscr{H}_{Q'}$ to be correctable by QECC with codespace $\mathscr{S}_Q$ is

$$S(\rho^Q) = S(\rho^{Q'}) - S(\rho^{E'}) = S(\rho^{Q'}) - S(\rho^{R'Q'})\,. \tag{22}$$

Here a reference system R is introduced, and $\rho^Q = \mathrm{Tr}_R(|\phi\rangle\!\langle\phi|^{RQ})$ where $|\phi\rangle\!\langle\phi|^{RQ}$ is the maximally entangled state between initial system Q and reference system R. So, we have the density operators after the error $\rho^{Q'} = \mathcal{E}(\rho^Q)/\mathrm{Tr}(\mathcal{E}(\rho^Q))$ and $\rho^{R'Q'} = \mathcal{I}_R\otimes\mathcal{E}(|\phi\rangle\!\langle\phi|^{RQ})$ where $\rho^{E'}$ the marginal state of the noise environment of $\mathcal{E}$ when expressed as

$$\mathcal{E}(\cdot) = \mathrm{Tr}_{E'}\Big((I_{Q'}\otimes\Pi)V\cdot V^\dagger(I_{Q'}\otimes\Pi)\Big) \tag{23}$$

for some isometry $V:\mathscr{S}_Q\to\mathscr{S}_{Q'}\otimes\mathscr{S}_{E'}$ and orthogonal projector $\Pi\in\mathscr{H}_{E'}$. Generalization of information-theoretic condition (22) to subsystem codes is shown in [27]. The term $S(\rho^{Q'}) - S(\rho^{R'Q'})$ is the so-called "coherent information", which quantifies the amount of information about ρ^Q contained in $\rho^{Q'}$ [24, 25, 27].

In a general QECC scenario, we instead have a sequence of completely positive map $\mathcal{E}^{(0)},\ldots,\mathcal{E}^{(l)}$. In what follows, we omit normalization for the states and density operators for notational simplicity. Now consider the density operator in $\mathscr{H}_{R_l'}\otimes\mathscr{H}_{Q_l'}\otimes\mathscr{H}_{M_l}\otimes\mathscr{H}_{E_l}$ with one-half of a maximally entangled state $\sum_i|i\rangle_{R_0}|i\rangle_{Q_0}$ as an input initial state in $\mathscr{S}_{Q_0}$ and given final memory state m_l

$$\rho^{R_l' Q_l' M_l E_l}_{m_l,e,e',o,o'} = \sum_{i,j} |i\rangle\langle j|_{R_0} \otimes \left(K_{e,m_l,o}|i\rangle\langle j|_{Q_0} K^\dagger_{e',m_l,o'}\right) \otimes |o\rangle\langle o'|_{M_l} \otimes |e\rangle\langle e'|_{E_l} \tag{24}$$

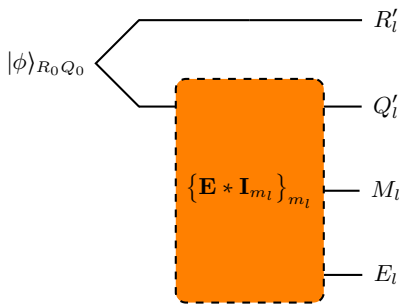


FIG. 3. QECC scenario where the initial code state is one-half of maximally entangled state $|\phi\rangle = \sum_i |i\rangle_{R_0}|i\rangle_{Q_0}$ between a reference R_0 system and the initial code space Q_0. After l rounds of errors and check measurements ending in final memory state m_l, we obtain the global density oeprator $\rho^{R_l' Q_l' M_l E_l}_{m_l}$ of the reference system, code system, check measurement outcome sequence, and noise environment.

where $o, o' \in O_{m_l}$ is a pair of sequences of check measurement outcomes resulting in final memory state m_l and $K_{e,m_l,o}$ is an operator defined by $|K_{e,m_l,o}\rangle\!\rangle = \langle\!\langle C_{m_l,o}|E_e\rangle\!\rangle$ (see eqn. (3). This scenario is illustrated in Fig. 3.

Now consider density operator

$$\rho^{R_l' Q_l' M_l E_l}_{m_l} := \sum_{e,e',o,o'} \rho^{R_l' Q_l' M_l E_l}_{m_l,e,e',o,o'} \,. \tag{25}$$

We also define the marginal density operators as $\rho^{R_l'}_{m_l} := \mathrm{Tr}_{Q_l' M_l E_l}(\rho^{R_l' Q_l' M_l E_l}_{m_l})$ and $\rho^{M_l E_l}_{m_l} := \mathrm{Tr}_{R_l' Q_l'}(\rho^{R_l' Q_l' M_l E_l}_{m_l})$. We also denote the density operator over all possible final memory state m_l as

$$\rho^{R_l' Q_l' M_l E_l} = \sum_{m_l} P_{M_l}(m_l) \tilde{\rho}^{R_l' Q_l' M_l E_l}_{m_l} \tag{26}$$

for $P_{M_l}(m_l) = \mathrm{Tr}(\rho^{R_l' Q_l' M_l E_l}_{m_l})$ and density operator $\tilde{\rho}^{R_l' Q_l' M_l E_l}_{m_l} = \rho^{R_l' Q_l' M_l E_l}_{m_l} / P_{M_l}(m_l)$. Here, $P_{M_l}(m_l)$ can be interpreted as the probability of the final memory state being m_l. Hence $\tilde{\rho}^{R_l' Q_l' M_l E_l}_{m_l}$ is the density operator at the start of the decoding round, given that the memory storing information about the check measurement outcomes is m_l.

Now we show a necessary and sufficient information-theoretic conditions for strategic code to correct error $\mathfrak{E} = \{|E_e\rangle\!\rangle\langle\!\langle E_e|\}_e$.

Theorem 2. *The following are equivalent:*

1. *A strategic code $(\mathscr{S}_{Q_0}, \mathbf{I})$ corrects error $\mathfrak{E}$.*
2. *$S(\rho^{R_l' M_l E_l}_{m_l}) = S(\rho^{R_l'}_{m_l}) + S(\rho^{M_l E_l}_{m_l})$ for all final memory state m_l such that $P_{M_l}(m_l) > 0$.*
3. *$I_{\rho^{R_l' M_l E_l}_{m_l}}(R_l' : M_l E_l) = 0$ for all final memory state m_l such that $P_{M_l}(m_l) > 0$.*

Proof. First we use Theorem 1 to show that eqn. (5) implies $S(\rho^{R_l' M_l E_l}_{m_l}) = S(\rho^{R_l'}_{m_l}) + S(\rho^{M_l E_l}_{m_l})$. The merginal density operator in $\mathscr{H}_{R_l'} \otimes \mathscr{H}_{M_l} \otimes \mathscr{H}_{E_l}$ can be expressed as

$$\begin{aligned}\rho^{R_l' M_l E_l}_{m_l} &:= \sum_{e,e',o,o'} \mathrm{Tr}_{Q_l'}\left(\rho^{R_l' Q_l' M_l E_l}_{m_l,e,e',o,o'}\right) \\ &= \sum_{e,e',o,o',i,j} |i\rangle\langle j|_{R_l'} \langle j|K^\dagger_{e',m_l,o'} K_{e,m_l,o}|i\rangle \\ &\quad \otimes |o\rangle\langle o'|_{M_l} \otimes |e\rangle\langle e'|_{E_l} \,.\end{aligned} \tag{27}$$

Now consider a unitary $[u_{\bar{e},e}]_{\bar{e},e}$ as defined in the sufficiency of eqn. (5) which performs the transformation $|F_e\rangle\!\rangle = \sum_{\bar{e}} u_{\bar{e},e}|E_{\bar{e}}\rangle\!\rangle$. Applying this to eqn. (27) transforms the Kraus operator $K_{e,m_l,o} \mapsto F_{e,m_l,o}$ and the noise environment basis $|e\rangle \mapsto |v^{(m_l)}_e\rangle = \sum_{\bar{e}} u_{\bar{e},e}|\bar{e}\rangle$. Also consider the decoding channel $\mathcal{D}_{m_l}$ with Kraus operators $\{D_{e|m_l}\}_e$ constructed in proof of the sufficiency of eqn. (5) to correct $\mathfrak{E}$. As $\sum_e D^\dagger_{e|m_l} D_{e|m_l} = I$, we obtain

$$\begin{aligned}&\rho^{R_l' M_l E_l}_{m_l} \\ &= \sum_{e,e',o,o',i,j,\tilde{e}} |i\rangle\langle j|_{R_l'} \langle j|F^\dagger_{e',m_l,o'} D^\dagger_{\tilde{e}|m_l} D_{\tilde{e}|m_l} F_{e,m_l,o}|i\rangle \\ &\quad \otimes |o\rangle\langle o'|_{M_l} \otimes |v^{(m_l)}_e\rangle\langle v^{(m_l)}_{e'}|_{E_l} \\ &= \Pi_{Q_0} \otimes \Big(\sum_{e,e',o,o',\tilde{e}} \tilde{\lambda}^*_{\tilde{e},e',m_l,o'} \tilde{\lambda}_{\tilde{e},e,m_l,o} |o\rangle\langle o'|_{M_l} \\ &\quad \otimes |v^{(m_l)}_e\rangle\langle v^{(m_l)}_{e'}|_{E_l} \Big)\end{aligned} \tag{28}$$

since $D_{\tilde{e}|m_l} F_{e,m_l,o}|i\rangle = \tilde{\lambda}_{\tilde{e},e,m_l,o}|i\rangle$ for some constant $\tilde{\lambda}_{\tilde{e},e,m_l,o} \in \mathbb{C}$. Thus $\rho^{R_l' M_l E_l}_{m_l} = \rho^{R_l'}_{m_l} \otimes \rho^{M_l E_l}_{m_l}$, which is equivalent to $S(\rho^{R_l' M_l E_l}_{m_l}) = S(\rho^{R_l'}_{m_l}) + S(\rho^{M_l E_l}_{m_l})$.

Now we show that $S(\rho^{R_l' M_l E_l}_{m_l}) = S(\rho^{R_l'}_{m_l}) + S(\rho^{M_l E_l}_{m_l})$ implies eqn. (4) by constructing a decoding channel recovering the initial code state. Now we consider a Schmidt decomposition on bipartition between codespace Q_l' and joint system $R_l' M_l E_l$ of $|\varphi_{m_l}\rangle = \sum_{i,e,o} |i\rangle_{R_0}(K_{m_l,o,e}|i\rangle_{Q_0})|o\rangle_{M_l}|e\rangle_{E_l}$ for each o, which gives

$$|\varphi_{m_l}\rangle = \sum_{i,\alpha} \sqrt{q^{(m_l)}_\alpha}|i\rangle_{R_l'}|u^{(m_l)}_\alpha\rangle_{M_l E_l}|v^{(m_l)}_{i,\alpha}\rangle_{Q_l'} \tag{29}$$

where $\{|u^{(m_l)}_\alpha\rangle_{M_l E_l}\}_\alpha$ is an eigenvector of $\rho^{M_l E_l}_{m_l}$ with corresponding eigenvalue $q^{(m_l)}_\alpha$ and $\{|v^{(m_l)}_{i,\alpha}\rangle\}_{i,\alpha}$ is a set of orthonormal vectors in code space $\mathscr{S}_{Q_l'}$.

Now consider decoding channel $\mathcal{D}_{m_l}$ with Kraus operators $\{D_{\alpha|m_l}\}_\alpha \cup \{\Pi^\perp\}$ defined by

$$D_{\alpha|m_l} = V_{m_l,\alpha} \sum_i |v^{(m_l)}_{i,\alpha}\rangle\!\rangle\langle v^{(m_l)}_{i,\alpha}|_{Q_l'} \,, \tag{30}$$

for unitary $V_{m_l,\alpha}:\mathscr{S}_{Q_l'}\to\mathscr{S}_{Q_0}$ such that $V_{m_l,\alpha}|v_{i,\alpha}^{(m_l)}\rangle_{Q_l'}=|i\rangle_{Q_0}$ for all i. Operator $\Pi^\perp$ is a projector onto subspace $\mathscr{V}^\perp$ orthogonal to $\mathrm{Span}\{|v_{i,\alpha}^{(m_l)}\rangle\}_\alpha$ to obtain normalization $\Pi^\perp+\sum_\alpha D_{\alpha|m_l}^\dagger D_{\alpha|m_l}=I$. Hence

$$\begin{aligned} D_{\alpha|m_l}|\varphi_{m_l}\rangle &= \sum_i \sqrt{q_\alpha^{(m_l)}}|i\rangle_{R_l'}|u_\alpha^{(m_l)}\rangle_{M_lE_l}|i\rangle_{Q_0} \\ &= |\phi\rangle_{R_l'Q_l'}\sqrt{q_\alpha^{(m_l)}}|u_\alpha^{(m_l)}\rangle_{M_lE_l} \end{aligned} \tag{31}$$

showing that the initial maximally entangled state is recovered. Thus the overall action of decoding channel $\mathcal{D}_{m_l}$ to the density operator $|E_e\rangle\!\rangle\langle\!\langle E_e|*\mathbf{I}_{m_l}*|\psi\rangle\langle\psi|_{Q_0}$ of system Q_l' at the start of the decoding round is

$$\begin{aligned} &\mathcal{D}_{m_l}(\mathbf{E}*\mathbf{I}_{m_l}*|\psi\rangle\langle\psi|_{Q_0}) \\ &= \sum_{i,j,e}\psi_i\psi_j^*\mathcal{D}_{m_l}(|E_e\rangle\!\rangle\langle\!\langle E_e|*\mathbf{I}_{m_l}*|i\rangle\langle j|_{Q_0}) \\ &= \sum_{i,j,e',e,o',o}\psi_i\psi_j^*\mathcal{D}_{m_l}(K_{e,m_l,o}|i\rangle\langle j|K_{e',m_l,o'}^\dagger)\langle e'|e\rangle\langle o'|o\rangle \\ &= \sum_{i,j,\alpha',\alpha}\psi_i\psi_j^*\sqrt{q_\alpha^{(m_l)}q_{\alpha'}^{(m_l)}}\mathcal{D}_{m_l}(|v_{i,\alpha}^{(m_l)}\rangle\langle v_{j,\alpha'}^{(m_l)}|) \\ &\quad\times\langle u_{\alpha'}^{(m_l)}|u_\alpha^{(m_l)}\rangle \\ &= \sum_{i,j,\alpha}\psi_i\psi_j^*q_\alpha^{(m_l)}\mathcal{D}_{m_l}(|v_{i,\alpha}^{(m_l)}\rangle\langle v_{j,\alpha}^{(m_l)}|) \\ &= \sum_{i,j,\alpha}\psi_i\psi_j^*q_\alpha^{(m_l)}|i\rangle\langle j|_{Q_0} \\ &= \lambda_{m_l}|\psi\rangle\langle\psi|_{Q_0} \end{aligned} \tag{32}$$

where $\lambda_{m_l}=\sum_\alpha q_\alpha^{(m_l)}$. To obtain the third equality, we use the change of basis on the joint memory - noise environment system M_lE_l to $|u_\alpha^{(m_l)}\rangle_{M_lE_l}=\sum_{o,e}\eta_{(o,e),\alpha}^{(m_l)}|o\rangle_{M_l}|e\rangle_{E_l}$ for some complex numbers $\{\eta_{(o,e),\alpha}^{(m_l)}\}_{o,e,\alpha}$ which also gives $K_{e,m_l,o}|i\rangle\mapsto\sqrt{q_\alpha^{(m_l)}}|u_{\alpha,i}^{(m_l)}\rangle=\sum_{o,e}\eta_{(o,e),\alpha}^{(m_l)}K_{e,m_l,o}|i\rangle$. Whereas the fourth equality is obtained by using eqn. (31). Thus decoding channel $\mathcal{D}_{m_l}$ recovers all initial codestate $|\psi\rangle_{Q_0}$ for any error sequence e.

Lastly, we show that $I_{\rho_{m_l}^{R_l'M_lE_l}}(R_l':M_lE_l)=0$ if and only if $S(\rho_{m_l}^{R_l'M_lE_l})=S(\rho_{m_l}^{R_l'})+S(\rho_{m_l}^{M_lE_l})$. This simply follows from the definition of von Neumann mutual information

$$I_{\rho_{m_l}^{R_l'M_lE_l}}(R_l':M_lE_l)=S(\rho_{m_l}^{R_l'})+S(\rho_{m_l}^{M_lE_l})-S(\rho_{m_l}^{R_l'M_lE_l})\,, \tag{33}$$

which is equal to 0 if and only if $S(\rho_{m_l}^{R_l'M_lE_l})=S(\rho_{m_l}^{R_l'})+S(\rho_{m_l}^{M_lE_l})$. □

Statement 2 of Theorem 2 reduces to the information-theoretic necessary and sufficient condition for static QECC in [24, 25] stating that the reduced density operator of the reference system and the environment after the error operation $\rho^{R'E'}$ is separable. Stated equivalently in terms of the von Neumann entropy, $S(\rho^{R'E'})=S(\rho^{R'})+S(\rho^{E'})$. On the other hand, statement 3 of Theorem 2 reduces to the necessary and sufficient condition in [26] for static error correction, stating that it must hold that the mutual information between the noise environment E' and the reference system R' after error operation is $I_{\rho^{R'E'}}(E':R')=0$. Namely, there is no correlation between E' and R'. In the general QECC case, the condition $S(\rho_{m_l}^{R_l'M_lE_l})=S(\rho_{m_l}^{R_l'})+S(\rho_{m_l}^{M_lE_l})$ and $I_{\rho_{m_l}^{R_l'M_lE_l}}(R_l':M_lE_l)=0$ indicates that the reference system R_l' and the joint check measurement outcome - noise environment system M_lE_l at the start of the decoding round are uncorrelated for each final memory state m_l. However in general, the check measurement outcome system M_l and the noise environment E_l exhibit some correlation.

III. ERROR-ADAPTED APPROXIMATE STRATEGIC CODE

So far we have been focusing on strategic codes which recovers logical information *exactly* by showing necessary and sufficient conditions of how to achieve this (Theorem 1 and Theorem 2). However in practice, resource limitations and some knowledge about characteristic of the relevant noise often allow us to relax the requirements on how well logical information should be recovered in exchange for a less resource-intensive code. These practical considerations gives rise to *approximate* (static) QECCs, which have been known to achieve a performance comparable to generic exact QECC in dealing with a particular error model in a more resource-efficient manner (see e.g. [61–66]).

To address this practical considerations we turn to *approximate strategic code*, namely one where we demand that logical information is recovered only up to a certain fidelity by a decoding channel after the l rounds of operation by the interrogator. To obtain this approximate code, we propose an optimization problem that given an ensemble of d'-dimensional quantum states, an l-rounds of error $\mathbf{E}$, and positive integer $d>d'$ and returns: (1) an encoding channel $\mathcal{C}^{(0)}$ mapping bounded linear operators on $\mathbb{C}^{d'}$ to bounded linear operators on subspace $\mathscr{S}_{Q_0}$ of $\mathbb{C}^d$, (2) an l-round interrogator $\mathbf{I}$, and (3) set of decoders $\mathbf{D}$ corresponding to each final memory state of interrogator $\mathbf{I}$. Note that as opposed to the previously considered QECC scenario where we start with the codespace $\mathscr{S}_{Q_0}$, here we start with a channel $\mathcal{C}^{(0)}$ that maps d'-dimensional density operators on $\mathbb{C}^{d'}$ to density operators with support on $\mathscr{S}_{Q_0}\subseteq\mathbb{C}^d$. Also, the decoding channel $\mathcal{D}_{m_l}$ for final memory state m_l maps density operators with support on $\mathscr{S}_{Q_l'}\subseteq\mathbb{C}^d$ (the codespace after the final error map) to density operators on $\mathbb{C}^{d'}$. Let us denote the space of operators on $\mathbb{C}^{d'}$ at the input of the

encoding channel by $\mathscr{H}_L$ and those at the output of the decoding channel by $\mathscr{H}_{L'}$.

We can describe the encoding, interrogator, and decoding as one single quantum comb

$$\mathbf{Q} = \sum_{m_{0:l}} \mathbf{D}_{m_l} \otimes \mathbf{C}^{(l)}_{m_l|m_{l-1}} \otimes \cdots \otimes \mathbf{C}^{(1)}_{m_1} \otimes \mathbf{C}^{(0)} \,. \tag{34}$$

Operator $\mathbf{Q}$ is positive semidefinite as a consequence of each $\mathbf{D}_{m_l}, \mathbf{C}^{(l)}_{m_l|m_{l-1}}, \ldots, \mathbf{C}^{(1)}_{m_1}, \mathbf{C}^{(0)}$ (Choi operators of CP maps $\mathcal{D}_{m_l}, \mathcal{C}^{(l)}_{m_l|m_{l-1}}, \ldots, \mathcal{C}^{(1)}_{m_1}, \mathcal{C}^{(0)}$) being positive semidefinite operator in $\mathscr{H}_{L'} \otimes \mathscr{H}_{Q'_l}$, $\mathscr{H}_{Q_l} \otimes \mathscr{H}_{Q'_{l-1}}, \ldots, \mathscr{H}_{Q_1} \otimes \mathscr{H}_{Q'_0}$, $\mathscr{H}_{Q_0} \otimes \mathscr{H}_L$, respectively. The sequence of errors described similarly as $\mathbf{E} = \sum_e |E_e\rangle\!\rangle\langle\!\langle E_e|$, which is also positive semidefinite.

Let $Q = \{L, Q_0, Q'_0, \ldots, Q_l, Q'_l, L'\}$ be the set of labels of the code spaces in the dynamical code and for $\tilde{Q} \subseteq Q$ denote $(\cdot)^{\top_{\tilde{Q}}}$ as partial transpose over spaces with labels in $\tilde{Q}$ and $\mathrm{Tr}_{\tilde{Q}}$ as partial trace over spaces with labels in $\tilde{Q}$ and $I_{\tilde{Q}} = \bigotimes_{Q' \in \tilde{Q}} I_{Q'}$. Consider a channel $\mathcal{T} : \mathscr{H}_L \to \mathscr{H}_{L'}$ composed of the sequence of the check instruments $\{\mathcal{C}^{(l)}_{m_l|m_{l-1}}, \ldots, \mathcal{C}^{(1)}_{m_1}, \mathcal{C}^{(0)}\}_m$ for sequence of memory state $m = m_1, \ldots, m_l$, error maps $\mathcal{E}^{(l)}, \ldots, \mathcal{E}^{(0)}$ and the final decoding channels $\{\mathcal{D}_{m_l}\}_{m_l}$. We use the entanglement fidelity of channel $\mathcal{T}$ on state ρ as our performance metric, which is defined as

$$\begin{aligned} F(\rho, \mathcal{T}) &= \mathrm{Tr}\big(\mathbf{E} * \mathbf{Q}\, |\rho\rangle\!\rangle\langle\!\langle\rho|\big) \\ &= \mathrm{Tr}\big((\mathbf{E}^\top \otimes I_{L',L})\, \mathbf{Q}\, (|\rho\rangle\!\rangle\langle\!\langle\rho| \otimes I_{Q\setminus L,L'})\big) \,, \end{aligned} \tag{35}$$

where $|\rho\rangle\!\rangle = \sum_j \rho|j\rangle|j\rangle$ is the vectorized form of density operator ρ.

For $r \in \{1, \ldots, l\}$, it holds that $\mathrm{Tr}_{Q_r}(\sum_{m_r} \mathbf{C}^{(r)}_{m_r|m_{r-1}}) = I_{Q'_{r-1}}$ since $\sum_{m_r} \mathcal{C}^{(r)}_{m_r|m_{r-1}}$ is a CPTP map. Similarly it also holds that $\mathrm{Tr}_{Q_0}(\mathbf{C}^{(0)}) = I_L$ and $\mathrm{Tr}_{L'}(\mathbf{D}_{m_l}) = I_{Q'_l}$ for each m_l. Thus for a given error operator $\mathbf{E}$ and initial state ρ, we can maximize entanglement fidelity (35) over $\mathbf{Q}$ as

$$\begin{aligned} &\max_{\mathbf{Q}} \mathrm{Tr}\big((\mathbf{E}^\top \otimes I_{L',L})\, \mathbf{Q}\, (|\rho\rangle\!\rangle\langle\!\langle\rho| \otimes I_{Q\setminus L,L'})\big) \\ &\text{such that} \\ &\mathbf{Q} = \sum_{m_{0:l}} \mathbf{D}_{m_l} \otimes \mathbf{C}^{(l)}_{m_l|m_{l-1}} \otimes \cdots \otimes \mathbf{C}^{(0)}_{m_0} \\ &\mathbf{D}_{m_l} \geq 0 \,, \quad \mathrm{Tr}_{L'}(\mathbf{D}_{m_l}) = I_{Q'_l} \\ &\mathbf{C}^{(0)} \geq 0 \,, \quad \mathrm{Tr}_{Q_0}\big(\mathbf{C}^{(0)}\big) = I_L \\ &\mathbf{C}^{(r)}_{m_r|m_{r-1}} \geq 0 \,,\ \mathrm{Tr}_{Q_r}\big(\sum_{m_r} \mathbf{C}^{(r)}_{m_r|m_{r-1}}\big) = I_{Q'_{r-1}} \,,\ \forall r \geq 1 \,. \end{aligned} \tag{36}$$

We can also impose this normalization condition to operator $\mathbf{Q}$ as follows. Let $\mathbf{Q}_{m_l} = \sum_{m_{0:l-1}} \mathbf{D}_{m_l} \otimes \mathbf{C}^{(l)}_{m_l|m_{l-1}} \otimes \cdots \otimes \mathbf{C}^{(1)}_{m_1} \otimes \mathbf{C}^{(0)}$ (hence $\mathbf{Q} = \sum_{m_l} \mathbf{Q}_{m_l}$) and for $r \in \{0, \ldots, l\}$ let $\mathbf{Q}^{(r)}_{m_r} = \sum_{m_{0:r-1}} \mathbf{C}^{(r)}_{m_r|m_{r-1}} \otimes \cdots \otimes \mathbf{C}^{(1)}_{m_1} \otimes \mathbf{C}^{(0)}$ (hence $\mathbf{Q}^{(1)}_{m_1} = \mathbf{C}^{(1)}_{m_1} \otimes \mathbf{C}^{(0)}$ and $\mathbf{Q}^{(0)} = \mathbf{C}^{(0)}$). Thus we can rewrite the conditions in (36) in this notation as

$$\begin{aligned} &\max_{\mathbf{Q}} \mathrm{Tr}\big((\mathbf{E}^\top \otimes I_{L',L})\, \mathbf{Q}\, (|\rho\rangle\!\rangle\langle\!\langle\rho| \otimes I_{Q\setminus L,L'})\big) \\ &\text{such that} \\ &\mathbf{Q} \geq 0 \,, \quad \mathrm{Tr}_{L'}(\mathbf{Q}) = \sum_{m_l} I_{Q'_l} \otimes \mathbf{Q}^{(l)}_{m_l} \\ &\mathrm{Tr}_{Q_r}\Big(\sum_{m_r} \mathbf{Q}^{(r)}_{m_r}\Big) = \sum_{m_{r-1}} I_{Q'_{r-1}} \otimes \mathbf{Q}^{(r-1)}_{m_{r-1}|m_{r-2}} \,,\ \forall r \geq 1 \\ &\mathbf{Q}^{(0)} \geq 0 \,, \quad \mathrm{Tr}_{Q_0}(\mathbf{Q}^{(0)}) = I_L \\ &\mathbf{Q}^{(r)}_{m_r|m_{r-1}} \geq 0 \,, \quad \forall r \geq 1 \,. \end{aligned} \tag{37}$$

The optimization problem in (37) is an instance of conic programming [67, 68], where the cone characterized by $\mathbf{Q}$ is a separable cone. The aforementioned conic programming can be solved using see-saw algorithm, where every iteration of the see-saw is a semidefinite program (SDP) [67]. In the special case of static QECC, our conic program in (37) reduces to the bi-convex optimization structure from Ref. [64] and can be solved using two SDPs running one after another, until convergence within a fixed tolerance is attained.

IV. DISCUSSIONS

In this work, we propose a unified framework for quantum error-correcting codes (QECC) called the strategic code. It encompasses all existing QECCs and all physically plausible QECCs to be discovered, including codes involving operational adaptivity and also considering effects of spatially and temporally (non-Markovian) correlated error models. The strategic code introduces a device called an interrogator which represents all operations performed by the coder in between encoding and decoding stages. The interrogator is general, in that it may contain any set of operations performed both spatially or temporally (in sequence) with classical or quantum memory. Within this framework we show an algebraic (Theorem 1 and an information-theoretic (Theorem 2) necessary and sufficient error-correction conditions. These conditions apply to all known variants of dynamical QECC (and all physically-allowed generalizations) and include the error-correction conditions for static QECC [23, 25, 26] as a special case. The generality of the results partly owes to the quantum combs formalism, which gives a natural spatio-temporal representation for a QECC, as it has been for many sequential tasks in quantum information and computation. In this formalism, we also propose an optimization problem that gives an approximate QECC that recovers logical information up to desired level of fidelity for a given error model, which again may exhibit non-Markovian correlations.

As mentioned in the main text, although we focus on the scenario where the interrogator only maintains classical memory, the strategic code also accommodates an

interrogator with quantum memory (as discussed in detail in Appendix B 1). This leads to many questions including: How does the size (dimension) quantum quantum memory affects error-correction? What are the necessary and sufficient conditions for error correction given a fixed size quantum memory? Moreover, as this generalization includes the entanglement-assisted QECC (EAQECC) [39–41] as a special case, one could investigate into relationships between error-correction conditions for EAQECC (e.g. [69]) to analogous conditions for strategic code. Also, another generalization mentioned in the main text to allow encoding of logical information in a susbsystem of the codespace, analogous to subsystem codes (as discussed in detail in Appendix B 2). As subsystem codes has a different error-correction conditions [27, 29, 60] compared to traditional static codes [23, 25, 26], it is an interesting future work to show necessary and sufficient error-correction condition of subsystem strategic code. Another interesting future work is to use the concept of quantum combs virtualization [70, 71] to the strategic code. This is essentially a method of approximating some operator $\mathbf{\Phi}$ which involves randomly choosing from a set of "allowed" l-rounds strategic codes $\{\mathbf{I}^{(k)}\}_k$ followed by a post-processing. The sampling procedure and post-processing are constructed based on a linear expansion of some operator $\mathbf{\Phi}$ in terms of $\{\mathbf{I}^{(k)}\}_k$. Here operator $\mathbf{\Phi}$ have the same dimension as $\mathbf{I}^{(k)}$, but it may correspond to a non-physical process, such as those involving indefinite causal order or causally inseparable [47, 52, 72–78]. One could also explore how a strategic code equipped with such exotic causal structure performs. For more detailed discussion on strategic code virtualization and strategic code with more exotic causal structures, see Appendix B 3.

Further work could be done on an explicit construction of dynamical QECCs such as a Floquet code, that corrects a sequence of error maps by using the strategic code framework and conditions in Theorem 1 and Theorem 2. It would also be an interesting to explore further whether adaptive strategic code can provide any advantage over codes with fixed sequence of operations. Such advantage could take the form of larger code distance or capability of storing more logical information. A notion of approximate strategic code can also be explored further and optimized using our optimization method. Particularly, one could perhaps show an approximate error-correction condition for strategic code with respect to logical information recovery up to a certain fidelity, analogous to approximate static QECC conditions in [79]. It is also interesting to understand further the relationship between our conditions and the operator algebraic condition in [15, 20] which is formulated in terms of non-Abelian gauge group defined by the sequence of Clifford gates and Pauli measurements, as well as relationship between the strategic code and other QECC frameworks [19–22].

ACKNOWLEDGEMENTS

This work is supported by the NRF2021-QEP2-02-P06 from the Singapore Research Foundation, the Singapore Ministry of Education Tier 1 Grant RG77/22 (S), the FQXi R-710-000-146-720 Grant "Are quantum agents more energetically efficient at making predictions?" from the Foundational Questions Institute, Fetzer Franklin Fund (a donor-advised fund of Silicon Valley Community Foundation) and A*STAR C230917003. AT is supported by CQT PhD scholarship. The authors thank Tobias Haug, Varun Narsimhachar and Yunlong Xiao for interesting discussions.

[1] Matthew B Hastings and Jeongwan Haah. Dynamically generated logical qubits. *Quantum*, 5:564, 2021.
[2] Craig Gidney, Michael Newman, Austin Fowler, and Michael Broughton. A fault-tolerant honeycomb memory. *Quantum*, 5:605, 2021.
[3] Christophe Vuillot. Planar floquet codes. *arXiv preprint arXiv:2110.05348*, 2021.
[4] Jeongwan Haah and Matthew B Hastings. Boundaries for the honeycomb code. *Quantum*, 6:693, 2022.
[5] Craig Gidney, Michael Newman, and Matt McEwen. Benchmarking the planar honeycomb code. *Quantum*, 6:813, 2022.
[6] Margarita Davydova, Nathanan Tantivasadakarn, and Shankar Balasubramanian. Floquet codes without parent subsystem codes. *PRX Quantum*, 4(2):020341, 2023.
[7] James R Wootton. Measurements of floquet code plaquette stabilizers. *arXiv preprint arXiv:2210.13154*, 2022.
[8] Oscar Higgott and Nikolas P Breuckmann. Constructions and performance of hyperbolic and semi-hyperbolic floquet codes. *arXiv preprint arXiv:2308.03750*, 2023.
[9] Zhehao Zhang, David Aasen, and Sagar Vijay. X-cube floquet code: A dynamical quantum error correcting code with a subextensive number of logical qubits. *Physical Review B*, 108(20):205116, 2023.
[10] David Aasen, Jeongwan Haah, Zhi Li, and Roger S. K. Mong. Measurement quantum cellular automata and anomalies in floquet codes, 2023.
[11] Adam Paetznick, Christina Knapp, Nicolas Delfosse, Bela Bauer, Jeongwan Haah, Matthew B Hastings, and Marcus P da Silva. Performance of planar floquet codes with majorana-based qubits. *PRX Quantum*, 4(1):010310, 2023.
[12] Ali Fahimniya, Sheryl Mathew, Hossein Dehghani, Kishor Bharti, Alicia Kollar, Alexey Gorshkov, and Michael Gullans. Hyperbolic floquet quantum error correcting codes. In *APS March Meeting Abstracts*, volume 2023, pages N64–009, 2023.
[13] Arpit Dua, Nathanan Tantivasadakarn, Joseph Sullivan, and Tyler D Ellison. Engineering 3d floquet codes by rewinding. *P R X Quantum*, 5:020305, 2024.

[14] Dave Bacon, Steven T Flammia, Aram W Harrow, and Jonathan Shi. Sparse quantum codes from quantum circuits. *IEEE Transactions on Information Theory*, 63(4):2464–2479, 2017.

[15] Daniel Gottesman. Opportunities and challenges in fault-tolerant quantum computation. *arXiv preprint arXiv:2210.15844*, 2022.

[16] Nicolas Delfosse and Adam Paetznick. Spacetime codes of clifford circuits, 2023.

[17] Matt McEwen, Dave Bacon, and Craig Gidney. Relaxing hardware requirements for surface code circuits using time-dynamics. *Quantum*, 7:1172, 2023.

[18] Noah Berthusen and Daniel Gottesman. Partial syndrome measurement for hypergraph product codes. *arXiv preprint arXiv:2306.17122*, 2023.

[19] Margarita Davydova, Nathanan Tantivasadakarn, Shankar Balasubramanian, and David Aasen. Quantum computation from dynamic automorphism codes. *arXiv preprint arXiv:2307.10353*, 2023.

[20] Xiaozhen Fu and Daniel Gottesman. Error correction in dynamical codes. *arXiv preprint arXiv:2403.04163*, 2024.

[21] Hector Bombin, Daniel Litinski, Naomi Nickerson, Fernando Pastawski, and Sam Roberts. Unifying flavors of fault tolerance with the zx calculus. *arXiv preprint arXiv:2303.08829*, 2023.

[22] Markus S Kesselring, Julio C Magdalena de la Fuente, Felix Thomsen, Jens Eisert, Stephen D Bartlett, and Benjamin J Brown. Anyon condensation and the color code. *PRX Quantum*, 5(1):010342, 2024.

[23] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, 1997.

[24] Benjamin Schumacher and Michael A Nielsen. Quantum data processing and error correction. *Physical Review A*, 54(4):2629, 1996.

[25] Michael A Nielsen, Carlton M Caves, Benjamin Schumacher, and Howard Barnum. Information-theoretic approach to quantum error correction and reversible measurement. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):277–304, 1998.

[26] Nicolas J Cerf and Richard Cleve. Information-theoretic interpretation of quantum error-correcting codes. *Physical Review A*, 56(3):1721, 1997.

[27] Michael A Nielsen and David Poulin. Algebraic and information-theoretic conditions for operator quantum error correction. *Physical Review A*, 75(6):064304, 2007.

[28] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[29] David Kribs, Raymond Laflamme, and David Poulin. Unified and generalized approach to quantum error correction. *Physical review letters*, 94(18):180501, 2005.

[30] Gregory AL White, Charles D Hill, Felix A Pollock, Lloyd CL Hollenberg, and Kavan Modi. Demonstration of non-markovian process characterisation and control on a quantum processor. *Nature Communications*, 11(1):6301, 2020.

[31] Simon Milz and Kavan Modi. Quantum stochastic processes and quantum non-markovian phenomena. *PRX Quantum*, 2(3):030201, 2021.

[32] Ángel Rivas, Susana F Huelga, and Martin B Plenio. Quantum non-markovianity: characterization, quantification and detection. *Reports on Progress in Physics*, 77(9):094001, 2014.

[33] Li Li, Michael JW Hall, and Howard M Wiseman. Concepts of quantum non-markovianity: A hierarchy. *Physics Reports*, 759:1–51, 2018.

[34] Fattah Sakuldee, Simon Milz, Felix A Pollock, and Kavan Modi. Non-markovian quantum control as coherent stochastic trajectories. *Journal of Physics A: Mathematical and Theoretical*, 51(41):414014, 2018.

[35] Dorit Aharonov, Alexei Kitaev, and John Preskill. Fault-tolerant quantum computation with long-range correlated noise. *Physical review letters*, 96(5):050504, 2006.

[36] Naomi H Nickerson and Benjamin J Brown. Analysing correlated noise on the surface code using adaptive decoding algorithms. *Quantum*, 3:131, 2019.

[37] Hui Khoon Ng and John Preskill. Fault-tolerant quantum computation versus gaussian noise. *Physical Review A*, 79(3):032318, 2009.

[38] John Preskill. Sufficient condition on noise correlations for scalable quantum computing. *arXiv preprint arXiv:1207.6131*, 2012.

[39] Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement. *science*, 314(5798):436–439, 2006.

[40] Min-Hsiu Hsieh, Igor Devetak, and Todd Brun. General entanglement-assisted quantum error-correcting codes. *Physical Review A*, 76(6):062313, 2007.

[41] Todd A Brun, Igor Devetak, and Min-Hsiu Hsieh. Catalytic quantum error correction. *IEEE Transactions on Information Theory*, 60(6):3073–3089, 2014.

[42] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009.

[43] Giulio Chiribella, G Mauro D'Ariano, and Paolo Perinotti. Quantum circuit architecture. *Physical review letters*, 101(6):060401, 2008.

[44] Christina Giarmatzi and Fabio Costa. Witnessing quantum memory in non-markovian processes. *Quantum*, 5:440, 2021.

[45] Felix A Pollock, César Rodríguez-Rosario, Thomas Frauenheim, Mauro Paternostro, and Kavan Modi. Non-markovian quantum processes: Complete framework and efficient characterization. *Physical Review A*, 97(1):012127, 2018.

[46] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574, 2007.

[47] Ognyan Oreshkov, Fabio Costa, and Časlav Brukner. Quantum correlations with no causal order. *Nature communications*, 3(1):1092, 2012.

[48] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[49] Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

[50] Min Jiang, Shunlong Luo, and Shuangshuang Fu. Channel-state duality. *Physical Review A*, 87(2):022310, 2013.

[51] Ge Bai, Ya-Dong Wu, Yan Zhu, Masahito Hayashi, and Giulio Chiribella. Efficient algorithms for causal order discovery in quantum networks. *arXiv preprint arXiv:2012.01731*, 2020.

[52] Fabio Costa and Sally Shrapnel. Quantum causal modelling. *New Journal of Physics*, 18(6):063032, 2016.

[53] Giulio Chiribella. Optimal networks for quantum metrology: semidefinite programs and product rules. *New Journal of Physics*, 14(12):125008, 2012.

[54] Qiushi Liu, Zihao Hu, Haidong Yuan, and Yuxiang Yang. Optimal strategies of quantum metrology with a strict hierarchy. *Physical Review Letters*, 130(7):070803, 2023.

[55] IA Luchnikov, SV Vintskevich, H Ouerdane, and SN Filippov. Simulation complexity of open quantum dynamics: Connection with tensor networks. *Physical review letters*, 122(16):160401, 2019.

[56] Gus Gutoski, Ansis Rosmanis, and Jamie Sikora. Fidelity of quantum strategies with applications to cryptography. *Quantum*, 2:89, 2018.

[57] Hlér Kristjánsson, Giulio Chiribella, Sina Salek, Daniel Ebler, and Matthew Wilson. Resource theories of communication. *New Journal of Physics*, 22(7):073014, 2020.

[58] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[59] David W Kribs, Raymond Laflamme, David Poulin, and Maia Lesosky. Operator quantum error correction. *arXiv preprint quant-ph/0504189*, 2005.

[60] David Poulin. Stabilizer formalism for operator quantum error correction. *Physical review letters*, 95(23):230504, 2005.

[61] Debbie W Leung, Michael A Nielsen, Isaac L Chuang, and Yoshihisa Yamamoto. Approximate quantum error correction can lead to better codes. *Physical Review A*, 56(4):2567, 1997.

[62] Daniel A Lidar and Todd A Brun. *Quantum error correction*. Cambridge university press, 2013.

[63] Claude Crépeau, Daniel Gottesman, and Adam Smith. Approximate quantum error-correcting codes and secret sharing schemes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 285–301. Springer, 2005.

[64] Andrew S Fletcher, Peter W Shor, and Moe Z Win. Optimum quantum error recovery using semidefinite programming. *Physical Review A*, 75(1):012338, 2007.

[65] Hui Khoon Ng and Prabha Mandayam. Simple approach to approximate quantum error correction based on the transpose channel. *Physical Review A*, 81(6):062342, 2010.

[66] Carlo Cafaro and Peter van Loock. Approximate quantum error correction for generalized amplitude-damping errors. *Physical Review A*, 89(2):022316, 2014.

[67] Stephen P Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[68] Arkadi Nemirovski. Advances in convex optimization: conic programming. In *International Congress of Mathematicians*, volume 1, pages 413–444, 2006.

[69] Markus Grassl, Felix Huber, and Andreas Winter. Entropic proofs of singleton bounds for quantum error-correcting codes. *IEEE Transactions on Information Theory*, 68(6):3942–3950, 2022.

[70] Ryuji Takagi, Xiao Yuan, Bartosz Regula, and Mile Gu. Virtual quantum resource distillation: General framework and applications. *Physical Review A*, 109(2):022403, 2024.

[71] Xiao Yuan, Bartosz Regula, Ryuji Takagi, and Mile Gu. Virtual quantum resource distillation. *Physical Review Letters*, 132(5):050203, 2024.

[72] Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, and Benoit Valiron. Quantum computations without definite causal structure. *Physical Review A*, 88(2):022318, 2013.

[73] 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):7913, 2015.

[74] Simon Milz, Felix A Pollock, Thao P Le, Giulio Chiribella, and Kavan Modi. Entanglement, non-markovianity, and causal non-separability. *New Journal of Physics*, 20(3):033033, 2018.

[75] 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):e1602589, 2017.

[76] Kaumudibikash Goswami, Christina Giarmatzi, Michael Kewming, Fabio Costa, Cyril Branciard, Jacquiline Romero, and Andrew G White. Indefinite causal order in a quantum switch. *Physical review letters*, 121(9):090503, 2018.

[77] Nicolas Loizeau and Alexei Grinbaum. Channel capacity enhancement with indefinite causal order. *Physical Review A*, 101(1):012340, 2020.

[78] Daniel Ebler, Sina Salek, and Giulio Chiribella. Enhanced communication with the assistance of indefinite causal order. *Physical review letters*, 120(12):120502, 2018.

[79] Cédric Bény and Ognyan Oreshkov. General conditions for approximate quantum error correction and near-optimal recovery channels. *arXiv preprint arXiv:0907.5391*, 2009.

[80] Ognyan Oreshkov and Christina Giarmatzi. Causal and causally separable processes. *New Journal of Physics*, 18(9):093020, 2016.

Appendix A: Necessary and sufficient algebraic conditions for static QECC

Knill-Laflamme's necessary and sufficient condition for exact QECC [23] states that for a given basis $\{|i\rangle_Q\}_i$ of code space $\mathscr{S}_Q$ and any distinct pair of code space basis $|i\rangle_Q, |j\rangle_Q \in \mathscr{S}_Q$, it holds that

$$\begin{gathered}\langle i|_Q E_a^\dagger E_b |i\rangle_Q = \langle j|_Q E_a^\dagger E_b |j\rangle_Q = \lambda_{a,b} \\ \text{and} \\ \langle i|_Q E_a^\dagger E_b |j\rangle_Q = 0\,,\end{gathered} \tag{A1}$$

for some constant $\lambda_{a,b} \in \mathbb{C}$. Equivalently for a projector $\Pi_Q = \sum_i |i\rangle\langle i|_Q$ onto codespace $\mathscr{S}_Q$, it holds that

$$\Pi_Q E_a^\dagger E_b \Pi_Q = \lambda_{a,b} \Pi_Q \ . \tag{A2}$$

For subsystem QECC with code space $\mathscr{S}_Q = \mathscr{S}_C \otimes \mathscr{S}_G$, where $\mathscr{S}_C$ is the code subsystem and $\mathscr{S}_G$ is the gauge subsystem, Nielsen-Poulin's necessary and sufficient condition for exact QECC [27] is

$$\Pi_Q E_a^\dagger E_b \Pi_Q = I_C \otimes g_{a,b} \tag{A3}$$

where $g_{a,b}$ is an operator on $\mathscr{S}_G$ and Π_Q projection onto code space $\mathscr{S}_Q$ defined as $\Pi = VV^\dagger$ where $V : \mathscr{S}_L \to \mathscr{S}_Q$ is an isometry that encodes logical states into code states.

Appendix B: Quantum combs representation of strategic code

Since $\mathcal{E}^{(r)}$ is a CP map and $\sum_{m_r} \mathcal{C}^{(r)}_{m_r|m_{r-1}}$ is a CPTP map their Choi operators $\mathbf{E}^{(r)}$ and $\mathbf{C}^{(r)}_{m_r|m_{r-1}}$ are positive definite. Hence $\mathbf{E}^{(r)}$ and $\mathbf{C}^{(r)}_{m_r|m_{r-1}}$ admits decomposition

$$\begin{aligned} \mathbf{E}^{(r)} &= \sum_{e_r} |E_{e_r}\rangle\!\rangle\langle\!\langle E_{e_r}| \\ \mathbf{C}^{(r)}_{m_r|m_{r-1}} &= \sum_{o_r : f(o_r, m_{r-1}) = m_r} |C_{o_r|m_{r-1}}\rangle\!\rangle\langle\!\langle C_{o_r|m_{r-1}}| \end{aligned} \tag{B1}$$

where $|E_{e_r}\rangle\!\rangle = \sum_{i,j} \langle i|E_{e_r}|j\rangle |i\rangle|j\rangle$ and $|C_{o_r|m_{r-1}}\rangle\!\rangle = \sum_{i,j} \langle i|C_{o_r|m_{r-1}}|j\rangle |i\rangle|j\rangle$ are the (unnormalized) eigenvectors of $\mathbf{E}^{(r)}$ and $\sum_{m_r} \mathbf{C}^{(r)}_{m_r|m_{r-1}}$, which are the vectorized canonical Kraus operators of CP maps $\mathcal{E}^{(r)}$ and $\sum_{m_r} \mathcal{C}^{(r)}_{m_r|m_{r-1}}$, respectively. Hence we can express $\mathbf{E}_e$ (for $e = e_0, \ldots, e_l$) and $\mathbf{I}_{m_l}$ as

$$\begin{aligned} \mathbf{E}_e &= |E_e\rangle\!\rangle\langle\!\langle E_e| \\ \mathbf{I}_{m_l} &= \sum_{o \in O_{m_l}} |C_{m_l,o}\rangle\!\rangle\langle\!\langle C_{m_l,o}| \ . \end{aligned} \tag{B2}$$

Here, $o = o_1, \ldots, o_l$ is a sequence of check measurement outcomes and O_{m_l} is the set of all check measurement outcome sequence o resulting in final memory state m_l, i.e. $o \in O_{m_l}$ if and only if there exists $m_1, \ldots, m_{l-1}$ such that $o = o_1, \ldots, o_l$ satisfies $f_1(o_1) = m_1$, $f_2(o_2, m_1) = m_2$, $\ldots$, $f_l(o_l, m_{l-1}) = m_l$. The vectors $|E_e\rangle\!\rangle$ and $|C_{m_l,o}\rangle\!\rangle$ are defined by

$$\begin{aligned} |C_{m_l,o}\rangle\!\rangle &= |C^{(l)}_{o_l|m_{l-1}}\rangle\!\rangle \otimes \cdots \otimes |C^{(1)}_{o_1}\rangle\!\rangle \\ |E_e\rangle\!\rangle &= \sum_{i_{0:l-1}, j_{0:l-1}} \Big(\langle i_{l-1}|_{E_{l-1}} E_{e_{l-1}} |j_{l-1}, i_{l-2}\rangle_{Q_{l-1}E_{l-2}} \otimes \cdots \otimes \langle i_1|_{E_1} E_{e_1} |j_1, i_0\rangle_{Q_1 E_0} \otimes \langle i_0|_{E_0} E_{e_0} |j_0\rangle_{Q_0} \Big) \\ &\quad \otimes E_{e_l} |j_l, i_{l-1}\rangle_{Q_l E_{l-1}} \otimes |j_{0:l}\rangle_{Q_0 \ldots Q_l} \end{aligned} \tag{B3}$$

where $|j_{0:l}\rangle_{Q_0 \ldots Q_l} = \bigotimes_{r=0}^{l-1} |j_r\rangle_{Q_r}$ and for some orthonormal bases $\{|i_r\rangle\}_{i_r}$ and $\{|j_r\rangle\}_{j_r}$ of the noise environment $\mathscr{S}_{E_r}$ and codespace $\mathscr{S}_{Q_r}$, respectively. Note that $|C_{m_l,o}\rangle\!\rangle \in \mathscr{S}_{Q'_0} \otimes \mathscr{S}_{Q_1} \otimes \cdots \otimes \mathscr{S}_{Q_{l-1}} \otimes \mathscr{S}_{Q_l}$ and $|E_e\rangle\!\rangle \in \mathscr{S}_{Q_0} \otimes \mathscr{S}_{Q'_0} \otimes \cdots \otimes \mathscr{S}_{Q_l} \otimes \mathscr{S}_{Q'_l}$. Using these formulas, we can now express complete interaction between the sequence of check instruments $\mathbf{I}_{m_l}$ and error maps $\mathbf{E}_e$ as

$$\mathbf{E}_e * \mathbf{I}_{m_l} = \sum_{o \in O_{m_l}} |K_{e,m_l,o}\rangle\!\rangle\langle\!\langle K_{e,m_l,o}| \tag{B4}$$

where

$$\begin{aligned} |K_{e,m_l,o}\rangle\!\rangle &= E_{e_l}(C^{(l)}_{o_l|m_{l-1}} \otimes I_{E_{l-1}}) E_{e_{l-1}} \ldots E_{e_1}(C^{(1)}_{o_1} \otimes I_{E_0}) E_{e_0} |j_0\rangle_{Q_0} \otimes |j_0\rangle_{Q_0} \\ &= \sum_{i_{0:l}, j_{1:l}, k_{1:l}} \Big(\langle j_l|_{Q_l} C^{(l)}_{o_l|m_{l-1}} |k_l\rangle_{Q'_{l-1}} \langle k_l, i_{l-1}|_{Q'_{l-1}E_{l-1}} E_{e_{l-1}} |j_{l-1}, i_{l-2}\rangle_{Q_{l-1}E_{l-2}} \ldots \langle k_2, i_1|_{Q'_1 E_1} E_{e_1} |j_1, i_0\rangle_{Q_1 E_0} \langle j_1|_{Q_1} C^{(1)}_{o_1} |k_1\rangle_{Q'_0} \\ &\quad \langle k_1, i_0|_{Q'_0, E_0} E_{e_0} |j_0\rangle_{Q_0} \Big) E_{e_l} |j_l, i_{l-1}\rangle_{Q_l E_{l-1}} \otimes |j_0\rangle_{Q_0} \ , \end{aligned} \tag{B5}$$

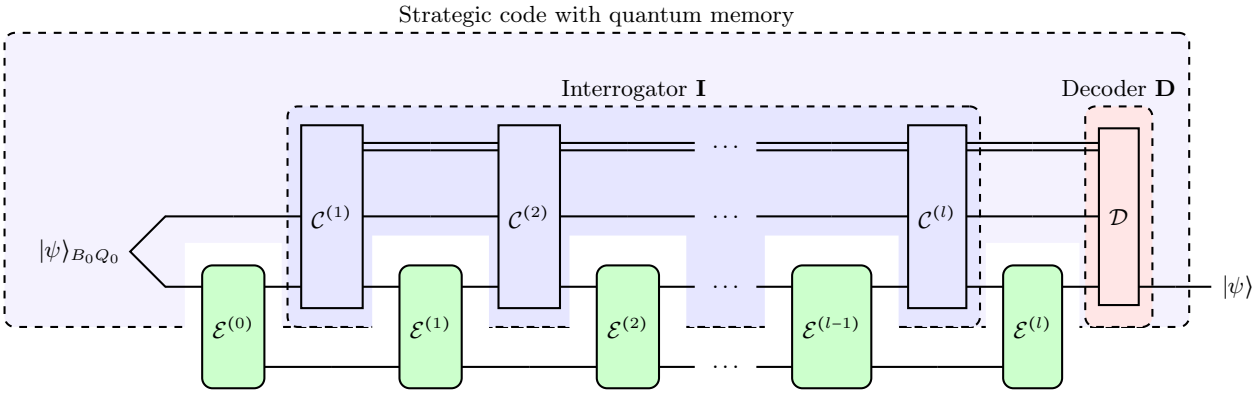


FIG. 4. Strategic code with quantum memory.

which is an vector in $\mathscr{S}_{Q'_l} \otimes \mathscr{S}_{Q_0}$.

We give a more explicit derivation of the operator representing the entire interaction between the errors and the check instruments and the decoding procedure. Consider operators $\mathbf{D}_{m_l} \in \mathscr{H}_D \otimes \mathscr{H}_{Q'_l}$ and $\mathbf{E}_e \in \bigotimes_{r=0}^{l} \mathscr{H}_{Q'_r} \otimes \mathscr{H}_{Q_r}$ and $\mathbf{C}^{(r)}_{m_r|m_{r-1}} \in \mathscr{H}_{Q_r} \otimes \mathscr{H}_{Q'_{r-1}}$. Let $Q = \{Q_0, Q'_0, \ldots, Q_l, Q'_l, D\}$ be the set of labels of the code spaces in the dynamical code and for $\tilde{Q} \subseteq Q$ denote $(\cdot)^{\mathsf{T}_{\tilde{Q}}}$ as partial transpose over spaces with labels in $\tilde{Q}$ and $\mathrm{Tr}_{\tilde{Q}}$ as partial trace over spaces with labels in $\tilde{Q}$ and $I_{\tilde{Q}} = \bigotimes_{Q' \in \tilde{Q}} I_{Q'}$. The entire dynamical encoding, error sequence, and decoding can be expressed as

$$
\begin{aligned}
&\sum_{m_{0:l}} \mathbf{D}_{m_l} * \mathbf{E}_{e_l} * \mathbf{C}^{(l)}_{m_l|m_{l-1}} * \cdots * \mathbf{E}_{e_1} * \mathbf{C}^{(1)}_{m_1} * \mathbf{E}_{e_0} \\
&= \sum_{m_{0:l}} \mathrm{Tr}_{Q\setminus DQ_0}\Big((\mathbf{D}_{m_l} \otimes I_{Q\setminus Q'_l}) \prod_{r=1}^{l} (\mathbf{E}_{e_r}^{\mathsf{T}_{Q'_r,Q_r}} \otimes I_{Q\setminus Q'_r,Q_r}) (\mathbf{C}^{(r)}_{m_r|m_{r-1}} \otimes I_{Q\setminus Q_r,Q'_{r-1}}) (\mathbf{E}_{e_0}^{\mathsf{T}_{Q'_0,Q_0}} \otimes I_{Q\setminus Q'_0,Q_0}) \Big) \\
&= \sum_{m_{0:l}} \mathrm{Tr}_{Q\setminus DQ_0}\Big((\mathbf{D}_{m_l} \otimes I_{Q\setminus Q'_l}) (\mathbf{E}_e^{\mathsf{T}} \otimes I_D) \big(\prod_{r=1}^{l} \mathbf{C}^{(r)}_{m_r|m_{r-1}} \otimes I_{Q\setminus Q_r,Q'_{r-1}} \big) \Big) \\
&= \mathrm{Tr}_{Q\setminus DQ_0}\Bigg((\mathbf{E}_e^{\mathsf{T}} \otimes I_D) \underbrace{\Big(\sum_{m_{0:l}} \mathbf{D}_{m_l} \bigotimes_{r=1}^{l} \mathbf{C}^{(r)}_{m_r|m_{r-1}} \Big)}_{\mathbf{Q} = \sum_{m_l} \mathbf{D}_{m_l} * \mathbf{I}_{m_l}} \Bigg) \\
&= \mathrm{Tr}_{Q\setminus DQ_0}\Big((\mathbf{E}_e^{\mathsf{T}} \otimes I_D)\, \mathbf{Q} \Big) \\
&= \mathbf{E}_e * \mathbf{Q}
\end{aligned}
\tag{B6}
$$

Note that $\mathbf{E}_e * \mathbf{Q} \in \mathscr{H}_D \otimes \mathscr{H}_{Q_0}$.

1. Strategic code with quantum memory

The strategic code in Definition 2 can be generalized further to the case where retention of some quantum information can be performed between rounds. In this case, the strategic code is equipped with a quantum memory represented by a sequence of quantum systems $\mathscr{S}_{B_0}, \mathscr{S}_{B_1}, \ldots, \mathscr{S}_{B_l}$ where system $\mathscr{S}_{B_r}$ is the quantum system being passed from check instrument in round r to the check instrument in round $r+1$ for $r \geq 1$. This is illustrated in Fig. 4. At round $r = 0$, without loss of generality we can think of the logical information being initially encoded in an entangled codestate $|\psi\rangle_{B_0Q_0}$ between the codespace $\mathscr{S}_{Q_0}$ and the quantum memory system $\mathscr{S}_{B_0}$ of the strategic code. The $\mathscr{S}_{B_0}$ part of the entangled codestate serves as an input to check instrument $\mathscr{C}^{(1)}$ in round 1. In this case the check instrument in round r has the form $\mathcal{C}^{(r)} : \mathscr{H}_{B_{r-1}} \otimes \mathscr{H}_{Q'_{r-1}} \to \mathscr{H}_{B_r} \otimes \mathscr{H}_{Q_r}$ since it receives the quantum system $\mathscr{S}_{B_{r-1}}$ from the preceding check instrument $\mathcal{C}^{(r-1)}$, whereas $\mathcal{C}^{(0)}$ receives the $\mathscr{S}_{B_0}$ part of the initial entangled codestate $|\psi\rangle_{B_0Q_0}$.

In the quantum combs representation of the interrogator $\mathbf{I}$, the eigenvectors of the interrogator operator $\mathbf{I}_{m_l}$ no longer has the tensor product structure as in the case when only classical memory is allowed in eqn. (B3). Namely in

general we have $|C_{m_l,o}\rangle\!\rangle \neq |C^{(l)}_{o_l|m_{l-1}}\rangle\!\rangle \otimes \cdots \otimes |C^{(1)}_{o_1}\rangle\!\rangle$. Here $|C_{m_l,o}\rangle\!\rangle$ instead takes the more general form of

$$\begin{aligned}|C_{m_l,o}\rangle\!\rangle = \sum_{k_{0:l-1},j_{0:l-1}} & C_{o_l,m_{l-1}}|k_{l-1},j_{l-1}\rangle_{B_{l-1}Q'_{l-1}} \otimes \cdots \otimes \langle k_2|_{B_2} C_{o_2|m_1}|k_1,j_1\rangle_{B_1Q'_1} \otimes \langle k_1|_{B_1} C_{o_1}|k_0,j_0\rangle_{B_0Q'_0} \\ & \otimes |k_0\rangle_{B_0} \otimes |j_{0:l-1}\rangle_{Q'_0\ldots Q'_l}\end{aligned} \tag{B7}$$

where $|j_{0:l-1}\rangle_{Q'_0\ldots Q'_l} = \bigotimes_{r=0}^{l-1} |j_r\rangle_{Q'_r}$ and for some orthonormal bases $\{|k_r\rangle\}_{k_r}$ and $\{|j_r\rangle\}_{j_r}$ of the quantum memory system $\mathscr{S}_{B_r}$ and codespace $\mathscr{S}_{Q'_r}$, respectively. Also as before $m_r = f_r(o_r, m_{r-1})$ for all $r > 1$ and $m_1 = f_1(o_1)$.

Note that when we set the number of rounds of the strategic code to $l = 0$, we recover the entanglement-assisted QECC (EAQECC) [39–41]. In this case we simply have the initial entangled codestate $|\psi\rangle_{B_0Q_0}$ followed by error map $\mathcal{E}^{(0)}$ then a decoder channel $\mathcal{D}$, which makes up an EAQECC.

It is an interesting future work to establish a necessary and sufficient error-correction conditions for a strategic code with quantum memory analogous to Theorem 1 and Theorem 2. In doing this one needs to restrict the dimension of the quantum memory of the interrogator, as otherwise one can always store the entire code in the quantum memory, bypassing the error maps. Also, one might also consider where the decoder also outputs a "residue" entangled state alongside the recovered initial codestate as in [69].

2. Subsystem strategic code

Another generalization of the strategic code in Definition 2 is to introduce additional system in the codespace in each round, i.e. $\mathscr{S}_{Q_r} = \mathscr{S}_{A_r} \otimes \mathscr{S}_{C_r}$ where logical information is stored in subsystem $\mathscr{S}_{A_r}$. This is analogous to subsystem QECC [27, 29, 59, 60] where the codespace is of the form $\mathscr{S}_Q = \mathscr{S}_A \otimes \mathscr{S}_C$. In this generalization, which we call a *subsystem strategic code*, we still retain the form of the interrogator operator $\mathbf{I}_{m_l} = \sum_{o\in O_{m_l}} |C_{m_l,o}\rangle\!\rangle\langle\!\langle C_{m_l,o}|$. Namely, $|C_{m_l,o}\rangle\!\rangle$ has the same expression as eqn. (B3), or as eqn. (B7) in the case where quantum memory is available Hence we can modify Definition 2 so that we say a subsystem strategic code $(\mathscr{S}_{Q_0}, \mathbf{I})$ corrects $\mathfrak{E}$ if

$$\mathcal{D}_{m_l}(\mathbf{E} * \mathbf{I}_{m_l} * (\rho \otimes \sigma)) = \rho \otimes \sigma_{m_l} \tag{B8}$$

for all density operators ρ in $\mathscr{H}_{A_0}$ and σ, σ_{m_l} operators in $\mathscr{H}_{C_0}$). Lastly, necessary and sufficient conditions in Theorem 1 generalized to the subsystem strategic codes should also reduce to the necessary and sufficient condition for subsystem codes [27] when we set the number of rounds $l = 0$,

$$\Pi_Q E^\dagger_{e'} E_e \Pi_Q = \Pi_A \otimes g_{e',e} \tag{B9}$$

where $g_{e',e}$ is an operator in $\mathscr{H}_C$. This generalized condition for subsystem strategic code, however, is left for future work.

3. Virtual strategic code and strategic codes with exotic causal structure

A recently proposed virtual quantum resource theory [70, 71] offers a framework of approximating a process Φ by performing sampling process from a set of allowed process $\mathscr{F}$ where $\Phi \notin \mathscr{F}$, followed by a post-processing, to achieve a certain task. As it is shown in [70] on how this framework can be applied to quantum combs, here we show how one can "virtualize" a strategic code, including those with more exotic causal structure such as an indefinite causal order or causal inseparability [47, 52, 72–78, 80].

First we can consider a set of l-rounds allowed strategic codes $\{\mathbf{I}^{(k)}\}_k$ (e.g. those that only maintains classical memory), where we include an encoding channel $\mathcal{G}^{(k)} : \mathscr{L}(\mathbb{C}^{d'}) \to \mathscr{H}^{(k)}_{Q_0}$ mapping linear operators on d' dimensional complex vector space to linear operators on an initial codespace $\mathscr{S}^{(k)}_{Q_0}$ in the strategic code $\mathbf{I}^{(k)}$. So a d' dimensional state $|\psi\rangle$ encoded with strategic code $\mathbf{I}^{(k)}$ with error $\mathbf{E}$ gives a state

$$\mathbf{E} * \mathbf{I}^{(k)}_{m_l} * |\psi\rangle\langle\psi| \tag{B10}$$

at the start of the decoding round for a final memory state m_l.

The sampling and post-processing processes are based on linear expansion of operator $\mathbf{\Phi} = \sum_k \beta_k \mathbf{I}^{(k)}$ where $\beta_k \in \mathbb{R}$ where $\mathbf{\Phi}$ represents some black-box process that allows input of initial state $|\psi\rangle\langle\psi|$ and interaction with error $\mathbf{E}$ as $\mathbf{I}^{(k)}$ do. Operator $\mathbf{\Phi}$ have the same dimension as $\mathbf{I}^{(k)}$, but it may not correspond to a quantum comb. Namely it

may correspond to a process involving indefinite causal order or causally inseparable, e.g. where the effect of errors between round r and $r' \neq r$ may not have a definite causal relation (as opposed to the strategic code where interaction between the investigator's operation and the error map at round $r = 1$ influences the interaction at round $r = 3$, but not the other way around). Here, operator $\mathbf{\Phi}$ is represented by a process matrix [47, 52, 80], which is more general object than a quantum comb.

To perform sampling, one constructs a probability distribution over k with probabilities $\gamma_k = \frac{|\beta_k|}{\tau}$ for $\tau = \sum_k |\beta_k|$ so that

$$\mathbf{\Phi} = \sum_k (\text{sign}(\beta_k)\tau)\gamma_k \mathbf{I}^{(k)} \ . \tag{B11}$$

Using this relation, one can sample from distribution $\{\gamma_k\}_k$ and upon obtaining outcome k, use strategy code $\mathbf{I}^{(k)}$ to encode some fixed state $|\psi\rangle$ and after applying noise $\mathbf{E}$ obtain the output state $\mathbf{E} * \mathbf{I}^{(k)}_{m_l} * |\psi\rangle\langle\psi|$ then apply "post-processing" by a multiplication by $(\text{sign}(\beta_k)\tau)$. As shown in [70, 71], by performing this sampling and post-processing multiple times we can obtain an approximation of

$$\text{Tr}\Big((\mathbf{E} * \mathbf{\Phi} * |\psi\rangle\langle\psi|)A\Big) \tag{B12}$$

for some bounded linear operator A. Lastly, we note that decoder may be included in $\mathbf{I}^{(k)}$ as well to have the entire QECC process where the output $\mathbf{E} * \mathbf{I}^{(k)}_{m_l} * |\psi\rangle\langle\psi|$ is the output of a decoder. It would be interesting to investigate into the performance of strategic code virtualization and how strategic codes with exotic causal structures can or cannot improve code performance. However, this is left for future work.

Appendix C: Spacetime Code in the Quantum Combs Formalism

Now we describe the spacetime code [14–16] in our dynamical QECC quantum combs framework. The spacetime code is first proposed by Bacon,et.al. for a circuit consisting of a subset of Clifford gates in [14], then a generalization to circuits consisting of any Clifford gates is done by Gottesman in [15]. In these two spacetime codes, Pauli measurements for syndrome extraction is performed after the last layer of Clifford gates is applied. This is later generalized by Delfosse,et.al. in [16] where Pauli measurements can be performed anywhere in the circuit. Here we consider the most general spacetime code defined in [16] in demonstrating how spacetime code fits in our framework.

A spacetime code is defined by a circuit that takes n qubits as input, followed by l layers of Clifford operations, where each layer consists of Clifford gates and Pauli measurements on disjoint qubits. In Gottesman's and Bacon,et.al.'s spacetime code [15] where measurements are restricted to the end of the circuit, the circuit takes q qubit input along with preparation of a ancilla qubits at the beginning of the circuit and q' output qubits with $\{|0\rangle, |1\rangle\}$ basis measurements on b qubits at the end of the circuit. In this circuit q, a, q', b must satisfy $n = q + a = q' + b$, where n is the width of the circuit and thus each layer consists only of Clifford gates.

We note that our dynamical QECC framework can also describe a *sequence* of such circuits $\mathbf{C}^{(1)}, \mathbf{C}^{(2)}, \ldots, \mathbf{C}^{(l)}$ where error syndromes from one circuit determines the structure of the subsequent circuit, hence induces adaptivity. This temporal dependence across circuits has been mentioned in [15] although was not explored further. The quantum combs formalism for dynamical QECC applied to spacetime code presented here allows such exploration with the natural temporal-dependence representation.

1. Dynamical QECC quantum combs representation of spacetime code

Now we describe the quantum combs dynamical QECC of a spacetime code with respect to a circuit with l layers (see Fig. 5). In our dynamical QECC framework, this spacetime code has l rounds. At round $r = 0$, error E_{e_0} is inflicted at the n qubit input. At round $r \geq 1$, Clifford operation C_r is applied to the n qubits, followed by error E_{e_r}. The Clifford operation consisting of Clifford gates and Pauli measurements performed on disjoint set of qubits is described by $C_r = \{C_{r,o_r}\}_{o_r \in O_r}$ where C_{r,o_r} is a bounded linear operator from $\mathbb{C}^{2^n}$ to $\mathbb{C}^{2^n}$ and $o_r \in O_r$ is a measurement outcome from the Pauli measurements with O_r being the set of all possible measurement outcomes. If there are k Pauli measurements in C_r then the outcome is in the form of a k-tuple $o_r = (o_{r_1}, \ldots, o_{r_k})$. If no Pauli measurement is performed at round r, then we set a constant outcome for this round, i.e. $O_r = \{o_r\}$ is a singleton set and C_{r,o_r} is a Clifford unitary. Clifford operation C_r at each round then defines a quantum instrument $\mathcal{C}_r = \{\mathcal{C}_{r,o_r}\}_{o_r}$ where $\mathcal{C}_{r,o_r}(\rho) = C_{r,o_r}\rho C^\dagger_{r,o_r}$ is a CP map such that $\sum_{o_r} \mathcal{C}_{r,o_r}$ is a CPTP map. When measurement outcome $o = o_1, \ldots, o_l$ is

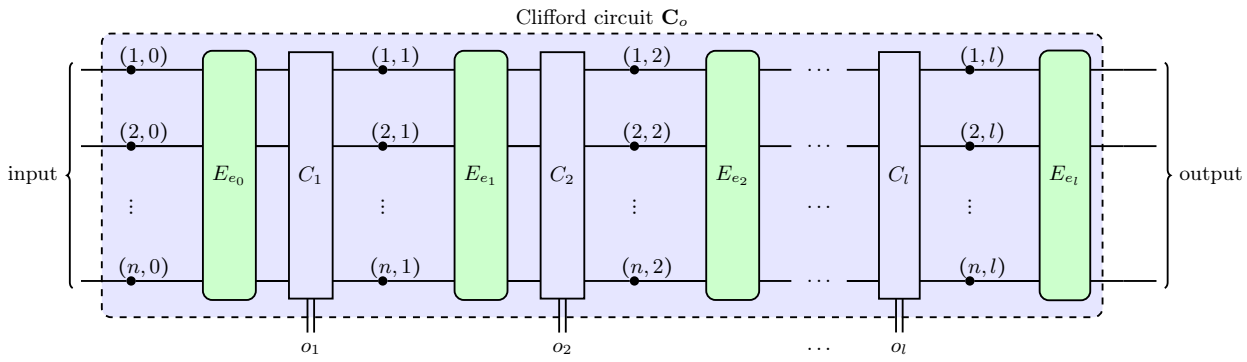


FIG. 5. Spacetime code Clifford circuit. Circuit $\mathbf{C}_o$ takes n qubits as input at the start of the circuit and outputs n qubits along with measurement outcomes $o = o_1, \ldots, o_l$ peformed throughout the circuit. Between the input and the output, the circuit contains l layers of Clifford operations $C_1, \ldots, C_l$, each layer C_r consist of Clifford gates and Pauli measurements with acting on disjoint subsets of the n qubits. Outcomes from Pauli measurements at layer r is denoted by o_r. Error operations are modelled to occur after the input (E_{e_0}) and after each layer ($E_{e_1}, \ldots, E_{e_l}$). Error E_{e_0} represents the noise on input qubits and error E_{e_r} for $r \geq 1$ represent noise from the Clifford gates and Pauli measurements in layer C_r. A spacetime code for circuit $\mathbf{C}$ is defined by $n(l+1)$-qubit stabilizer group, which in turn is defined by the circuit components. Each qubit (illustrated as black dots) is labeled by (i, r): for $r \geq 1$ it correspond to the i-th qubit output of C_r and for $r = 0$ it correspond to the i-th qubit of the input. Error E_{e_r} in round r is applied to qubits $\{(i, r)\}_i$.

obtained, the quantum combs representation of the circuit is

$$\mathbf{C}_o = |C_o\rangle\!\rangle\langle\!\langle C_o| = \bigotimes_{r=1}^{l} |C_{r,o_r}\rangle\!\rangle\langle\!\langle C_{r,o_r}| \tag{C1}$$

where $|C_{r,o_r}\rangle\!\rangle$ is the vectorized form of operator C_{r,o_r}.

Errors occurring throughout the circuit is described by a sequence of bounded linear operators $E_{e_0}, \ldots, E_{e_l}$ mapping vectors in $\mathbb{C}^{2^n}$ to $\mathbb{C}^{2^n}$. An error operator E_{e_r} takes the form of a tensor product of Paulis on qubits labeled by $\{(i, r)\}_{i\in[n]}$. Explicitly this can be expressed as $E_{e_r} = E_{1,e_r} \otimes \cdots \otimes E_{n,e_r}$ where $E_{i,e_r} \in \{I, X, Y, Z\}$ is a qubit Pauli operator where identity $E_{i,e_r} = I$ indicates no error is inflicted on qubit i at round r. In the quantum combs representation, we can express the error sequence $e = e_0, \ldots, e_l$ as a positive semidefinite operator $|E_e\rangle\!\rangle\langle\!\langle E_e| = \bigotimes_{r=0}^{l} |E_{e_r}\rangle\!\rangle\langle\!\langle E_{e_r}|$ where $|E_{e_r}\rangle\!\rangle = \bigotimes_{i=1}^{n} |E_{i,e_r}\rangle\!\rangle$ and $|E_{i,e_r}\rangle\!\rangle = \sum_{j',j} \langle j'|E_{i,e_r}|j\rangle |j'\rangle_{r,i}|j\rangle_{r,i}$. Hence the combs representation of the an error sequence can be expressed conveniently as a tensor product of Choi operator of error operators for each coordinate (i, r) in the spacetime grid

$$|E_e\rangle\!\rangle\langle\!\langle E_e| = \bigotimes_{r=0}^{l} \bigotimes_{i=1}^{n} |E_{i,e_r}\rangle\!\rangle\langle\!\langle E_{i.e_r}| \,, \tag{C2}$$

which closely resembles how errors are represented in spacetime code as a tensor product of the error operators $F_e = \bigotimes_{r=0}^{l} \bigotimes_{i=1}^{n} E_{i,e_r}$. Using both the quantum combs representation of the circuit (eqn.(C1)) and the error sequence, the interaction between then can be expressed using the link product as

$$|E_e\rangle\!\rangle\langle\!\langle E_e| * \mathbf{C}_o \tag{C3}$$

which is a positive semidefinite operator from $\mathbb{C}^{2^{2n}}$ to $\mathbb{C}^{2^{2n}}$ corresponding to a CP map from the n-qubit input to the n-qubit output.

Spacetime code is then defined by $n(l+1)$ qubit stabilizer group $\mathscr{S}_{\text{st}}$ where the qubits are placed in a grid and labeled by a tuple (i, r) where $i \in \{1, \ldots, n\}$ corresponds to a qubit register and $r \in \{0, \ldots, l\}$ corresponds to a layer in the circuit. So, qubits labeled by $\{(i, 0)\}_i$ are input qubits which error E_{e_0} are inflicted upon. Whereas for $r \geq 1$, qubits $\{(i, r)\}_i$ are the qubits placed at the output of Clifford operation C_r which error E_{e_r} occurs. If there are s Pauli measurements across the circuit with observables $S_1, \ldots, S_s$, then we can write the collection of the outcomes as a bit string $o = o_1, \ldots, o_s$ which is then being put through a function $f(o) = m$ which maps measurement outcomes to error syndromes. Error syndrome m is then used to choose which of the decoding channel $\{\mathcal{D}_m\}_m$ should be used at the circuit output.

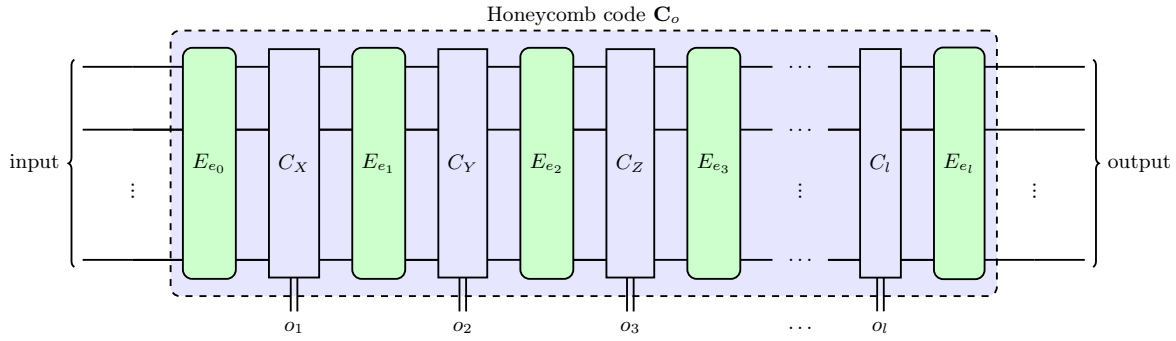


FIG. 6. Hastings-Haah honeycomb code interrogator.

In Delfosse,et.al.'s spacetime code [16] decoding is done in three steps. The first step is by using check bitstrings $\{u_1,\dots,u_q\}\subseteq\{0,1\}^s$ to define the function f mapping the measurement outcome bitstring o to syndrome bitstring $m=m_1\dots m_q\in\{0,1\}^q$. This is done by taking the inner product between u_j and o as the j-th bit of $f(o)=m$, i.e. $m_j=\langle u_j,o\rangle=u_{j,1}o_1+\cdots+u_{j,s}o_s$, which is to be understood as the j-th syndrome of measurement outcome o. The second step is to identify the circuit error $F_e=\bigotimes_{r=0}^{l}\bigotimes_{i=1}^{n}E_{i,e_r}$ (or $|E_e\rangle\!\rangle\langle\!\langle E_e|$ in the quantum combs form) using syndrome m. In [16], this is done by using a "most likely effect" (MLE) decoder on the nl-qubit spacetime stabilizer code. This stabilizer code is defined by circuit $\{\mathbf{C}_o\}_o$ and check bitstrings $\{u_1,\dots,u_q\}$ (or equivalently, function f). Given syndrome m, the MLE decoder outputs an nl-qubit Pauli $g(m)$ which is its guess of the true circuit error F_e. Now the third step is to propagate $g(m)$, denoted by $\overrightarrow{g(m)}$, and take its n-qubit Pauli corresponding to the last layer l of the circuit, denoted by $[\overrightarrow{g(m)}]_l$. Propagation of (a subset of) an $n(l+1)$-qubit Pauli P placed on the grid of the circuit is introduced as the spackle operation in [14]. Then we compute commutation relation between $\overrightarrow{g(m)}$ and observables $S_1,\dots,S_s$ corresponding to each measurement, to obtain bitstring $\gamma=\gamma_1,\dots,\gamma_s$ where $\gamma_j=[S_j,\overrightarrow{g(m)}]$. Then we can unflip measurement outcome string o by $o+\gamma$. Using $[\overrightarrow{g(m)}]_l$ and γ we can correct the output state from the circuit.

2. Spacetime code generalization in the strategic code framework

In the strategic code framework a generalization of the spacetime code can be constructed using adaptivity on the Clifford operations. Following the notation of the strategic code, we can denote the set of allowed Clifford operations in round r as $\{\mathcal{C}^{(r)}_{m_{r-1}}\}_{m_{r-1}}$, where $\mathcal{C}^{(r)}_{m_{r-1}}$ is a CP map defined by its action $\mathcal{C}^{(r)}_{m_{r-1}}(\rho)=\sum_{o_r}C^{(r)}_{o_r|m_{r-1}}\rho C^{(r)\dagger}_{o_r|m_{r-1}}$. As before, $C^{(r)}_{o_r|m_{r-1}}$ consists of Clifford gates and Pauli measurements on disjoint set of qubits. For simplicity, we assume that m_r has a one-to-one correspondence with the sequence of measurement outcomes $o_1,\dots,o_r$ hence we can still describe the circuit as $\mathbf{C}=\{\mathbf{C}_o\}_o$ as a sequence of outcomes $o=o_1,\dots,o_l$ is maintained in the classical memory of the code until the decoding round. For example, when a Pauli measurement S_1 in round 1 gives an outcome $o_1=+1$, we apply Clifford operation $\mathcal{C}^{(2)}_{+1}(\cdot)=\sum_{o_2}C^{(2)}_{o_2|+1}\cdot C^{(2)\dagger}_{o_2|+1}$ in round 2, otherwise we apply Clifford operation $\mathcal{C}^{(2)}_{-1}(\cdot)=\sum_{o_2}C^{(2)}_{o_2|-1}\cdot C^{(2)\dagger}_{o_2|-1}$ where Clifford gates and Pauli measurements in $C^{(2)}_{o_2|+1}$ and $C^{(2)}_{o_2|-1}$ may differ.

In this case we have a family of spacetime codes, one for each trajectory defined by a sequence of measurement outcomes o. Using the same method in obtaining the stabilizer group of the spacetime code (i.e. from the backpropagated measurement observables), we obtain a stabilizer group for each outcome sequence o. A simple case where this may happen can be seen using the example mentioned at the end of the previous paragraph. Suppose $C^{(2)}_{+1|+1}=U_2\otimes|0\rangle\langle 0|$ and $C^{(2)}_{+1|-1}=U_2\otimes|+\rangle\langle +|$, then their corresponding measurement observables are Z and X.

Appendix D: Hastings-Haah honeycomb Floquet code as a strategic code

Here we look into how the strategic code framework can be used in determining correctable error in the Hastings-Haah honeycomb Floquet code. For simplicity, we consider a single hexagon in the honeycomb code with corresponding

stabilizer $ZZZZZZ$. Measurement observables in round 1 and 2 are

$$\begin{aligned} &XXIIII, IIXXII, IIIIXX \\ &IYYIII, IIIYYI, YIIIIY\,, \end{aligned} \tag{D1}$$

respectively, and the outcomes are $o_1, o_2 \in \{+1,-1\}^3$, where $\{+1,-1\}$ are the corresponding eigenvalues of the two eigenstates for each observable. Hence the check instruments $\mathcal{C}_X^{(1)}$ and $\mathcal{C}_Y^{(2)}$ at these two rounds have Kraus operators

$$\begin{aligned} C^{(1)}_{+1,+1,+1|X} &= \left(|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|\right)_{1,2} \otimes \left(|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|\right)_{3,4} \otimes \left(|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|\right)_{5,6} \\ &\vdots \\ C^{(1)}_{-1,-1,-1|X} &= \left(|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|\right)_{1,2} \otimes \left(|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|\right)_{3,4} \otimes \left(|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|\right)_{5,6} \\ C^{(2)}_{+1,+1,+1|Y} &= \left(|{+}i,{+}i\rangle\langle{+}i,{+}i| + |{-}i,{-}i\rangle\langle{-}i,{-}i|\right)_{2,3} \otimes \left(|{+}i,{+}i\rangle\langle{+}i,{+}i| + |{-}i,{-}i\rangle\langle{-}i,{-}i|\right)_{4,5} \otimes \left(|{+}i,{+}i\rangle\langle{+}i,{+}i| + |{-}i,{-}i\rangle\langle{-}i,{-}i|\right)_{6,1} \\ &\vdots \\ C^{(2)}_{-1,-1,-1|Y} &= \left(|{+}i,{-}i\rangle\langle{+}i,{-}i| + |{-}i,{+}i\rangle\langle{-}i,{+}i|\right)_{2,3} \otimes \left(|{+}i,{-}i\rangle\langle{+}i,{-}i| + |{-}i,{+}i\rangle\langle{-}i,{+}i|\right)_{4,5} \otimes \left(|{+}i,{-}i\rangle\langle{+}i,{-}i| + |{-}i,{+}i\rangle\langle{-}i,{+}i|\right)_{6,1} \end{aligned} \tag{D2}$$

where subscripts indicates which qubits the projector is acting on and $|\pm\pm\rangle = |\pm\rangle \otimes |\pm\rangle$ and $|\pm i, \pm i\rangle = |\pm i\rangle \otimes |\pm i\rangle$ and $|\pm\rangle, |\pm i\rangle$ are ± 1 eigenstates of Pauli X and Y, respectively.

Consider two errors $E_{e_0} = ZIIIII$ and $E_{e_0'} = IZIIII$ at round 0 (recall that round r error occurs after round r operation and before round $r+1$ operation), and no further errors occur in round 1 and 2 i.e. $E_{e_1} = E_{e_2} = IIIIII$. Both of these errors are correctable by the honeycomb code as both errors $E_{e_0} = ZIIIII$ and $E_{e_0'} = IZIIII$ flips the outcome of both round 1 and round 2 measurements, allowing the decoder to detect the error. In the strategic code framework, we have a pair of error sequences $e = e_0, e_1, e_2$ and $e' = e_0', e_1, e_2$ with corresponding vectorized error operators

$$\begin{aligned} |E_e\rangle\!\rangle &= |ZIIIII\rangle\!\rangle \otimes |IIIIII\rangle\!\rangle \otimes |IIIIII\rangle\!\rangle \\ |E_e'\rangle\!\rangle &= |IZIIII\rangle\!\rangle \otimes |IIIIII\rangle\!\rangle \otimes |IIIIII\rangle\!\rangle\,. \end{aligned} \tag{D3}$$

Consider orthogonal states $|j\rangle, |k\rangle$ in the initial codespace $\mathscr{S}_{Q_0}$. Then since all check outcomes are stored in the memory of the honeycomb code interrogator, by Corollary 1 it holds that

$$\langle\!\langle E_{e'}|(|C_o\rangle\!\rangle\langle\!\langle C_o| \otimes |k\rangle\langle j|)|E_e\rangle\!\rangle = \delta_{k,j}\lambda_{e,e',o} \tag{D4}$$

for some constant $\lambda_{e,e',o}$. Since the Z pauli flips the $|\pm\rangle$ to $|\mp\rangle$ and $|\pm i\rangle$ to $|\mp i\rangle$, we obtain outcomes $o_1 = (-1,+1,+1)$ and $o_2 = (+1,+1,-1)$ for E_e and $o_1 = (-1,+1,+1)$ and $o_2 = (-1,+1,+1)$ for $E_{e'}$ (since without error both initial codestate $|j\rangle$ and $|k\rangle$ gives all + outcomes for both o_1 and o_2)

We can verify that this condition holds for error sequences e, e' as

$$\langle\!\langle E_{e'}|(|C_o\rangle\!\rangle\langle\!\langle C_o| \otimes |k\rangle\langle j|)|E_e\rangle\!\rangle = \langle k|E_{e_0'}C_{o_1}^{(1)\dagger}C_{o_2}^{(2)\dagger}C_{o_2}^{(2)}C_{o_1}^{(1)}E_{e_0}|j\rangle = 0 \tag{D5}$$

for all $o = o_1, o_2$. One can see this by noting that $C_{o_2}^{(2)\dagger}C_{o_2}^{(2)}C_{o_1}^{(1)}E_{e_0}|j\rangle = 0$ for all $o_1 \neq (-1,+1,+1)$ and $o_2 \neq (+1,+1,-1)$ while $\langle k|E_{e_0'}C_{o_1}^{(1)\dagger}C_{o_2}^{(2)\dagger} = 0$ for all $o_1 \neq (-1,+1,+1)$ and $o_2 \neq (-1,+1,+1)$. Namely, the sequence of check measurement outcomes maps $E_{e_0}|j\rangle$ and $E_{e_0'}|k\rangle$ to different subspaces (even with $j = k$), which allows one to construct a decoder detecting and distinguishing these errors.

Extended abstract: The i.i.d. State Convertibility in the Resource Theory of Asymmetry for Finite and Lie Groups

Tomohiro Shitara * †[1] Hiroyasu Tajima* ‡[2 3]

[1] *NTT Computer and Data Science Laboratories, NTT Corporation, 3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan*
[2] *Department of Communication Engineering and Informatics, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan*
[3] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

Abstract. Recently the connection between symmetry and physics has been actively studied in the framework called the resource theory of asymmetry (RTA). In RTA, the resource measures characterizing the asymptotic conversion rate between i.i.d. states are not known except for $U(1)$ and $\mathbb{Z}_2$ symmetry. In this work, we address the optimal conversion rate for both finite group symmetry and continuous group symmetry. For finite symmetries, we (1) derive the formula for the exact conversion rate, and (2) show that the approximate conversion rate diverges. For continuous symmetry, we give the upper limit of the approximate conversion rate in terms of the ratio of the Fisher information matrices, and conjecture that this limit is achievable.

Keywords: resource theory of asymmetry, i.i.d. conversion rate, quantum Fisher information

1 Introduction

Symmetry is one of the most powerful guiding principle in modern physics [1, 2], imposing a significant constraint on possible physical theories or possible quantum phases of matter. It can also constrains the set of possible operations one can perform, the situation of which is studied from the viewpoint of quantum information theory.

Resource theories provide a powerful framework to analyse such situations. It defines quantum "resources" in a variety of situations under some constraints on possible operations, and examines, in a general framework, what can be done when a resource is used, compared to when it is not. There are several types of resource theory depending on which property of system is considered resource [3], such as entanglement theory [4, 5, 6] and quantum thermodynamics [7, 8, 9], which treat entanglement and athermality as resources, respectively. In particular, the resource theory of asymmetry (RTA) deals with the "degree of symmetry breaking" (e.g., the noncommutativity between the conserved charge corresponding to the symmetry and the state) of a state as a resource, allowing the restrictions imposed by the symmetry to be treated in a unified framework [10, 11, 12, 13, 14, 15, 16, 17, 18, 19]. Because of its properties, RTA has found application in a great number of symmetry-related subjects such as speed limits [20], implementation of quantum computation gates [21, 23, 32, 33], clocks [22], coherence broadcasting [24, 25], measurement theory [26, 27, 28, 29, 30, 31, 32], quantum error correction [32, 33, 34, 35, 36], coherence cost of thermodynamic process [32], and black hole physics [32, 33].

Despite its importance and potential, RTA still has many open problems in its foundations. One of the most important problem is to identify a resource measure or a set of resource measures that characterizes the convertibility between the independent and identically distributed (i.i.d.) states. The convertibility between i.i.d. states is the most important problem in resource theory. For example, the entanglement entropy [4] in the case of entanglement and the Helmholtz free energy [7] in the case of quantum thermodynamics (for isothermal processes) determine the optimal conversion rates between the i.i.d. states. In RTA, on the other hand, this problem has been solved only for $U(1)$ symmetry [10, 15, 16] and $\mathbb{Z}_2$ symmetry [10], the simplest of the continuous and discrete symmetries, respectively. This fact means that the most fundamental quantities in RTA have not been known yet, preventing the further analysis of symmetries.

In this work, we solve this problem for symmetry described by a finite group, and partially for continious groups. For finite symmetries, we determine the optimal conversion rate between two i.i.d. states under covariant operations, or the free operation in RTA, in

*Both authors contributed equally to this work.
†tomohiro.shitara@ntt.com
‡hiroyasu.tajima@uec.ac.jp

two cases: when the transformation is error-free and when it allows negligibly small errors. Surprisingly, the results in these two cases are totally different from each other. We show that the optimal conversion rate in the error-free case is characterized by a set of resource measures, while in the case of allowing negligibly small errors, any state can be produced from any resource state with arbitrarily high rate. For continuous symmetries, we rigorously derive the upper limit of the approximate conversion rate in terms of the ratio of the quantum Fisher information matrices (QFIMs). We also argue that the obtained limit is expected to be achievable from two viewpoints, namely, argument based on the central limit theorem, and two examples ($U(1)$ and $SU(2)$ in part) where the QFIM-based upper limit is achievable. Together with the fact that the QFIM is a resource monotone in any compact and connected Lie group [19], we argue that the QFIM is the most fundamental quantity in RTA, playing a similar role of entanglement entropy in entangelment theory.

Technical details of our work are given in Ref. [37].

2 Settings

We adopt the standard formulation of RTA [10, 11, 28], where we consider systems with a symmetry described by a group G. The action of symmetry transformation with respect to an element $g \in G$ is represented by a unitary operator $U(g)$. Since the successive operation of two symmetry transformations is also a symmetry transformation, we have $U(g)U(g') = e^{i\omega(g,g')}U(gg')$, or equivalently

$$\mathcal{U}_g \circ \mathcal{U}_{g'}(...) = \mathcal{U}_{gg'}(...), \tag{1}$$

where $\mathcal{U}_g(...) = U_g ... U_g^\dagger$ is the conjugate operation of U_g. Namely, $U(g)$ is a projective unitary representation of G. We hereafter use the abbreviation $\mathcal{U}_G = \{\mathcal{U}_g\}_{g\in G}$.

Similarly to other resource theories, RTA has free states and free operations. Free states in RTA are called *symmetric states*, defined as states satisfying

$$\mathcal{U}_g(\rho) = \rho, \ \ \forall g \in G. \tag{2}$$

Free operations in RTA are called *covariant operations*. When a CPTP-map Λ from a quantum system S to S' and projective unitary representations $\mathcal{U}_G$ and $\mathcal{U}'_G$ on S and S' satisfy the following equation, Λ is called a covariant operation with respect to $\mathcal{U}_G$ and $\mathcal{U}'_G$:

$$\mathcal{U}'_g \circ \Lambda(...) = \Lambda \circ \mathcal{U}_g(...), \ \ \forall g \in G. \tag{3}$$

Under the settings described above, we define two types of i.i.d. state conversion rate. The first one is the *approximate* asymptotic state conversion rate:

$$R_{\rm ap}(\psi \to \phi) := \sup\{r | \exists \{\epsilon_N\}, \text{ s.t. } \lim_{N\to\infty} \epsilon_N = 0, \\ |\psi\rangle^{\otimes N} \overset{\mathcal{U}_G-cov}{\to}_{\epsilon_N} |\phi\rangle^{\otimes rN}\}, \tag{4}$$

where $|\psi\rangle^{\otimes N} \overset{\mathcal{U}_G-cov}{\to}_{\epsilon_N} |\phi\rangle^{\otimes rN}$ means that there exists a covariant operation Λ such that $\|\Lambda(\psi^{\otimes N}) - \phi^{\otimes rN}\|_1 \le \epsilon_N$. Most resource theories, including $U(1)$-symmetry RTA, deal only with the optimal rate of approximate asymptotic conversion. However, as we will see later, the optimal rate of the approximate asymptotic transformations diverges in RTA for finite groups. Therefore, following the previous studies on $\mathbb{Z}_2$-symmetry RTA [10], we introduce the second notion of the conversion rate in *exact* asymptotic transformation:

$$R_{\rm ex}(\psi \to \phi) := \sup\{r | \exists N_0, \forall N > N_0, \\ |\psi\rangle^{\otimes N} \overset{\mathcal{U}_G-cov}{\to}_{0} |\phi\rangle^{\otimes rN}\}. \tag{5}$$

3 Key quantities

In this section, we introduce two quantities that characterize the i.i.d. state convertibility in RTA. The first quantity is the logarithm of the characteristic function defined as

$$L(\psi, g) := -\log |\chi_\psi(g)|, \tag{6}$$

where $\chi_\psi(g) := \langle\psi|U(g)|\psi\rangle$ is the characteristic function. Since $|\chi_\psi(g)|$ monotonically increases under covariant operations [28], $L(\psi, g)$ is a resource monotone measure, which is not necessarily faithful. We will see the set of $L(\psi, g)$ characterizes the exact i.i.d. state conversion rate for finite symmetries.

The second quantity is the QFIM, or more precisely, the symmetric logarithmic derivative Fisher information matrix. For a state ρ with the spectral decomposition $\rho = \sum_k p_k \psi_k$ and a set of Hermitian operators $\vec{X} := (X_1, .., X_m)$, the (i, j)-component of the QFIM $\hat{F}_\rho(\vec{X})$ is given by

$$(F_\rho(\vec{X}))_{i,j} = \sum_{k,l} \frac{2(p_l - p_l)^2}{p_k + p_l} \langle\psi_k| X_i |\psi_l\rangle \langle\psi_l| X_j |\psi_k\rangle . \tag{7}$$

We note that when G is a connected Lie group, there exists a set of Hermitian operators $\vec{X}_{\mathcal{U}_G}$ whose $\hat{F}_\rho(\vec{X}_{\mathcal{U}_G})$ is a resource measure in RTA [19].

4 RTA for finite groups

First, we show that when the symmetry G is finite, there is *no* optimal rate for the approximate i.i.d. transformation. Indeed, $R_{\rm ap}(\psi \to$

ϕ) either diverges or equals zero as stated by the following theorem.

Theorem 1 *Let G be a finite group. We also take $|\psi\rangle$ and $|\phi\rangle$ as arbitrary pure states satisfying $G_{\psi,0} \subset G_{\phi,0}$. Then,*

$$R_{\rm ap}(\psi \to \phi) = \begin{cases} \infty & {\rm Sym}_G(\psi) \subset {\rm Sym}_G(\phi), \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

In other words, for arbitrary real positive number $r > 0$, there exists a sequence of real positive numbers $\{\epsilon_N\}$ satisfying $\lim_{N\to\infty} \epsilon_N = 0$ and

$$|\psi\rangle^{\otimes N} \overset{\mathcal{U}_G - cov}{\to}_{\epsilon_N} |\phi\rangle^{\otimes rN}. \tag{9}$$

Theorem 1 shows that when ψ has resource $L(\psi, g)$ for all $g \in G$ except for $g = e$, we can transform ψ to arbitrary state ϕ with approximate i.i.d. transformation.

Therefore, we consider the exact conversion rate instead of the approximate one. To state our result, we define the subset of G where $L(\phi, g)$ diverges whenever $g \in G_{\phi,\infty}$, as

$$G_{\phi,\infty} := \{g \in G | \chi_\phi(g) = 0\}. \tag{10}$$

Then, we show the following theorem.

Theorem 2 *Let G be a finite group. We assume that $L(\phi, g) = 1$ holds only when $g = e$. Then, the following equality holds:*

$$R_{\rm ex}(\psi \to \phi) = \begin{cases} \min\limits_{g \in G\setminus(\{e\}\cup G_{\phi,\infty})} \dfrac{L(\psi,g)}{L(\phi,g)} & (G_{\phi,\infty} \subset G_{\psi,\infty}), \\ 0 & (G_{\phi,\infty} \not\subset G_{\psi,\infty}). \end{cases} \tag{11}$$

When G is commutative, we can remove the assumption that $L(\phi, g) = 0$ holds only when $g = e$. In that case, we can substitute the following subset of G for $\{e\}$ in (11):

$$G_{\phi,0} := \{g \in G | |\xi_\phi(g)| = 1\}. \tag{12}$$

The theorem 2 shows that the optimal rate of the exact i.i.d. transformation is determined by the ratios of the resource measures $L(\psi, g)$ and $L(\phi, g)$. When G is $\mathbb{Z}_2$, the theorem 2 reduces to Gour and Sppekens' result [**?**] for the optimal rate of the exact i.i.d. transformation for RTA for $\mathbb{Z}_2$ symmetry.

5 RTA for Lie groups

We next deal with continuous symmetry. We focus on the case where G is a compact connected Lie group. In that case, we can show that the above divergence of the optimal rate of the approximate i.i.d. transformation never happen. In fact, the optimal rate $R_{\rm ap}(\psi \to \phi)$ is bounded by the ratio of the QFIMs:

Theorem 3 *Let G be a compact and connected Lie group. Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary pure states. Now we define the ratio r_F as follows:*

$$r_F(\psi, \phi) := \sup\{r | \hat{F}_\psi(\vec{X}_{\mathcal{U}_G}) \ge r \hat{F}_\phi(\vec{X}_{\mathcal{U}_G})\} \tag{13}$$

Then, the following inequality holds:

$$R_{\rm ap}(\psi \to \phi) \le r_F(\psi, \phi). \tag{14}$$

Theorem 3 shows that the behavior of the optimal rate is very different between the RTA governed by the symmetry described by a finite group and that governed by the symmetry described by a Lie group. Unlike the case of finite groups, in the case of Lie groups, the optimal rates never diverge and remain at finite values.

Theorem 3 also strongly implies that when G is a compact and connected Lie group, the optimal rate $R_{\rm ap}(\psi \to \phi)$ is determined by $r_F(\psi, \phi)$. Actually there are some evidences based on a central-limit-theorem-like argument [37] that the following conjecture is valid:

Conjecture 1 *The converse of Theorem 3 is also valid. In other words, the following relation holds:*

$$R_{\rm ap}(\psi \to \phi) \ge r_F(\psi, \phi). \tag{15}$$

If this conjecture is correct, then $R_{\rm ap}(\psi \to \phi) = r_F(\psi, \phi)$ holds. Namely, in that case, the optimal rate is characterized by the "ratio" of the QFIMs. This conjecture holds true for $U(1)$ symmetry, and is consistent with the partial result on $SU(2)$ symmetry [10].

References

[1] J. McGreevy. Generalized symmetries in condensed matter. Annu. Rev. Condens. Matter Phys. **14**, 57 (2023).

[2] H. Georgi. Lie algebras in particle physics: from isospin to unified theories

[3] E. Chitambar and G. Gour, Quantum resource theories, Reviews of Modern Physics 91, 025001 (2019) .

[4] C. H. Bennett, H. j. Bernstein, S.Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Physical Review A 53, 2046 (1996) .

[5] 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 (1996).

[6] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying entanglement, Physical Review Letters 78, 2275 (1997).

[7] F. G. S. L. Brand ☒ ao, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Resource theory of quantum states out of thermal equilibrium, Phys. Rev. Lett. 111, 250404 (2013) .

[8] 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).

[9] M. Horodecki and J. Oppenheim, Fundamental limitations for quantum and nanoscale thermodynamics, Nature communications 4, 1 (2013).

[10] G. Gour and R. W. Spekkens The resource theory of quantum reference frames: manipulations and monotones New Journal of Physics 10, 033023 (2008).

[11] I. Marvian and R. W. Spekkens The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations, New Journal of Physics 15, 033001 (2013).

[12] I. Marvian Symmetry, Asymmetry and Quantum Information PhD thesis, the University of Waterloo (2012).

[13] C. Zhang, B. Yadin, Z.-B. Hou, H. Cao, B.- H. Liu, Y.-F. Huang, R. Maity, V. Vedral, C.- F. Li, G.-C. Guo, and D. Girolami Detecting metrologically useful asymmetry and entanglement by a few local measurements Phys. Rev. A 96, 042327 (2017).

[14] R. Takagi Skew informations from an operational view via resource theory of asymmetry, Sci. Rep. 9, 14562 (2019).

[15] I. Marvian Coherence distillation machines are impossible in quantum thermodynamics Nat. Commun. 11, 25 (2020).

[16] I. Marvian, Operational interpretation of quantum fisher information in quantum thermodynamics, Phys. Rev. Lett. 129, 190502 (2022)

[17] K. Yamaguchi and H. Tajima , Beyond i.i.d. in the resource theory of asymmetry: An information-spectrum approach for quantum fisher information, Phys. Rev. Lett. 131, 200203 (2023).

[18] K. Yamaguchi and H. Tajima, Smooth Metric Adjusted Skew Information Rates, Quantum 7 , 1012 (2023) .

[19] D. Kudo and H. Tajima, Fisher information matrix as a resource measure in the resource theory of asymmetry with general connected-lie-group symmetry, Phys. Rev. A 107, 062418 (2023).

[20] I. Marvian, R. W. Spekkens, and P. Zanardi/ Quantum speed limits, coherence, and asymmetry. Physical Review A 93, 052331 (2016).

[21] H. Tajima, N. Shiraishi, and K. Saito, Uncertainty relations in implementation of unitary operations. Phys. Rev. Lett. 121, 110403 (2018).

[22] M. P. Woods, R. Silva, and J. Oppenheim Autonomous Quantum Machines and Finite-Sized Clocks. Annales Henri Poincaré 20, 125 (2019)

[23] H. Tajima, N. Shiraishi, and K. Saito Coherence cost for violating conservation laws. Phys. Rev. Research 2, 043374 (2020)

[24] I. Marvian and R. W. Spekkens No-broadcasting theorem for quantum asymmetry and coherence and a trade-off relation for approximate broadcasting. Physical review letters 123, 020404(2019).

[25] M. Lostaglio and M. P. M ¨ uller Coherence and asymmetry cannot be broadcast. Physical review letters 123, 020403 (2019).

[26] K. Korezekwa Resource theory of asymmetry. PhD thesis, Imperial College London (2013).

[27] M. Ahmadi, D. Jennings, and T. Rudolph The WAY theorem and the quantum resource theory of asymmetry New J. Phys 15, 013057 (2013).

[28] I. Marvian and R. W. Spekkens An information-theoretic account of the Wigner-Araki-Yanase theorem arXiv:1212.3378 (2012)

[29] H. Tajima and H. Nagaoka Coherence-variance uncertainty relation and coherence cost for quantum measurement under conservation laws arXiv:1909.02904 (2019).

[30] Y. Kuramochi and H. Tajima, Wigner-arakiyanase theorem for continuous and unbounded conserved observables Phys. Rev. Lett. 131, 210201 (2023).

[31] H. Emori and H. Tajima Error and disturbance as irreversibility with applications: Unified definition, wigner – araki – yanase theorem and out-oftime-order correlator , arXiv:2309.14172 [quantph] (2023)

[32] H. Tajima, R. Takagi, and Y. Kuramochi Universal trade-off structure between symmetry, irreversibility, and quantum coherence in quantum processes , arXiv:2206.11086 [quant-ph] (2022)

[33] H. Tajima and K. Saito Universal limitation of quantum information recovery: symmetry versus coherence, arXiv:2103.01876 [quant-ph] (2022).

[34] S. Zhou, Z.-W. Liu, and L. Jiang New perspectives on covariant quantum error correction Quantum 5, 521 (2021).

[35] Y. Yang, Y. Mo, J. M. Renes, G. Chiribella, and M. P. Woods Optimal Universal Quantum Error Correction via Bounded Reference Frames, arXiv:2007.09154 (2020).

[36] Z.-W. Liu and S. Zhou , Approximate symmetries and quantum error correction arXiv:2111.06355 (2021).

.

[37] T. Shitara and H. Tajima, The i.i.d. State Convertibility in the Resource Theory of Asymmetry for Finite Groups and Lie groups, arXiv: 2312.15758 (2023).

Digital Quantum Simulation of Quench-Induced State Transition and the Spectroscopy of Lattice Field Theory

Dongwook Ghim[1 2 *] Masazumi Honda[1 2 †]

[1] *Interdisciplinary Theoretical and Mathematical Sciences Program (iTHEMS), RIKEN, Wako, Saitama 351-0198, Japan*

[2] *Yukawa Institute for Theoretical Physics (YITP), Kyoto University, Kyoto 606-8502, Japan*

Abstract. We present a method for computing energy spectra in lattice field theory using digital quantum simulation. The method, inspired by coherent imaging spectroscopy, perturbs the vacuum with a time-oscillating quench and analyzes the resulting loss in vacuum-to-vacuum probability to identify excited levels. We apply this technique to (1+1)-dimensional quantum electrodynamics with topological angle, known as the Schwinger model. Using a classical simulator, we prepare the vacuum on a lattice with the adiabatic method and apply various quenches through Suzuki-Trotter approximation. The computational complexity estimation suggests the method be potentially efficient with early fault-tolerant quantum computers.

Keywords: digital quantum simulation, lattice gauge theory, spectroscopy, quantum state transition, quench, Schwinger model, sign problem

1 Introduction

Recent technological advances in quantum computers have drawn the attention of the high-energy physics community [1]. The digital quantum simulation of field theory is, in particular, of interest because it naturally embeds the Hamiltonian formulation of quantum field theory in its architecture [2, 3]. A great advantage of the Hamiltonian formulation over the conventional Monte Carlo approach is the absence of the infamous sign problem [4, 5, 6]. Instead, we typically have to deal with a huge vector space corresponding to the Hilbert space but one may overcome that by utilizing quantum computers in the future. Therefore it is worth demonstrating the utility of quantum simulation in the context of high-energy physics.

In this poster, we discuss the energy spectroscopy of field theory as an application of quantum simulation to the problems in lattice gauge theories [7]. Inspired by the experimental technique, called coherent imaging spectroscopy [8], we provide a quantum algorithm that captures the energy eigenvalues of the lattice Hamiltonian.

For the demonstration of our method, we consider the Scwhinger model, $(1+1)$-dimensional quantum electrodynamics with non-trivial topological angle [9, 10]. The Lagrangian density of the Schwinger model reads

$$\mathcal{L}_0 = \frac{1}{2g^2}F_{01}^2 + \frac{\theta}{2\pi}F_{01} + \overline{\psi}i\gamma^\mu\left(\partial_\mu + iA_\mu\right)\psi - m\overline{\psi}\psi\,, \tag{1}$$

where m, g, and θ stand for the mass of the electron, the coupling constant and the topological angle, respectively. The two-component Dirac spinor of electron is denoted by ψ and the gauge field and the field strength are by A_μ and F_{01}, respectively. Since the model carries the non-trivial topological term, sign problem makes it hard to measure the observable with Monte Carlo sampling. Thus, it is nice to perform its quantum simulation to unveil its physics Monte Carlo techniques are not accessible to.

*dongwook.ghim@riken.jp

†masazumi.honda@riken.jp

2 Simulation Method for the Spectroscopy

We outline the simulation method for the spectroscopy of the lattice regularized theory. We prepare the ground state of a system and quench the state by an operator periodically oscillating in time with a particular frequency ω and measure the survival probability of the ground state. If ω is close to the energy difference between one of excited states and the ground state, Loschmidt probability for the vacuum state becomes small since the transition to the excited state is facilitated. Repeating this for various values of ω, one can estimate the energy spectrum.

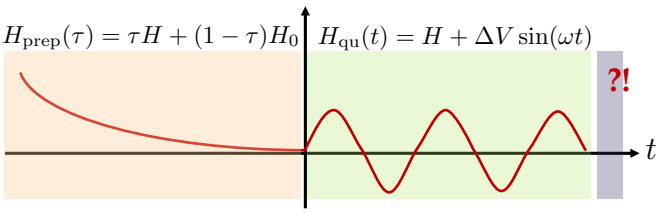


Figure 1: The cartoon of the simulation procedure. The red line schematically represents the coefficients in the Hamiltonian. In the first stage (orange), we ramp the coefficients so that they interpolates the simple initial Hamiltonian to the target Hamiltonian. The next stage (green) simulates the sinusoidal oscillation of the parameters, either triggered by operator insertion or parameter quench. At the end, we measure the Loschmidt probability for the vacuum state.

In detail, we have freedom of choice in quantum algorithms at two moments: the ground state preparation and implementation of time evolution. In this work, we simply adopt the adiabatic state preparation for the

ground state and the 2nd order Suzuki-Trotter approximation for the time evolution [11, 12, 13] while one could use different algorithms like variation-based ones depending on purposes.

3 Lattice Formulation of the Schwinger Model and its Simulation on Qubits

3.1 Lattice Hamiltonian and the Quenches

To put the theory on quantum computer, we first put the Schwinger model on a lattice and map it to a spin system. Here, rather than directly working with (1), we consider another equivalent Lagrangian obtained by the chiral rotation $\psi \to e^{i\theta\gamma_5/2}\psi$ to absorb the θ-term as in [14, 15] via transform of path integral measure [16]:

$$\mathcal{L} = \frac{1}{2g^2}F_{01}^2 + \overline{\psi} i\gamma^\mu \left(\partial_\mu + iA_\mu\right)\psi - m\overline{\psi}e^{i\theta\gamma^5}\psi\,. \tag{2}$$

Then we put the theory on a lattice with open boundary condition. The parameters are defined in terms of lattice spacing a and coupling constant g as follows.

$$J = \frac{g^2 a}{2}, \quad w = \frac{1}{2a}, \quad m_{\rm lat} = m - \frac{g^2}{16w}, \tag{3}$$

where we measure all the dimensionful quantities in the unit of g and the last relation comes according to [17, 18]. Solving the Gauss law and applying the Jordan-Wigner transformation [19] to the staggered fermion [20, 21] at each site n: $\chi_n = \left(\prod_{\ell<n} -iZ_\ell\right)\frac{X_n - iY_n}{2}$ with the Pauli spins (X_n, Y_n, Z_n) at each site, we obtain the following spin Hamiltonian [15]

$$H = H_{ZZ} + H_{XX} + H_{YY} + H_Z,$$

where

$$\begin{aligned}
H_{ZZ} &= \frac{J}{2}\sum_{n=1}^{N-2}\sum_{0\le k<\ell\le n} Z_k Z_\ell = \frac{J}{2}\sum_{n=1}^{N-2}\sum_{k<n}(N-n-1)Z_k Z_n\,,\\
H_{XX} &= \frac{1}{2}\sum_{n=0}^{N-2}\left\{w - (-1)^n\frac{m_{\rm lat}}{2}\sin\theta\right\}X_n X_{n+1}\,,\\
H_{YY} &= \frac{1}{2}\sum_{n=0}^{N-2}\left\{w - (-1)^n\frac{m_{\rm lat}}{2}\sin\theta\right\}Y_n Y_{n+1}\,,\\
H_Z &= \frac{m_{\rm lat}\cos\theta}{2}\sum_{n=0}^{N-1}(-1)^n Z_n + \frac{J}{2}\sum_{n=0}^{N-2}\mathrm{mod}(n+1,2)\sum_{\ell=0}^{n} Z_\ell\,.
\end{aligned} \tag{4}$$

Next, we introduce the gauge-invariant operator quench. Specifically, we consider the pseudo-chiral condensate $V = \int\overline{\psi}\gamma_5\psi$. With the spatial modulation f_n taken into account, the quench on the lattice is translated into Pauli spin operators on qubits,

$$\Delta H(t) = \frac{B_p}{2}\sum_{n=0}^{N-2}(-1)^{n+1} f_n \sin(\omega t)\left(X_n X_{n+1} + Y_n Y_{n+1}\right)\,. \tag{5}$$

The coefficient B_p with the mass dimension 1 controls the strength of the external quench. Besides the operator-type quench, we consider the time-sinusoidal fluctuation in the topological angle, whose profile on the lattice reads,

$$\widetilde{\theta}(t,n) = \theta + \frac{B_p}{g} f_n \sin(\omega t)\,. \tag{6}$$

The spatial modulation factor can decorate the quench as introduced by site-dependent function f_n in (5). A canonical choice for its basis is

$$\left\{f_n^{(k)}\right\}_{k=0,1,2\cdots} \equiv \left\{\cos\left(\frac{k\pi n}{N-1}\right)\right\}\,, \tag{7}$$

which is the discrete version of $\{\mathfrak{f}^{(k)}\,|\,\mathfrak{f}^{(k)}(x) = \cos\left(\frac{\pi k x}{L}\right)$ for $k = 0, 1, 2, \cdots\}$. We call the integer k above as a mode number.

During the quench, the 2nd-order Suzuki-Trotter approximation approximates the time evolution on a circuit at each Trotter step Δt_{ST},

$$\begin{aligned}
e^{-i\Delta t_{ST}H} \simeq\; & e^{-i\frac{\Delta t_{ST}}{2}H_{XX}}e^{-i\frac{\Delta t_{ST}}{2}H_{YY}}e^{-i\Delta t_{ST}(H_{ZZ}+H_Z)}\\
& \times e^{-i\frac{\Delta t_{ST}}{2}H_{YY}}e^{-i\frac{\Delta t_{ST}}{2}H_{XX}} + \mathcal{O}(1/M^3)\,,
\end{aligned} \tag{8}$$

where an integer M stands for the total number of time steps during the quench. Along the quench, we tune the coefficient of Hamiltonian (4) following either (5) or (6). Finally, we carry out the measurement of the Loschmidt probability for the vacuum state, or vacuum-to-vacuum probability,

$$\left|\langle{\rm vac}|e^{-i\int dt(H+\Delta H(t))}|{\rm vac}\rangle\right|^2\,, \tag{9}$$

after the quench. Technically, the last measurement procedure requires the adiabatic preparation of vacuum on the bra vector $\langle{\rm vac}|$ at the end of the simulation circuit.

3.2 Parameter Set-Up

We set the length of the spatial interval L, by confirming the agreement of analytic continuum spectra and the lattice result obtained by the exact diagonalization at the massless case with $\theta = 0$. We used python-based package `QuSpin` [22, 23] in the exact diagonalization computation up to $N = 17$ qubits. A good agreement is achieved at the interval length choice $gL = 10$.

On the temporal scale side, we identify four kinematic frequency scales:

- Trotterization frequency $\omega_{ST} = 2\pi/\Delta t_{ST}$,
- quench frequency $\omega \sim \Delta E_{\rm gap}$,
- simulation time $T = M\Delta t_{ST}$ and its frequency Ω,
- resolution in the frequency domain $\Delta\omega$.

In addition, the perturbation theory in terms of B_p suggests a useful dimensionless quantity $\gamma := |\langle f\,|\Delta V|\,{\rm vac}\rangle|$ where ΔV is defined by the relation $\Delta H(t) = B_p\Delta V\sin(\omega t)$ and the bra $\langle f|$ stand for the target excited energy eigenstate. Further analysis can be carried out based on the perturbation theory [24], which says that the transition probability between two states whose energy gap is $\Delta E_{\rm gap}$ is given by

$$P_{{\rm vac}\to f}(t) = (\gamma B_p)^2\,\frac{\sin^2\left[(\Delta E_{\rm gap}-\omega)\,t\right]}{(\Delta E_{\rm gap}-\omega)^2} + \mathcal{O}\left(B_p^3\right)\,. \tag{10}$$

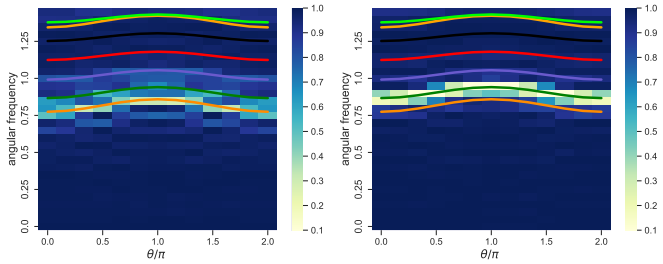
However this analysis should assume two conditions on the dynamics of transition: (a) a state transition occurs

in a short enough simulation time in which the perturbation theory is valid, (b) a window of quench frequency $\Delta\omega$ is fine enough so that the argument inside the sin function in the numerator of (10) is small enough, *i.e.* $\Delta\omega\, T < 1$, near the energy gap $\omega \sim \Delta E_{\rm gap}$.

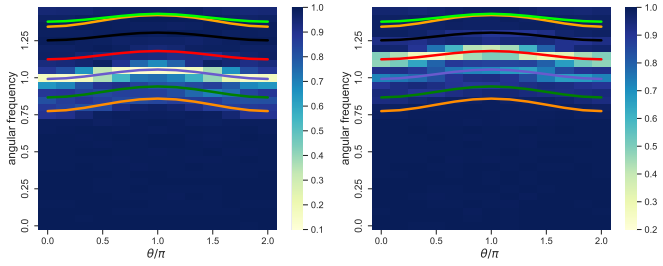
Now, let us set the probability threshold $P_{\rm th}$ such that $0 \lesssim P_{\rm th} < 1$ as follows. When the Loschmidt probability for the vacuum after the quench is smaller than $1 - P_{\rm th}$, we identify the loss of vacuum so read the frequency of quench as the energy gap. Then, the lower bound of estimated simulation time $T_{\rm th}$ reads in terms of characteristic scale and preset parameters; $T > T_{\rm th} = \frac{\sqrt{P_{\rm th}}}{\gamma B_p}$.

The resolution of probe frequency $\Delta\omega$ should be smaller than the differences in the excitation energies, which are mostly attributed to the higher momentum modes in field theories. In the regime of small electron mass and small topological angle $m \simeq 0\,, \theta \simeq 0$, we have $\Delta\omega/\omega < (\pi/L)/M_S$ where M_S stands for the mass of dual scalar Schwinger meson at $\theta = 0$. The right-hand side of the inequality is $\mathcal{O}(1)$ in our simulation.

The reliable simulation under Suzuki-Trotter approximation requires the accumulative error ϵ_{ST} to be small. Since the order of magnitude of accumulative error scales as $\epsilon_{ST} \sim \mathcal{O}\left(M\left(\omega\Delta t_{ST}\right)^3\right) \sim \mathcal{O}\left(\omega^3\omega_{ST}^{-2}\Omega^{-1}\right)$. Thus, and we find $\omega_{ST} \gg \Omega^{-\frac{1}{2}}\omega^{\frac{3}{2}}$. Synthesizing the scaling laws obtained above, we obtain the hierarchy between frequency scales; $\Delta\omega < \Omega < \omega < \omega_{ST}$. The specific number consistent with this estimate will be presented in the poster.



(a) $k = 0$ (uniform quench) (b) $k = 1$

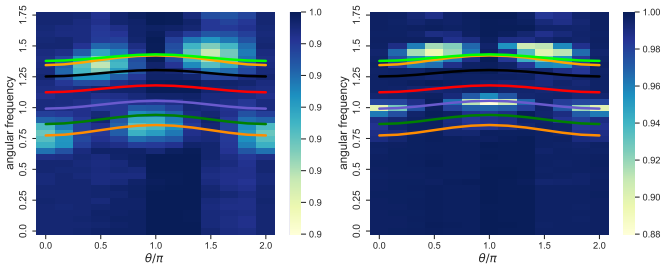


(c) $k = 2$ (d) $k = 3$

Figure 2: The density plot for the vacuum-to-vacuum Loschmidt probability for various topological angles $\theta \in [0\,, 2\pi]$ and fixed $m = 0.100$ under the pseudo-chiral condensate quench (5). Solid lines denote the exact diagonalization result with `QuSpin`. The strength coefficient of quench is chosen at $B_p = 0.011$.

4 Result of Simulation

Figure 2 and Figure 3 present the simulation results with a classical emulator `Aer` of `IBM Qiskit` for the two types of quench. Though the open boundary condition violates the translation symmetry the mode number introduced in (7) turns out to be able to label and distinguish the low-energy eigenstates.



(a) $k = 0$ (uniform quench) (b) $k = 2$

Figure 3: The density plot for the vacuum-to-vacuum Loschmidt probability for various topological angles $\theta \in [0\,, 2\pi]$ and fixed $m = 0.100$ under the topological angle quench (6). Solid lines denote the exact diagonalization result with `QuSpin`. The strength coefficient of quench is chosen at $B_p = 0.500$.

Unlike the pseudo-chiral condensate case, Figure 3 exhibits the excitations at higher energy near $\theta = \frac{\pi}{2}$ and $\frac{3\pi}{2}$. We suspect that they correspond to 2-particle states under $\theta \to 0$ limit and the transition amplitude between the 2-particle state and the vacuum under the theta fluctuation is non-trivial whereas its counterpart amplitude with the pseudo-chiral condensate operator almost vanishes.

5 Conclusion and Outlook

In this work, we showed that the quench-induced state transition of a quantum system can be used to capture the excited state spectra of abelian lattice gauge theory in (1+1)-dimensions. We introduced two types of gauge-invariant quench and observed the low-energy excited spectra can be read off from the loss in the Loschmidt probability for the vacuum under the quench at specific frequency.

The analysis in Section 3.2 further allows the estimation of how many controlled-Z (CZ) or CNOT is necessary to carry reliable simulation given probability threshold $P_{\rm th}$. The number of the controlled gates at each Trotterized step depends quadratically on the number of qubits, as shown in (4). Hence, the total number of controlled gates for M Trotterized steps is bounded below by $\mathcal{N}_{CZ} \sim \mathcal{O}\left(MN^2\right) > \mathcal{O}\left(\left(\omega\sqrt{P_{\rm th}}/\gamma B_p\right)^{\frac{3}{2}} N^2\right)$.

There are various interesting future directions. Besides the implementation on a real quantum device, interesting is to compare the computational complexity of our algorithm with those of other algorithms based on tensor network, which is a yet powerful approach to the Schwinger model [17, 25, 26, 27, 28].

References

[1] A. Di Meglio et al., *Quantum Computing for High-Energy Physics: State of the Art and Challenges. Summary of the QC4HEP Working Group*, 2307.03236.

[2] S. P. Jordan, K. S. M. Lee and J. Preskill, *Quantum Algorithms for Quantum Field Theories*, *Science* **336** (2012) 1130–1133, [1111.3633].

[3] S. P. Jordan, K. S. M. Lee and J. Preskill, *Quantum Algorithms for Fermionic Quantum Field Theories*, 1404.7115.

[4] P. de Forcrand, *Simulating QCD at finite density*, *PoS* **LAT2009** (2009) 010, [1005.0539].

[5] G. Aarts, *Introductory lectures on lattice QCD at nonzero baryon number*, *J. Phys. Conf. Ser.* **706** (2016) 022004, [1512.05145].

[6] K. Nagata, *Finite-density lattice QCD and sign problem: Current status and open problems*, *Prog. Part. Nucl. Phys.* **127** (2022) 103991, [2108.12423].

[7] M. C. Bañuls, K. Cichy, K. Jansen and J. I. Cirac, *The mass spectrum of the Schwinger model with Matrix Product States*, *JHEP* **11** (2013) 158, [1305.3765].

[8] C. Senko, J. Smith, P. Richerme, A. Lee, W. C. Campbell and C. Monroe, *Coherent imaging spectroscopy of a quantum many-body spin system*, *Science* **345** (jul, 2014) 430–433, [1401.5751].

[9] J. S. Schwinger, *Gauge Invariance and Mass*, *Phys. Rev.* **125** (1962) 397–398.

[10] J. S. Schwinger, *Gauge Invariance and Mass. 2.*, *Phys. Rev.* **128** (1962) 2425–2429.

[11] M. Suzuki, *General theory of fractal path integrals with applications to many-body theories and statistical physics*, *Journal of Mathematical Physics* **32** (1991) 400–407, [https://doi.org/10.1063/1.529425].

[12] S. Lloyd, *Universal quantum simulators*, *Science* **273** (1996) 1073–1078.

[13] N. Hatano and M. Suzuki, *Finding Exponential Product Formulas of Higher Orders*, *Lect. Notes Phys.* **679** (2005) 37, [math-ph/0506007].

[14] C. J. Hamer, W.-h. Zheng and J. Oitmaa, *Series expansions for the massive Schwinger model in Hamiltonian lattice theory*, *Phys. Rev.* **D56** (1997) 55–67, [hep-lat/9701015].

[15] B. Chakraborty, M. Honda, T. Izubuchi, Y. Kikuchi and A. Tomiya, *Digital Quantum Simulation of the Schwinger Model with Topological Term via Adiabatic State Preparation*, 2001.00485.

[16] K. Fujikawa, *Path Integral Measure for Gauge Invariant Fermion Theories*, *Phys. Rev. Lett.* **42** (1979) 1195–1198.

[17] R. Dempsey, I. R. Klebanov, S. S. Pufu and B. Zan, *Discrete chiral symmetry and mass shift in the lattice Hamiltonian approach to the Schwinger model*, *Phys. Rev. Res.* **4** (2022) 043133, [2206.05308].

[18] R. Dempsey, I. R. Klebanov, S. S. Pufu, B. T. Søgaard and B. Zan, *Phase Diagram of the Two-Flavor Schwinger Model at Zero Temperature*, 2305.04437.

[19] P. Jordan and E. Wigner, *Über das paulische äquivalenzverbot*, *Zeitschrift für Physik* **47** (Sep, 1928) 631–651.

[20] J. B. Kogut and L. Susskind, *Hamiltonian Formulation of Wilson's Lattice Gauge Theories*, *Phys. Rev. D* **11** (1975) 395–408.

[21] L. Susskind, *Lattice Fermions*, *Phys. Rev.* **D16** (1977) 3031–3039.

[22] P. Weinberg and M. Bukov, *QuSpin: a Python package for dynamics and exact diagonalisation of quantum many body systems part I: spin chains*, *SciPost Phys.* **2** (2017) 003, [1610.03042].

[23] P. Weinberg and M. Bukov, *QuSpin: a Python package for dynamics and exact diagonalisation of quantum many body systems. Part II: bosons, fermions and higher spins*, *SciPost Phys.* **7** (2019) 020, [1804.06782].

[24] P. A. M. Dirac, *Quantum theory of emission and absorption of radiation*, *Proc. Roy. Soc. Lond. A* **114** (1927) 243.

[25] M. C. Banuls, K. Cichy, K. Jansen and H. Saito, *Chiral condensate in the Schwinger model with Matrix Product Operators*, *Phys. Rev.* **D93** (2016) 094512, [1603.05002].

[26] L. Funcke, K. Jansen and S. Kühn, *Topological vacuum structure of the Schwinger model with matrix product states*, *Phys. Rev. D* **101** (2020) 054507, [1908.00551].

[27] M. Honda, E. Itou and Y. Tanizaki, *DMRG study of the higher-charge Schwinger model and its 't Hooft anomaly*, *JHEP* **11** (2022) 141, [2210.04237].

[28] T. Okuda, *Schwinger model on an interval: Analytic results and DMRG*, *Phys. Rev. D* **107** (2023) 054506, [2210.00297].

Uncorrectable error injection based fault-tolerant and secure quantum state transmission

IlKwon Sohn[1] * Boseon Kim[1] Kwangil Bae[1] Wooyeong Song[1] Chankyun Lee[1]
Kabgyun Jeong[2] Wonhyuk Lee[1]

[1]*Korea Institute of Science and Technology Information, Daejeon 34141, Republic of Korea*
[2]*Research Institute of Mathematics, Seoul National University, Seoul 08826, Republic of Korea*

Abstract. The quantum teleportation is a widely used quantum scheme to transmit arbitrary quantum states. However, it requires entanglement swapping and purification for entanglements distribution over long distances, which introduces significant overhead. In this vein, we propose a scheme to directly transmit quantum states encoded with error correction codes. Our scheme is a secure quantum state transmission with fault-tolerance, by encoding with quantum error correction codes and injecting uncorrectable errors.

Keywords: Quantum state transmission, Quantum error correction codes, Uncorrectable error

1 Background

The quantum internet refers to a network that connects distant quantum devices [1, 2, 3]. It is expected to offer functionalities beyond the capabilities of the current internet. To realize it, it is essential to transmit arbitrary quantum states. Quantum teleportation is a protocol used for this purpose [4]. However, it requires an pre-shared entangled pair and entanglement swapping is needed for long range entanglement distribution. For the long distances distribution, the success probability decreases exponentially with the number of nodes because of the success probability of the bell state measurement (BSM) is 50% in linear optical setup. Therefore, when performing logical BSM using quantum error correction codes (QECCs), the success probability increases to $1-1/2^{n_s}$ based on the code length n_s, but this results in an n_s-fold overhead [6]. Besides, to enhance the fidelity of the shared entanglement, entanglement purification must be performed and the overhead increases further. Using the method in Ref. [7], high fidelity can be achieved with only two ancilla qubits. However, for the case of long distance distribution it requires multiple stages of entanglement swapping and purification as shown in Fig. 1. The overhead can increase exponentially over the number of relay nodes. Therefore, it might be more efficient to encode the quantum states using QECCs and transmit it in a manner similar to classical communication. Therefore, in this presentation, we aim to introduce a scheme by encoding quantum states with QECCs and injecting uncorrectable errors to enable secure and fault-tolerant long-distance transmission of quantum states. The uncorrectable error in our scheme ensures that an eavesdropper cannot interpret the received information, thereby providing security equivalent to the inherent security of the quantum teleportation.

2 The proposed scheme

In this section, we will describe a scheme for transmitting quantum states in a fault-tolerant and secure manner by injecting uncorrectable errors into encoded states.

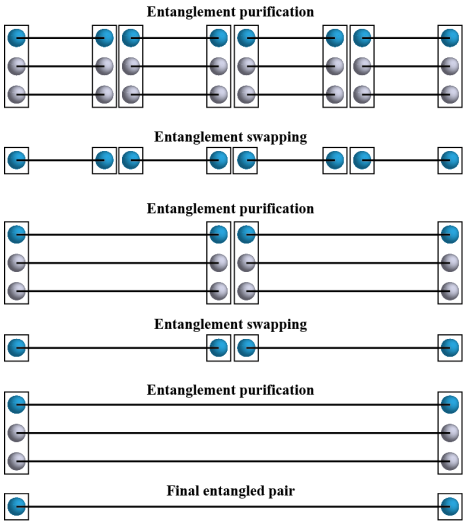


Figure 1: **Long distance entanglement distribution** The blue spheres represent the entangled pairs and the gray spheres represent the ancilla qubits. By repeatedly performing entanglement purification and entanglement swapping, it is possible to share entangled pairs over long distances.

Setup We consider a system model where a noisy and insecure quantum channel and an authenticated classical channel protected by a quantum key distribution protocol, etc., are connected between the sender and the receiver. To transmit arbitrary quantum states, the sender first measures the quantum bit error rate of the quantum channel. Based on it, the sender determines the error correction capability t of the QECCs.

Encoding and Encryption The sender selects a $[[n, k, d]]$ QECC that satisfies t determined during the **Setup** phase, and provides sufficient security. To facilitate the security assessment discussed in the Sec 3, we will consider only non-degenerate quantum codes. The sender then encodes the k-qubit quantum state $|\psi\rangle =$

*d2estiny@kisti.re.kr

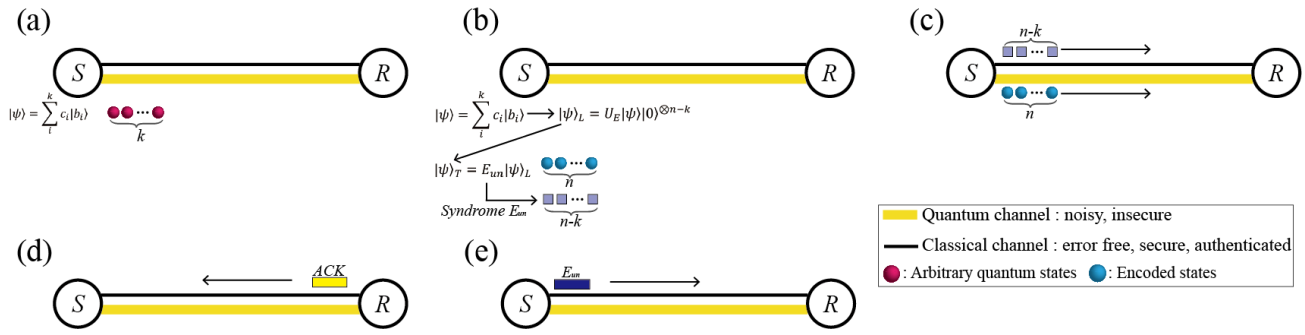


Figure 2: **Schematic picture of the proposed scheme**: (a) The sender prepares the arbitrary quantum states. (b) The Sender encodes them and injects E_{un}. (c) The Sender broadcasts s and sends $|\psi_T\rangle$. Then, the receiver performs error correction based on s (d) The receiver sends the ACK to the sender upon receiving the quantum state. (e) The sender informs the receiver of E_{un}. The receiver applies it to the received state and performs syndrome extraction to verify if a zero vector is obtained. If the syndrome is not a zero vector, sender and receiver abort the process.

$\sum_i^{2^k} c_i|b_i\rangle$ into a logical state using the encoding operator U_E of this QECC. Additionally, to perform encryption, a Pauli error operator E_{un} with an appropriate weight, which the chosen QECC cannot correct, is injected into the encoded logical state $|\psi\rangle_L$. The resulting state $|\psi\rangle_T$ is as follows,

$$|\psi\rangle_T = E_{un}|\psi\rangle_L = E_{un}U_E \sum_i^k c_i|b_i\rangle$$

The sender calculates the syndrome s of E_{un}.

Transmission and Reception The sender transmits $|\psi\rangle_T$ through the quantum channel and sends s through the classical channel to the receiver. Upon receiving $|\psi\rangle_T$ and s, the receiver extracts the syndrome of $|\psi\rangle_T$ and performs error correction based on s. Subsequently, the receiver sends an ACK to the sender indicating the reception of the state. Upon receiving the ACK, the sender transmits the information of E_{un} to the receiver through an authenticated secure classical channel. The receiver applies the received E_{un} to $|\psi\rangle_T$ and performs syndrome extraction again to ensure that an all-zero vector is obtained. If an all-zero vector syndrome is not obtained, it is assumed that there was an eavesdropper's attack, and the process is aborted.

Distance extension The advantage of the proposed approach lies in its ability to extend the distance despite encryption, as error correction is still feasible. Similar to what the receiver does in the **Transmission and Reception**, relay nodes perform error correction based on s and then pass it to the next node, enabling fault-tolerant transmission. Furthermore, since E_{un} is injected, relay nodes cannot obtain any information about the quantum states.

3 Results

In this section, we will discuss the general security and overhead of the proposed scheme.

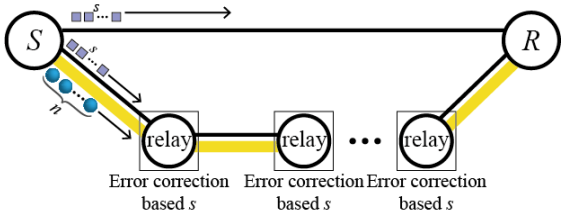


Figure 3: **Distance extension of the proposed scheme** Relay nodes can perform error correction based on s, ensuring that relay nodes cannot obtain any information about the quantum states.

3.1 Overhead analysis

To calculate the overhead of the quantum teleportation, the total number of the nodes is required. For simplicity, we assume that the total number of nodes is $2^N + 1$. The minimum number of qubits required for entanglement purification [7] O_{EP} is as follows,

$$O_{EP} = \sum_{i=0}^{N} N_A 2^{N-i} \times 2, \tag{1}$$

where N_A is the number of the ancilla qubits for the entanglement purification. In the case of the entanglement swapping the number of BSMs is as follows,

$$O_{ES} = \sum_{i=1}^{N} 2^{N-i}. \tag{2}$$

To increase the success probability of BSMs, $P_{ES} = 1 - (1/2)^{n_s}$, we can use the logical BSM mentioned in the Sec 1. Then the probability that all O_{ES} BSMs succeed is $(1 - (1/2)^{n_s})^{O_{ES}}$. Therefore, the approximate number of repetitions required for the process to succeed at least once is $\lceil (\frac{2^{n_s}}{2^{n_s}-1})^{O_{ES}} \rceil$. Finally, the total number of qubits O_T required for a single successful long-distance entanglement distribution is as follows,

$$O_T = (O_{EP} + 2O_{ES}(n_{bsm} - 1)) \times \lceil (\frac{2^{n_s}}{2^{n_s}-1})^{O_{ES}} \rceil. \tag{3}$$

For example, if N_A is 2 with physical error rate $p = 0.01$ and the total number of nodes is 5, the total number of qubits required for entanglement purification is 28. Then, if assuming the logical BSM with $n_s = 2$, the success probability is $(3/4)^3$. Consequently, the number of repetitions needed for at least one successful attempt is approximately 3. Thus, a total of 93 qubits are required for the 5-node distance entanglement distribution.

The overhead of the proposed scheme is determined by the logical error probability of quantum stabilizer codes, p_L. The p_L on a depolarizing channel with the physical error rate p is given as [9],

$$p_L = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}. \tag{4}$$

To approximate the p_L of the proposed scheme, we use the following quantum singleton bound [10],

$$n - k \geq 2(d-1) \tag{5}$$

Since it is not feasible to use codes that perfectly satisfy this quantum singleton bound, we modified this bound as follows,

$$\frac{n-k}{4} \geq t. \tag{6}$$

Assuming $R = \frac{1}{2}$ and substituting the relationship between n, k, and t into Eq. (6) yields the following result:

$$p_L = 1 - \sum_{i=0}^{\frac{n}{8}} \binom{n}{i} p^i (1-p)^{n-i}. \tag{7}$$

In the case of 93 qubits derived from the previous quantum teleportation overhead example, considering only a physical error rate of 0.01, the p_L value is at least 1.9689×10^{-10}. This value is lower than the performance of quantum teleportation, which is 4.1215×10^{-6}, assuming that all rounds prior to the final purification round of long-distance entanglement distribution and the teleportation process are noiseless.

3.2 Analysis of number of uncorrectable errors

The security of the proposed scheme is determined by the number of uncorrectable errors N_u assigned to each syndrome can be estimated as follows,

$$N_u \sim \frac{4^n - \sum_{i=0}^{t} 3^i \binom{n}{i} (2^{n-k} + 2^{2k})}{2^n - k} \times \frac{1}{2^{n-k}}. \tag{8}$$

The term 4^n of Eq. (8) represents the number of all Pauli error patterns of length n, while $\sum_{i=0}^{t} 3^i \binom{n}{i}$ denotes the number of all errors that the QECCs can correct. Later on, for simplicity, we'll refer to this as N_c. The subsequent terms multiplied by N_c, represents the count of errors with different weights sharing the same syndrome as correctable errors within N_c. Among these terms, 2^{n-k} is the total number of the stabilizers. When it is multiplied by N_c, it accounts for errors that share the same syndrome and behavior as correctable errors within N_c. On the other hand, 2^{2k} represents the total number of logical Pauli operators. When it is multiplied by N_c, it accounts for the uncorrectable errors that share the same syndrome but have different behaviors because of the logical operators. The uncorrectable errors, when multiplied by stabilizers, have the same behavior and the syndrome. Therefore, they should be considered as a single error. To account for this, we adjust by dividing by the total number of stabilizers, 2^{n-k}, which serves as the denominator. The final $\frac{1}{2^{n-k}}$ term is used to calculate the average number. Here, 2^{n-k} represents the total number of syndromes which are bit strings of length $n-k$.

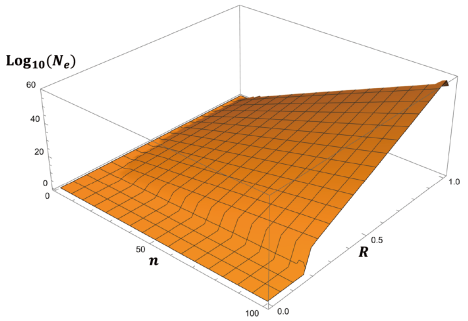


Figure 4: **Security analysis graph** This graph illustrates the order of N_u as Eq. (10).

We can substitute N_c with a function of n and k by using the Hamming bound for QECCs [8]. The quantum Hamming bound is as follows,

$$e^{n-k} \geq \sum_{i=0}^{t} 3^i \binom{n}{i}. \tag{9}$$

Then, substituting the code rate $k/n = R$ into the Eq. (8), the below bound is derived as,

$$N_u \geq 2^{2Rn}(1 - (\frac{e}{4})^{(1-R)n}) - (\frac{e}{2})^{(1-R)n}. \tag{10}$$

According to Eq. (10), the graph of N_u over the range $1 \leq n \leq 100$ is shown in Fig. 4. As seen in Fig. 4, N_u has very small value when R is below approximately 0.18. Therefore, to ensure adequate security, it is necessary to use QECCs with a sufficiently large R. For the case with a total of 5 nodes and 102 required qubits, the number of N_u when $R = 0.5$ is approximately 5.0706×10^{30}.

4 Conclusion

In this presentation, we have demonstrated an efficient quantum state transmission scheme with low overhead and higher fidelity compared to quantum teleportation. However, the scheme is not yet fully refined, and future work will focus on analyzing the security of the proposed scheme under specific attack models, rather than solely based on N_u. Additionally, we aim to develop an algorithm to appropriately selecting either of the proposed scheme and quantum teleportation by comprehensively considering factors such as the overhead, the target fidelity, the initial fidelity, and the physical error rate.

Acknowledgments

This research was supported by Korea Institute of Science and Technology Information(KISTI).(K24L4M1C2). This research was supported by the National Research Council of Science & Technology(NST) grant by the Korea government (MSIT) (No. CAP22053-000)

References

[1] H. J. Kimble. The quantum internet. *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[2] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. *Science*, vol. 362, no. 6412, p. eaam9288, 2018.

[3] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi. Quantum internet: Networking challenges in distributed quantum computing. *IEEE Network*, vol. 34, no. 1, pp. 137–143, 2019.

[4] 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*, vol. 70, no. 13, p. 1895, 1993.

[5] M. Weber. Experimental quantum memory applications and demonstration of an elementary quantum repeater link with entangled light-matter interfaces. 2012.

[6] S.-H. Lee, S.-W. Lee, and H. Jeong. Loss-tolerant concatenated bell-state measurement with encoded coherent-state qubits for long-range quantum communication. *Physical Review Research*, vol. 3, no. 4, p. 043205, 2021.

[7] J. Kim, S. Seo, J. Yun, and J. Bae. Static quantum errors and purification. *arXiv preprint arXiv:2405.06291*, 2024.

[8] A. Ekert and C. Macchiavello. Quantum error correction for communication. *Physical Review Letters*, vol. 77, no. 12, p. 2585, 1996.

[9] D. Forlivesi, L. Valentini, and M. Chiani. Performance analysis of quantum error-correcting codes via macwilliams identities. *arXiv preprint arXiv:2305.01301*, 2023.

[10] E. Knill and R. Laflamme Theory of quantum error correcting codes *Physical Review A*, vol. 55, no. 2, p. 900, 1997.

Corrupted sensing quantum state tomography

Mengru Ma[1] * Jiangwei Shang[1] †

[1] *Key Laboratory of Advanced Optoelectronic Quantum Architecture and Measurement (MOE), School of Physics, Beijing Institute of Technology, Beijing 100081, China*

Abstract. In this work we propose the concept of corrupted sensing quantum state tomography (QST) which enables the simultaneous reconstruction of quantum states and structured noise with the aid of simple Pauli measurements only. Without additional prior information, we investigate the reliability and robustness of the framework. The power of our protocol is demonstrated by assuming Gaussian and Poisson sparse noise for low-rank state tomography. In particular, our approach is able to achieve a high quality of the recovery with incomplete sets of measurements and is also suitable for performance improvement of large quantum systems.

Keywords: quantum tomography, corrupted sensing, Pauli measurement, sparse noise

1 Corrupted sensing QST protocol

Considering an n-qubit quantum system with dimension $d = 2^n$, the unknown state of the system is denoted by ρ, which satisfies $\mathrm{tr}(\rho) = 1$ and $\rho \geq 0$. An n-qubit Pauli operator takes on the general form

$$P = \bigotimes_{i=1}^{n} \sigma_i \,, \tag{1}$$

where $\sigma_i \in \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}$. Here, $\sigma_x, \sigma_y, \sigma_z$ are the three Pauli matrices, and $\mathbb{I}$ represents the identity matrix. In total there are $d^2 = 4^n$ such Pauli operators.

In general, the simultaneous reconstruction of quantum state and corrupted noise consists of the following two steps: First select Pauli operators at random to measure the quantum state and obtain the noisy data; then choose a suitable convex optimization algorithm for data post-processing to get the estimations of the state and noise.

To be specific, the scheme of corrupted sensing quantum state tomography proceeds as follows. Choose m Pauli operators $\{P_1, P_2, \cdots, P_m\}$ independently and uniformly, and measure the expectation values $\mathrm{tr}(P_k\rho)$. These operators are chosen randomly without replacement. To get an estimate of the expectation value $\mathrm{tr}(P_k\rho)$, we use N copies of the state ρ.

Define the linear map $\mathcal{M} : \mathbb{H}^d \to \mathbb{R}^m$ for all P_ks as

$$[\mathcal{M}(\rho)]_k = \mathrm{tr}(P_k\rho) \,. \tag{2}$$

Then, the output of the entire measurement process can be written as a vector

$$\mathbf{y} = \mathcal{M}(\rho) + \mathbf{v} + \mathbf{z} \,. \tag{3}$$

Here the structured noise (or structured corruption) is modeled as a stochastic vector $\mathbf{v}$, which is a general consideration as noise can manifest in any process. And $\mathbf{z}$ is any other kind of unstructured noise including statistical noise. In particular, if there's no corruption, i.e., $\mathbf{v} = 0$, the model in Eq. (3) reduces to the standard compressed sensing problem [1, 2].

*mengru.ma@bit.edu.cn
†jiangwei.shang@bit.edu.cn

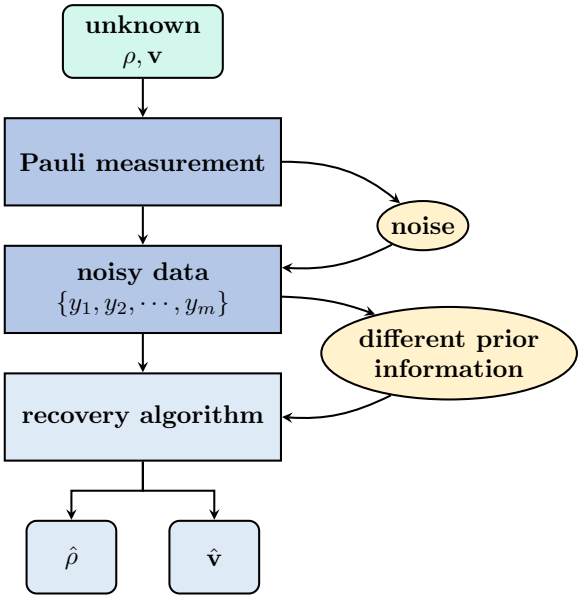


Figure 1: Schematic procedure of the corrupted sensing quantum state tomography. For the unknown state ρ and noise $\mathbf{v}$, Pauli measurements are employed to get the noisy data $\mathbf{y} = \{y_1, y_2, \cdots, y_m\}$. With different prior information, one can choose various recovery algorithms to get the reconstructed state $\hat{\rho}$ and noise $\hat{\mathbf{v}}$; see Eqs. (4).

Generally speaking, the problem in Eq. (3) is ill-posed, and tractable recovery is only possible when both the state ρ and the noise $\mathbf{v}$ are suitably structured. See Fig. 1 for a schematic framework of the corrupted sensing quantum state tomography. By randomly selecting m Pauli operators to measure the quantum state, an estimation of both the state and noise from the acquired noisy data is then performed. Here we consider the general setting where no prior information about the quantum state ρ or the structured noise $\mathbf{v}$ is taken into account.

2 Corrupted sensing QST estimator

We consider the general case where the structure of the state and noise can be characterized by a suitable

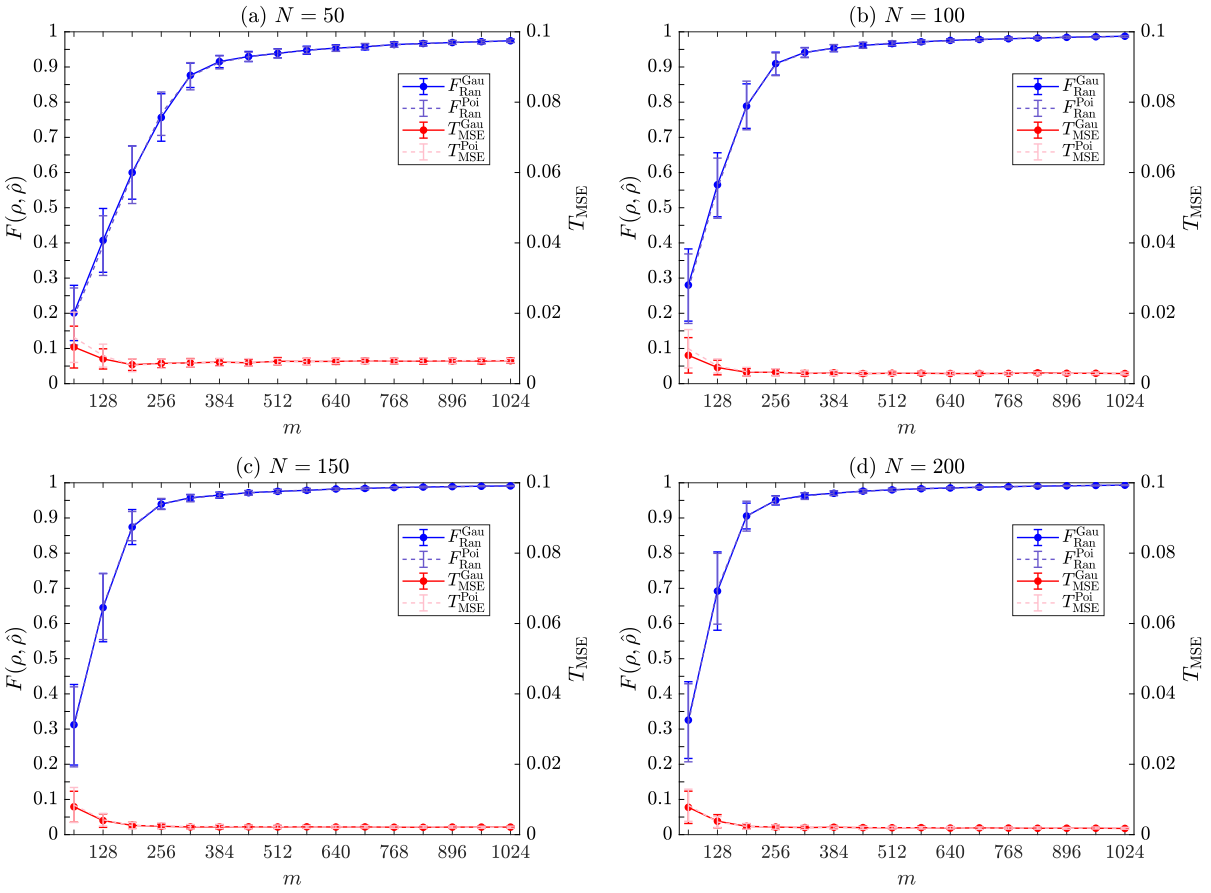


Figure 2: Fidelity $F(\rho, \hat{\rho})$ and MSE T_{MSE} as functions of the number of sampled Pauli operators m (ranging from 64 to 1024 with steps of 64) over 120 runs with $n = 5$ qubits. The blue solid curve (purple dashed curve) represents the fidelity between the reconstructed state and true state in the case of Gaussian (Poisson) noise. Meanwhile, the red solid curve (pink dashed curve) represents the MSE between the reconstructed Gaussian (Poisson) noise and true Gaussian (Poisson) noise. The number of copies of the input random pure states used for each experiment in (a), (b), (c), and (d) are $N = 50, 100, 150$, and 200, respectively. Standard deviation of the Gaussian noise and parameter of the Poisson noise are both set to $\sigma = \lambda = 4$. Additionally, the regularization parameters are chosen as $\tau_1 = 0.011m$, $\tau_2 = 0.16$, and the sparsity level is defined as $s = \lfloor 0.04m \rfloor$.

norm function. Typical examples of such structures include low-rank matrices and sparse vectors. Hereafter, let $f(\cdot)$ and $g(\cdot)$ denote the suitable norms which fully characterize the structures of the state and noise respectively.

The reconstruction of the unknown state ρ and structured noise $\mathbf{v}$ without prior assumptions can be formulated as the following convex optimization problem

$$\min_{\tilde{\rho}, \tilde{\mathbf{v}}} \quad \frac{1}{2}\|\mathbf{y} - \mathcal{M}(\tilde{\rho}) - \tilde{\mathbf{v}}\|_2^2 + \tau_1 \cdot f(\tilde{\rho}) + \tau_2 \cdot g(\tilde{\mathbf{v}}), \quad (4)$$

where $\tau_1, \tau_2 > 0$ are regularization parameters, and $\tilde{\rho}$ and $\tilde{\mathbf{v}}$ represent the variables to be solved. The intuition of the problem is to find $\tilde{\rho}, \tilde{\mathbf{v}}$ which fit the data $\mathbf{y}$ while minimizing the least-squares linear regression with suitable norm regularizations.

Here we consider minimizing the trace norm $\|X\|_{\mathrm{tr}} = \mathrm{tr}(\sqrt{X^\dagger X})$, which is an alternative to minimizing the rank of X for the quantum state and the l_1-norm for the sparse noise. Therefore, the estimators $\hat{\rho}, \hat{\mathbf{v}}$ are obtained by

$$(\hat{\rho}, \hat{\mathbf{v}}) = \arg\min_{\tilde{\rho} \geq 0, \tilde{\mathbf{v}}} \quad \frac{1}{2}\|\mathbf{y} - \mathcal{M}(\tilde{\rho}) - \tilde{\mathbf{v}}\|_2^2 + \tau_1 \cdot \|\tilde{\rho}\|_{\mathrm{tr}} + \tau_2 \cdot \|\tilde{\mathbf{v}}\|_1, \tau_1, \tau_2 > 0\,. \quad (5)$$

Whenever the trace of the resulting estimate of the quantum state is not equal to 1, we renormalize it as $\hat{\rho}/\mathrm{tr}(\hat{\rho}) \mapsto \hat{\rho}$. To quantify the goodness of the reconstruction, we employ the (squared) fidelity

$$F(\rho, \hat{\rho}) = \left(\mathrm{tr}\sqrt{\sqrt{\hat{\rho}}\rho\sqrt{\hat{\rho}}}\right)^2, \quad (6)$$

and the mean squared error (MSE)

$$T_{\mathrm{MSE}} = \frac{1}{m}\sum_{i=1}^{m}(\mathbf{v}_i - \hat{\mathbf{v}}_i)^2 \quad (7)$$

for the estimators $\hat{\rho}$ and $\hat{\mathbf{v}}$ respectively. Note that sometimes we simplify the fidelity $F(\rho, \hat{\rho})$ by F.

3 Main results

Using Pauli measurements, we numerically simulate the reconstruction of $n = 5$ qubit random states and W states under the corruption of s-sparse statistical noise. In light of the convex characteristic of our problem in Eq. (5), we rely on the CVX package [3] for efficient numerical solutions.

Figure 2 displays the fidelity $F(\rho, \hat{\rho})$ and the MSE T_{MSE} as functions of the number of sampled Pauli operators m (ranging from 64 to 1024 with steps of 64) over 120 runs. For each Pauli operator P_k, we take N $(= 50, 100, 150, 200$ respectively for the four subfigures) copies of the input random states in order to get the estimated value of $\text{tr}(P_k\rho)$. Several features are immediately available.

Under sparse Gaussian noise, the fidelity $F(\rho, \hat{\rho})$ (blue solid curve) improves along with the increasing number of sampled Pauli operators m. For instance, in Fig. 2 (b), the fidelity can quickly reach to ~ 0.987 with $m = 1024$ and $N = 100$. Normally, to obtain the fidelity of $F(\rho, \hat{\rho}) \approx 0.95$, only $m \approx 37.5\%d^2$ measurements are needed. In addition, a large number of samples prove advantageous in enhancing the precision and stability of the reconstruction. In Fig. 2 (a)-(d) with $N = 50, 100, 150,$ and 200, achieving $F(\rho, \hat{\rho}) \approx 0.95$ necessitates $m \approx 640, 384, 320,$ and 256, respectively.

On the other hand, the MSEs T_{MSE} between the reconstructed noise and true noise (red solid curve) are all in the order of 10^{-3} for Fig. 2 (a)-(d) as long as the fidelity of the corresponding reconstructed state reaches the threshold of 0.95. Expectedly, the MSE declines and stabilizes as m and N grow.

Notably, sparse Poisson noise exhibits effects on reconstruction similar to sparse Gaussian noise under specific parameter settings, despite their different probability distributions and statistical characteristics. This reflects the universality of our reconstruction technique to statistical noise, providing further insights for selecting appropriate noise models.

4 Impact and Significance

The rapid advancement of quantum information science hinges on precisely characterizing quantum states and taming underlying noise. Quantum state tomography, playing a pivotal role in quantum system characterization, has seen a surge in diverse techniques over recent years. However, noise, inevitable in any quantum system, often renders the procedure intricate and challenging. Therefore, the reliable characterization of quantum states as well as any potential noise in various quantum systems is crucial for advancing quantum technologies.

Our work highlights several key points:

- We offer a new method for tomography such that the quantum state and structured noise can be reconstructed simultaneously.
- Using incomplete Pauli measurements, our technique can greatly reduce resource consumption in noisy quantum systems and achieve high fidelity.
- Our protocol not only provides a way to diagnose and characterize noise, but also applies to scenarios where measurement data is corrupted by noise.

See Ref. [4] for the arXiv version of this paper.

References

[1] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker and J. Eisert. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.*, 105, 150401, 2010.

[2] S. T. Flammia, D. Gross, Y.-K. Liu and J. Eisert. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators. *New J. Phys.*, 14, 095022, 2012.

[3] M. Grant and S. Boyd. CVX: Matlab software for disci- plined convex programming, version 2.1. http://cvxr. com/cvx, 2014.

[4] M. Ma and J. Shang. Corrupted sensing quantum state tomography. quant-ph/2405.14396, 2024.

Locking and unlocking quantum nonlocality in quantum state discrimination by postmeasurement information

Jinhyeok Heo[1] Donghoon Ha[2] Jeong San Kim[2] *

[1] *Department of Mathematics, Kyung Hee University, Seoul 02447, Republic of Korea*
[2] *Department of Applied Mathematics and Institute of Natural Sciences, Kyung Hee University, Yongin 17104, Republic of Korea*

Abstract. In discriminating quantum states, nonlocality arises when the optimal state discrimination cannot be realized by local operations and classical communication. Recently, it has been found that the postmeasurement information about the prepared subensemble can lock or unlock nonlocality in quantum state discrimination. Here, we show that locking or unlocking nonlocality of quantum state discrimination depends on the choice of postmeasurement information. Furthermore, we provide a method in terms of entanglement witness to construct bipartite quantum state ensembles where locking or unlocking quantum nonlocality arises depending on the choice of subensembles provided by postmeasurement information.

Keywords: quantum state discrimination, postmeasurement information, quantum nonlocality

Quantum nonlocality is an interesting phenomenon in bipartite quantum systems [1–3]. In quantum state discrimination, quantum nonlocality occurs when the optimal state discrimination cannot be realized only by *local operations and classical communication*(LOCC) [4–8].

In discriminating quantum states, quantum nonlocality can be *locked* by the *postmeasurement information*(PI) about the prepared subensemble; there exists a set of bipartite quantum states that cannot be optimally discriminated only by LOCC measurements, but can be optimally discriminated using LOCC measurements when PI about prepared subensemble is available. Similarly, nonlocality in quantum state discrimination can be *unlocked* if optimal state discrimination by global and LOCC measurements can be gapped in the presence of PI [9–12].

Here, we consider bipartite quantum state discrimination, and show that nonlocality of quantum state discrimination can be locked(or unlocked) depending on the choice of subensembles provided by PI. We provide a method to construct quantum state ensembles where locking(or unlocking) nonlocality of state discrimination depends on the choice of subensembles provided by PI.

For a bipartite Hilbert space $\mathcal{H} = \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, let $\mathbb{H}$ be the set of all Hermitian operators acting on $\mathcal{H}$. We denote by $\mathbb{H}_+$ the set of all positive-semidefinite operators in $\mathbb{H}$, that is,

$$\mathbb{H}_+ = \{E \in \mathbb{H} \,|\, \langle v| E |v\rangle \geqslant 0 \ \forall |v\rangle \in \mathcal{H}\}. \tag{1}$$

A bipartite quantum state is described by a density operator ρ, that is, a positive-semidefinite operator $\rho \in \mathbb{H}_+$ with unit trace $\mathrm{Tr}\,\rho = 1$. A measurement is represented by a positive operator-valued measure $\{M_i\}_i$, that is, a set of positive-semidefinite operators $M_i \in \mathbb{H}_+$ satisfying the completeness relation $\sum_i M_i = \mathbb{1}$, where $\mathbb{1}$ is the identity operator in $\mathbb{H}$. For the state ρ, the probability of obtaining the measurement outcome with respect to M_j is $\mathrm{Tr}(\rho M_j)$.

*freddie1@khu.ac.kr

Definition 1 *$E \in \mathbb{H}_+$ is called* separable *if it can be described as*

$$E = \sum_l A_l \otimes B_l, \tag{2}$$

where A_l and B_l are positive-semidefinite operators acting on $\mathbb{C}^{d_A}$ and $\mathbb{C}^{d_B}$ of $\mathcal{H}$, respectively.

We denote the set of all *separable* operators in $\mathbb{H}_+$ as

$$\mathbb{SEP} = \{E \in \mathbb{H}_+ \,|\, E : \text{separable}\}, \tag{3}$$

and its dual set as $\mathbb{SEP}^*$, that is,

$$\mathbb{SEP}^* = \{E \in \mathbb{H} \,|\, \mathrm{Tr}(EF) \geqslant 0 \ \forall F \in \mathbb{SEP}\}. \tag{4}$$

An element in $\mathbb{SEP}^*$ is also called *block positive*.

A measurement $\{M_i\}_i$ is called a *separable measurement* if $M_i \in \mathbb{SEP}$ for all i, and a measurement is called a *LOCC measurement* if it can be realized by LOCC. Note that every LOCC measurement is a separable measurement [13].

Definition 2 *$W \in \mathbb{H}$ is called an* entanglement witness*(EW) if $\mathrm{Tr}(\sigma W) \geqslant 0$ for any state σ in $\mathbb{SEP}$ but $\mathrm{Tr}(\rho W)$ for some state ρ in $\mathbb{H}_+ \setminus \mathbb{SEP}$, or equivalently*

$$W \in \mathbb{SEP}^* \setminus \mathbb{H}_+. \tag{5}$$

Throughout this paper, we only consider the situation of discriminating *bipartite* quantum states from the ensemble of the form,

$$\mathcal{E} = \{\eta_i, \rho_i\}_{i\in\Lambda}, \ \Lambda = \{1, 2, 3, 4\}, \tag{6}$$

where the state ρ_i is prepared with the probability η_i.

For a given two-element subset S of Λ, let us consider the two subensembles,

$$\mathcal{E}_0 = \left\{\frac{\eta_i}{\sum_{j\in\Lambda}\eta_j}, \rho_i\right\}_{i\in S},$$
$$\mathcal{E}_1 = \left\{\frac{\eta_i}{\sum_{j\in\Lambda^c}\eta_j}, \rho_i\right\}_{i\in S^c}, \ S^c = \Lambda \setminus S. \tag{7}$$

For the case that the state ρ_i belongs to $\mathcal{E}_0$ in Eq. (7), we note that the preparation of ρ_i with probability η_i from the ensemble $\mathcal{E}$ is equivalent to the preparation of the subensemble $\mathcal{E}_0$ with probability $\sum_{j\in S}\eta_j$ followed by the preparation of ρ_i from $\mathcal{E}_0$ with probability $\eta_i/\sum_{j\in S}\eta_j$. We denote by PI_S the classical information $b\in\{0,1\}$ about the prepared subensemble $\mathcal{E}_b$ defined in Eq. (7) after performing a measurement, that is

$$\mathrm{PI}_S = \begin{cases} 0, & i\in S, \\ 1, & i\in S^{\mathsf{c}}, \end{cases} \tag{8}$$

where i is the index of the prepared state ρ_i.

Let us consider the quantum state discrimination of $\mathcal{E}$ in Eq. (6) using a measurement $\mathcal{M}=\{M_i\}_{i\in\Lambda}$. Here, the detection of M_i means that the prepared state is guessed to be ρ_i. The *minimum-error discrimination*(ME) of $\mathcal{E}$ is to achieve the optimal success probability,

$$p_{\mathrm{G}}(\mathcal{E}) = \max_{\mathcal{M}} \sum_{i\in\Lambda} \eta_i \,\mathrm{Tr}(\rho_i M_i), \tag{9}$$

where the maximum is taken over all possible measurements [14].

When the available measurements are limited to LOCC measurements, we denote the maximum success probability by

$$p_{\mathrm{L}}(\mathcal{E}) = \max_{\mathrm{LOCC}\,\mathcal{M}} \sum_{i\in\Lambda} \eta_i \,\mathrm{Tr}(\rho_i M_i). \tag{10}$$

Similarly, we denote the maximum success probability over all possible separable measurements as

$$p_{\mathrm{SEP}}(\mathcal{E}) = \max_{\mathrm{Separable}\,\mathcal{M}} \sum_{i\in\Lambda} \eta_i \,\mathrm{Tr}(\rho_i M_i). \tag{11}$$

From the definitions, we have

$$p_{\mathrm{L}}(\mathcal{E}) \leqslant p_{\mathrm{SEP}}(\mathcal{E}) \leqslant p_{\mathrm{G}}(\mathcal{E}). \tag{12}$$

In discriminating the states from the ensemble $\mathcal{E}$, quantum nonlocality occurs if the optimal success probability in Eq. (9) cannot be achieved only by LOCC measurements, that is,

$$p_{\mathrm{L}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E}). \tag{13}$$

From Inequality (12), we can easily see that Inequality (13) holds if

$$p_{\mathrm{SEP}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E}). \tag{14}$$

For an ensemble $\mathcal{E}$ in Eq. (6) and a two-element subset S of Λ, let us consider the situation of discriminating the quantum states from $\mathcal{E}$ when PI_S is given. In this situation, a measurement can be represented by a positive operator-valued measure $\tilde{\mathcal{M}}=\{\tilde{M}_{\vec{\omega}}\}_{\vec{\omega}\in\Omega_S}$ where the outcome space is the Cartesian product,

$$\Omega_S = S\times S^{\mathsf{c}}. \tag{15}$$

Here, the detection of $\tilde{M}_{(\omega_0,\omega_1)}$ means that we guess the prepared state as ρ_{ω_0} or ρ_{ω_1} according to $\mathrm{PI}_S=0$ or 1, respectively [9, 10].

ME of $\mathcal{E}$ with PI_S is to maximize the average probability of correct guessing where the optimal success probability is defined as

$$p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S) = \max_{\tilde{\mathcal{M}}}\Big(\sum_{i\in S}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S^{\mathsf{c}}}\tilde{M}_{(i,j)}\big] + \sum_{i\in S^{\mathsf{c}}}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S}\tilde{M}_{(j,i)}\big]\Big), \tag{16}$$

where the maximum is taken over all possible measurements. Note that when ρ_i is prepared and $\mathrm{PI}_S=b$ is given, the prepared state is correctly guessed if we obtain a measurement outcome $\vec{\omega}\in\Omega_S$ with $\omega_b=i$.

When the available measurements are limited to LOCC measurements, we denote the maximum success probability by

$$p_{\mathrm{L}}^{\mathrm{PI}}(\mathcal{E},S) = \max_{\mathrm{LOCC}\,\tilde{\mathcal{M}}}\Big(\sum_{i\in S}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S^{\mathsf{c}}}\tilde{M}_{(i,j)}\big] + \sum_{i\in S^{\mathsf{c}}}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S}\tilde{M}_{(j,i)}\big]\Big). \tag{17}$$

Similarly, we denote

$$p_{\mathrm{SEP}}^{\mathrm{PI}}(\mathcal{E},S) = \max_{\mathrm{Separable}\,\tilde{\mathcal{M}}}\Big(\sum_{i\in S}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S^{\mathsf{c}}}\tilde{M}_{(i,j)}\big] + \sum_{i\in S^{\mathsf{c}}}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S}\tilde{M}_{(j,i)}\big]\Big), \tag{18}$$

where the maximum is taken over all possible separable measurements. From the definitions, we have

$$p_{\mathrm{L}}^{\mathrm{PI}}(\mathcal{E},S) \leqslant p_{\mathrm{SEP}}^{\mathrm{PI}}(\mathcal{E},S) \leqslant p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S). \tag{19}$$

We note that for a given measurement $\{\tilde{M}_{\vec{\omega}}\}_{\vec{\omega}\in\Omega}$, the success probability, that is, the right-hand side of Eq. (16) without maximization, can be rewritten as

$$\begin{aligned} &\sum_{i\in S}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S^{\mathsf{c}}}\tilde{M}_{(i,j)}\big] + \sum_{i\in S^{\mathsf{c}}}\eta_i \mathrm{Tr}\big[\rho_i \sum_{j\in S}\tilde{M}_{(j,i)}\big] \\ = \;& 2\sum_{\vec{\omega}\in\Omega}\tilde{\eta}_{\vec{\omega}}\mathrm{Tr}(\tilde{\rho}_{\vec{\omega}}\tilde{M}_{\vec{\omega}}), \end{aligned} \tag{20}$$

where

$$\tilde{\eta}_{\vec{\omega}} = \frac{1}{2}\sum_{b\in\{0,1\}}\eta_{w_b},\;\; \tilde{\rho}_{\vec{\omega}} = \frac{\sum_{b\in\{0,1\}}\eta_{w_b}\rho_{\omega_b}}{\sum_{b'\in\{0,1\}}\eta_{w_{b'}}}. \tag{21}$$

Since $\{\tilde{\eta}_{\vec{\omega}}\}_{\vec{\omega}\in\Omega_S}$ and $\{\tilde{\rho}_{\vec{\omega}}\}_{\vec{\omega}\in\Omega_S}$ are a probability distribution and a set of states, respectively, Eq. (20) implies

$$\begin{aligned} p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S) &= 2p_{\mathrm{G}}(\tilde{\mathcal{E}}), \\ p_{\mathrm{L}}^{\mathrm{PI}}(\mathcal{E},S) &= 2p_{\mathrm{L}}(\tilde{\mathcal{E}}), \\ p_{\mathrm{SEP}}^{\mathrm{PI}}(\mathcal{E},S) &= 2p_{\mathrm{SEP}}(\tilde{\mathcal{E}}), \end{aligned} \tag{22}$$

where $\tilde{\mathcal{E}}$ is the ensemble consisting of the average states $\tilde{\rho}_{\vec{\omega}}$ prepared with the probabilities $\tilde{\eta}_{\vec{\omega}}$ in Eq. (21),

$$\tilde{\mathcal{E}} = \{\tilde{\eta}_{\vec{\omega}},\tilde{\rho}_{\vec{\omega}}\}_{\vec{\omega}\in\Omega_S}. \tag{23}$$

In ME of $\mathcal{E}$ with PI_S, quantum nonlocality occurs if the optimal success probability in Eq. (16) cannot be achieved only by LOCC measurements, that is,

$$p_{\mathrm{L}}^{\mathrm{PI}}(\mathcal{E},S) < p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S). \tag{24}$$

From Inequality (19), we can easily verify that Inequality (24) holds if

$$p_{\mathrm{SEP}}^{\mathrm{PI}}(\mathcal{E},S) < p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S). \tag{25}$$

The following theorem provides a sufficient condition for nonlocality in terms of ME with PI.

Theorem 3 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i\in\Lambda}$, a two-element subset S of Λ and $\vec{\mu} \in \Omega_S$,*

$$p_{\mathrm{SEP}}^{\mathrm{PI}}(\mathcal{E},S) = 2\tilde{\eta}_{\vec{\mu}} < p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S) \tag{26}$$

if and only if $\tilde{\eta}_{\vec{\mu}}\tilde{\rho}_{\vec{\mu}} - \tilde{\eta}_{\vec{\omega}}\tilde{\rho}_{\vec{\omega}}$ is block positive for all $\vec{\omega} \in \Omega_S$ and there exists an EW in $\{\tilde{\eta}_{\vec{\mu}}\tilde{\rho}_{\vec{\mu}} - \tilde{\eta}_{\vec{\omega}}\tilde{\rho}_{\vec{\omega}}\}_{\vec{\omega}\in\Omega_S}$.

Definition 4 *For an ensemble $\mathcal{E}$ in Eq. (6) and a two-element subset S of Λ, we say that* PI_S locks *nonlocality if nonlocality occurs in discriminating the states of $\mathcal{E}$ and the availability of* PI_S *vanishes the occurrence of nonlocality, that is,*

$$p_{\mathrm{L}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E}),\ p_{\mathrm{L}}^{\mathrm{PI}}(\mathcal{E},S) = p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S). \tag{27}$$

Also, we say that PI_S unlocks *nonlocality if nonlocality does not occur in discriminating the states of $\mathcal{E}$ and the availability of* PI_S *releases the occurrence of nonlocality, that is,*

$$p_{\mathrm{L}}(\mathcal{E}) = p_{\mathrm{G}}(\mathcal{E}),\ p_{\mathrm{L}}^{\mathrm{PI}}(\mathcal{E},S) < p_{\mathrm{G}}^{\mathrm{PI}}(\mathcal{E},S). \tag{28}$$

The following theorem establishes a sufficient condition for nonlocality arising in discriminating quantum states to be locked depending on the choice of subensembles provided by PI.

Theorem 5 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i\in\Lambda}$, if*

$$\begin{aligned}
&\eta_1\rho_1 - \eta_2\rho_2 \in \mathbb{H}_+,\\
&\eta_1\rho_1 - \eta_3\rho_3 \in \mathbb{SEP}^* \setminus \mathbb{H}_+,\\
&\eta_2\rho_2 - \eta_4\rho_4 \in \mathbb{SEP}^*,\\
&\eta_3\rho_3 - \eta_4\rho_4 \in \mathbb{H}_+,
\end{aligned} \tag{29}$$

then $\mathrm{PI}_{\{1,2\}}$ *locks nonlocality but* $\mathrm{PI}_{\{1,3\}}$ *does not lock nonlocality.*

Now, we provide a method in terms of EW to construct quantum state ensembles where $\mathrm{PI}_{\{1,2\}}$ locks nonlocality but $\mathrm{PI}_{\{1,3\}}$ does not lock nonlocality. For an EW W, let us consider the ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i\in\Lambda}$ consisting of

$$\begin{aligned}
\eta_1 &= \tfrac{\mathrm{Tr}(2W_+ + W_-)}{4\,\mathrm{Tr}(W_+ + W_-)},\ \rho_1 = \tfrac{2W_+ + W_-}{\mathrm{Tr}(2W_+ + W_-)},\\
\eta_2 &= \tfrac{\mathrm{Tr}\, W_+}{4\,\mathrm{Tr}(W_+ + W_-)},\ \rho_2 = \tfrac{W_+}{\mathrm{Tr}\, W_+},\\
\eta_3 &= \tfrac{\mathrm{Tr}(W_+ + 2W_-)}{4\,\mathrm{Tr}(W_+ + W_-)},\ \rho_3 = \tfrac{W_+ + 2W_-}{\mathrm{Tr}(W_+ + 2W_-)},\\
\eta_4 &= \tfrac{\mathrm{Tr}\, W_-}{4\,\mathrm{Tr}(W_+ + W_-)},\ \rho_4 = \tfrac{W_-}{\mathrm{Tr}\, W_-}
\end{aligned} \tag{30}$$

where $W_\pm$ is the positive-semidefinite operator satisfying

$$\mathrm{Tr}(W_+W_-) = 0,\ W = W_+ - W_-. \tag{31}$$

A straightforward calculation leads us to

$$\begin{aligned}
\eta_1\rho_1 - \eta_2\rho_2 = \eta_3\rho_3 - \eta_4\rho_4 &= \tfrac{W_+ + W_-}{4\,\mathrm{Tr}(W_+ + W_-)},\\
\eta_2\rho_2 - \eta_4\rho_4 = \eta_1\rho_1 - \eta_3\rho_3 &= \tfrac{W}{4\,\mathrm{Tr}(W_+ + W_-)},
\end{aligned} \tag{32}$$

which imply Condition (29) in Theorem 5. Thus, $\mathrm{PI}_{\{1,2\}}$ locks nonlocality but $\mathrm{PI}_{\{1,3\}}$ does not lock nonlocality.

The following theorem establishes a sufficient condition for nonlocality arising in discriminating quantum states to be unlocked depending on the choice of subensembles provided by PI.

Theorem 6 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i\in\Lambda}$, if*

$$\begin{aligned}
&\eta_1\rho_1 - \eta_2\rho_2 \in \mathbb{H}_+,\\
&\eta_1\rho_1 - \eta_3\rho_3 \in \mathbb{H}_+,\\
&\eta_2\rho_2 - \eta_4\rho_4 \in \mathbb{H}_+,\\
&\eta_3\rho_3 - \eta_4\rho_4 \in \mathbb{SEP}^* \setminus \mathbb{H}_+,
\end{aligned} \tag{33}$$

then $\mathrm{PI}_{\{1,2\}}$ *unlocks nonlocality but* $\mathrm{PI}_{\{1,3\}}$ *does not unlock nonlocality.*

Now, we provide a method in terms of EW to construct quantum state ensembles where $\mathrm{PI}_{\{1,2\}}$ unlocks nonlocality but $\mathrm{PI}_{\{1,3\}}$ does not unlock nonlocality. For an EW W, let us consider the ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i\in\Lambda}$ consisting of

$$\begin{aligned}
\eta_1 &= \tfrac{\mathrm{Tr}(2W_+ + W_-)}{\mathrm{Tr}(4W_+ + 3W_-)},\ \rho_1 = \tfrac{2W_+ + W_-}{\mathrm{Tr}(2W_+ + W_-)},\\
\eta_2 &= \tfrac{\mathrm{Tr}(W_+ + W_-)}{\mathrm{Tr}(4W_+ + 3W_-)},\ \rho_2 = \tfrac{W_+ + W_-}{\mathrm{Tr}(W_+ + W_-)},\\
\eta_3 &= \tfrac{\mathrm{Tr}\, W_+}{\mathrm{Tr}(4W_+ + 3W_-)},\ \rho_3 = \tfrac{W_+}{\mathrm{Tr}\, W_+},\\
\eta_4 &= \tfrac{\mathrm{Tr}\, W_-}{\mathrm{Tr}(4W_+ + 3W_-)},\ \rho_4 = \tfrac{W_-}{\mathrm{Tr}\, W_-},
\end{aligned} \tag{34}$$

where $W_\pm$ is the positive-semidefinite operator satisfying Eq. (31).

From a straightforward calculation, we can verify that

$$\begin{aligned}
\eta_1\rho_1 - \eta_2\rho_2 &= \tfrac{W_+}{\mathrm{Tr}(4W_+ + 3W_-)},\\
\eta_1\rho_1 - \eta_3\rho_3 &= \tfrac{W_+ + W_-}{\mathrm{Tr}(4W_+ + 3W_-)},\\
\eta_2\rho_2 - \eta_4\rho_4 &= \tfrac{W_-}{\mathrm{Tr}(4W_+ + 3W_-)},\\
\eta_3\rho_3 - \eta_4\rho_4 &= \tfrac{W}{\mathrm{Tr}(4W_+ + 3W_-)},
\end{aligned} \tag{35}$$

which imply Condition (33) in Theorem 6. Thus, $\mathrm{PI}_{\{1,2\}}$ unlocks nonlocality but $\mathrm{PI}_{\{1,3\}}$ does not unlock nonlocality.

References

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[2] A. M. Childs, D. Leung, L. Mancinska, and M. Ozols, A framework for bounding nonlocality of state discrimination, Commun. Math. Phys. **323**, 1121 (2013).

[3] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[4] A. Peres and W. K. Wooters, Optimal Detection of Quantum Information, Phys. Rev. Lett. **66**, 1119 (1991).

[5] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wooters, Quantum nonlocality without entanglement, Phys. Rev. A **59**, 1070 (1999).

[6] S. Ghosh, G. Kar, A. Roy, A. Sen (De), and U. Sen, Distinguishability of Bell States, Phys. Rev. Lett. **87**, 277902 (2001).

[7] E. Chitambar and M.-H. Hsieh, Revisiting the optimal detection of quantum information, Phys. Rev. A **88**, 020302(R) (2013).

[8] E. Chitambar, D. Leung, L. Mancinska, and M. Ozols, and A. Winter, Everything you always wanted to know about LOCC(but were afraid to ask), Commun. Math. Phys. **328**, 303 (2014).

[9] M. A. Ballester, S. Wehner, and A. Winter, State discrimination with post-measurement information, *IEEE Trans. Inf. Theory* **54**, 4183 (2008).

[10] D. Gopal and S. Wehner, Using postmeasurement information in state discrimination, *Phys. Rev. A* **82**, 022326 (2010).

[11] D. Ha and J. S. Kim, Annihilating and creating nonlocality without entanglement by postmeasurement information, Phys. Rev. A **105**, 022422 (2022).

[12] D. Ha and J. S. Kim, Locking and unlocking of quantum nonlocality without entanglement in local discrimination of quantum states, Sci. Rep. **12**, 3961 (2022).

[13] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), Commun. Math. Phys. **328**, 303 (2014).

[14] C. W. Helstrom, Quantum detection and estimation theory, J. Stat. Phys. **1**, 231 (1969).

Extended abstract for "Exploring entanglement spectrum and phase diagram in multi-electron quantum dot chains"

Guanjie He[1] * Xin Wang[1] †

[1] *Department of Physics, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong SAR, China, and City University of Hong Kong Shenzhen Research Institute, Shenzhen, Guangdong 518057, China*

Abstract. We explore the unique entanglement properties of semiconductor quantum dot systems using the extended Hubbard model, focusing on how variations in potential energy and electron interactions affect these systems. By examining a four-site quantum dot spin chain with different electron counts ($N = 4$ and $N = 6$), we discover that adjusting the potential energy in specific dots significantly redistributes electron configurations and alters entanglement properties. Phase diagrams illustrate these findings, revealing how interaction strengths and potential energy adjustments lead to complex entanglement dynamics and phase transitions. Our research provides valuable insights into how quantum dots can be manipulated for advanced quantum information processing, simulation and computation, highlighting their potential for developing robust quantum technologies.

Keywords: Quantum entanglement, Quantum dot systems, Extended Hubbard Model

1 Introduction

Quantum entanglement is crucial in quantum communication and information processing [1, 2], and in condensed matter physics, it is a fundamental criterion for quantum phase transitions and many-body localization [3, 4, 5, 6]. Stable and controllable, semiconductor quantum dots are ideal for simulating many-body systems, particularly Fermi-Hubbard physics [7, 8, 9, 10, 11]. The Fermi-Hubbard model describes quantum dot systems at low temperatures and strong Coulomb interactions, with applications in quantum information processing [12, 13, 14].

We investigate the entanglement patterns of ground states in multi-electron quantum dot systems using the extended Hubbard model (EHM), focusing on one-site and two-site reduced density matrices. Our study reveals that without potential energy differences, the system's entanglement properties align with the EHM in either half-filled or non-half-filled states [15, 16, 17]. Introducing potential energy differences in selected dots leads to distinct phases and phase boundaries in the entanglement spectrum, influenced by coupling strengths and energy differences. These findings highlight the significant impact of local potential modifications on electron configurations and entanglement properties, providing insights into the design of advanced quantum technologies.

2 Extended Hubbard Model

We consider a Multiple-Quantum-Dot system (MQD) (Fig. 1), described by an EHM with short-range Coulomb interactions and tunneling restricted to nearest-neighbor sites within the same energy level and the nearest-neighbor energy level. The Hamiltonian is:

$$\begin{aligned} H = &- \sum_{i,\nu,\overline{\nu},\sigma} (t_\nu c^\dagger_{i,\nu,\sigma} c_{i+1,\nu,\sigma} + t_{\nu,\overline{\nu}} c^\dagger_{i,\nu,\sigma} c_{i+1,\overline{\nu},\sigma} + \text{H.c.}) \\ &+ \sum_{i,\nu,\overline{\nu},\sigma} (V_\nu n_{i,\nu,\sigma} n_{i+1,\nu,\sigma'} + V_{\nu,\overline{\nu}} n_{i,\nu,\sigma} n_{i+1,\overline{\nu},\sigma'} \\ &+ V'_{\nu,\overline{\nu}} n_{i,\nu,\sigma} n_{i,\overline{\nu},\sigma'}) + \sum_{i,\nu} U_\nu n_{i,\nu\downarrow} n_{i,\nu\uparrow} \\ &+ \sum_{i,\sigma} \varepsilon_{i,\sigma} n_{i\sigma}, \end{aligned} \tag{1}$$

where i indicates the quantum dot site, ν and $\overline{\nu}$ denote different orbital levels (g: ground, e: excited), σ and σ' refer to spins ($\uparrow$, $\downarrow$). $\varepsilon_{i,\sigma}$ is the potential energy, t_ν and $t_{\nu,\overline{\nu}}$ are the tunneling energies, U_ν is the on-site Coulomb interaction, V_ν, $V_{\nu,\overline{\nu}}$, and $V'_{\nu,\overline{\nu}}$ are the nearest Coulomb interactions. The Hilbert space dimension for an L-site MQD chain with K orbitals per site is 4^{LK}. The configuration basis states are $|v_1, v_2, ..., v_L\rangle = \prod_{i=1}^{L} |v_i\rangle_i$, where $|v_i\rangle_i = \prod_{\nu=1}^{K} |v\rangle_{i,\nu}$ represents the i-th site basis. We study N and $N+2$ electrons in $L = N$ sites systems, restricting to the ground and first excited orbitals ($\nu = g, e$) per quantum dot.

3 Reduced density matrices and Entanglement

We first obtain the ground state (GS) $|\psi_{\text{GS}}\rangle$ by diagonalizing the Hamiltonian. The GS is a linear superposition of electron configuration basis states $|\psi_m\rangle$: $|\psi_{\text{GS}}\rangle = \sum_m c_m |\psi_m\rangle$, where c_m are the coefficients. The density matrix ρ_{GS} is: $\rho_{\text{GS}} = \sum_m P_m |\psi_m\rangle\langle\psi_m|$. The reduced density matrix ρ_A for subsystem A is: $\rho_A = \text{Tr}_B \rho_{\text{GS}}$. The von Neumann entropy $E(\rho_A)$ measures the entanglement: $E(\rho_A) = -\text{Tr}(\rho_A \log_2 \rho_A)$.

*guanjiehe2-c@my.cityu.edu.hk
†x.wang@cityu.edu.hk

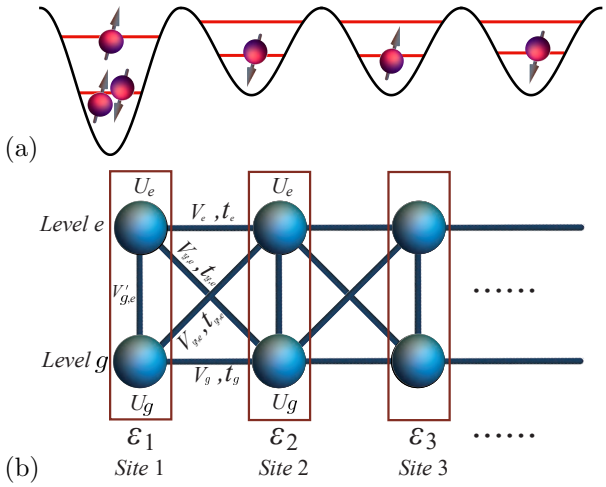


Figure 1: (a) Four-site quantum dot spin chain with six electrons. (b) Hubbard model with detuning energy ε_i for each site i.

3.1 Local Entanglement of multi-electron quantum dot

We focus on GaAs QD. In GaAs QD, electrons prefer to doubly occupy ground states before filling the first excited states. The state space of a single site is spanned by nine bases: $\{|0,0\rangle, |\uparrow_g,0\rangle, |\downarrow_g,0\rangle, |\uparrow_g\downarrow_g,0\rangle, |\uparrow_g,\downarrow_e\rangle, |\downarrow_g,\uparrow_e\rangle, |\uparrow_g\downarrow_g,\uparrow_e\rangle, |\uparrow_g\downarrow_g,\downarrow_e\rangle, |\uparrow_g\downarrow_g,\uparrow_e\downarrow_e\rangle\}$. The one-site reduced density matrix for site i is: $\rho_i = \mathrm{Tr}_i(\rho_{\mathrm{GS}})$. Expressing in terms of basis, ρ_i is a 9×9 matrix. For the four-site system, local bipartite entanglement can be analyzed as $E(\rho_1)$, $E(\rho_2)$, $E(\rho_3)$, and $E(\rho_4)$.

3.2 Pairwise Entanglement of multi-electron quantum dot

For sites i and j, the two-site reduced density matrix is: $\rho_{ij} = \mathrm{Tr}_{ij}(\rho_{\mathrm{GS}})$. With $9^2 = 81$ possible configurations, ρ_{ij} is an 81×81 matrix. Dropping two energetically unfavorable bases, ρ_{ij} is a 49×49 matrix. Pairwise bipartite entanglement can be analyzed as $E(\rho_{12})$ and $E(\rho_{34})$, $E(\rho_{13})$ and $E(\rho_{24})$, $E(\rho_{14})$ and $E(\rho_{23})$.

4 Results

In our GaAs quantum dots system, we set parameters such that tunneling and Coulomb interactions vary with orbital levels: $t_e < t_{g,e} < t_g$, $U_g < V'_{g,e} < U_e$, and $V_g < V_{g,e} < V_e$. We analyze two cases: $U_g > 2V_g$ (charge density wave) and $U_g < 2V_g$ (spin density wave). Parameters: $V_g = \alpha U_g$, $V_{g,e} = \alpha V'_{g,e}$, $V_e = \alpha U_e$, $V'_{g,e} = 1.5U_g$, $U_e = 2U_g$, $t_e = 0.3t_g$, $t_{g,e} = 0.6t_g$, with $\alpha = 0.2$ or 0.7. All results shown in Fig. 2

4.1 Entanglement Analysis for $\varepsilon_1 = 0$

The local entanglement analysis for a four-site quantum dot system ($L = 4$) with $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = 0$ examines both $N = 4$ and $N = 6$ electron configurations under coupling strengths $\alpha = 0.2$ and $\alpha = 0.7$. For $N = 4$ and $\alpha = 0.2$, end sites exhibit lower local entanglement than middle sites due to single occupancy preference, with configurations such as $|\uparrow_g,\downarrow_g,\uparrow_g,\downarrow_g\rangle$ dominating as U increases. For $\alpha = 0.7$, double occupancy becomes favorable, leading to configurations like $|\uparrow_g\downarrow_g,0,\uparrow_g,\downarrow_g\rangle$. In the $N = 6$ case, the system shows different behaviors: at $\alpha = 0.2$, configurations with two extra electrons significantly influence entanglement values, and as U increases, end sites favor double occupancy, resulting in rapid entanglement decrease. For $\alpha = 0.7$, double occupancy is more pronounced, causing distinct entanglement behavior changes. Pairwise entanglement in the same system, with all sites having equal potential energy, shows symmetrical relations $\rho_{12} = \rho_{34}$ and $\rho_{13} = \rho_{24}$, and $\rho_{14} = \rho_{23}$ due to finite size effects. At $N = 4$ and $\alpha = 0.2$, pairwise entanglement aligns with theoretical predictions for non-interacting systems, while for $\alpha = 0.7$, strong coupling regimes reveal balanced entanglement levels across different site pairs due to preferred electron configurations. For $N = 6$, uneven electron distribution leads to increased entanglement, with rapid declines in configurations favoring double occupancy as U increases, especially for $\alpha = 0.7$.

4.2 Entanglement Analysis for $\varepsilon_1 \neq 0$

The entanglement analysis for a quantum dot system with $N = 4$ electrons and non-zero potential energy ε_1 reveals significant variations in entanglement behavior influenced by coupling strength ratio α, interaction strength U, and potential energy ε_1. For $\alpha = 0.2$ and $\alpha = 0.7$, the local and pairwise entanglement measures, $E(\rho_i)$ and $E(\rho_{ij})$, respectively, are studied across different regimes. In weak coupling regimes, potential energy variations lead to distinct transitions in electron occupancy configurations, significantly altering entanglement values. For example, positive ε_1 values generally cause a decline in local entanglement due to electron dispersion, while negative ε_1 values localize electrons, reducing entanglement. As U increases, systems tend toward specific electron configurations, such as $|\bullet,\bullet,\bullet,\bullet\rangle$ for strong coupling, where entanglement measures stabilize, $\bullet$ represents one electron. For $N = 6$, similar trends are observed with additional complexity due to the imbalance in electron configurations, requiring consideration of multiple occupancy states, especially in strong coupling regimes where specific configurations like $|\bullet\bullet,\bullet,\bullet,\bullet\bullet\rangle$ dominate, leading to distinctive entanglement profiles based on ε_1 and α, $\bullet\bullet$ represent two electrons. More details are in the main text.

5 Conclusions

This study systematically explores the entanglement properties of semiconductor quantum dots within a multi-site lattice using the Extended Hubbard Model (EHM). Our findings reveal that local and pairwise entanglement measures are highly sensitive to the interplay between Coulomb interactions and tunneling effects, influenced by electronic configurations and external potential energy variations. We observed distinct phase transitions in entanglement characteristics, heavily influenced by coupling strength ratios and potential energy changes.

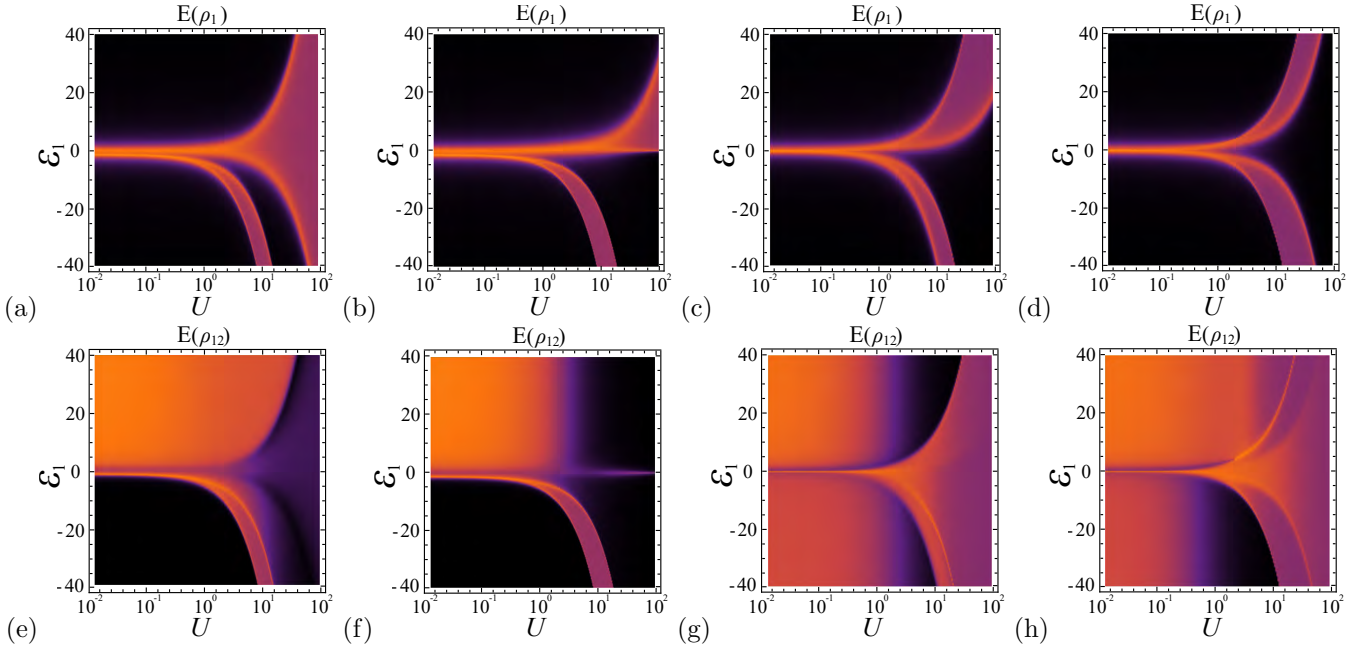


Figure 2: Local entanglement measures $E(\rho_1)$ from (e) to (h), pairwise entanglement measures $E(\rho_{12})$ from(a) to (d). (a) and (e)$N = 4$, $\alpha = 0.2$. (b) and (f)$N = 4$, $\alpha = 0.7$. (c) and (g)$N = 6$, $\alpha = 0.2$. (d) and (h)$N = 6$, $\alpha = 0.7$.

Modifying the potential energy of a specific dot significantly alters ground state configurations and entanglement measures, especially in both weak and strong coupling regimes, suggesting that potential energy adjustments can effectively control entanglement in quantum dot systems.

References

[1] Samuel L. Braunstein et al. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77(2):513–577, 2005.

[2] Sanaa Abaach et al. Long distance entanglement and high-dimensional quantum teleportation in the Fermi–Hubbard model. *Scientific Reports*, 13(1):964, 2023.

[3] Luigi Amico et al. Entanglement in many-body systems. *Rev. Mod. Phys.*, 80(2):517–576, 2008.

[4] M. Schulz et al. Stark Many-Body Localization. *Phys. Rev. Lett.*, 122(4):040606, 2019.

[5] Shankar Iyer et al. Many-body localization in a quasiperiodic system. *Phys. Rev. B*, 87(13):134202, 2013.

[6] Arijeet Pal et al. Many-body localization phase transition. *Phys. Rev. B*, 82(17):174411, 2010.

[7] Federico Fedele et al. Simultaneous Operations in a Two-Dimensional Array of Singlet-Triplet Qubits. *PRX Quantum*, 2(4):040306, 2021.

[8] Justyna P. Zwolak et al. Colloquium: Advances in automation of quantum dot devices control. *Rev. Mod. Phys.*, 95(1):011006, 2023.

[9] M. D. Reed et al. Reduced Sensitivity to Charge Noise in Semiconductor Spin Qubits via Symmetric Operation. *Phys. Rev. Lett.*, 116(11):110402, 2016.

[10] MengKe Feng et al. Control of dephasing in spin qubits during coherent transport in silicon. *Phys. Rev. B*, 107(8):085427, 2023.

[11] Zhan Shi et al. Fast Hybrid Silicon Double-Quantum-Dot Qubit. *Phys. Rev. Lett.*, 108(14):140503, 2012.

[12] Xin Wang et al. Quantum theory of the charge-stability diagram of semiconductor double-quantum-dot systems. *Phys. Rev. B*, 84(11):115301, 2011.

[13] S. Das Sarma et al. Hubbard model description of silicon spin qubits: Charge stability diagram and tunnel coupling in Si double quantum dots. *Phys. Rev. B*, 83(23):235314, 2011.

[14] Shuo Yang et al. Generic Hubbard model description of semiconductor quantum-dot spin qubits. *Phys. Rev. B*, 83(16):161301, 2011.

[15] Alberto Anfossi et al. Entanglement in extended Hubbard models and quantum phase transitions. *Phys. Rev. B*, 75(16):165106, 2007.

[16] Shi-Jian Gu et al. Entanglement and Quantum Phase Transition in the Extended Hubbard Model. *Phys. Rev. Lett.*, 93(8):086402, 2004.

[17] Sanaa Abaach et al. Long-range entanglement in quantum dots with Fermi-Hubbard physics. *Phys. Rev. A*, 106(2):022421, 2022.

Estimation of photon number distribution of photon-pair sources

Sang Min Lee[1] *

[1]*Korea Research Institute of Standards and Science*

Abstract. In quantum information experiments based on photon-pair sources, the upper limit of the experimental qualities is determined by the light source, especially the photon number distribution. Therefore, it is important to accurately evaluate the photon number distribution of the light source and the derived characteristics such as pair generation rate, heralding efficiency, and second-order correlation function. In this presentation, we will discuss how to accurately measure the photon number distribution of light sources with very low average photon number, such as photon pair sources, and the uncertainties of the derived characteristics through repeated simulations and bootstrapped experimental data.

Keywords: Estimation of photon number distribution, Charateristics of photon-pair source.

Photon pairs generated via spontaneous parametric down-conversion (SPDC) or spontaneous four wave mixing (SFWM) are primarily used as (heralded) single-photon sources and entangled photon-pair sources, which are the main resources of optical experiments on quantum information processing. Most photon-pair sources (PPSs) have spectral correlations and use bandpass filters (BPFs) to remove them. However, with BPFs, the main characteristics of the PPS such as (single or coincident) count rate, heralding efficiency, and the value of the second-order correlation function are changed. Typically, the use of BPFs increases photon indistinguishabilities but reduces count rates and heralding efficiencies. In this way, the main characteristics of PPSs change due to the effects of filtering or loss of optical elements frequently used in experiments, but these are fundamentally secondary phenomena caused by changes in the photon number distribution (PND).

In this presentation, we first theoretically describe the PND of a PPS under ideal circumstances and then the changes in the PND under conditions of spectral/spatial filtering and losses. In particular, in the process of calculating the probability of two-pair events, we derive an analytic expression for the number of effective modes of the joint spectral density, which is the first to our knowledge.

We also describe the characteristics of PPSs, such as pair generation probability, heralding efficiency, and second-order correlation functions, based on the PND. Since the characteristics of PPSs are related to the PND, they are also affected by photon counting errors (noise) in measurement setups. Therefore, we assume the most commonly used measurement settings and describe changes in photon counting results due to noise. Then we analyze the effect of noise on previous methods of estimating the second-order correlation functions using photon counting rates. The results show that, in general, as noise increases, the estimated values of the second-order correlation functions approach 1. It is also discussed that even in the absence of noise, previous methods based on counting rates may generally overestimate the second-order correlation functions for heralded single photons.

Since the characteristics of a PPS are determined by the PND and influenced by noise, accurately estimating the PND by considering (or removing) the influence of noise is equivalent to accurately estimating the characteristics of the PPS. So, we present an improved method for estimating the PND of PPSs that eliminates noise effects and achieves higher accuracy than previous methods. The improved accuracy of our methodology is indirectly confirmed through simulation results for a single-partite PPS, and a qualitative explanation is provided. Additionally, to further clarify the accuracy of the estimated PND, we use a more appropriate metric instead of the previously used fidelity. In the case of a PPS, the probability of no photon is close to 1, so the fidelity between the true and estimated PND is close to 1 no matter how large the differences in other probabilities are. Together with the simulation results of the PND of a PPS, the uncertainties (for 100 repetitions) and errors (from noise) of the estimated values of the second-order correlation functions are also discussed in comparison with previous methods (based on counting rates).

Finally, we report and analyze experimental results obtained by applying different combinations of BPFs to a PPS coupled with single-mode fibers (SMFs) based on SPDC. Unlike in simulations, since the true values of the characteristics are not known in experiments, only the uncertainties are evaluated by applying the bootstrapping method to the experimental data, for the reason that this method removes the need for repeated experiments to evaluate uncertainty. For example, in challenging situations where the counting rates are very low, such as PPSs based on ultra-thin materials, a single experiment takes a long time and repeat experiments are difficult, making it natural to obtain uncertainties through resampling (bootstrapping) of the experimental data. Detailed theoretical calculation procedures and experimental conditions are covered in [1].

References

[1] Sang Min Lee. Estimation of photon number distribution and derivative characteristics of photon-pair sources. arXiv:2309.04217.

*samini@kriss.re.kr

Harvesting hardware power to foster variational quantum algorithms

Daniil Rabinovich[1,2] * Soumik Adhikary[3] † Ernesto Campos[2] Alexey Uvarov[4]
Olga Lakhmanskaya[1] Kirill Lakhmanskiy[1]

[1]*Russian Quantum Center, Skolkovo, Moscow, Russian Federation*
[2]*Skolkovo Institute of Science and Technology, Moscow, Russian Federation*
[3]*Centre for quantum technologies, National university of Singapore, Singapore*
[4]*Department of Physical and Environmental Sciences, University of Toronto Scarborough, Toronto, Canada*

Abstract. Variational Quantum Algorithms (VQAs) have become critical for utilizing Noisy Intermediate Scale Quantum (NISQ) devices. Nevertheless, these algorithms are still known to suffer from stochastic noise and gate errors. This work proposes hardware-inspired modifications to improve VQA performance on NISQ devices. We introduce a version of the Quantum Approximate Optimization Algorithm (QAOA) for ion-based quantum computers, leveraging native multi-qubit interactions to reduce the number of gates in the circuit. Additionally, a hardware-inspired Zero Noise Extrapolation (ZNE) technique is proposed to estimate noiseless expectation values from noisy circuits. These strategies promise a performance improvement for quantum algorithms on NISQ hardware.

Keywords: Variational Quantum Algorithms, QAOA, Optimization, NISQ devices, Zero Noise Extrapolation

Variational Quantum Algorithms (VQA) have become a de-facto model of quantum computation for today's Noisy Intermediate Scale Quantum (NISQ) devices. In this approach a short depth parameterized quantum circuit is tuned using a classical co-processor, in an attempt to minimize a given cost function, encoded as a problem Hamiltonian. While these variational algorithm can alleviate certain limitations of NISQ devises, they are still prone to stochastic noise and gate errors.

In the present work we propose hardware inspired strategies and modifications to the existing variational algorithms, thus ensuring efficient implementation on NISQ devices. First, we propose [1] a modification of the so called Quantum Approximate Optimization Algorithm (QAOA)[2]—a type of VQA designed to solve combinatorial problems—tailored to ion based quantum computers. In our implementation we employ native multiqubit interaction in order to minimize certain problem Hamiltonians, not native to the hardware considered. We simplify algorithm execution by avoiding the gate based approach, and demonstrate performance improvement in terms of lower resources (circuit depth) required to minimize the instances. Second, motivated by inhomogeneities in the errors of entangling gates between different pairs of qubits in NISQ devices, we propose a hardware inspired Zero Noise Extrapolation (ZNE) technique [3]. By considering different abstract-to-physical qubit mappings, this approach allows to approximate noiseless expectation values, using energies measured from noisy circuits. We demonstrate that the ZNE recovered energy can be orders of magnitude closer to the noiseless expectation value, than energies measured from any of the noisy circuits.

Traditional QAOA ansatz. Traditional QAOA makes use of an ansatz state

$$|\Psi_p(\boldsymbol{\beta},\boldsymbol{\gamma})\rangle = \Big(\prod_{k=1}^{p} e^{-i\beta_k H_x} e^{-i\gamma_k H_P}\Big)\,|+\rangle^{\otimes n}, \quad (1)$$

where $H_x = \sum_{k=1}^{n} X_k$. The ground state of H_P is then prepared by tuning $2p$ parameters β, γ variationally following the minimization $\min_{\beta,\gamma} \langle\Psi_p(\beta,\gamma|\, H_P\, |\Psi_p(\beta,\gamma\rangle$. An evident problem of traditional gate based implementation of (1) is that propagator $e^{-i\gamma_k H_P}$, which typically has no efficient implementation, has to be decomposed into a sequence of single and two qubit gates. This, together with potentially large depth of the circuit p, required to minimize H_P, can translate into large gate counts, which can fall out of the capabilities of NISQ devices.

Ion native QAOA ansatz. To circumvent the realization of propagator $e^{-i\gamma_k H_P}$ in (1), we replace it with a propagator of the tunable Hamiltonian

$$H_I = \frac{1}{2}\sum_{j\neq k} J_{jk} X_j X_k, \quad J_{jk} \approx \frac{J_{\max} A_j A_k}{|j-k|^{\alpha}}, \quad (2)$$

which can natively be realized in an ion based quantum computer. Here j and k indicate positions of ions in a chain and A_j are proportional to Rabi frequencies of oscillations induced for jth ion. Thus, we develop an ansatz

$$|\Psi_p(\beta,\gamma\rangle = \\ = \prod_{k=1}^{p} \exp(-i\beta_k \mathcal{H}_x)\mathrm{H}_+\Big(\exp(-i\gamma_k \mathcal{H}_I)\Big)\mathrm{H}_+^{\dagger}\,|+\rangle^{\otimes n}, \quad (3)$$

where $\mathrm{H}_+ = (|+\rangle\langle 0| + |-\rangle\langle 1|)^{\otimes n}$, and use it to minimize a problem H_P. We benchmark this algorithm by minimizing instances of $n = 6$ qubit Sherrington-Kirkpatrick

*daniilrabinovich.quant@gmail.com
†soumik@nus.edu.sg

(SK) Hamiltonian

$$H_P = \frac{1}{2}\sum_{j\neq k} K_{jk} Z_j Z_k, \quad K_{jk} \in \{1, -1\} \tag{4}$$

with respect to the ansatz (3). We exhaustivelly solve all SK instances and study the fraction of instances that got solved at each respective depth for various configurations of A_j. The results are demonstrated in figure 1. Here the

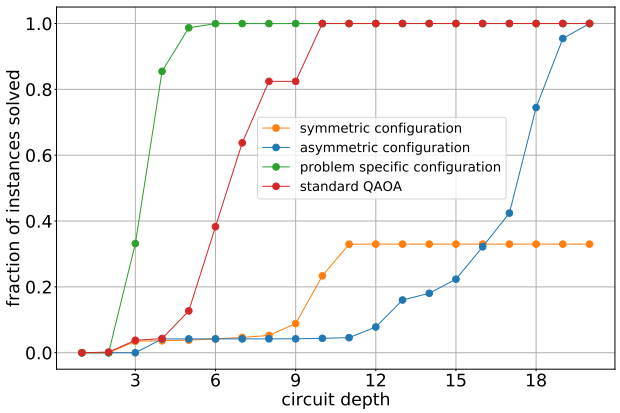


Figure 1: Fraction of $n = 6$ qubit SK instances that could be minimized by the proposed QAOA ansatz.

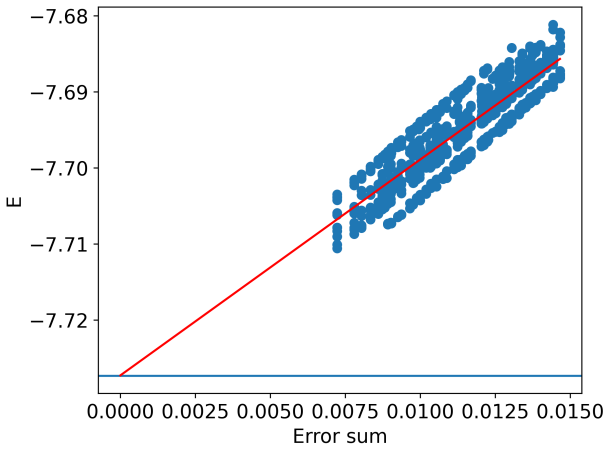
orange curve shows the results for the symmetric configuration $A_j = 1$ in (2) for all ions. The fraction of instances solved saturates due to symmetry protection, induced by symmetric configuration. The blue curve shows a typical result for a specific fixed non-symmetric configuration. It is seen that the fraction of instances solved slowly increases and reaches 100% at depth $p = 20$. Moreover, if we do not keep the same values of A_j for all the instances, but take a best possible configuration (out of 50 random ones) for each instance, already by depth $p = 6$ all the instances can get solved (green curve). This result even exceeds the performance of standard QAOA, which requires depth up to $p = 10$ to solve all the instances (red curve).

Zero noise extrapolation. In alternative scenarios, where the gate based approach is unavoidable, certain error mitigating techniques become necessary. Here we propose a hardware inspired ZNE technique, which allows to reconstruct noiseless VQE energy from noisy expectation values.

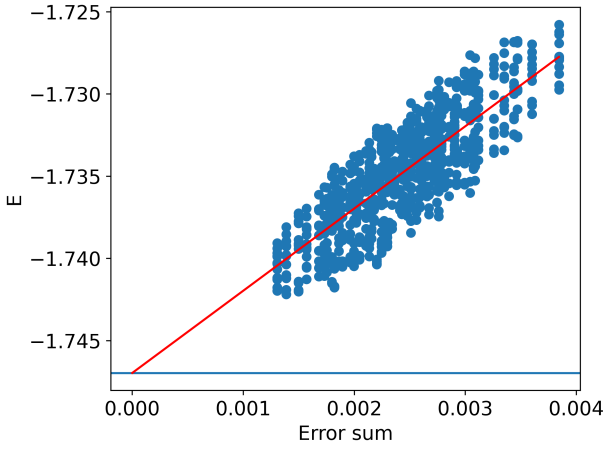
To simulate a noisy circuit, we assume that every two-qubit gate is followed by a noisy channel of strength q_{ij}, which transforms quantum state as $\rho \to (1 - q_{ij})\rho + q_{ij}\mathcal{E}(\rho)$. Here noise strength q_{ij} depends on the pair of physical qubits (i, j), to which the gate is applied. In that case the energy of the state, prepared by noisy circuit can be written as

$$E = E_{noiseless} + \sum_{gates} q_{ij} E_{ij} + O(q^2) = E_{noiseless} + \langle E\rangle \sum_{gates} q_{ij} + \sum_{gates} q_{ij}(E_{ij} - \langle E\rangle) + O(q^2), \tag{5}$$

where energies E_{ij} are expectations of the problem Hamiltonian in the state, where only one gate gets perturbed. Importantly, in practical realities the errors q_{ij} depend on the pair of physical qubits the gate is applied to. Therefore, the sum over gates $\sum_{gates} q_{ij}$ depends on the abstract to physical qubit mapping. Thus, by changing this mapping, one can control this error sum of the circuit, allowing to perform ZNE. To test this proposal in our work we perform VQE for different types of Hamiltonians, introduce noise to the gates, calculate energy for different qubit permutations and perform linear extrapolation of data. The results are summarized in figure 2.



(a)



(b)

Figure 2: Zero noise extrapolation performed over all permutations for $n = 6$ qubit transverse field Ising Hamiltonian (a) and water molecule Hamiltonian (b). Blue dots represent energy E as per (5) for different qubit permutations and the red line is a linear fit taken over energies corresponding to all possible permutations. The blue horizontal lines show the noiseless VQE energy.

It can be seen that the proposed ZNE protocol indeed allows to recover noiseless VQE energy with a good precision, surpassing energies even of the least noisy circuits. The similar results were obtained for various noise

channels $\mathcal{E}$, error distributions $\{q_{ij}\}$ and problem sizes, demonstrating potential of the proposed technique.

Conclusion. Variational quantum algorithms, while being promising for NISQ devises, still suffer from hardware imperfections. Nevertheless, in certain algorithms the effect of noise can be reduced by employing the system's native Hamiltonian and bypassing the gate model completely. Moreover, even when gate errors are unavoidable, their inhomogeneity can be used to foster the algorithm performance by performing Zero Noise Extrapolation over different abstract to physical qubit mappings. Both proposed strategies can assist quantum algorithms, promising performance improvement even in the era of NISQ devices.

Acknowledgements. This work was supported by Rosatom in the framework of the Roadmap for Quantum computing (Contract No. 868-1.3-15/15-2021 dated October 5, 2021)

References

[1] Daniil Rabinovich, Soumik Adhikary, Ernesto Campos, Vishwanathan Akshay, Evgeny Anikin, Richik Sengupta, Olga Lakhmanskaya, Kirill Lakhmanskiy, and Jacob Biamonte. Ion-native variational ansatz for quantum approximate optimization. *Phys. Rev. A*, 106:032418, 2022.

[2] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

[3] Alexey Uvarov, Daniil Rabinovich, Olga Lakhmanskaya, Kirill Lakhmanskiy, Jacob Biamonte, and Soumik Adhikary. Mitigating quantum gate errors for variational eigensolvers using hardware-inspired zero-noise extrapolation. *Phys. Rev. A*, 110:012404, Jul 2024.

How to Certify Deletion with Constant-Length Verification Key

XU Duo[1] *

[1] *Graduate School of Informatics, Nagoya University*

Abstract. The certified deletion process involves transmitting a ciphertext and confirming its deletion via a digital certificate. In this context, the term "deletion" refers to the fact that no information-processing procedure can decipher the cyphertext if the certificate is valid. We proposed a method for Certified Deletion that requires only $O(\lambda)$ bit of verification key, while all the prior works require at least $O(\lambda n)$ bit of verification key. We are the first to attempt to reduce the key's length to reduce storage costs and key leakage risks.

Keywords: Quantum Cryptography, Certified Deletion, One-way Function

1 Introduction

1.1 Background

Cryptography with Certified Deletion is proposed first by Broadbent and Islam [5]. It is divided into two phases by the deletion. In the first phase, a ciphertext is sent, and it is computationally secure, which means a polynomial time algorithm is unable to read the plaintext, but an unbounded time algorithm is able. After a successful deletion, let us move on to the second phase. The ciphertext is information-theoretically deleted, which means even an unbounded time algorithm cannot recover the plaintext.

Nowadays, files are usually encrypted and stored in cloud storage. One may want to delete them from the server, and Certified Deletion provides a certificate to ensure deletion is complete. Recall that the protocol must remain computationally secure during the execution, so the decryption key cannot be distributed in advance, naturally giving rise to the following question.

Where else can certified deletion be useful?

In [10], a commitment with certified deletion is proposed and succeeded in building zero-knowledge proof (ZKP) with certified deletion. ZKP is a protocol that consists of a verifier and a prover. Zero-knowledge (ZK) means that the prover convinces the verifier of a statement without providing any information other than the truth of that statement [8]. However, ZKP is only considered ZK against polynomial-time verifiers for NP-complete problems and QMA-complete problems [6, 14]. By leveraging certified deletion, witnesses are deleted after the execution of the protocol, and the protocol becomes ZK even against unbounded adversaries. In addition to their work on commitment and ZKP, the authors of [10] proposed public-key and attribute-based encryption (ABE) with certified deletion [9], as well as functional encryption (FE) with certified deletion in [18]. Furthermore, [16] introduced fully homomorphic encryption (FHE) with certified deletion. FHE, FE, and ABE enable a receiver owning the ciphertext to process information without decryption.

*xu.duo.x3@s.mail.nagoya-u.ac.jp

Table 1: Comparison between the prior works and our result. n stands for the length of the plaintext.

Methods	Verification Key	Key Length
BK23 [2]	Private Key	$O(\lambda n)$
BKMPW23 [3]	Public Key	$O(\lambda n)$
This paper	Private Key	$O(\lambda)$

There are also researches implementing a generic compiler to add the certified deletion property to a range of protocols. They are called "Certified Everlasting Lemma" in [12] and we will also adopt the name in this manuscript. In [2], public-key encryption, ABE, witness encryption, timed-release encryption, and statistically-binding commitment with certified deletion are proposed. Their method uses a private key as the verification key to verify if a certificate of deletion is valid. In [3, 12], a method utilizing a public key as the verification key is proposed. The three methods [2, 3, 12] introduced here use weaker assumptions than those of prior works such as [9, 10, 16]. [2] requires no additional computational assumptions, and [3] requires only cryptographic primitives with one-wayness which is considered minimal. For example, one-way functions, one-way state generators [15], e.g.

It may be hard to imagine under what circumstances a polynomial-time adversary will become unbounded. Here are a few possible scenarios. Firstly, the encryption scheme may be broken due to a breakthrough in algorithms. The hardness of factoring, which was thought unbreakable but got broken by Shor's algorithm [17], is a good example. A second scenario is the leakage of a secret key used in the protocol. Certified deletion makes it sufficient to design a currently secure protocol without worrying about being broken in the future.

1.2 Our Results

We proposed a method whose verification key does not grow with the plaintext's length to realize Certified Deletion for a range of protocols. In contrast, all the prior works require a verification key growing in proportion to the length of plaintexts [2,3]. Our method has asymptotically shorter verification keys than theirs. In table 1, our

method is compared with the prior researches. Also, we believe that we introduced a new direction for researches about Certified Deletion: shortening the verification key. The method is detailed in section 3.

2 Preliminaries

2.1 Cryptography

QPT QPT is short for Quantum Polynomial Time. For the sake of simplicity, readers can consider it as Polynomial Time. In the rest of this article, QPT adversary and QPT algorithm will be used interchangeably.

security parameter λ stands for security parameters if without additional explanation and indicates how secure the protocol is. Usually, the chance of a QPT adversary breaking the protocol will decrease exponentially in λ.

poly(λ) Stands for all polynomial functions such as $\lambda^{1/2}, \lambda, \lambda^2$, etc. It is used with the same nuance as that for big O notation. For example, $1/2 + \text{poly}(\lambda)$ and a single poly(λ).

negl(λ) Usually write negl(λ) to represent some functions that become negligible in λ. It is the same as the big O notation, and we will write $f(\lambda) = \text{negl}(\lambda)$, which means

$$\forall p(\lambda) = \text{poly}(\lambda), \exists x', \forall \lambda' \geq x', |f(\lambda')| \leq 1/p(\lambda')$$

Also, $1/2 + \text{negl}(\lambda)$ and a single negl(λ) will be used with the same nuance as that for big O notation.

trace distance $\text{TD}(\rho, \sigma)$ is the trace distance between distributions ρ and σ. Consider a game as follows. Draw a sample from ρ or σ, and guess whether it is from ρ or σ. The optimal probability to make a correct guess is exactly $\frac{1}{2} + \frac{1}{2}\text{TD}(\rho, \sigma)$ [11]. Note that quantum states can be considered as distributions, thus trace distance can be defined between two quantum states.

OWF and PRF One-way functions are polynomial-time computable functions that, on the output given, are hard to compute the input. Formally, f is a one-way function (OWF) if and only if the following holds for any QPT algorithm A^λ:

$$\Pr_x[y = f(x') | x' \leftarrow A^\lambda(y), y \coloneqq f(x)] = \text{negl}(\lambda)$$

Also, it is well known that pseudo-random function (PRF) is equivalent to OWF [7, 20]. PRF is a collection of functions $\{g_k\}$ defined by the following equation, in which A^f and A^{g_k} are any QPT algorithms calling f and g_k as oracles.

$$|\Pr_f[A^f(1^\lambda) = 1] - \Pr_k[A^{g_k}(1^\lambda) = 1]| = \text{negl}(\lambda)$$

The left side of the above equation is the trace distance between outputs of $A^f(1^\lambda)$ and $A^{g_k}(1^\lambda)$. Thus, no QPT algorithm can distinguish a PRF and a random function with a non-negligible probability larger than 1/2.

3 Main Result

First we describe our theorem in the table.

Theorem 1 *Let $\{Z^\lambda(\cdot,\cdot)\}_{\lambda\in\mathbb{N}}$ be a sequence of (quantum) processes referenced by λ. The first argument is a poly(λ)-bit string to which the semantic security holds (Equation 1). The second argument of $Z^\lambda(\cdot,\cdot)$ is an arbitrary quantum register.*

$$\forall m \in \{0,1\}^{poly(\lambda)}, |\Pr_{A^\lambda}[A^\lambda(Z^\lambda(m, \mathcal{A})) = 1] - \Pr_{A^\lambda}[A^\lambda(Z^\lambda(0^{poly(\lambda)}, \mathcal{A})) = 1]| = \text{negl}(\lambda) \quad (1)$$

Let us define the distribution $\tilde{Z}^\lambda(m)$ for any adversary B^λ. Fix a collection of PRFs $\{g_k\}_{k\in\{0,1\}^\lambda}$ and consider an experiment as follows.

1. *Sample a $k \in \{0,1\}^\lambda$ uniformly. Compute $x_{i,0} \coloneqq g_k(2i)$ and $x_{i,1} \coloneqq g_k(2i+1)$ for ith bit of m. Prepare $\frac{1}{\sqrt{2}}(|x_{i,0}\rangle + (-1)^{m_i}|x_{i,1}\rangle)$ in registers $\mathcal{B}_i$ respectively.*
2. *Use $Z^\lambda(k, (\mathcal{B}_1, \mathcal{B}_2 \dots \mathcal{B}_n))$ as input of algorithm B^λ and run the algorithm.*
3. *Parse the output as n strings $x'_1, x'_2, \dots, x'_n$ and a residue register $\mathcal{B}'$. For every $i = 1, 2, \dots, n$, check whether $x'_i \in \{x_{i,0}, x_{i,1}\}$. If it is satisfied, output register $\mathcal{B}'$. Else, output $\perp$.*

The statement is that

$$\forall m, \text{TD}(\tilde{Z}^\lambda(m), \tilde{Z}^\lambda(0^n)) = \text{negl}(\lambda) \quad (2)$$

The experiment defined above models the entire flow of our certified deletion. Here we will describe it in an informal way. In step 1, the key to PRF k is sampled as the verification key. The ciphertext to m_i is $\frac{1}{\sqrt{2}}(|x_{i,0}\rangle + (-1)^{m_i}|x_{i,1}\rangle)$.

How to certify the deletion When an honest receiver is asked to delete the ciphertext, he measures the states $\frac{1}{\sqrt{2}}(|x_{i,0}\rangle + |x_{i,1}\rangle)$ in the computational basis. Let the measurement outcome x'_i be the certificates. The sender checks whether $x'_i \in \{x_{i,0}, x_{i,1}\}$. He can calculate $x_{i,0}$ and $x_{i,1}$ with k easily.

How to decrypt The receiver decrypts k first. With k decrypted, the receiver can calculate $x_{i,0}$ and $x_{i,1}$ by itself and recover all m_i [1, 3].

Equation (2) is an analog of the security for multi-bit plaintexts in [2] and resembles the semantic security. With semantic security, an adversary cannot even check if the plaintext is a specific value. Informally, not one bit of information about the plaintext is leaked.

An example of how to instantiate a concrete protocol with Theorem 1 is given below.

The process $Z^\lambda(\cdot,\cdot)$ is an abstraction of a base protocol, which can be encryption, bit commitment, etc. The specific construction that attaches the base protocol with Certified Deletion is described in [2, 3]. An example of how to use Theorem 1 is given as follows.

Example 1 (Informal.) *A commitment is a protocol consisting of two parties, Alice and Bob. Furthermore, it can be divided into two phases.*

- commit phase *Alice decides a string m which is to be committed to. Then, communicate with Bob, during which the transcript will be denoted as $COMM(m)$.*

- reveal phase *Alice publishes a string m' which she declares is the real value committed in the commit phase. Then, communicate with Bob and prove that m' equals m. It is called to open $COMM(m)$.*

If no cheating QPT (resp. unbounded time) Bob can decrypt $COMM(m)$ in the commit phase, then the protocol is computational (resp. statistical) hiding. Similarly, if no cheating QPT (resp. unbounded time) Alice can open a m' that is different from m in the commit phase, then the protocol is computational (resp. statistical) binding.

Assume a computational hiding commitment as the base protocol. Then, a commitment with Certified Deletion, which can delete $COMM(m)$ before the reveal phase, can be constructed as follows.

- commit phase *Alice chooses a k randomly and prepares $\frac{1}{\sqrt{2}}(|x_{i,0}\rangle + (-1)^{m_i}|x_{i,1}\rangle)$ in register $\mathcal{A}_i$ as described before. Then commit to k with the base protocol and send $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_i, \ldots, \mathcal{A}_n$ altogether as the new $COMM'(m)$ in the new protocol.*

- reveal phase *Alice just opens $COMM(k)$ as in the base protocol to reveal the key k to Bob. With k, Bob can check the real value of m.*

- deletion before reveal *Bob measures every $\mathcal{A}_i$ in the computational basis and the outcomes will be the certificates.*

Second, we state the result from [2].

Theorem 2 (Privately Verifiable Deletion from [2]) *Let $Z^\lambda(\cdot,\cdot,\cdot)$ be a sequence of (quantum) processes. $Z^\lambda(\cdot,\cdot,\cdot)$ is semantically secure in the first argument. The definition can be referenced in equation (1) with only a difference in the number of parameters. The first, the second, and the third arguments receive a string, one bit, and a quantum register, respectively.*

Let us define the distribution $\tilde{Z}^\lambda(b)$ for any adversary B^λ.

1. *Sampling $x, \theta \in \{0,1\}^\lambda$ from uniform distributions.*
2. *Use $Z^\lambda(x, b\oplus(x\cdot\theta), |x\rangle_\theta)$ as input of algorithm B^λ and run the algorithm. $|x\rangle_\theta := \bigotimes_i H^{\theta_i}|x_i\rangle$ is the conjugate coding/BB84 state [4, 19].*
3. *Parse the output as a string x' and a residue register $\mathcal{B}'$. For all $i \in \{1,\ldots,\lambda\}$ that the ith bit of θ equals 0, check if the ith bits of x' and x are equal. If satisfied, output register $\mathcal{B}'$. Else output $\perp$.*

The statement is that

$$\mathrm{TD}(\tilde{Z}^\lambda(0), \tilde{Z}^\lambda(1)) = \mathrm{negl}(\lambda) \tag{3}$$

Finally, let us state the result from [3].

Theorem 3 (Publicly Verifiable Deletion from [3]) *Let $Z^\lambda(\cdot,\cdot,\cdot,\cdot)$ be a sequence of (quantum) processes. $Z^\lambda(\cdot,\cdot,\cdot,\cdot)$ is semantically secure in the first argument. The definition can be referenced in equation (1) with only a difference in the number of parameters. Arguments received from left to right: string, string, string, and quantum register.*

Let us define the distribution $\tilde{Z}^\lambda(b)$ for any adversary B^λ. Fix a one-way function f.

1. *Sample $x_0, x_1 \in \{0,1\}^\lambda$ from uniform distributions. Calculate $y_0 := f(x_0)$ and $y_1 := f(x_1)$.*
2. *Use $Z^\lambda(x_0 \oplus x_1, y_0, y_1, |x\rangle_\theta)$ as input of algorithm B^λ and run the algorithm.*
3. *Parse the output as a string x' and a residue register $\mathcal{B}'$. If $f(x') \in \{y_0, y_1\}$ then output register $\mathcal{B}'$. Else output $\perp$.*

The statement is that

$$\mathrm{TD}(\tilde{Z}^\lambda(0), \tilde{Z}^\lambda(1)) = \mathrm{negl}(\lambda) \tag{4}$$

In Table 2, certificates are compared to help readers understand why our method achieves a shorter verification key.

Table 2: the certificates for this work and prior works

Work	Certificates	Comments
This work	k	for n bits message
BK23 [2]	θ	for every single bit
BKMPW23 [3]	(y_0, y_1)	for every single bit

Finally, we will discuss about two drawbacks compared to the prior works. First, our method assumes that OWF exists, while OWSG is enough in [3] and no additional assumption is needed in [2]. OWSG is a primitive introduced in [15], and there is an oracle relative to which OWSG exists but OWF does not [13]. Second, the verification key k used is a private key, which means anyone having k can generate certificates without really deleting the ciphertext. It gives rise to the necessity of keeping the verification key safe. This is a drawback from [3, 12] which use a public key.

References

[1] S. Aaronson, Y. Atia, and L. Susskind. On the hardness of detecting macroscopic superpositions. *arXiv preprint arXiv:2009.07450*, 2020.

[2] J. Bartusek and D. Khurana. Cryptography with certified deletion. In *Advances in Cryptography - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023*, pages 192–223. Springer, 2023.

[3] J. Bartusek, D. Khurana, G. Malavolta, A. Poremba, and M. Walter. Weakening assumptions for publicly-verifiable deletion. In *Theory of Cryptography - 21st International Conference, TCC 2023*, pages 183–197. Springer, 2023.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[5] A. Broadbent and R. Islam. Quantum encryption with certified deletion. In *Theory of Cryptography: 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part III 18*, pages 92–122. Springer, 2020.

[6] L. Fortnow. The complexity of perfect zero-knowledge. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 204–209, 1987.

[7] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

[8] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304, 1985.

[9] T. Hiroka, T. Morimae, R. Nishimaki, and T. Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I 27*, pages 606–636. Springer, 2021.

[10] T. Hiroka, T. Morimae, R. Nishimaki, and T. Yamakawa. Certified everlasting zero-knowledge proof for QMA. In *Advances in Cryptology – CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022*, pages 239–268. Springer, 2022.

[11] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[12] F. Kitagawa, R. Nishimaki, and T. Yamakawa. Publicly verifiable deletion from minimal assumptions. In *Theory of Cryptography - 21st International Conference, TCC 2023*, pages 228–245. Springer, 2023.

[13] W. Kretschmer. Quantum pseudorandomness and classical complexity. *arXiv preprint arXiv:2103.09320*, 2021.

[14] S. Menda and J. Watrous. Oracle separations for quantum statistical zero-knowledge. *arXiv preprint arXiv:1801.08967*, 2018.

[15] T. Morimae and T. Yamakawa. Quantum commitments and signatures without one-way functions. In *Advances in Cryptology – CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022*, pages 269–295. Springer, 2022.

[16] A. Poremba. Quantum proofs of deletion for learning with errors. *arXiv preprint arXiv:2203.01610*, 2022.

[17] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[18] T. Hiroka and T. Morimae and R. Nishimaki and T. Yamakawa. Certified everlasting functional encryption. Cryptology ePrint Archive, Paper 2022/969, 2022. `https://eprint.iacr.org/2022/969`.

[19] S. Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[20] M. Zhandry. How to construct quantum random functions. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 679–687. IEEE, 2012.

Cryogenic reconfigurable photonics integrated with SNSPDs for energy-time entanglement distribution

Zhiyun Shu[1 2 *] Hao Li[1 2 †] Lixing You[1 2 ‡]

[1] *National Key Laboratory of Materials for Integrated Circuits, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences (CAS), Shanghai 200050, China*
[2] *CAS Center for Excellence in Superconducting Electronics, Shanghai 200050, China*

Abstract. Superconducting nanowire single-photon detectors (SNSPDs) offer excellent performance for quantum information science due to their high detection efficiency, low dark counts and low timing jitter. Integrated quantum photonics has unparalleled scalability and stability, thus integration of SNSPDs with quantum photonic components is particularly appealing. While reconfigurable photonic circuits is crucial for active manipulation of quantum states of light, its integration with SNSPDs still remains challenging due to the sensitive cryogenic environment. Here, we explore thermally reconfigurable unbalanced Mach-Zehnder interferometers (UMZIs) by utilizing multi-mode silicon waveguides, which greatly reduces the propagation loss, thus enabling the increase of UMZIs' arm length to 30 mm and decrease of half-wave modulation power consumption to 10 mW. By integrating SNSPDs at the outputs of the UMZIs, we demonstrate a cryogenic reconfigurable receiver chip for energy-time entanglement distribution, which provides a promising platform towards full integration of large-scale quantum photonic systems on chip.

Keywords: Superconducting nanowire single-photon detector, Energy-time entanglement, Integrated quantum photonics, Cryogenic reconfigurability

References

[1] A. Politi, et al., "Silica-on-Silicon Waveguide Quantum Circuits," Science 320, 646-649 (2008).

[2] E. Pelucchi, G. Fagas, I. Aharonovich et al., "The potential and global outlook of integrated photonics for quantum technologies," Nature Reviews Physics 4, 194-208 (2021).

[3] J. Chang, J. Gao, I. Esmaeil Zadeh et al., "Nanowire-based integrated photonics for quantum information and quantum sensing," Nanophotonics 12, 339-358 (2023).

[4] L. You, "SNSPDs for quantum information," Nanophotonics 9, 2673-2692 (2020).

[5] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, "High-visibility interference in a Bell-inequality experiment for energy and time," Phys Rev A 47, R2472-R2475 (1993).

[6] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, "Long-distance Bell-type tests using energy-time entangled photons," Physical Review A 59, 4150 (1999).

[7] J. D. Franson, "Bell inequality for position and time," Phys Rev Lett 62, 2205-2208 (1989).

[8] D. Oser, S. Tanzilli, F. Mazeas et al., "High-quality photonic entanglement out of a stand-alone silicon chip," npj Quantum Information 6 (2020).

[9] E. Lomonte, et al., "Single-photon detection and cryogenic reconfigurability in lithium niobate nanophotonic circuits," Nat Commun 12, 6847 (2021).

*zyshu@mail.sim.ac.cn
†lihao@mail.sim.ac.cn
‡lxyou@mail.sim.ac.cn

Measurement-Device-Independent Detection of Beyond-Quantum State

Baichu Yu[1 2 *] Masahito Hayashi[3 2 4 †]

[1] *Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Nanshan District, Shenzhen, 518055, China*

[2] *International Quantum Academy (SIQA), Shenzhen 518048, China*

[3] *School of Data Science, The Chinese University of Hong Kong, Shenzhen, Longgang District, Shenzhen, 518172, China*

[4] *Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan*

Abstract. In quantum theory, a quantum state on a composite system of two parties realizes a non-negative probability with any measurement element with a tensor product form. However, there also exist non-quantum states which satisfy the above condition. Such states are called beyond-quantum states, and cannot be detected by standard Bell tests. To distinguish a beyond-quantum state from quantum states, we propose a measurement-device-independent (MDI) test for beyond-quantum state detection, which is composed of quantum input states on respective parties and quantum measurements across the input system and the target system on respective parties. The performance of our protocol is independent of the forms of the tested states and the measurement operators, which provides an advantage in practical scenarios. We also discuss the importance of tomographic completeness of the input sets to the detection.

Keywords: Beyond-Quantum State Detection, Measurement-Device-Independent Protocol, General Probabilistic Theory,

1 Introduction

The standard framework of quantum theory works very well in explaining the experiment observations, but there are still ambiguities in understanding the meaning of this framework. Also, it is unknown whether quantum theory is the most general physical theory. To study these problems, a more general framework called General Probabilistic Theory (GPT) is often considered [1]. GPT is a theory equipped with general states and measurements, which together produce probability distribution for experimental outcomes. It includes quantum and non-quantum theories.

Either one wants to prove or disprove a non-quantum theory, a crucial task is to design a protocol to distinguish it from the quantum theory. Most of the recent protocols proposed for this task are related to composite systems [2, 3]. These protocols distinguish non-quantum correlations (correlations mean the input-output statistics) from quantum correlations without the knowledge of the theory or the experimental devices. Such property is called device-independent (DI).

A natural question would be whether Bell test, the most well-known DI protocol, can distinguish all non-quantum theories. The negative answer was shown by the existence of a family of GPT states which is more general than quantum states, but produces only quantum correlations in DI Bell tests [4]. Such states are locally quantum and generate valid probability distribution under local (separable) measurements, therefore are called positive over all pure tensors (POPT) states. The set of POPT states includes the set of quantum states, and also some non-quantum states which have negative eigenvalues. In the following, we refer to such non-quantum POPT states as beyond-quantum states.

Briefly speaking, the reason that DI Bell test cannot identify/detect beyond-quantum state is the inability to place restrictions on the measurement operators. In order to detect beyond-quantum states with local measurements, we need a more restrictive protocol. A straightforward idea is to consider device-dependent (DD) protocol, where the form of the measurement operators are known [4]. However, such requirement is very strong practically, e.g., sometimes the measurement devices cannot be trusted. In those cases, the soundness of the result cannot be guaranteed. Therefore we consider a type of an intermediate protocol between DI and DD ones, called a measurement-device-independent (MDI) protocol.

The key property of an MDI protocol is that it transfers the trust on measurement devices onto the trust on state preparations, such that the soundness of the protocol is independent of the knowledge of measurement operators. For example, recent studies [5] introduced an MDI Bell test as a type of a generalized Bell test for entanglement detection, in which the classical inputs of the standard Bell test are replaced by quantum input states, and measurements are made across the input system and the local system of the tested state. In Fig. 1, we present more details of the protocol of such MDI Bell test.

In a recent work, it was shown that an MDI Bell test can be used to detect beyond-quantum states [6]. More specifically, the authors proved that for any given beyond-quantum state, it is possible to construct an MDI witness to detect it, which is a linear function of the correlations $\{p(a,b|\tau_{x,A'},\tau_{y,B'})\}_{a,b,x,y}$. However the construction of the witness is dependent on the form of the tested state and the measurement operators. In a practical MDI Bell test, the form of the tested state or measurement operators is usually not assumed to be known. In that case, the proper witness for detection cannot be determined,

*yubc@sustech.edu.cn

†hmasahito@cuhk.edu.cn

Protocol 1 MDI detection protocol with SDP

1: We choose a set of quantum input states $\{\tau_{x,A'}, \tau_{y,B'}\}_{x,y}$ according to the local dimension to be tomographically complete.
2: We randomly choose a pair of input state $\tau_{x,A'}, \tau_{y,B'}$ from the input set each round and make measurements as shown in Fig. 1. After many rounds we obtain correlations $\{p(a,b|\tau_{x,A'}, \tau_{y,B'})\}_{a,b,x,y}$.
3: We input the correlations $\{p(a,b|\tau_{x,A'}, \tau_{y,B'})\}_{a,b,x,y}$ into SDP (1). Beyond-quantumness is detected whenever $c_{ab} > 0$.

which may greatly influence the detectability (the ability of detecting a given beyond-quantum state) of the protocol.

2 Our Work and Contributions

In our work, we proposed an MDI beyond-quantum state detection protocol which is different from the one in [6]. Our method provides the first beyond-quantumness detection protocol whose soundness and detectability are optimized and independent of the knowledge of the tested state and the measurement operators. It achieves better detectabiliy for beyond-quantum state with less requirements than all existing protocols. Also, we discussed the importance of choosing a tomographically complete input set to the performance of our MDI protocol.

More specifically, our protocol does not reconstruct a witness for beyond-quantumness, but processes the experimental correlations $p(a,b|\tau_{x,A'}, \tau_{y,B'})$ using a Semi-definite Program (SDP) as below:

$$c_{ab} := \min_{(X^+_{ab}, X^-_{ab}) \in (\mathcal{M}_+^{A'B'})^2} \{\mathrm{Tr} X^-_{ab} | (2) \text{ holds.}\} \qquad (1)$$

Here, $\mathcal{M}^{A'B'}$ is the set of $d_{A'}d_{B'} \times d_{A'}d_{B'}$ matrices, $\mathcal{M}_+^{A'B'}$ is the set of positive semi-definite matrices, and the condition (2) is given as

$$\mathrm{Tr}[X_{ab}(\tau_{x,A'} \otimes \tau_{y,B'})] = p(a,b|\tau_{x,A'}, \tau_{y,B'}), \forall x, y \qquad (2)$$

with $X_{ab} := X^+_{ab} - X^-_{ab}$. When there exists a pair (a,b) such that $c_{a,b} > 0$, we consider that the tested state is beyond-quantum. We present the entire procedure of our protocol as Protocol 1. More details and explanations about our protocol can be found in the complete version on arXiv [7].

To assess the performance of our protocol, we proposed three criteria: completeness, universal completeness and soundness, which are defined as follows.

Definition 1. Completeness*: Let S be a set of beyond-quantum states. A protocol is called complete for the set S when any beyond-quantum state in S can be detected by the protocol under the assumption that the experimental devices are properly chosen.*

Definition 2. Universal completeness*: A protocol is called universally complete when it is complete for the set of all beyond-quantum states (with certain fixed local dimensions).*

Definition 3. Soundness*: Any quantum state will never be detected as a beyond-quantum state by the protocol.*

We see that completeness and universal completeness assess the detectability of a protocol according to the quantity of beyond-quantum states it can detect when the settings (parameters) of the protocol is fixed. Soundness assess the reliability of the detection result.

We showed the power of our protocol by the following two theorems.

Theorem 1. *When $M_{A'A}$ and $M_{BB'}$ are quantum measurements on system $A'A$ and BB', and $\{\tau_{x,A'}\}_x$ and $\{\tau_{y,B'}\}_y$ are chosen to be sets of states in $\mathcal{H}^{d_{A'}}$ and $\mathcal{H}^{d_{B'}}$, where $d_{A'}, d_{B'}$ are the dimensions of the auxiliary systems A' and B', the tested state is beyond-quantum whenever we obtain $c_{ab} > 0$ for some outcomes a, b with SDP (1).*

Therefore, whenever the form of the quantum input states $\{\tau_{x,A'}\}_x$ and $\{\tau_{y,B'}\}_y$ are known, our detection protocol satisfies soundness.

Theorem 2. *Given the assumption that the dimensions of A and B are d_A and d_B respectively, any beyond-quantum state ρ_{AB} can be detected by our MDI protocol when $\{\tau_{x,A'}\}_x$ and $\{\tau_{y,B'}\}_y$ are tomographically complete sets of states on $\mathcal{H}^{d_A}$ and $\mathcal{H}^{d_B}$, and measurement operators $M^a_{A'A}$ and $M^b_{BB'}$ are entangled pure, with Schmidt rank d_A and d_B respectively.*

Theorem 2 shows that our protocol satisfies universal completeness with the knowledge of the form of quantum input states $\{\tau_{x,A'}\}_x$ and $\{\tau_{y,B'}\}_y$ and the dimension of local systems.

3 Comparison with existing protocols

Here we compare our protocol with two existing beyond-quantum state detection protocols [4, 6].

For the device-dependent protocol proposed in Ref. [4], the knowledge of the forms of the measurement operators is required to satisfy soundness, and the form of the tested state is additionally required to satisfy completeness. For the MDI protocol proposed in Ref. [6], the knowledge of the form of quantum input states is required to satisfy soundness, and the knowledge of the forms of the tested state and the measurement operators is additionally required to satisfy completeness. For our protocol, while the knowledge of the form of quantum inputs is also required to satisfy soundness, only the knowledge of the local dimensions of the tested state is additionally required to satisfy completeness. We summarize the above differences in Table 1.

It is worth noting that our protocol also satisfies universal completeness, since it detects any beyond-quantum state with a fixed protocol. The protocols in Ref. [4] and

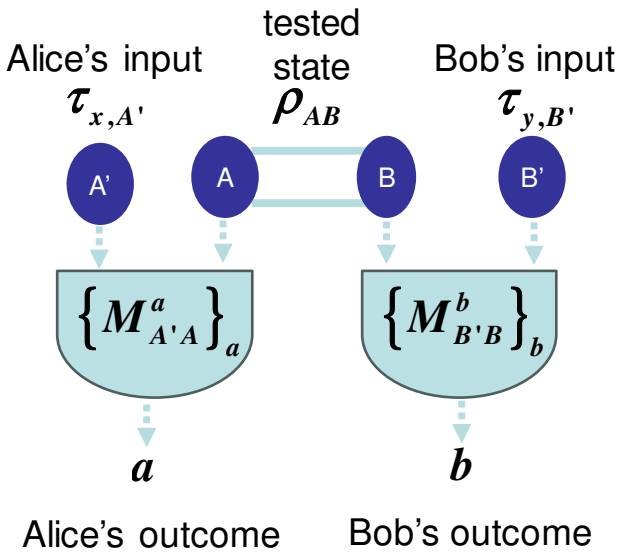


Figure 1: The Protocol of MDI Bell test. An MDI Bell test is composed of the target state ρ_{AB}, quantum input states $\{\tau_{x,A'}\}_x$, $\{\tau_{y,B'}\}_y$, and quantum measurements $M_{A'A} = \{M^a_{A'A}\}_a$ and $M_{BB'} = \{M^b_{BB'}\}_b$ across the input system and the target system in respective parties. As the result of this experiment, the MDI protocol generates the correlation set $\{p(a,b|\tau_{x,A'}, \tau_{y,B'})\}$. The details of these notations will be given in Section **??**.

Ref. [6] do not satisfy universal completeness, although they can detect any given beyond-quantum state. This is because the form of the witness (therefore the protocol) needs to be changed according to the form of the tested state. With a fixed MDI witness (protocol), only a part of beyond-quantum states can be detected.

Moreover, in Ref. [6], it is only shown that when the measurements $M_{A'A}$ and $M_{B'B}$ both contain maximally entangled states as one of the measurement operators, completeness can be satisfied. However we prove later that in our protocol, (universal) completeness can be satisfied as long as $M_{A'A}$ and $M_{B'B}$ both contain entangled pure measurement operators. This result improves the practicality of the protocol.

In summary, our protocol is the first beyond-quantumness detection protocol which satisfies soundness and (universal) completeness without knowing the form of the tested state and measurement operators. It attains a better performance with weaker assumptions than existing protocols.

Table 1: Requirement to satisfy the two criteria, soundness and completeness. In the table, we summarize the knowledge needed to satisfy soundness and completeness for the three protocols. The "+" sign means the condition is additionally required besides the condition for soundness. It can be seen that our protocol satisfies the two criteria with relatively weaker assumptions.

	Soundness	Completeness
Ref.[4]	forms of measurement operators	+ form of the tested state
Ref.[6]	forms of quantum input states	+ forms of the tested state and measurement operators
Our protocol	forms of quantum input states	+ dimension of the local systems

References

[1] M. Plávala. General probabilistic theories: An introduction. Physics Reports, 1033: 1-64, 2023.

[2] 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, 96(25): 250401, 2006.

[3] M. Pawłowski, et al. Information causality as a physical principle. Nature, 461(7267), 1101-1104, 2009.

[4] H. Arai, B. Yu, and M. Hayashi. Detection of Beyond-Quantum Non-locality based on Standard Local Quantum Observables. and discrete logarithms on a quantum computer. arXiv preprint arXiv:2301.04196, 2023.

[5] C. Branciard, et al. Measurement-device-independent entanglement witnesses for all entangled quantum states Physical review letters 110.6: 060405, 2013.

[6] E. P. Lobo, et al. Certifying beyond quantumness of locally quantum no-signaling theories through a quantum-input Bell test. Physical Review A, 106(4), L040201, 2022.

[7] B. Yu, and M. Hayashi. Measurement-Device-Independent Detection of Beyond-Quantum State arXiv preprint arXiv:2312.06151, 2023.

Simulating conical intersections with multiconfigurational methods on a quantum processor

Shoukuan Zhao[1] Diandong Tang[2] Zhendong Li[2] Xiaoxia Cai[1] *

[1] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2] *Key Laboratory of Theoretical and Computational Photochemistry, Ministry of Education College of Chemistry, Beijing Normal University, Beijing 100875, China*

Abstract. Conical intersections play a vital role in photochemical processes. The standard quantum chemistry approach to study conical intersections between ground and excited states are the state-average multi-configurational methods, which at least require solving an active space problem whose computational cost on classical computers scales exponentially in the worst case. Quantum computing offers an alternative tool to solve this problem. In this poster, we report a hybrid quantum-classical state-average complete active space self-consistent field method based on the variational quantum eigensolver (VQE-SA-CASSCF) for the first time on a programmable superconducting quantum processor, and applied it to study conical intersections of triatomic hydrogen H_3. We show that a combination of different strategies can lead to a qualitatively correct reproduction of conical intersections using VQE-SA-CASSCF. These results allow us to identify the challenges to be overcome in the future and pave the way for using quantum computers to study conical intersections of more complex systems.

Keywords: VQE, CASSCF, conical intersection.

1 Introduction

Conical interactions plays a key role in photochemistry. With the breakdown of the Born–Oppenheimer approximation, the adiabatic potential energy surfaces (PES) are no longer independent and will become degenerate, allowing ultrafast radiationless transition from one adiabatic excited state to the ground state or another excited state by internal conversion or intersystem crossing[1, 2, 3, 4]. A fundamental task in quantum chemistry is to compute PES accurately, in particular, in the region of conical intersections[5, 6]. Since multiple closely lying electronic states are involved, multi-configurational methods are required to correctly describe conical intersections. The standard quantum chemistry approach are state-averaged complete active space self-consistent field (SA-CASSCF)[7] and its various extensions to include dynamical correlations. While there have been successful numerical methods for solving the active space problem[8, 9, 10], in the worst scenario the computational cost on classical computers still scales exponentially with respect to the number of active orbitals.

Quantum computing is generally believed to have the potential to benefit computational physics and quantum chemistry[11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21], as well as promote the development of material science and other related fields. Very recently, several efforts have been made to develop quantum algorithms to simultaneously solve the active space problem and optimize molecular orbitals (OO) in either state-specific[22, 23, 24, 25, 26] or state-average formalism[27, 28, 29, 26], which are often referred to as (state-average) orbital-optimized VQE (OO-VQE). Besides, algorithms for energy gradients and nonadiabatic couplings were also developed[29, 30], which are essential for performing nonadiabatic molecular dynamics near conical intersections. Despite these efforts, it is still very challenging to implement SA-CASSCF based on VQE (VQE-SA-CASSCF) on NISQ quantum device. Because unlike VQE for a single electronic state, SA-CASSCF typically requires to solve the Schrödinger equation for multiple states many times sequentially in order to update the molecular orbitals until convergence. This puts a stringent requirement for the gate fidelity and coherence time of quantum hardware. To the best of knowledge, albeit with its importance for studying nonadiabatic photochemical processes, successful applications of VQE-SA-CASSCF to conical intersections have not been reported on real quantum devices yet.

2 Theory

For molecules and materials, the electronic Schrödinger equation to be solved reads $\hat{H}|\Psi\rangle = E|\Psi\rangle$, where the Hamiltonian $\hat{H}$ in second-quantization is written as[31]

$$\hat{H} = \sum_{pq} h_{pq}\hat{a}_p^\dagger \hat{a}_q + \frac{1}{4}\sum_{pqrs} v_{pq,rs}\hat{a}_p^\dagger \hat{a}_q^\dagger \hat{a}_s \hat{a}_r, \tag{1}$$

with h_{pq} and $v_{pq,rs}$ being molecular integrals computable on classical computers and $\hat{a}_q^{(\dagger)}$ being Fermionic annihilation (creation) operators. To solve this equation using quantum computers, the problem needs to be mapped to a qubit problem. There exist different fermion-to-qubit transformations such as the Jordan-Wigner[32], parity, and Bravyi-Kitaev[33] encodings, after which $\hat{H}$ becomes a qubit Hamiltonian written as a linear combination of Pauli terms, i.e., $\hat{H} = \sum_k h_k P_k$ with $P_k \in \{I, X, Y, Z\}^{\otimes N}$. The many-body wavefunction can be expressed as $|\Psi\rangle = \sum_{\boldsymbol{q}} \Psi(\boldsymbol{q})|\boldsymbol{q}\rangle$ with $|\boldsymbol{q}\rangle \equiv |q_1 \cdots q_N\rangle$ ($q_i \in \{0, 1\}$) being the basis vector. Solving this problem exactly is prohibitive for most systems. In fact, it is often the case that only a subset of MOs are relevant for the interested chemical processes, such that it

*caixx@baqis.ac.cn

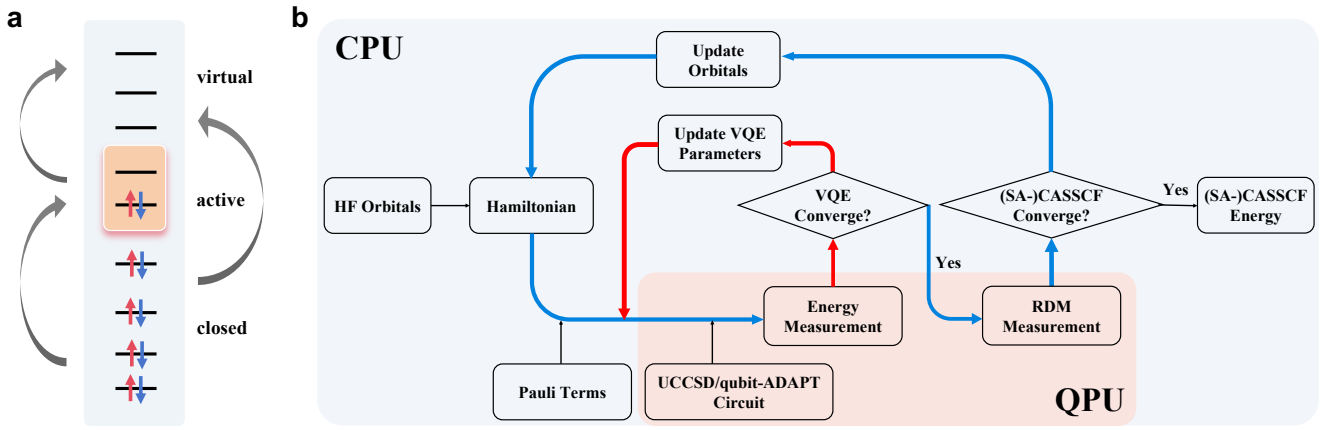


Figure 1: (a) Complete active space (CAS) model. The molecular orbitals are partitioned into three classes: closed-shell orbitals with double occupancy, active orbitals with partial occupancy, and virtual orbitals with zero occupancy. The CASSCF method is defined as a variational method, which solves the active space problem exactly while optimizing the orbitals thorough orbital rotations (gray arrows). (b) Flowchart of VQE-SA-CASSCF. The whole procedure involves two closed-loop iterative processes. One is for solving the active space problem using the hybrid quantum-classical VQE (red arrows), and the other is for optimizing molecular orbitals (blue arrows) on classical computers given the reduced density matrices (RDMs) produced by the former part. The single update of both VQE parameters and the molecular orbitals will be referred to as one macro iteration.

is sensible to only solve Eq. (1) for those important orbitals[34, 24]. This is the basic idea of CASSCF[7], in which the MOs are partitioned into three subsets (see Fig. 1a): closed-shell orbitals with double occupancy, active orbitals with partial occupancy, and virtual orbitals with zero occupancy. The analog of Eq. (1) is only solved for active orbitals with the active electrons distributed in all possible ways, while other parts are treated at a mean-field level. This ansatz is described by the CASCI (complete active space configuration interaction) wavefunction $|\Psi_{\text{CASCI}}\rangle = |\Psi_{\text{act}}\rangle|\Psi_{\text{core}}\rangle$, where $|\Psi_{\text{core}}\rangle$ describes the doubly occupied parts and $|\Psi_{\text{act}}\rangle$ describes the correlated many-body wavefunction within the active space. The CASSCF (complete active space self-consistent field) ansatz further improves CASCI by allowing orbital rotations among different subspaces[31]

$$|\Psi_{\text{CASSCF}}\rangle = e^{-\sum_{pq}\kappa_{pq}\hat{a}_p^\dagger\hat{a}_q}|\Psi_{\text{act}}\rangle|\Psi_{\text{core}}\rangle, \qquad (2)$$

where κ_{pq} is an anti-Hermitian matrix for orbital rotations (see Fig. 1a). Thus, apart from the wavefunction parameters in $|\Psi_{\text{act}}\rangle$, κ_{pq} also needs to be determined by the variational principle. For simplicity, we will denote these two sets of parameters by $\mathbf{x}_c$ and $\mathbf{x}_o$, respectively.

The flowchart used for optimizing $\mathbf{x}_c$ and $\mathbf{x}_o$ in this work is summarized in Fig. 1b. The whole procedure involves two closed-loop iterative processes: one for optimizing $\mathbf{x}_c$ using the hybrid quantum-classical VQE and the other for optimizing $\mathbf{x}_c$ on classical computers. Details of this two-step VQE-SA-CASSCF procedure are described as follows:

(1) Perform a Hartree-Fock calculation to obtain an initial set of MOs.

(2) Construct the active space Hamiltonian using the obtained MOs and apply a fermion-to-qubit transformation to obtain a qubit Hamiltonian.

(3) Setup a Parameterized quantum circuit (PQC) for each interested state $|\Psi_I(\mathbf{x}_c^I)\rangle$ within the active space. Depending on the complexity of molecules, either the PQC derived from UCCSD or qubit-ADAPT will be used in this work[35, 36, 37].

(4) Solve the active space problem by VQE or its excited-state extensions[38] to optimize $\mathbf{x}_c^I$ using both quantum and classical computers. This gives the energy E_I for each state $|\Psi_I\rangle$ as well as the one- and two-particle reduced density matrices (1,2-RDMs) defined by $\gamma_{pq}^I \equiv \langle\Psi_I(\mathbf{x}_c^I)|\hat{a}_p^\dagger\hat{a}_q|\Psi_I(\mathbf{x}_c^I)\rangle$ and $\Gamma_{pqrs}^I \equiv \langle\Psi_I(\mathbf{x}_c^I)|\hat{a}_p^\dagger\hat{a}_q^\dagger\hat{a}_s\hat{a}_r|\Psi_I(\mathbf{x}_c^I)\rangle$, respectively.

(4) With 1,2-RDMs, define an energy function for $\mathbf{x}_o$ as

$$E_{\text{av}}(\mathbf{x}_o) \equiv \sum_{pq} h_{pq}(\mathbf{x}_o)\bar{\gamma}_{pq} + \frac{1}{4}\sum_{pqrs} v_{pq,rs}(\mathbf{x}_o)\bar{\Gamma}_{pqrs}, \qquad (3)$$

where $\bar{\gamma}_{pq} = \sum_I w_I\gamma_{pq}^I$ and $\bar{\Gamma}_{pqrs} = \sum_I w_I\Gamma_{pqrs}^I$ with w_I being the weight for the I-th state in SA-CASSCF. Usually, $w_I = 1/M$ is chosen with M being the number of interested electronic states. Then, optimize Eq. (3) on classical computers to obtain a set of optimized MOs.

(5) Check energy convergence. If not converged, repeat steps (2)-(5) until convergence is reached.

3 Results and discussions

The triatomic hydrogen H_3 is a typical system with a symmetry-required conical intersection[39] between the ground and the first excited states occurred at all equilateral triangular geometries. In our study, the first two hydrogen atoms are positioned along the x-axis with the distance between them set to be 0.818 Å, and the position of the third hydrogen is varied from 0.4 Å to 0.71

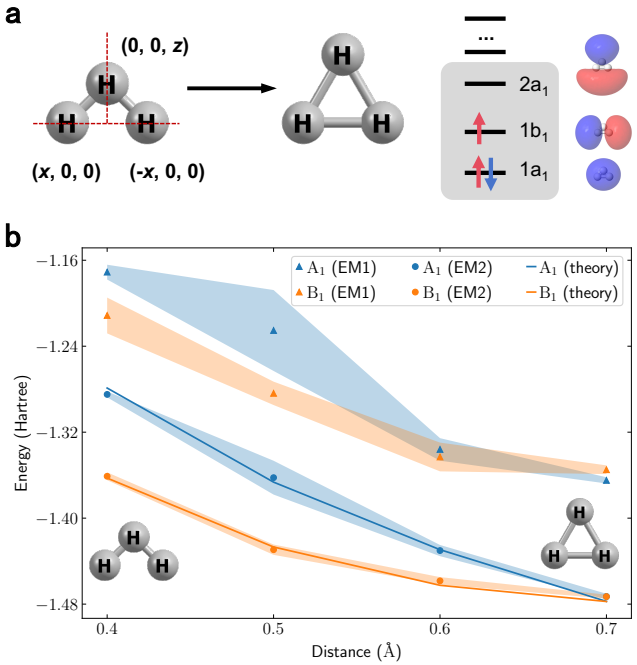


Figure 2: (a) Structure of the H_3 model, where two of the hydrogen atoms on the x-axis are fixed ($x = 0.409$ Å) and the remaining hydrogen on the z-axis is allowed to move in the z direction. Molecular orbital diagrams and the three-electron-in-three-orbital active space denoted by CAS(3e,3o). (b) Potential energy curves of the ground and the lowest excited state obtained by VQE-SA-CASSCF with CAS(3e,3o) using the cc-pVDZ basis set and two error mitigation methods. The conical intersection is located at the equilateral triangle structure ($z \approx 0.708$ Å). The shaded region represents the error bars estimated by repeating the calculations twice.

Å along the z-axis (see Fig. 2a). A conical intersection between the lowest two electronic states presents at the equilateral triangle structure ($z \approx 0.708$ Å) with the D_{3h} symmetry, while for other values of z, the structure has the C_{2v} symmetry. To correctly describe the conical intersection, a minimal active space with three electrons distributed in three active orbitals, denoted by CAS(3e,3o), is required. Figure 2 shows the three relevant MOs with a_1, b_1, and a_1 symmetries, respectively. The ground state and the first excited state has the B_1 and A_1 symmetries, respectively.

We used the qubit-ADAPT[37] performed on noiseless simulators to derive simpler PQCs, while maintaining the accuracy with respect to the exact energy below 1 milli-Hartree. The qubits on our superconducting chip have been properly chosen to avoid nonadjacent two-qubit gates, which would otherwise require the introduction of swap gates. We used a grouping technique[40], which utilizes the qubit-wise commutativity between Pauli terms in the Hamiltonian or 2-RDMs, to reduce the number of measurements.

Apart from these algorithmic improvements, a few other adjustments were implemented to make the VQE-SA-CASSCF experiments robust. On the hardware implementation side, the fast-reset method[41] is utilized to reduce the trigger repeat period to 20 microseconds. Besides, the fidelity of the gate is regularly checked every 10 minutes to mitigate potential fluctuations in the system state. We have also replaced the COBYLA algorithm for optimizing wavefunction parameters by the Bayesian optimization with skopt[42] for having a better performance in the presence of noises. These adjustments are crucial for the VQE-SA-CASSCF experiments. Note that due the increased impact of noise, VQE-SA-CASSCF can only converge with a loose criteria ($\Delta E_{\text{av}} < 3 \times 10^{-3}$ Hartree) in this case.

Figure 2b displays the PECs of the ground and the first excited states for H_3 obtained using two different EM strategies. The first EM strategy (labeled by EM1) is the symmetry projection[43]. Specifically, the nonphysical states which do not belong to the B_1 symmetry for the ground state or the A_1 symmetry for the first excited state are projected out. The second more sophisticated EM strategy (labeled by EM2) further modifies upon the first EM strategy for expectation values of the Pauli-Z operators[44], by recycling the information of nonphysical states to suppress the errors from depolarization[44]. As shown in Fig. 2b, the PECs obtained by EM1 are too high and have larger fluctuations. In addition, the conical intersection at the equilateral triangular geometry is not well reproduced. These suggest that simply removing the nonphysical components is not sufficient for the present four-qubit case, and the errors within the physical subspace also need to be mitigated. In comparison, the PECs obtained by EM2 agree much better with the theoretical PECs, reproducing the the conical intersection with significantly smaller variations. Thus, for longer circuits, EM2 is more advantageous than EM1. This example demonstrates the feasibility of applying near-term quantum computers to study conical intersections using the VQE-SA-CASSCF method together with hardware and algorithmic improvements.

The paper related to this poster have been accepted by the journal of physical chemistry letter. Here, we only list the part of authors in the paper and the complete list of authors and contents can be found at *https://arxiv.org/abs/2402.12708* and *https://arxiv.org/abs/2402.10480*.

References

[1] Matsika, S. & Krause, P. nonadiabatic events and conical intersections. *Annu. Rev. Phys. Chem.* **62**, 621–643 (2011). PMID: 21219147.

[2] Levine, B. G. *et al.* conical intersections at the nanoscale: molecular ideas for materials. *Annu. Rev. Phys. Chem.* **70**, 21–43 (2019). PMID: 30633637.

[3] Shen, L. *et al.* role of multistate intersections in photochemistry. *J. Phys. Chem. Lett.* **11**, 8490–8501 (2020).

[4] Matsika, S. electronic structure methods for the description of nonadiabatic effects and conical intersections. *Chem. Rev.* **121**, 9407–9449 (2021).

[5] Yarkony, D. R. diabolical conical intersections. *Rev. Mod. Phys.* **68**, 985–1013 (1996).

[6] De Sio, A. *et al.* intermolecular conical intersections in molecular aggregates. *Nat. Nanotechnol.* **16**, 63–68 (2021).

[7] Lischka, H. *et al.* multireference approaches for excited states of molecules. *Chem. Rev.* **118**, 7293–7361 (2018).

[8] White, S. R. & Martin, R. L. ab initio quantum chemistry using the density matrix renormalization group. *J. Chem. Phys.* **110**, 4127–4130 (1999).

[9] Chan, G. K.-L. & Sharma, S. the density matrix renormalization group in quantum chemistry. *Annu. Rev. Phys. Chem.* **62**, 465–481 (2011).

[10] Booth, G. H., Thom, A. J. & Alavi, A. fermion monte carlo without fixed nodes: a game of life, death, and annihilation in slater determinant space. *J. Chem. Phys.* **131**, 054106 (2009).

[11] Aspuru-Guzik, A., Dutoi, A. D., Love, P. J. & Head-Gordon, M. simulated quantum computation of molecular energies. *Science* **309**, 1704–1707 (2005).

[12] Lanyon, B. P. *et al.* towards quantum chemistry on a quantum computer. *Nat. Chem.* **2**, 106–111 (2010).

[13] Kassal, I., Whitfield, J. D., Perdomo-Ortiz, A., Yung, M.-H. & Aspuru-Guzik, A. simulating chemistry using quantum computers. *Annu. Rev. Phys. Chem.* **62**, 185–207 (2011).

[14] Kandala, A. *et al.* hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature* **549**, 242–246 (2017).

[15] Cao, Y. *et al.* quantum chemistry in the age of quantum computing. *Chem. Rev.* **119**, 10856–10915 (2019).

[16] McArdle, S., Endo, S., Aspuru-Guzik, A., Benjamin, S. C. & Yuan, X. quantum computational chemistry. *Rev. Mod. Phys.* **92**, 015003 (2020).

[17] Bauer, B., Bravyi, S., Motta, M. & Chan, G. K.-L. quantum algorithms for quantum chemistry and quantum materials science. *Chem. Rev.* **120**, 12685–12717 (2020).

[18] Motta, M. & Rice, J. E. emerging quantum computing algorithms for quantum chemistry. *Wiley Interdiscip. Rev. Comput. Mol. Sci.* e1580 (2021).

[19] Whitlow, J. *et al.* quantum simulation of conical intersections using trapped ions. *Nat. Chem.* **15**, 1509–1514 (2023).

[20] Valahu, C. H. *et al.* direct observation of geometric-phase interference in dynamics around a conical intersection. *Nat. Chem.* **15**, 1503–1508 (2023).

[21] Wang, C. S. *et al.* observation of wave-packet branching through an engineered conical intersection. *Phys. Rev. X* **13**, 011008 (2023).

[22] Sokolov, I. O. *et al.* quantum orbital-optimized unitary coupled cluster methods in the strongly correlated regime: Can quantum algorithms outperform their classical equivalents? *J. Chem. Phys.* **152**, 124107 (2020).

[23] Mizukami, W. *et al.* orbital optimized unitary coupled cluster theory for quantum computer. *Phys. Rev. Res.* **2**, 033421 (2020).

[24] Tilly, J. *et al.* reduced density matrix sampling: Self-consistent embedding and multiscale electronic structure on current generation quantum computers. *Phys. Rev. Res.* **3**, 033230 (2021).

[25] Bierman, J., Li, Y. & Lu, J. improving the accuracy of variational quantum eigensolvers with fewer qubits using orbital optimization. *J. Chem. Theory Comput.* **19**, 790–798 (2023).

[26] de Gracia Triviño, J. A., Delcey, M. G. & Wendin, G. complete active space methods for nisq devices: The importance of canonical orbital optimization for accuracy and noise resilience. *J. Chem. Theory Comput.* **19**, 2863–2872 (2023).

[27] Yalouz, S. *et al.* a state-averaged orbital-optimized hybrid quantum–classical algorithm for a democratic description of ground and excited states. *Quantum Sci. Technol.* **6**, 024004 (2021).

[28] Fitzpatrick, A. *et al.* a self-consistent field approach for the variational quantum eigensolver: orbital optimization goes adaptive. *arXiv preprint arXiv:2212.11405* (2022).

[29] Omiya, K. *et al.* analytical energy gradient for state-averaged orbital-optimized variational quantum eigensolvers and its application to a photochemical reaction. *J. Chem. Theory Comput.* **18**, 741–748 (2022).

[30] Yalouz, S. *et al.* analytical nonadiabatic couplings and gradients within the state-averaged orbital-optimized variational quantum eigensolver. *J. Chem. Theory Comput.* **18**, 776–794 (2022).

[31] Helgaker, T., Jørgensen, P. & Olsen, J. *molecular electronic-structure theory* (John Wiley & Sons, 2014).

[32] Jordan, P. & Wigner, E. about the pauli exclusion principle. *Z. Phys.* **47**, 631 (1928).

[33] Seeley, J. T., Richard, M. J. & Love, P. J. the bravyi-kitaev transformation for quantum computation of electronic structure. *J. Chem. Phys.* **137**, 224109 (2012).

[34] Takeshita, T. *et al.* increasing the representation accuracy of quantum simulations of chemistry without extra quantum resources. *Phys. Rev. X* **10**, 011004 (2020).

[35] McClean, J. R., Kimchi-Schwartz, M. E., Carter, J. & De Jong, W. A. hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states. *Phys. Rev. A* **95**, 042308 (2017).

[36] Grimsley, H. R., Economou, S. E., Barnes, E. & Mayhall, N. J. an adaptive variational algorithm for exact molecular simulations on a quantum computer. *Nat. Commun.* **10**, 3007 (2019).

[37] Tang, H. L. *et al.* qubit-adapt-vqe: an adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor. *PRX Quantum* **2**, 020310 (2021).

[38] Higgott, O., Wang, D. & Brierley, S. variational quantum computation of excited states. *Quantum* **3**, 156 (2019).

[39] Domcke, W., Yarkony, D. & Köppel, H. *conical intersections: electronic structure, dynamics & spectroscopy*, vol. 15 (World Scientific, 2004).

[40] Verteletskyi, V., Yen, T.-C. & Izmaylov, A. F. measurement optimization in the variational quantum eigensolver using a minimum clique cover. *J. Chem. Phys.* **152**, 124114 (2020).

[41] McEwen, M. *et al.* removing leakage-induced correlated errors in superconducting quantum error correction. *Nat. Commun.* **12**, 1761 (2021).

[42] Head, T., Kumar, M., Nahrstaedt, H., Louppe, G. & Shcherbatyi, I. scikit-optimize/scikit-optimize (v0.9.0) (2021).

[43] Huang, K. *et al.* variational quantum computation of molecular linear response properties on a superconducting quantum processor. *J. Phys. Chem. Lett.* **13**, 9114–9121 (2022).

[44] Wang, R. *et al.* leveraging junk information to enhance the quantum error mitigation. *arXiv preprint arXiv:2402.10480* (2024).

Tunable Coupling Architectures Using Bypass Capacitance for Large-Scale Multiple Qubits Scheme

Zhong-Cheng Xiang[1 2 *] Gui-Han Liang[1] Dong-Ning Zheng[1 2]

[1] *Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*
[2] *Hefei National Laboratory, Hefei 230088, China*

Abstract. We have proposed and experimentally verified a tunable interqubit coupling scheme for large-scale integration of superconducting qubits. The key feature of the scheme is the insertion of connecting pads between the qubit and tunable coupling element. In such a way, the distance between two qubits can be increased considerably to a few millimeters, leaving enough space for arranging control lines, readout resonators, and other necessary structures. By using this design, we have successfully prepared a 78Bit quantum device using flip-chip technique. In this device, we verified the low crosstalk performance of this architecture and achieved higher CZ gate fidelity.

Keywords: Superconducting Qubits, Flip-Chip Technique, Tunable Coupling

1 Introduction

In the development of future large-scale quantum processors, the tunable coupling of superconducting qubits is crucial for the implementation of high-fidelity two-qubit gates and diverse quantum simulation schemes. Tunable coupling schemes based on capacitive[1] and inductive[2] coupling have been demonstrated and implemented in large-scale multiqubit processors. In these schemes, a coupling-off point can be realized and high qubit decoherence time can be maintained. A widely used scheme based on capacitive coupling with a high ON:OFF ratio has been proposed[1] . However, in this design, the tunable coupler is a grounded transmon, and a large enough direct capacitive coupling between qubits is required in the implementation of the tunable coupler. This could limit the circuit design because qubits cannot be placed too far apart, making it difficult to provide adequate space for arranging readout resonators, control lines, airbridges, Purcell filters, and other necessary structures.

To address these issues, we propose a tunable coupling scheme that can increase the distance between qubits. We call it tunable coupler with capacitively connecting pad (TCCP)[3] . TCCP architectures consist of a grounded coupler and capacitively connecting pads. These architectures can achieve a high ON:OFF ratio and do not require direct capacitive coupling between qubits. With TCCP, qubits and tunable couplers can be designed with relatively small sizes, which can more effectively reduce parasitic capacitance caused by another layer along the stacking direction in the flip-chip process. In addition, TCCP architectures can provide a connection form with tunable coupling between chips. Moreover, by using this design, we have successfully prepared a 78Bit quantum device using flip-chip technique. In this device, we verified the low crosstalk performance of this architecture and achieved higher CZ gate fidelity.

*zcxiang@iphy.ac.cn

2 TCCP Architectures

Fig.1(a) shows one of such TCCP architectures with the arrangement of grounded qubit—connecting pad—grounded coupler—connecting pad—grounded qubit. Fig.1(b) presents its lumped-element circuit model, where the direct capacitance between the qubits is neglected. This implies that the qubits are spaced far enough apart that mutual capacitance C_{12} can be disregarded.

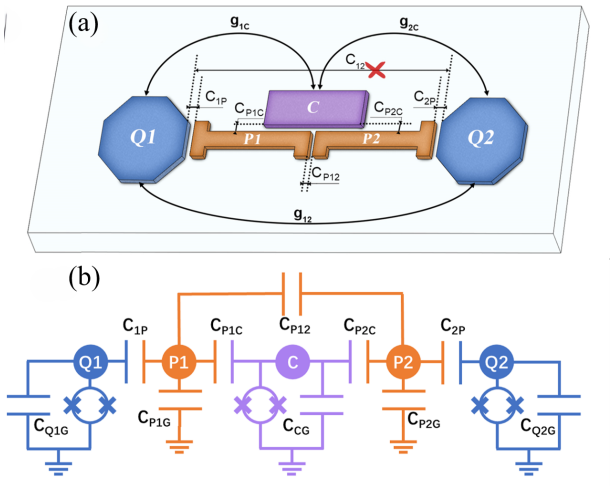


FIG. 1: (a) The schematic diagram of TCCP architecture with two connecting pads. It displays the capacitances and couplings between the nearest-neighbor pads, while the capacitance between two qubits is negligible. (b) The lumped-element circuit model of (a).

We can model this BCC architecture readily using the Hamiltonian given by:

$$\begin{aligned}\hat{H} = & \sum_{j=1,\mathrm{C},2}\left[\omega_j + \frac{E_{Cj}}{2}\left(1-\frac{5\xi_j}{18}\right) - \frac{E_{Cj}}{2}\left(1-\frac{\xi_j}{6}\right)\hat{a}_j^\dagger\hat{a}_j\right] \\ & \times\hat{a}_j^\dagger\hat{a}_j + \sum_{k=1,2} g_{j\mathrm{C}}(\hat{a}_k^\dagger - \hat{a}_k)(\hat{a}_\mathrm{C}^\dagger - \hat{a}_\mathrm{C}) \\ & + g_{12}(\hat{a}_1^\dagger - \hat{a}_1)(\hat{a}_2^\dagger - \hat{a}_2)\end{aligned} \tag{1}$$

where $\omega_j/2\pi$, E_{Cj}, and E_{Jj} are the frequencies, charging energies, and Josephson energies of qubits ($j = 1, 2$) and tunable coupler ($j = \mathrm{C}$), respectively, $\xi_j = \sqrt{2E_{Cj}/E_{Jj}}$ are the sixth-order correction, and $\hat{a}_j$ ($\hat{a}_j^\dagger$) are the annihilation (creation) operators.

The effective qubit-qubit Hamiltonian can be obtained by approximating the qubits and the tunable coupler by their lowest two energy levels and applying a second-order SWT (Schrieffer-Wolff transformation) [4]. The resulting effective Hamiltonian can be expressed as:

$$\hat{H}_{\mathrm{eff}} = \sum_{k=1}^{2}\left(-\frac{1}{2}\omega_k^{\mathrm{eff}}\hat{\sigma}_k^z\right) + g_{\mathrm{eff}}(\hat{\sigma}_1^+\hat{\sigma}_2^- + H.C.) \tag{2a}$$

$$\omega_k^{\mathrm{eff}} = \omega_k - g_{k\mathrm{C}}^2\left(\frac{1}{\Delta_k} + \frac{1}{\Sigma_k}\right),\ k \in \{1, 2\} \tag{2b}$$

where g_{eff} is the effective coupling strength between qubits,and $\Delta_k = \omega_{\mathrm{C}} - \omega_k$, $\Sigma_k = \omega_{\mathrm{C}} + \omega_k$. If $\Delta_k = \omega_{\mathrm{C}} - \omega_k > 0$, i.e., when the frequency of the tunable coupler is above both frequencies of qubits, the virtual exchange interaction term $g_{1\mathrm{C}}g_{2\mathrm{C}}/\Delta_k > 0$, and g_{eff} can be tuned from negative to positive monotonically by increasing the frequency of the tunable coupler. Therefore, a critical value $\omega_{\mathrm{C}}^{\mathrm{off}}$ can always be reached to turn off the effective qubit-qubit coupling, i.e., $g_{\mathrm{eff}}(\omega_{\mathrm{C}}^{\mathrm{off}}) = 0$. It is important to note that we assume that the qubits are far enough apart spatially so that the direct qubit-qubit capacitance C_{12} is negligible. As a result, g_{eff} does not depend on C_{12} and is related to the direct capacitances between qubits and bypass pads $C_{1\mathrm{B}}$, $C_{2\mathrm{B}}$ and the direct capacitance between bypass pads C_{B12} .

To validate the feasibility of the BCC architectures, we designed and fabricated a device with the TCCP architectures. As shown in Fig.2 We found that g_{eff} of the TCCP architectures could be modulated between +3 MHz and −25 MHz, which is a sufficiently wide tunable range to enable most experimental schemes.

Advantage: We have summarized the advantages of the TCCP architecture as follows:

- The effective coupling between qubits can be switched on and off.
- Increase the distance between qubits to realize more wiring space in the flip-chip process.
- Qubit and coupler are grounded transmons with small sizes to reduce parasitic capacitance.
- The long distance connecting pads can reduce crosstalk between qubits.

3 Flip-Chip Device

The TCCP architecture is particularly suitable for the design of large-scale qubit processors due to its aforementioned advantages. The schematic diagram Fig. 3(a) demonstrates the feasibility of the scaling up of qubits based on flip-chip techique [5] using TCCP architectures.

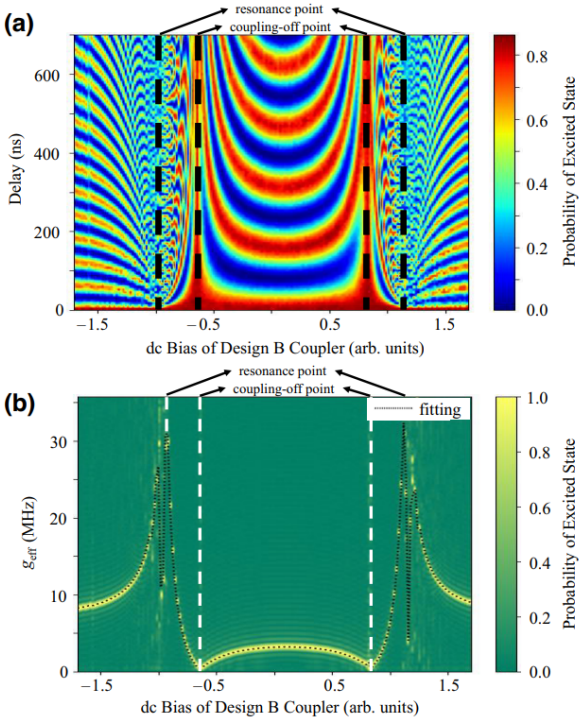


FIG. 2: (a) The spectral diagram of the SWAP operation performed on TCCP device for different frequencies of the tunable coupler, during a period of delay. The abscissa represents the dimensionless parameter of the DC bias applied to the tunable coupler, which correlates inversely with the frequency of the tunable coupler. The colors indicate the probability that one qubit is in the excited state. (b) g_{eff} as a function of the frequency of the tunable coupler was obtained by Fourier transforming the data in (a). The dashed line represents the fitting result.

Sufficient space is available between two qubits to accommodate readout resonators, readout lines, control lines, (tubular) airbridges, indium bumps, and other components.

Due to the introduction of connecting pads, most control lines driving other qubits can be placed far from the qubit as shown in Fig. 3(b), thus greatly reducing the crosstalk between them. Simultaneously, for the control lines close to the qubit, rows of indium can be used instead of indium bumps to block the crosstalk more effectively. Furthermore, the relatively small size of qubits and tunable couplers can reduce parasitic capacitances caused by another layer along the stacking direction effectively. By adjusting each pad, we can achieve a wide enough tunable range and turn-off point for g_{eff} in the flip-chip design, which is comparable to those in the plane design.

We have prepared the 78bit device based on the schematic diagram mentioned above, which consists of two dies bonded together using the flip-chip technique (see Fig.4). The qubit of the device is arranged in the form of a grid array, comprising 6 rows and 13 columns. Each column shares one readout line, and a TCCP-style

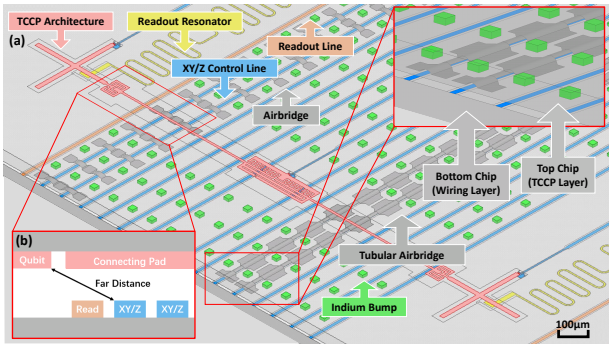


FIG. 3: (a) A schematic diagram of the flip-chip process using TCCP architecture. TCCP architecture on the top chip provides sufficient space for the bottom chip to accommodate readout resonators, readout lines, control lines, (tubular) airbridges, indium bumps, and other components. (b) Schematic cross-section of the marked location in (a). Because of the connecting pads, the qubit is far away from the control lines.

coupler is placed between each pair of nearest-neighbor qubits, resulting in a total of 137 couplers. Fig.4(b) illustrates the average Energy relaxation time ($\overline{T}_1$) of qubits, with a mean value of 26.4μs. We have also measured the Z crosstalk and XY crosstalk for 78Bit device, The Z crosstalk generally ranges from 0.1% to0.01%, and the XY crosstalk ranges from 1% to 0.1%. These measurements verify the excellent performance of the TCCP-style coupler in superconducting qubit applications.

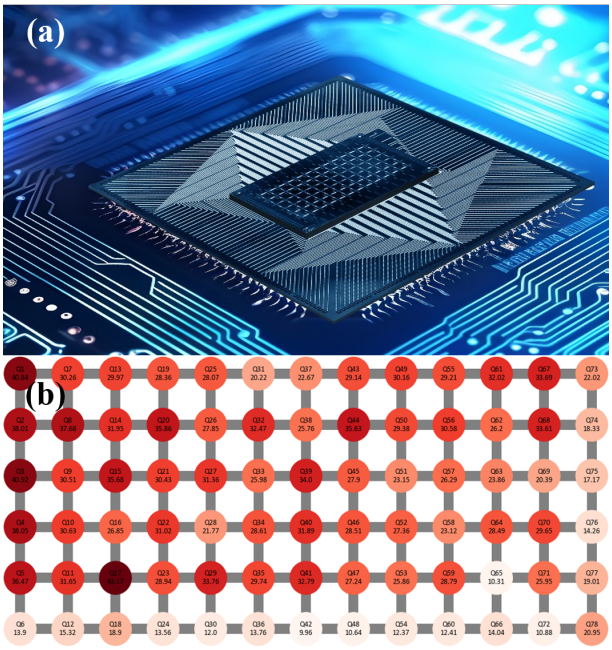


FIG. 4: (a)The photo of 78Bit flip-chip device. (b) Typical distribution of single-qubit T_1 parameters over the device,.

4 Conclusion

We have introduced connecting pads between qubits and a tunable coupler to design a new tunable coupler architecture called TCCP. By eliminating direct capacitive coupling between qubits, TCCP architectures can separate two qubits by several millimeters, providing sufficient wiring space for the flip-chip process and reducing crosstalk from other control lines to the qubits. Using this design, we successfully fabricated a 78-bit quantum device with the flip-chip technique and verified the excellent performance of the TCCP architecture. In conclusion, TCCP architectures offer a promising approach to the realization of large-scale superconducting quantum processors.

References

[1] F. Yan. et al, Tunable coupling scheme for implementing high-fidelity two-qubit gates. *Phys. Rev. Appl.*, 10: 054062, 2018.

[2] C. Yu. et al, Qubit Architecture with High Coherence and Fast Tunable Coupling. *Phys. Rev. Lett.*, 113: 220502, 2014.

[3] G. H. Liang. et al, Tunable-coupling architectures with capacitively connecting pads for large-scale superconducting multiqubit processors. *Phys. Rev. Appl.*, 20: 044028, 2023.

[4] S. Bravyi. et al, SchriefferWolff transformation for quantum many-body systems. and discrete logarithms on a quantum computer. *Ann. Phys.*, 326: 2793, 2011.

[5] B. Foxen. et al, Qubit compatible superconducting interconnects. *Quantum Sci. Technol.*, 3: 014005, 2017.

Revealing crosstalk errors of information scrambling in quantum devices

Hsiang-Wei Huang[1 2] Yi-Te Huang[1 2] Jhen-Dong Lin[1 2] Yueh-Nan Chen[1 2 3 *]

[1] *Department of Physics, National Cheng Kung University, Tainan 701401, Taiwan*
[2] *Center for Quantum Frontiers of Research and Technology (QFort), Tainan 701401, Taiwan*
[3] *Physics Division, National Center for Theoretical Sciences, Taipei 106319, Taiwan*

Abstract. Quantum information scrambling refers to the process of spreading local information into global information across all degrees of freedom. Within this framework, the faithful teleportation fidelity under the Hayden-Preskill decoding protocol serves as a metric for distinguishing genuine information scrambling from decoherence effects. However, the teleportation fidelity, in general, cannot rule out the possibility of crosstalk errors. To tackle this challenge, we propose a spatio-temporal quantum steering task for the decoding protocol, showing that the steerability not only can measure the information scrambling but also signify the presence of crosstalk errors. Moreover, we validate this approach through simulations conducted on IonQ quantum devices.

Keywords: Quantum information scrambling, Crosstalk, Quantum steering, Quantum correlations

1 Motivation

Recently, quantum information scrambling has been studied in various fields such as quantum circuits [1], qutrit processor [2], quantum neural networks [3], and many-body scarred systems [4]. Quantum information scrambling characterizes the dispersal of local information into global systems. For instance, suppose a global system $\rho_A \otimes \rho_B$ is initially composed of two local systems ρ_A and ρ_B. One can correlate local systems ρ_A and ρ_B by performing a global unitary U called "scrambler". With the scrambler U, the information of local systems flows out as the sense of local entropy accumulation. However, the entropy of the global system remains unchanged. This phenomenon can be concluded that the local information is redistributed from the local system to the entire system, and be phrased as "quantum information scrambling".

To quantify the degree of quantum information scrambling, one can use the out-of-time-order correlation (OTOC) [5, 6] defined as

$$\langle V^\dagger U(t) W^\dagger U^\dagger(t) V U(t) W U^\dagger(t)\rangle, \tag{1}$$

where V and W are some unitary operators, and $U(t) = \exp(-iHt)$ is also a unitary operator that evolves the system under the Hamiltonian H. We can also express Eq. (1) under the Heisenberg picture, namely

$$\langle V^\dagger(0) W^\dagger(t) V(0) W(t)\rangle. \tag{2}$$

The OTOC serves as a correlation measure between the initial time $t = 0$ and the later time t. As the unitary $U(t)$ evolves, the operator W changes from local operator to global operator, destroying the correlation in time, and leads to the decrease of the value of OTOC. Thus, one can quantify the quantum information scrambling by the decay of OTOC. However, Ref. [7] shows that the value of OTOC can still be low under a strong decoherence map. Since the decoherence map flows the information out from the entire system, the value of OTOC can decrease with the absence of quantum information scrambling. This shows that OTOC fails to distinguish the quantum information scrambling and the decoherence map.

To disentangle quantum scrambling and decoherence map, Ref. [7] proposed a protocol based on the Hayden-Preskill decoding protocol [8]. This protocol replaces the black hole in the Hayden-Preskill decoding protocol with the scrambler U. The value of teleportation fidelity (decoding fidelity) then depends on the degree of the quantum information scrambling. Once the decoherence map occurs, the value of teleportation fidelity will decrease and never increase since successful teleportation requires undamaged information. Thus, one can verify genuine quantum information scrambling by the value of teleportation fidelity.

However, the current stage of the quantum computer is still in the noisy intermediate-scale quantum (NISQ) era. The protocol may not only be influenced by the decoherence map but also complicated errors such as non-Markovian effect [9], or crosstalk errors [10–12]. Throughout this work, we consider the effect of crosstalk errors on the protocol. We observe that the protocol fails to quantify genuine quantum information scrambling under inevitable crosstalk errors.

To quantify genuine quantum information scrambling, we utilize a metric called spatio-temporal steering robustness (STSR). STSR quantifies the quantum correlation between two systems that are spatio-temporally separated. It can be used to quantify nonclassicality [13–15] and witness information scrambling [16]. We reinterpret the protocol proposed in Ref. [17] by the spatio-temporal steering (STS) scenario and quantify the genuine quantum information scrambling with STSR. We characterize the crosstalk errors by the violation of the no-signaling in time (NSIT) condition under the STS scenario [15]. We perform the proof-of-principle experiment on the IonQ cloud quantum computer. We validate the existence of crosstalk errors and show that STSR (together with the NSIT condition) is a better metric for quantum information scrambling.

*yuehnan@mail.ncku.edu.tw

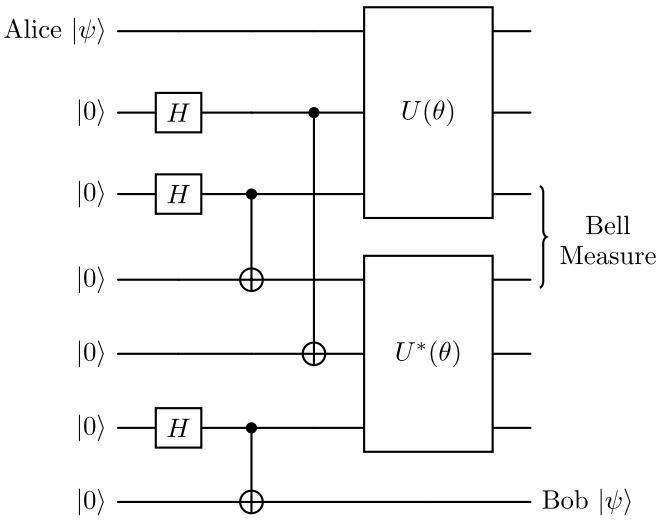


Figure 1: Teleportation circuit based on the Hayden-Preskill decoding protocol [8]. The two scramblers $[U(\theta)$ and $U^*(\theta)]$ encode Alice's state (information) into the global system. After performing the Bell state measurement, Bob can decode Alice's state by post-selecting the outcome corresponding to the $|\text{EPR}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ state.

2 Information Scrambling

One of the measure for OTOC and quantum information scrambling is to calculate the tripartite mutual information I_3 to investigate the distribution of information [18–20]. Here, I_3 is defined as

$$-I_3 = I(A:CD) - I(A:C) - I(A:D), \tag{3}$$

where $I(A:B) = S(A) + S(B) - S(AB)$ is mutual information, and S is the von Neumann entropy. The higher value of $-I_3$ implies a higher degree of quantum information scrambling. We define the "maximal scrambler" as the scrambler that maximizes the value of $-I_3$. In practice, measuring $-I_3$ for a given scrambling unitary U requires the full access of both input and output quantum states of U [16].

The protocol, as shown in Fig. 1, proposed in Ref. [7] provides an efficient method to quantify the quantum information scrambling by only calculating the average teleportation fidelity. To accomplish a successful teleportation, the scrambling unitary U and the post-selection of the outcome corresponding to the $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ state are necessary. In the ideal case, when the scrambling unitary is tuned to the maximal scrambler, the teleportation is perfectly successful, and thus, the average teleportation fidelity equals to unity.

3 Definition of Crosstalk error

During each stage of information processing, crosstalk errors inevitably cause errors, and thus, lead to the imperfection of the results [11, 12]. As introduced in Ref. [12], it is hard to define the source of crosstalk errors generally. Here, we focus on the crosstalk errors generated by a global input-dependent quantum channel. Consider a quantum system for which the number of subsystems is n, and crosstalk errors can be expressed as

$$\tilde{\rho}_{\text{t}} = \Lambda_{\rho_i}[\rho_1 \otimes \cdots \otimes \rho_i \otimes \cdots \otimes \rho_n], \tag{4}$$

where the global channel Λ_{ρ_i} depends on the input state of i-th subsystem ρ_i, and $\tilde{\rho}_{\text{t}}$ represents the total output state. This kind of crosstalk error may leak information to one another through this channel. Under the existence of crosstalk errors, teleportation fidelity may be increased and failed to witness the genuine quantum scrambling.

Here, we provide a concrete example where the teleportation fidelity fails to witness quantum information scrambling. Consider the global channel in Eq. (4) is an input-dependent SWAP operation. It swaps the states between Alice and Bob only when Alice's input state is under certain states. In this case, the teleportation fidelity will always be unity, but it is irrelevant to the degree of quantum information scrambling. Therefore, crosstalk errors may induce unexpected information exchange in the protocol and make the teleportation fidelity unreliable.

4 Information Scrambling in STS Scenario

In order to quantify the quantum information scrambling and also reveal crosstalk errors, we utilize the spatio-temporal steering (STS) scenario, which describes the non-classicality between two spatio-temporally separated quantum systems. It has been reported in Ref. [15] that one can also benchmark quantum teleportation with STS. Therefore, we can also utilize spatio-temporal steering robustness (STSR) as our quantification of quantum information scrambling. Moreover, we can detect crosstalk errors by calculating the violation of the no-signaling in time (NSIT) condition under the STS scenario.

In general, the steering scenario must obey the NSIT condition [21, 22], which assumes that Alice and Bob are not allowed to communicate via sub-channel. In other words, Alice's measurement input (labeled as x) does not affect the statistics on Bob's state at any time t, namely

$$\sum_a \rho_{a|x}(t) = \sum_{a'} \rho_{a'|x'}(t) \quad \forall \quad x, x', t, \tag{5}$$

where a (a') is the corresponding outcome of Alice's input x (x'). Once the above condition is violated, Alice and Bob are able to communicate via classical channels. In this case, one cannot distinguish whether the correlation between Alice and Bob is genuine quantum. The degree of the violation can be quantified by the following quantity [15]:

$$D(\{\rho_{a|x}(t)\}) = \max_{x \neq x'} \frac{1}{2} \left\| \sum_a \rho_{a|x}(t) - \sum_{a'} \rho_{a'|x'}(t) \right\|_1 \tag{6}$$

where $\{\rho_{a|x}(t)\}$ is the steering assemblage in STS scenario. Here, we point out that the crosstalk errors defined in Eq. (4) is a necessary condition for the violation

Table 1: The experiment results are obtained from the ideal simulator and IonQ cloud quantum computer. Here, we initialize Alice's qubit in the six eigenstates of Pauli matrices and conduct the experiments on two quantum devices provided by IonQ. We show the result by comparing the value between STSR, D, and average teleportation fidelity F_{avg}.

Device	STSR	D	F_{avg}
Ideal Simulator	0.2681	0.0113	1.0000
IonQ Aria1	0.1555	0.0491	0.9057
IonQ Harmony	0.0948	0.0948	0.7418

of NSIT condition, namely

$$\sum_a \Lambda_a[\rho_{a|x}(t)] \neq \sum_{a'} \Lambda_{a'}[\rho_{a'|x'}(t)]. \tag{7}$$

Therefore, with the quantity D introduced in Eq. (6), we can detect crosstalk errors and compare it with the value of STSR to verify whether the process of information scrambling is genuine quantum.

5 Experiment in Quantum Device

We implement the teleportation to quantify the degree of quantum information scrambling on two quantum devices of the IonQ cloud quantum cloud computer. The circuit design is depicted in Fig. 1. In the beginning, we prepare Alice's state $|\psi\rangle$ and three pairs of $|\text{EPR}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ states. The scramblers $U(\theta)$ and $U^*(\theta)$ are then performed simultaneously to scramble the local information to the global system. Next, we perform quantum state tomography on Bob's state. The measurement results are obtained through 10,000 shots in each procedure of the state tomography. At the end, we perform Bell state measurement and post-select the outcomes corresponding to the EPR state.

To calculate STSR, we repeat the experiment by initializing $|\psi\rangle$ into the following six states: $|0\rangle, |1\rangle, |\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and $|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. Here, $|0\rangle$ and $|1\rangle$ are the eigenstates of Pauli-Z matrix. In our experiment, the scramblers $U(\theta)$ and $U^*(\theta)$ are tuned to be the maximal scrambler, as shown in Fig. 2.

Both theoretical prediction and experimental results are shown in Table 1. The experimental results obtained from IonQ Harmony shows that the value of STSR and D are equal, which means that the correlations between Alice and Bob can be fully described by classical correlations [15]. Although the value of fidelity exceeds 2/3 (classical bound), it could be induced by crosstalk errors, and thus, it is not certified as genuine quantum information scrambling. By contrast, one can observe that the value of STSR is much larger than the value of D from the experimental results obtained from IonQ Aria 1. Therefore, the experiment conducted in this device is more convincing to be genuine quantum information scrambling.

6 Summary

Quantum information scrambling is the key component to quantum supremacy. Developing a general method to quantify the ability to generate quantum information scrambling thus becomes a crucial task. Although the teleportation protocol can successfully distinguish the decoherence map from genuine quantum information scrambling, crosstalk errors may influence the protocol and cause unexpected results. Since crosstalk errors are inevitable in the NISQ era, we reinterpret the teleportation protocol within the STS scenario.

We show that one can quantify genuine quantum information scrambling by the value of STSR together with the NSIT condition under the STS scenario. We are able to detect the existing crosstalk errors in the teleportation protocol with the quantity D. Moreover, we conduct experiments on the IonQ cloud quantum computer and validate our theory. We conclude that the value of STSR together with NSIT condition is a better metric for quantifying genuine quantum information scrambling in the NISQ era.

References

[1] X. Mi, P. Roushan, C. Quintana, S. Mandrà, J. Marshall, C. Neill, F. Arute, K. Arya, J. Atalaya, R. Babbush, J. C. Bardin, R. Barends, J. Basso, A. Bengtsson, S. Boixo, A. Bourassa, M. Broughton, B. B. Buckley, D. A. Buell, B. Burkett, N. Bushnell, Z. Chen, B. Chiaro, R. Collins, W. Courtney, S. Demura, A. R. Derk, A. Dunsworth, D. Eppens, C. Erickson, E. Farhi, A. G. Fowler, B. Foxen, C. Gidney, M. Giustina, J. A. Gross, M. P. Harrigan, S. D. Harrington, J. Hilton, A. Ho, S. Hong, T. Huang, W. J. Huggins, L. B. Ioffe, S. V. Isakov, E. Jeffrey, Z. Jiang, C. Jones, D. Kafri, J. Kelly, S. Kim, A. Kitaev, P. V. Klimov, A. N. Korotkov, F. Kostritsa, D. Landhuis, P. Laptev, E. Lucero, O. Martin, J. R. McClean, T. McCourt, M. McEwen, A. Megrant, K. C. Miao, M. Mohseni, S. Montazeri, W. Mruczkiewicz, J. Mutus, O. Naaman, M. Neeley, M. Newman, M. Y. Niu, T. E. O'Brien, A. Opremcak, E. Ostby, B. Pato, A. Petukhov, N. Redd, N. C. Rubin, D. Sank, K. J. Satzinger, V. Shvarts, D. Strain, M. Szalay, M. D. Trevithick, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, I. Aleiner, K. Kechedzhi, V. Smelyanskiy, and Y. Chen, "Information scrambling in quantum circuits", Science **374**, 1479–1483 (2021).

[2] M. S. Blok, V. V. Ramasesh, T. Schuster, K. O'Brien, J. M. Kreikebaum, D. Dahlen, A. Morvan, B. Yoshida, N. Y. Yao, and I. Siddiqi, "Quantum information scrambling on a superconducting qutrit processor", Phys. Rev. X **11**, 021010 (2021).

[3] H. Shen, P. Zhang, Y.-Z. You, and H. Zhai, "Information scrambling in quantum neural networks", Phys. Rev. Lett. **124**, 200504 (2020).

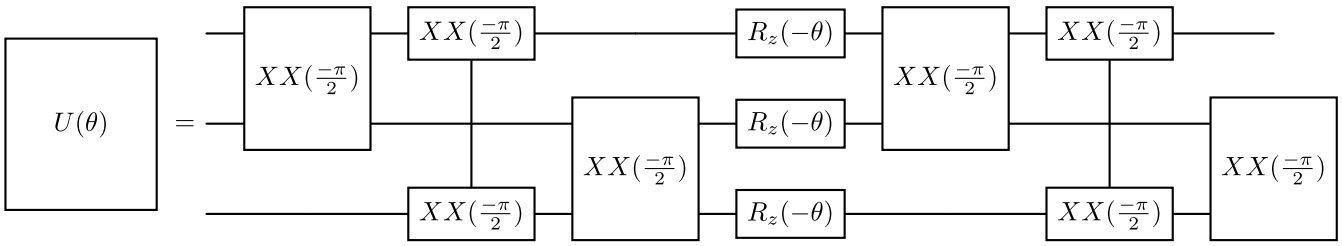


Figure 2: The circuit implementation of XX scrambler. One can adjust θ to obtain different degrees of scrambling. XX scrambler is a maximal scrambler when $\theta = \pi/2$.

[4]D. Yuan, S.-Y. Zhang, Y. Wang, L.-M. Duan, and D.-L. Deng, "Quantum information scrambling in quantum many-body scarred systems", Phys. Rev. Res. **4**, 023095 (2022).

[5]S. H. Shenker and D. Stanford, "Black holes and the butterfly effect", Journal of High Energy Physics **2014**, 10.1007/jhep03(2014)067 (2014).

[6]J. Maldacena, S. H. Shenker, and D. Stanford, "A bound on chaos", Journal of High Energy Physics **2016**, 10.1007/jhep08(2016)106 (2016).

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

[8]P. Hayden and J. Preskill, "Black holes as mirrors: quantum information in random subsystems", Journal of High Energy Physics **2007**, 120–120 (2007).

[9]J. Morris, F. A. Pollock, and K. Modi, "Quantifying non-markovian memory in a superconducting quantum computer", Open Systems amp; Information Dynamics **29**, 10.1142/s123016122250007x (2022).

[10]Y. Xie, M. Nikdast, J. Xu, W. Zhang, Q. Li, X. Wu, Y. Ye, X. Wang, and W. Liu, "Crosstalk noise and bit error rate analysis for optical network-on-chip", in Proceedings of the 47th design automation conference, DAC '10 (2010), pp. 657–660.

[11]S. Seo and J. Bae, "Measurement crosstalk errors in cloud-based quantum computing", IEEE Internet Computing **26**, 26–33 (2022).

[12]M. Sarovar, T. Proctor, K. Rudinger, K. Young, E. Nielsen, and R. Blume-Kohout, "Detecting crosstalk errors in quantum information processors", Quantum **4**, 321 (2020).

[13]S.-L. Chen, N. Lambert, C.-M. Li, A. Miranowicz, Y.-N. Chen, and F. Nori, "Quantifying non-markovianity with temporal steering", Phys. Rev. Lett. **116**, 020503 (2016).

[14]S.-L. Chen, N. Lambert, C.-M. Li, G.-Y. Chen, Y.-N. Chen, A. Miranowicz, and F. Nori, "Spatio-temporal steering for testing nonclassical correlations in quantum networks", Scientific Reports **7**, 10.1038/s41598-017-03789-4 (2017).

[15]Y.-T. Huang, J.-D. Lin, H.-Y. Ku, and Y.-N. Chen, "Benchmarking quantum state transfer on quantum devices", Phys. Rev. Res. **3**, 023038 (2021).

[16]J.-D. Lin, W.-Y. Lin, H.-Y. Ku, N. Lambert, Y.-N. Chen, and F. Nori, "Quantum steering as a witness of quantum scrambling", Phys. Rev. A **104**, 022614 (2021).

[17]K. A. Landsman, C. Figgatt, T. Schuster, N. M. Linke, B. Yoshida, N. Y. Yao, and C. Monroe, "Verified quantum information scrambling", Nature **567**, 61–65 (2019).

[18]P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, "Chaos in quantum channels", Journal of High Energy Physics **2016**, 10.1007/jhep02(2016)004 (2016).

[19]D. A. Roberts and B. Yoshida, "Chaos and complexity by design", Journal of High Energy Physics **2017**, 10.1007/jhep04(2017)121 (2017).

[20]R. Fan, P. Zhang, H. Shen, and H. Zhai, "Out-of-time-order correlation for many-body localization", Science Bulletin **62**, 707–711 (2017).

[21]J. Kofler and C. Č. Brukner, "Condition for macroscopic realism beyond the leggett-garg inequalities", Phys. Rev. A **87**, 052115 (2013).

[22]L. Clemente and J. Kofler, "Necessary and sufficient conditions for macroscopic realism from quantum mechanics", Phys. Rev. A **91**, 062103 (2015).

Applicability and Limitations of Quantum Circuit Cutting with Classical Computers: Order Estimation

Mitsuhiro Matsumoto[1] * Takahiko Satoh[2] Junya Nakamura[1] Shigetora Miyashita[2]
Hiroki Kuji[3 2] Takaharu Yoshida[3 2] Shinichiro Sanji[1]

[1] *Technology Laboratory, PwC Consulting LLC, Japan*
[2] *Faculty of Science and Technology, Keio University, Japan*
[3] *Department of Physics, Tokyo University of Science, Japan*

Abstract. Circuit cutting is a technique to execute large quantum circuits with small computers. Quantum computers are expected to achieve substantial speed-up over classical ones. However, state vector simulation with a classical computer is still effective in running quantum circuits in the Noisy Intermediate-Scale Quantum Computer (NISQ) era. To confirm the achievement of quantum supremacy, we need to understand classical computing's performance limitations. Therefore, we investigate the cutting method's applicability with a classical computer. Specifically, we estimate the maximum number of cuts to reduce the circuit execution time with a classical computer. In addition, we compare circuit execution time with a classical computer and that with a quantum computer in the application of circuit cutting. Our work enables the appropriate use of quantum and classical computers when utilizing circuit cutting technique.

Keywords: Quantum Circuit Cutting, Classical-Quantum Crossover, Order Estimation, NISQ

1 Introduction

Quantum computing is a promising computational approach to offer exponential speedups over classical computing for certain computational problems [1]. However, today's quantum computers are Noisy Intermediate-Scale Quantum Computer (NISQ) devices [2]. Running a large quantum circuit with a NISQ device is challenging due to limitations on the quantity and quality of qubits. Therefore, classical computing such as state vector simulations and tensor network simulations [3] are still powerful to perform quantum circuit evaluations because they are noiseless simulations. Although tensor network simulations are effective for simulating sparse large circuits, we focus on state vector simulations, which can simulate dense small circuits, in order to compare classical computers with small quantum computers (NISQ). There is a limit to execute quantum circuits by state vector simulation because storing the entire state vector in memory requires $\mathcal{O}(2^n)$ memory, where n is the number of qubits. Quantum supremacy [4] stems from the limitation. Therefore, to confirm the achievement of quantum advantage, we need to grasp the performance limitation of classical computing.

Circuit cutting is a promising technique to expand the reach of small computers [5]. Peng et al. introduced wire cutting, which cuts qubit-wires along the direction of time [6]. Mitarai and Fujii proposed gate cutting, which decomposes two-qubit gates directly [7]. This cutting enables us to run a large circuit with a NISQ device. In compensation for saving qubits, the overhead in terms of additional number of circuit evaluations increases to $\mathcal{O}(5^c)$, where c is the number of cuts[8]. Moreover, there are a lot of works to reduce overheads such as wire cutting with classical communication [9], parallel wire cutting [10] and multi-control gate cutting [11].

*mitsuhiro.matsumoto@pwc.com

In this work, we discuss the efficiency of gate cutting with state vector simulations by answering the following two questions. One is how often we can cut two-qubit gates to reduce the circuit execution time with a classical computer. The other is how a quantum computer performs a large circuit faster than a classical computer. Note that we only estimate execution time to run partitioned circuits and ignore other overheads such as preprocessing time to cut an original circuit, compilation time of partitioned circuits and post-processing time to combine the results of executing partitioned circuits.

2 Limitations of Quantum Circuit Cutting With Classical Computers

The maximum size of a quantum circuit that can be performed by naive state vector simulation is 49 qubits because of the memory requirement [12]. We use the circuit cutting technique to reduce the necessary memory size, considering the overhead in the number of partitioned circuits to be executed. Understanding the tradeoff between memory reduction and circuit cutting overhead is important in order to fully utilize the technique.

In this section, we investigate the maximum number of cuts that can reduce the circuit execution time when state vector simulations are performed on a classical computer. Circuit execution time T with a classical computer increases exponentially with the number of qubits q:

$$T \sim \mathcal{O}(2^q). \tag{1}$$

Here, we ignore other factors, such as depth, because the number of qubits has a significant impact on the execution time.

When we perform state vector simulation of decomposed circuits on a classical computer, CZ gate can be partitioned as follows [13]:

$$CZ = \frac{i}{1+i}\left(S \otimes S + iS^\dagger \otimes S^\dagger\right), \tag{2}$$

where S is the phase gate. This indicates that the number of partitioned circuits increases exponentially ($\sim 2^c$) with the number of gate-cuts c.

Divide-in-Half We investigate how often we can cut two-qubit gates to reduce the circuit execution time with a classical computer. Let us consider dividing a circuit with q qubits into in half (two circuits with $q/2$ qubits) by c-cuts (see Fig.1). The execution time 2^q of the original circuit changes as follows:

$$2^q \to 2^{q/2} \times 2^c \times 2. \tag{3}$$

We can save the execution time as long as the right hand side is smaller than the left hand side, that is,

$$c < \frac{q}{2} - 1. \tag{4}$$

This result is shown in Fig.3. For example, when we cut a circuit with 100 qubits in half, the execution time can be reduced by circuit cutting up to 48 times.

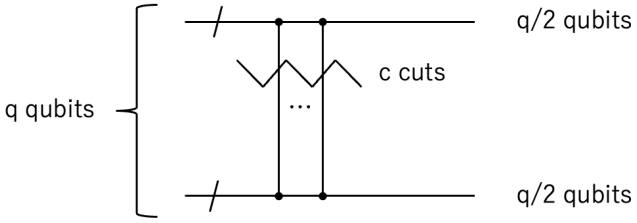


Figure 1: Schematic of dividing a circuit in half with c-cuts.

Divide-into-Thirds What changes if a circuit is divided into thirds? Let us consider dividing a circuit with q qubits into three segments A, B, and C (see Fig.2). We cut c_1 gates between A and B, c_2 gates between B and C, and c_3 gates between C and A, respectively. The execution time 2^q of the original circuit changes as follows:

$$2^q \to 2^{q/3} \times \left(2^{c_1+c_2} + 2^{c_2+c_3} + 2^{c_3+c_1}\right). \tag{5}$$

Let us consider the simple case $c_1 = c_2 = c_3 = c/3$ for order estimation, that is,

$$2^q \to 2^{q/3} \times 2^{2c/3} \times 3. \tag{6}$$

Therefore, the condition where circuit cutting reduces the execution time of a quantum circuit is

$$c < q - \frac{3\log_2 3}{2}. \tag{7}$$

For example, when we divide a circuit with 100 qubits into thirds, the execution time is reduced with the circuit cutting up to 96 times. The number of cuts in the Divide-into-Thirds case is twice as much as that in the Divide-in-Half case (See Fig.3).

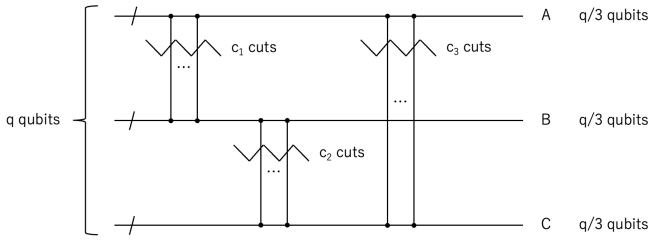


Figure 2: Schematic of dividing a circuit into thirds with $(c_1 + c_2 + c_3)$-cuts.

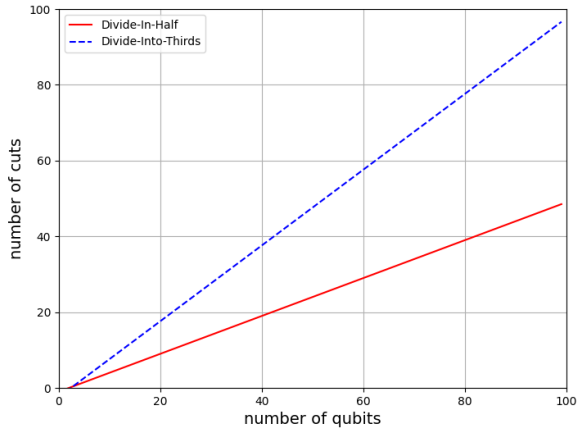


Figure 3: Thresholds of the number of cuts. Circuit cutting reduces the execution time of a quantum circuit under the line. The red solid line is the threshold for the Divide-in-Half case, and the blue dashed line is that for the Divide-into-Thirds case.

3 Classical-Quantum Crossover on Circuit Cutting

In this section, we compare circuit execution time with a classical computer and with a quantum computer. For simplicity, we consider the Divide-into-Thirds case with the same number of cuts ($c_1 = c_2 = c_3 = c/3$). For the comparison, we need three parameters: overheads of cutting, speeds of processing one quantum circuit, and numbers of shots on classical and quantum computers, which are shown in Table 1. The execution time with a quantum computer is shorter than that with a classical computer when

$$\frac{c_c \times 1}{v_c} > \frac{c_q \times s}{v_q}. \tag{8}$$

To calculate this inequality, we evaluate c_q. Unlike with a classical computer, an increase in the number of qubits does not increase the execution time with a quantum computer. Therefore, the overhead of cutting is determined by the number of cuts. Recalling the overhead $\mathcal{O}(5^c)$ with a quantum computer, we obtain

$$c_q = 5^{2c/3} \times 3. \tag{9}$$

As Table 1 shows, we assume the one circuit execution speed as $v_q (= v_c/2^{10})$ and the number of shots of a quan-

Table 1: Parameters for estimating execution times for classical and quantum computers. We assume the one circuit execution speed and the number of shots of a quantum computer as the values in the table for order estimation.

Computing system	Cutting overhead	Execution speed	Number of shots
Classical	2^c	v_c	1
Quantum	5^c	$v_q(= v_c \times 2^{10})$	$s(= 2^{13})$

tum as $s(= 2^{13})$. Eq.(8) leads to

$$c < \frac{q-9}{2\left(\log_2 5 - 1\right)}. \tag{10}$$

This result is shown in Fig.4. For example, when a quantum circuit with 100 qubits is performed, a quantum computer has an advantage in the circuit execution time compared to a classical computer with up to 34 cuts.

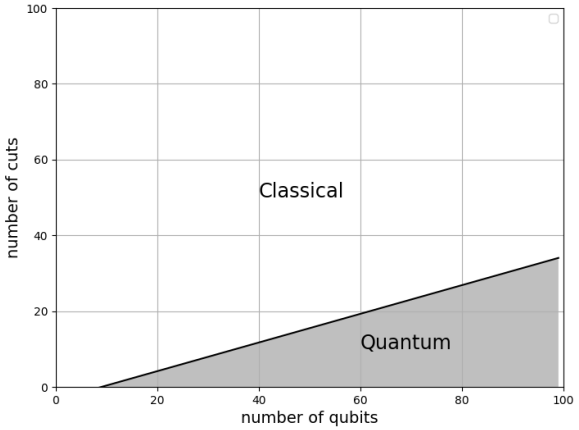


Figure 4: Classical-Quantum Crossover with quantum circuit cutting. In the shaded region, the execution time of a quantum circuit on a quantum computer is shorter than that on a classical computer.

4 Conclusion and Discussion

In this work, we estimated the applicability and limitations of quantum circuit cutting with classical computers. When we run a quantum circuit with 100 qubits on a classical computer, circuit cutting reduces the circuit execution time by up to 48 cuts in the Divide-in-Half case and up to 96 cuts in the Divide-in-Thirds case. We found that the number of cuts in the Divide-into-Thirds case is twice as much as that in the Divide-in-Half case. Moreover, we compared circuit execution time with a classical computer and that with a quantum computer. When we divide a quantum circuit with 100 qubits into thirds, a quantum computer can execute the circuit faster than a classical computer up to 34 cuts.

In future work, we plan to estimate the realistic amount of time it takes to treat many cuts and qubits for practical applications. We also plan to estimate other overheads such as pre-/post- processing and compilation.

Acknowledgment

This work is supported by New Energy and Industrial Technology Development Organization (NEDO). The authors would like to thank Hideaki Kawaguchi and Hana Ebi for their fruitful discussions. TS is supported by JST Grant Number JPMJPF2221, and MEXT KAKENHI Grant Number 22K1978.

References

[1] John M. Shalf and Robert Leland. Computing beyond Moore's Law. Computer 48, 12 (2015), 14-23.

[2] John Preskill. Quantum Computing in the NISQ era and beyond. Quantum 2, 79 (2018).

[3] Xiao Yuan, Jinzhao Sun, Junyu Liu, Qi Zhao, and You Zhou. Quantum simulation with hybrid tensor networks. arXiv:2007.00958 (2020).

[4] John Preskill. Quantum computing and the entanglement frontier. arXiv:1203.5813 (2012).

[5] Sergey Bravyi, Graeme Smith, and John A Smolin. Trading classical and quantum computational resources. Phys. Rev. X 6, 021043 (2016).

[6] Tianyi Peng, Aram W. Harrow, Maris Ozols, and Xiaodi Wu. Simulating Large Quantum Circuits on a Small Quantum Computer. Phys. Rev. Lett. 125, 150504 (2020).

[7] Kosuke Mitarai and Keisuke Fujii. Constructing a virtual two-qubit gate by sampling single-qubit operations. New J. Phys. 23 (2021) 023021.

[8] Akhil Pratap Singh, Kosuke Mitarai, Yasunari Suzuki, Kentaro Heya, Yutaka Tabuchi, Keisuke Fujii, and Yasunobu Nakamura. Experimental demonstration of a high-fidelity virtual two-qubit gate. Phys. Rev. Research 6, 013235 (2024).

[9] Lukas Brenner, Christophe Piveteau and David Sutter. Optimal wire cutting with classical communication. arXiv:2302.03366 (2023).

[10] Hiroyuki Harada, Kaito Wada, and Naoki Yamamoto. Doubly optimal parallel wire cutting without ancilla qubits. arXiv:2303.07340 (2023).

[11] Christian Ufrecht, Maniraman Periyasamy, Sebastian Rietsch, Daniel D. Scherer, Axel Plinge, and Christopher Mutschler. Cutting multi-control quantum gates with ZX calculus. Quantum 7, 1147 (2023).

[12] Edwin Pednault, John A. Gunnels, Giacomo Nannicini, Lior Horesh, Thomas Magerlein, Edgar Solomonik, and Robert Wisnief. Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits. arXiv:1710.05867 (2017).

[13] Simon C. Marshall, Casper Gyurik, and Vedran Dunjko. High dimensional quantum machine learning with small quantum computers. Quantum 7, 1078 (2023).

A Novel Approach for Quantum Simulation Software Framework

Ki-Sung Jin[1] * Jin-Ho On[1] † Gyu-Il Cha[1] ‡

[1] *Future Computing Research Division, ETRI, Daejeon, Republic of Korea*

Abstract. Rapid advances in quantum computing lead to an increasing requirement for digital quantum simulators that enable both quantum algorithm design and the verification of results obtained from quantum hardware. We introduce a new quantum simulator framework for computationally simulating the evolution of quantum states. The proposed framework ensures quantum circuit execution in a lightweight, scalable, and fast manner compared to traditional simulators. This feature enables an optimized environment for various quantum circuit simulations and, in particular, offers a great advantage in the efficient execution of specific large-scale quantum circuits. In this study, we present a comparison of the proposed idea with conventional simulators through both analytical and experimental approach.

Keywords: quantum computing, quantum simulator, quantum circuit, reduced Hilbert space

1 Introduction

Quantum simulators are software tools designed to simulate the behavior of complex quantum systems using classical computers. These tools provide quantum researchers with the opportunity to design various quantum algorithms and verify the measurement results from quantum hardware. Moreover, their importance is increasing because physical quantum hardware is still in its infancy, and most researchers have limited access to it. So far, numerous software-based quantum simulators have been introduced to the academic world[1] and are widely used by most quantum computing researchers in the development of quantum algorithms. Nevertheless, due to various factors such as simulation performance, software stability, various operation methods, and the available execution scale of quantum circuits, it is not easy for users to select a quantum simulator suitable for their practical use.

In this study, we propose a new quantum simulator framework called QPlayer[2, 3]. QPlayer supports the statevector simulation approach and introduces a novel scheme to run simulations by dynamically selecting computational memory space between the full Hilbert space and the reduced Hilbert space depending on quantum circuits[2]. QPlayer software framework consists of two layers: (1) quantum simulation frontend, (2) quantum circuit execution engine. The former is responsible for the interpretation of a given quantum circuit, decision of execution policies, circuit optimization, and their control flows. The latter handles the gate operations of the optimized quantum circuit. To ensure faster quantum simulations, we designed the execution engine to operate on both CPU and GPU.

Furthermore, we compare the proposed idea with conventional quantum simulators[4, 5, 6] by applying both analytical and experimental methods. According to our analysis, QPlayer not only provides faster simulation performance than conventional simulators but can also simulate more qubits for specific circuits.

*ksjin@etri.re.kr
†onjinho@etri.re.kr
‡gicha@etri.re.kr

2 Methods

2.1 Software Architecture

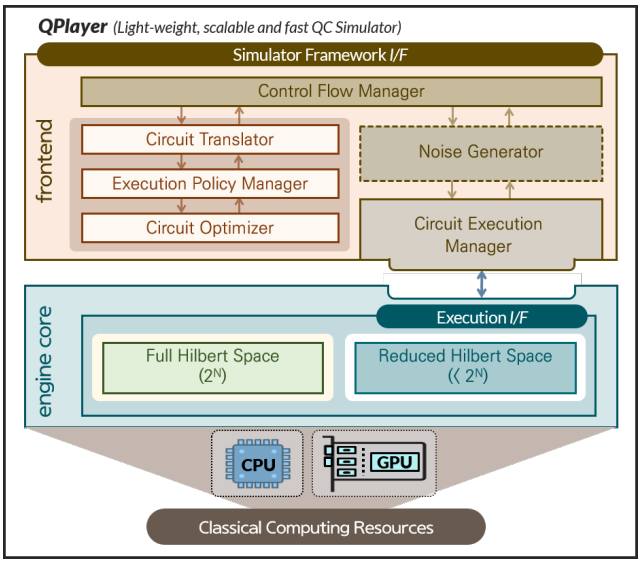


Figure 1: QPlayer software architecture.

QPlayer is a software framework consisting of a front end for preprocessing input quantum circuits and a simulation engine core for gate operations.

2.1.1 Simulation Frontend

simulator framework I/F receives quantum circuits written in native C++, OpenQASM 2.0, and Python. Additionally, users can specify the number of circuit executions, a noise model, optimization level, and a processor type to perform gate operations.

control flow manager is in charge of the workflow for preprocessing the quantum circuit. This includes orchestrating the entire job cycle, such as transforming the circuit to optimal execution conditions, combining it with a noise policy, delivering it to the engine core, and postprocessing the measurement results.

circuit translator interprets the syntax of a given quantum code and transforms it into a low-level interface that the engine core can recognize.

Table 1: Analytical comparison of the quantum simulators.

Category†		QPlayer	Qiskit Aer	Cirq qsim	QuEST
		ETRI(2021∼)	IBM(2017∼)	Google(2018∼)	Oxford univ.(2019)
Simulation	quantum space	Reduced & Full	Full	Full	Full
	qubits‡	128	34	34	34
	optimization	2024/4Q	gate fusion	gate fusion	X
	performance	fast or fastest	fast	fast	slow or moderate
	interface	python,OpenQASM,C++	python,OpenQASM	python,OpenQASM	C
Operating Environment	memory(bytes)⋆	$\leq 2^{(n+4)}$	$2^{(n+4)}$	$2^{(n+4)}$	$2^{(n+4)}$
	GPU	O	O	O	X

†categorizes statevector-based simulators ‡assumes a single server with 512MB memory

⋆QPlayer shows variable memory usage depending on the quantum algorithm

execution policy manager determines the type of the computational space needed to perform gate operations in the engine core by analyzing the gate patterns of the quantum algorithm. If the number of quantum states is predicted to be significantly less than 2^n, it selects the reduced Hilbert space, otherwise it specifies the full Hilbert space.

circuit optimizer transforms the quantum circuit to minimize the execution cost of the engine core through the synthesis of multiple gates or the decomposition of commutable gates.

circuit execution manager delivers the optimized quantum circuit to the simulation engine core via a low-level interface.

2.1.2 Execution Engine Core

execution I/F provides low-level interfaces for the execution of quantum gates transformed by the frontend. These interfaces consist of basic gate operations, multi-gate operations, synthesized gate operations, and measurements.

full Hilbert space executes gate operations in computing memory space equal to $2^{(n+4)}$ bytes for a given number of qubits, n. This approach has the advantage of ensuring optimal execution for synthesized gate operations, but it is difficult to avoid an exponential increase in both memory and computation as the number of qubits increases.

reduced Hilbert space supports executing quantum operations in a reduced quantum memory space while selectively tracking only quantum states with amplitudes greater than 0. The smaller the proportion of superposed states, the faster execution performance is guaranteed. [2] has reported that fast simulation is guaranteed when quantum states with amplitudes greater than zero are within 70% of the total quantum space of 2^n.

2.2 Analytical Comparison

This chapter presents a comparative analysis of the features of quantum simulator software. To this end, we have classified four statevector quantum simulators widely used by quantum computing researchers. Table 1 outlines the features of these simulators. We have used (1) simulation processing and (2) the operating environment as the criteria for comparison.

3 Simulation Result

All experiments were performed on a Dell PowerEdge T640 single server with two Intel Xeon Gold 6132 CPUs, 512GB of DRAM memory, and an NVIDIA H100 GPU. We categorized three test categories to simulate: quantum search and QEC on CPU, and quantum benchmarks on GPU.

3.1 Quantum Search

In the case of the Grover algorithm, it can be seen that QPlayer supports the execution of algorithms up to 49 qubits, while QuEST, Cirq, and Qiskit cannot simulate more than 34 qubits. This is because QPlayer runs simulations of Grover algorithm at minimal cost in the reduced Hilbert space. Even in the same 33-qubit comparison, QPlayer completed the task in 3.49 seconds, while it took about 3,200 seconds for other simulators as shown in Figure 2(a).

3.2 QEC

Surface code is an algorithm specialized for quantum error correction that encodes multiple physical qubits to provide a logical qubit. A unique feature of the logical qubit generated by the surface code is that the number of quantum states with amplitudes greater than zero is only 2^5, not 2^n(in case of distance 3). Therefore, for such algorithms, simulating the reduced Hilbert space can ensure optimal results. In Figure 2(b), QuEST, Cirq, and Qiskit can only generate two logical qubits (33 physical qubits), while QPlayer can support up to six logical qubits (95 physical qubits).

3.3 Algorithm benchmark on GPU

Figure 2(c) shows the results of simulating a quantum algorithm benchmark using QASMBench on a GPU accelerator. According to our analysis, QPlayer demonstrated excellent results compared to other simulators. The main reason Cirq is on average about twice as fast as Qiskit is that it uses float precision for complex numbers instead of double precision. Meanwhile, QPlayer

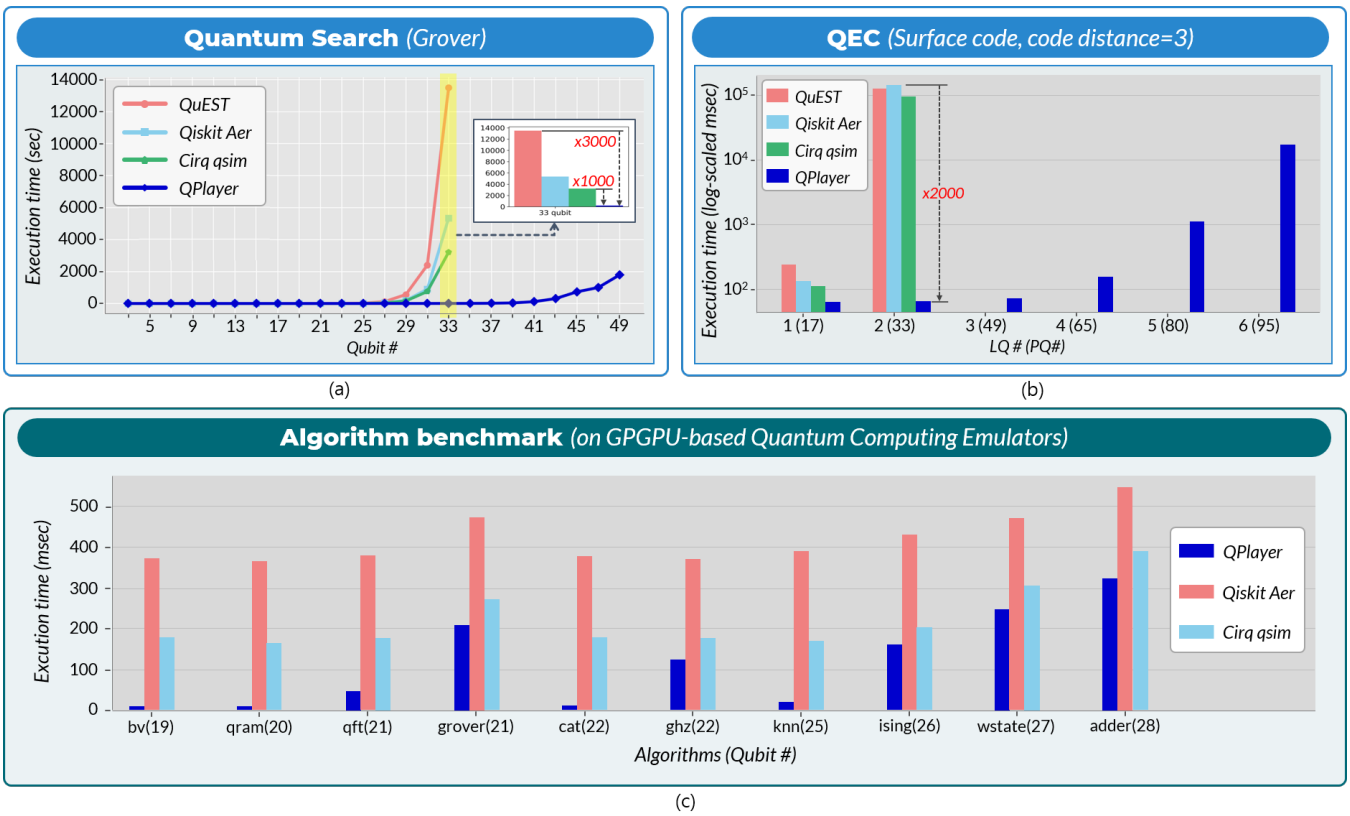


Figure 2: Experimental comparison of quantum circuit simulation. (a) Grover: quantum search algorithm. (b) Surface Code: quantum error correction(code distance=3). (c) QASMBench: various quantum benchmark algorithms.

shows faster simulation performance than other simulators in most algorithms. For example, in the bv algorithm, QPlayer took 11 milliseconds, while Qiskit and Cirq took 375 milliseconds and 181 milliseconds, respectively. As the number of qubits increased in algorithms such as ising, wstate, and Adder, the performance gap decreased, but it was found that QPlayer guaranteed performance two to three times faster.

4 Conclusions

This study introduces the architecture and operational flows of a quantum simulation software framework called QPlayer. It consists of a frontend for preprocessing quantum circuits and a simulation engine core for gate operations. Notably, QPlayer dynamically applies a Hilbert space suitable for quantum simulations, depending on the pattern of quantum circuit. In addition, we presented comparative studies of various quantum simulators through both analytical and experimental approaches. Experimental results have shown that QPlayer guarantees relatively faster simulation compared to other simulators. In particular, we confirmed that QPlayer has a comparative advantage over conventional simulators in some specific quantum algorithms.

Acknowledgements

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00014, A Technology Development of Quantum OS for Fault-tolerant Logical Qubit Computing Environment).

References

[1] List of quantum software simulators. Available from: https://quantiki.org/wiki/list-qc-simulators [last accessed August, 2024].

[2] K. S. Jin and G. I. Cha. QPlayer: Lightweight, scalable, and fast quantum simulator. *ETRI Journal* , pages 304–317, 2023.

[3] K. S. Jin and G. I. Cha. Multilayered logical qubits and synthesized quantum bits. *Quantum Science and Technology* , 8.3: 035008, 2023.

[4] T. Jones, A. Brown, I. Bush and S. C. Benjamin. QuEST and high-performance simulation of quantum computers. *Scientific reports*, 9.1, 2019.

[5] Google Cirq: Quantum Simulator. Available from: https://quantumai.google/cirq [last accessed August, 2024].

[6] IBM Qiskit: Quantum Simulator. Available from: https://www.ibm.com/quantum/qiskit [last accessed August, 2024].

Mercer decomposition of quantum kernels and entangled tensor kernels

Seongwook Shin[1] * Ryan Sweke[2] † Hyunseok Jeong[1] ‡

[1] *Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea*
[2] *IBM Quantum, Almaden Research Center, San Jose, CA, USA*

Abstract. Understanding the eigendecomposition (Mercer decomposition) of a kernel operator is crucial for evaluating the effectiveness of kernel algorithms, including quantum kernel algorithms. We introduce a tensor network approach to obtain the Mercer decomposition of quantum kernels. Additionally, we present an entangled tensor kernel—a generalized product kernel—and classify quantum kernels as a specific subclass of it. With this perspective, we observe that useful quantum kernels utilize a small dimensional function space, which is spanned by highly entangled functions. Finally, using introduced techniques we analyze single-layer quantum kernels.

Keywords: Quantum kernel, Tensor network

1 Introduction

A kernel method is a non-parametrized machine learning algorithm that obtains optimal functions using convex optimization with a kernel matrix $\mathbf{K}$ constructed from kernel functions. Each element $\mathbf{K}_{ij} = \mathcal{K}(\mathbf{x}_i, \mathbf{x}_j)$ is calculated by the Kernel function $\mathcal{K} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, where $\mathbf{x} \in \mathcal{X}$ denotes the data vector. The performance of the kernel method is closely related to its eigendecomposition [1, 2], or *Mercer's decomposition*, of $\mathcal{K}$, which is defined as $\mathcal{K}(x, y) = \sum_{j=1}^{\infty} \gamma_j e_j(x) e_j(y)$, where $\langle e_i, e_j \rangle_{\mathcal{L}^2} = \delta_{ij}$, and γ_is are eigenvalues. Informally, kernels perform well only when the target function aligns with the eigensubspace associated with high-eigenvalues of $\mathbf{K}$. In other words, each kernel has its own specific strengths, and understanding Mercer's decomposition is crucial for addressing it.

A quantum kernel method that utilizes a data-dependent quantum circuit as a kernel matrix evaluator, is one of the most popular quantum machine learning algorithms. A distinctive character of the quantum kernel method is that the kernel function is given by quantum-circuit generated values such as

$$\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') := \left| \langle 0|^{\otimes n} \mathcal{U}^\dagger(\mathbf{x}; \mathcal{E}) \mathcal{U}(\mathbf{x}'; \mathcal{E}) |0\rangle^{\otimes n} \right|^2. \quad (1)$$

We introduce a tensor network perspective to obtain Mercer's decomposition for general quantum kernels, building on recent work [4]. This perspective inspires a generalized tensor product kernel, which is an entangled version of the conventional tensor product of kernels. Using this entangled kernel, we classify quantum kernels as a subclass within these kernels, arguing that a quantum kernel is a special way to generate a large dimensional kernel from smaller dimensional kernels, characterized by its highly entangled feature maps. Finally, we argue that the usefulness of quantum kernels lies in the highly entangled eigenfunctions.

*wookshin@snu.ac.kr
†ryan.sweke@ibm.com
‡h.jeong37@gmail.com

2 Mercer's decomposition of quantum kernels

Given $\mathcal{U}(\mathbf{x}; \mathcal{E})$ in Eq. (1), we decompose all encoding gates into single-qubit Pauli-Z rotation gates. Then we can represent it with alternating layers of diagonal, tensor-product encoding part and non-parametrized part,

$$\mathcal{U}(\mathbf{x}; \mathcal{E}) = \prod_{j=1}^{L} S_j(\mathbf{x}) \mathbf{W}_j, \qquad S_j(\mathbf{x}) := \left(\bigotimes_{k=1}^{n} e^{-i\phi_{jk}(\mathbf{x}) Z_k/2} \right). \quad (2)$$

We denoted pre-processing functions that depend on the $\mathcal{E}$ as ϕ, non-parametrized unitaries as $\mathbf{W}$, and Z_k denotes the Pauli-Z operator on kth qubit. Then using the technique in Ref. [4], we obtain

$$\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') = \langle \mathbf{T}(\mathbf{x}) | \, \mathbf{C_T} \, | \mathbf{T}(\mathbf{x}') \rangle \,, \quad (3)$$

with

$$|\mathbf{T}(\mathbf{x})\rangle := \bigotimes_{j=1}^{L} \bigotimes_{k=1}^{n} \left| \mathbf{T}^{(jk)}(\mathbf{x}) \right\rangle = \bigotimes_{j}^{L} \bigotimes_{k}^{n} \begin{pmatrix} 1 \\ \cos\phi_{jk}(\mathbf{x}) \\ \sin\phi_{jk}(\mathbf{x}) \end{pmatrix}, \quad (4)$$

and $\mathbf{C_T}$ is the tensor having $2nL$ 3-dimensional legs. This core tensor $\mathbf{C_T}$ is $3^{nL} \times 3^{nL}$ symmetric, positive semi-definite (PSD) matrix, and obtained only from non-data dependent parts, $\mathbf{W}_j$s of the circuit. Derivation and definitions can be found in the Appendix Section 2.

To obtain a Mercer decomposition, we first orthonormalize the functions in the components of $|\mathbf{T}(\mathbf{x})\rangle$ by using the Gram-Schmidt procedure and truncate the zero elements resulting from linearly dependent functions. This generates a D dimensional $\left|\tilde{\mathbf{T}}(\mathbf{x})\right\rangle$, where all components are orthonormalized. All these procedures induce the transformation of $\mathbf{C_T}$ into $D \times D$ $\tilde{\mathbf{C}}_\mathbf{T}$ matrix that is symmetric and PSD as well. Finally, we diagonalize $\tilde{\mathbf{C}}_\mathbf{T}$,

getting a Mercer form

$$\begin{aligned}\mathcal{K}_Q(\mathbf{x},\mathbf{x}') &= \left\langle \mathbf{T}(\tilde{\mathbf{x}}) \right| \tilde{\mathbf{C}}_{\mathbf{T}} \left| \mathbf{T}(\tilde{\mathbf{x}}) \right\rangle \\ &= \left\langle \mathbf{T}(\tilde{\mathbf{x}}) \right| \mathbf{U}^\dagger \mathbf{D} \mathbf{U} \left| \mathbf{T}(\tilde{\mathbf{x}'}) \right\rangle \\ &= \sum_{j=1}^{D} \mathbf{D}_{jj} \left(\sum_{l=1} \mathbf{U}^*_{jl} \tilde{\mathbf{T}}_l(\mathbf{x}) \right) \left(\sum_{l'=1} \mathbf{U}_{jl'} \tilde{\mathbf{T}}_{l'}(\mathbf{x}') \right).\end{aligned} \tag{5}$$

Again we refer to the Appendix Section 2 for a definition of $\tilde{\mathbf{C}}_{\mathbf{T}}$.

3 Entangled tensor kernels

Given two kernels $K^{(1)} : \mathcal{X}_1 \times \mathcal{X}_1 \to \mathbb{R}$ and $K^{(2)} : \mathcal{X}_2 \times \mathcal{X}_2 \to \mathbb{R}$, one can construct a new kernel K in the domain of $\mathcal{X}_1 \times \mathcal{X}_2$ with tensor product by defining

$$K((\mathbf{x}_1,\mathbf{x}_2),(\mathbf{x}_1',\mathbf{x}_2')) = K^{(1)}(\mathbf{x}_1,\mathbf{x}_1')K^{(2)}(\mathbf{x}_2,\mathbf{x}_2'). \tag{6}$$

The Mercer decomposition of this product kernel becomes

$$\sum_i^{d_1} \sum_j^{d_2} \gamma_i^{(1)} \gamma_j^{(2)} e_i^{(1)}(\mathbf{x}_1) e_j^{(2)}(\mathbf{x}_2) e_i^{(1)}(\mathbf{x}_1') e_j^{(2)}(\mathbf{x}_2'), \tag{7}$$

where $\gamma_i^{(1/2)}, e_i^{(1/2)}(\mathbf{x}_{1/2})$ are eigenvalues and eigenfunctions for respective kernel, and $d_{1,2}$ is the dimension of corresponding Hilbert space. However, if we have access to feature maps $\left|F^{(1/2)}(\mathbf{x}_{1/2})\right\rangle$ which satisfies $K^{(1/2)}(\mathbf{x},\mathbf{x}') = \left\langle F^{(1/2)}(\mathbf{x}) \middle| F^{(1/2)}(\mathbf{x}') \right\rangle$, we can *entangle* basis functions of two kernels using $d_1 d_2 \times d_1 d_2$ PSD matrix $\mathbf{C}$, generating an (unnormalized) *entangled tensor kernel* which is defined as follows:

$$\begin{aligned}&K_C((\mathbf{x}_1,\mathbf{x}_2),(\mathbf{x}_1',\mathbf{x}_2')) \\ &= \left\langle F^{(1)}(\mathbf{x}_1) \right| \left\langle F^{(2)}(\mathbf{x}_2) \right| \mathbf{C} \left| F^{(1)}(\mathbf{x}_1') \right\rangle \left| F^{(2)}(\mathbf{x}_2') \right\rangle \\ &= \left\langle e^{(1)}(\mathbf{x}_1) \right| \left\langle e^{(2)}(\mathbf{x}_2) \right| (\sqrt{\mathbf{\Gamma}_1} \otimes \sqrt{\mathbf{\Gamma}_2}) \mathbf{C} \times \\ &(\sqrt{\mathbf{\Gamma}_1} \otimes \sqrt{\mathbf{\Gamma}_2}) \left| e^{(1)}(\mathbf{x}_1') \right\rangle \left| e^{(2)}(\mathbf{x}_2') \right\rangle.\end{aligned} \tag{8}$$

This entangled kernel's eigenfunctions are given by

$$\phi_k(\mathbf{x}) = \mathbf{U}_{k,ij} e_i^{(1)}(\mathbf{x}_1) e_j^{(2)}(\mathbf{x}_2), \tag{9}$$

where $\mathbf{U}$ diagonalizes $(\sqrt{\mathbf{\Gamma}_1} \otimes \sqrt{\mathbf{\Gamma}_2}) \mathbf{C} (\sqrt{\mathbf{\Gamma}_1} \otimes \sqrt{\mathbf{\Gamma}_2})$. These eigenfunctions are entangled functions of eigenfunctions of the usual tensor product kernels, and this is where the *entangled* tensor kernel name follows. Note that a usual product kernel as in Eq. (6) corresponds to the special case where $\mathbf{C} = \mathbf{I}$.

This entangled kernel can be generalized to be composed of arbitrary N kernels, by utilizing $\Pi_{j=1}^N d_j \times \Pi_{j=1}^N d_j$ PSD matrix, we can generate entangled kernels from given N kernels that can utilize nontrivial, high dimensional eigenfunctions.

3.1 Computational complexity of entangled tensor kernels

For simplicity, let all feature spaces' dimensions be d. To calculate $K_C(\mathbf{x},\mathbf{x}')$, one needs $O(d^2 N)$ multiplications, which is exponential to the number of composing kernels. However, by recognizing that the feature map is a tensor product of N d-dimensional vectors, we can represent $\mathbf{C}$ with an N-site matrix product operator (MPO). The computational complexity of calculating K_C with $\mathbf{C}$ having a maximum bond dimension of χ is $O(d^2 \chi^2 N)$, implying that a low-bond dimensional MPO enables an efficient entangled tensor kernel with exponentially large feature space.

3.2 Quantum kernels as entangled tensor kernels

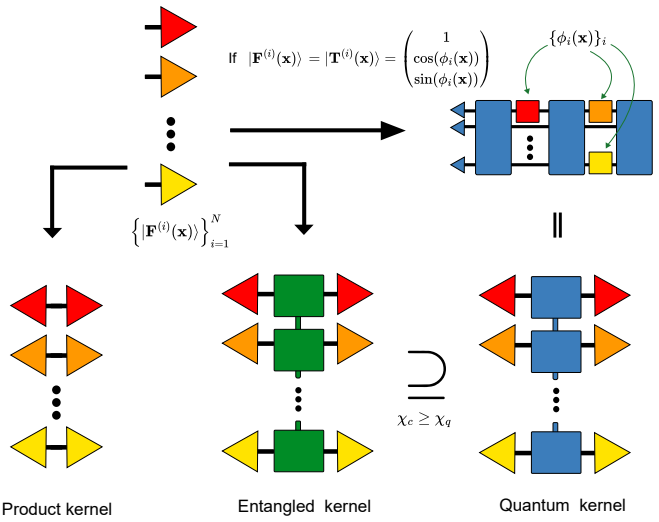


Figure 1: Relationships among composite kernels that can be constructed from tensor product feature maps.

Now one can notice that a quantum kernel $\mathcal{K}_Q$ is an entangled tensor kernel constructed with feature maps $\left|\mathbf{T}^{(jk)}(\mathbf{x})\right\rangle$, and a quantum-circuit generated PSD $\mathbf{C}_{\mathbf{T}}$. In other words, one can view quantum kernels as a subclass of entangled tensor kernels, but now the core tensor is constructed with quantum circuits.

From the above complexity argument, we see that if $\mathbf{C}_{\mathbf{T}}$ allows efficient tensor network representations such as low-bond dimensional MPO, then that quantum kernel is classically efficiently generatable. Therefore, classically hard quantum kernels should possess high entanglement in $\mathbf{C}_{\mathbf{T}}$. Unfortunately, when a quantum kernel is given, identifying whether the $\mathbf{C}_{\mathbf{T}}$ of it has an efficient tensor network description is a nontrivial task in general. However, it has been numerically confirmed that typical efficient quantum circuits—using only a polynomial number of quantum gates—can generate high bond dimensional $\mathbf{C}_{\mathbf{T}}$ [4]. Thus, we expect that quantum kernels are efficient methods for generating highly entangled core tensors that are not tractable by classical means.

4 Generalizability and way to possible quantum advantage

We want to approximate the target function using as few samples as possible. Especially for the quantum kernels, we wish to use only $O(poly(N))$ samples where N is the number of qubits used. This is possible only when the largest eigenvalues scale as $O(1/poly(N))$ [3]. Moreover, only eigenvectors associated with $O(1/poly(N))$ scaling eigenvalues can be learned with $O(poly(N))$ samples [1].

This implies that generalizable quantum kernels have effective dimensions that scale only polynomially, $D = O(poly(N))$, even though they have exponentially large function spaces. That quantum kernel could be replaceable by truncated kernels

$$\tilde{\mathcal{K}}_Q(\mathbf{x}, \mathbf{x}') := \sum_{j=1}^{D} \gamma_j \phi_j(\mathbf{x}) \phi_j(\mathbf{x}'), \tag{10}$$

where ϕ_js are the top D eigenfunctions of $\mathcal{K}_Q$. Now note that if those eigenfunctions are classically efficiently calculable, $\mathcal{K}_Q$ can be efficiently replaced by $\tilde{\mathcal{K}}_Q$. Therefore, we characterize useful (generalizable) yet classically hard quantum kernels as those that utilize polynomially large function spaces, which are spanned by classically intractable eigenfunctions such as highly entangled eigenfunctions.

5 Single-layer, single-encoding case

We look for the $L = 1$, n-qubit circuit case,

$$\begin{aligned} \mathcal{U}(\mathbf{x}) &= \left(\bigotimes_{k=1}^{n} e^{-i\mathbf{x}_k Z_k/2} \right) \mathbf{W} \\ &= \mathbf{S}(\mathbf{x}) \mathbf{W}, \end{aligned} \tag{11}$$

where $\mathbf{x} \in [-\pi, \pi)^n$.

In this scenario,

$$\begin{aligned} \mathcal{K}_Q(\mathbf{x}, \mathbf{x}') &= \left(\begin{pmatrix} 1 \\ e^{i\mathbf{x}_k} \\ e^{-i\mathbf{x}_k} \end{pmatrix}^{\top} \right)^{\otimes N} \tilde{\mathbf{C}} \begin{pmatrix} 1 \\ e^{-i\mathbf{x}'_k} \\ e^{i\mathbf{x}'_k} \end{pmatrix}^{\otimes N} \\ &= \sum_{\alpha \in \{00,01,10\}^N} \tilde{\mathbf{C}}_{\alpha,\alpha} e^{-i\omega_\alpha \cdot (\mathbf{x} - \mathbf{x}')}, \end{aligned} \tag{12}$$

where frequency vectors $\omega_\alpha \in \{-1, 0, 1\}^N$ are defined as

$$(\omega_\alpha)_k = \begin{cases} 0 & \text{if } \alpha_{2k-1}\alpha_{2k} = 00 \\ 1 & \text{if } \alpha_{2k-1}\alpha_{2k} = 01 \\ -1 & \text{if } \alpha_{2k-1}\alpha_{2k} = 10 \end{cases} \tag{13}$$

$$\tilde{\mathbf{C}}_{\alpha,\alpha} = \sum_{\alpha \in \mathcal{I}_\alpha} \psi^2_{\alpha_1\alpha_3,\ldots,\alpha_{2N-1}} \psi^2_{\alpha_2\alpha_4,\ldots,\alpha_{2N}}, \tag{14}$$

and $\mathcal{I}_\alpha$ is the set of all 2^N length bitstrings containing 00 and 11 sequences where $\alpha_{2k-1}\alpha_{2k} = 00$. For $n = 2$ instances, $\mathcal{I}_{0000} = \{0000, 0011, 1100, 1111\}$, $\mathcal{I}_{0011} = \{0011, 1111\}$, and so on. Here $\psi^2_{\mathbf{i}}$ is the squared components of $|\psi\rangle = \mathbf{W}|0\rangle^N$.

This analysis indicates that if the Born probability of $|\psi\rangle$ can be represented by an efficient MPS, then single-layer quantum kernels can be dequantized. We could also identify the concentration tendency to low-degree eigenfunctions. Additionally, because the eigenfunctions are in a product form, generalizable models that rely on a polynomial number of eigenfunctions to span their effective function space can also be dequantized using efficient entangled tensor kernels.

6 Summary and Conclusion

We introduced a method for obtaining Mercer decompositions of quantum kernels by representing them using tensor networks. Although this approach is inefficient, it allows us to separate the data-dependent and non-dependent parts, avoiding the need to integrate the data-dependent quantum state over the data space, as done in previous work [3]. Inspired by the tensor network form of quantum kernels, we introduced entangled tensor kernels generated by multiple kernels, a generalized version of the product of kernels. We assert that a quantum kernel is a method to create a new high-dimensional kernel from several kernels and efficiently generate highly entangled eigenfunctions. For quantum kernels to be advantageous over classical kernels, they should have small effective dimensions while their eigenfunctions should be highly entangled, making them resistant to efficient classical approximations. Finally, using the introduced techniques, we analyze the single-layer quantum kernel, which is more general than previously studied tensor-product quantum kernels [2, 3], enriching the understanding of quantum kernels.

References

[1] Abdulkadir Canatar, Blake Bordelon, and Cengiz Pehlevan. Spectral bias and task-model alignment explain generalization in kernel regression and infinitely wide neural networks. *Nature Communications*, 12(1):2914, 2021.

[2] Abdulkadir Canatar, Evan Peters, Cengiz Pehlevan, Stefan M. Wild, and Ruslan Shaydulin. Bandwidth enables generalization in quantum kernel models, 2023.

[3] Jonas M Kübler, Simon Buchholz, and Bernhard Schölkopf. The Inductive Bias of Quantum Kernels. *arXiv*, 2021.

[4] Seongwook Shin, Yong Siah Teo, and Hyunseok Jeong. Dequantizing quantum machine learning models using tensor networks. *Phys. Rev. Res.*, 6:023218, May 2024.

Appendix : Mercer decomposition of quantum kernels and entangled tensor kernels

Seongwook Shin[1], Ryan Sweke[2], and Hyunseok Jeong[1]

[1]Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea
[2]IBM Quantum, Almaden Research Center, San Jose, CA, USA

This serves as an appendix of the extended abstract for the AQIS2024 submission. The contents are not yet complete but supplement what is needed.

1 Introduction

A kernel method is a non-parametrized machine learning algorithm that obtains optimal functions using convex optimization with a kernel matrix $\mathbf{K}$ constructed from kernel functions. Each element $\mathbf{K}_{ij} = \mathcal{K}(\mathbf{x}_i, \mathbf{x}_j)$ is calculated by the Kernel function $\mathcal{K} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, where $\mathbf{x} \in \mathcal{X}$ denotes the data vector. The performance of the kernel method is closely related to its eigendecomposition [1, 2], or *Mercer's decomposition*, of $\mathcal{K}$, which is defined as $\mathcal{K}(x, y) = \sum_{j=1}^{\infty} \gamma_j e_j(x) e_j(y)$, where $\langle e_i, e_j \rangle_{\mathcal{L}^2} = \delta_{ij}$, and γ_is are eigenvalues. Informally, kernels perform well only when the target function aligns with the eigensubspace associated with high-eigenvalues of $\mathcal{K}$. In other words, each kernel has its own specific strengths, and understanding Mercer's decomposition is crucial for addressing it.

A quantum kernel method that utilizes a data-dependent quantum circuit as a kernel matrix evaluator, is one of the most popular quantum machine learning algorithms. A distinctive character of the quantum kernel method is that the kernel function is given by quantum-circuit generated values such as

$$\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') := \left| \langle 0|^{\otimes n} \mathcal{U}^\dagger(\mathbf{x}; \mathcal{E}) \mathcal{U}(\mathbf{x}'; \mathcal{E}) |0\rangle^{\otimes n} \right|^2. \tag{1}$$

We introduce a tensor network perspective to obtain Mercer's decomposition for general quantum kernels, building on recent work [3]. This perspective inspires a generalized tensor product kernel, which is an entangled version of the conventional tensor product of kernels. Using this entangled tensor kernel, we classify quantum kernels as a subclass within these kernels, arguing that a quantum kernel is a special way to generate a large dimensional kernel from smaller dimensional kernels, characterized by its highly entangled feature maps. Finally, we analyze the single-layer quantum kernels to elaborate more on the introduced techniques.

2 Mercer decomposition of quantum kernels

A kernel is a symmetric, positive function $\mathcal{K} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, where $\mathbf{x} \in \mathcal{X}$ denotes the data vector. By Mercer's theorem we can eigendecompose this to get a *Mercer decomposition* of $\mathcal{K}$, which is defined as

$$\mathcal{K}(x, y) = \sum_{j=1}^{\infty} \gamma_j e_j(x) e_j(y), \tag{2}$$

where $\langle e_i, e_j \rangle_{\mathcal{L}^2} = \delta_{ij}$, and γ_is are eigenvalues. The performance of kernel method is highly related to its eigenvalue distributions and eigen functions [1, 2]. Therfore, it is important to obtain Mercer decomposition of quantum kernels to unpack their abilities.

We consider quantum kernels using n qubits,

$$\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') := \left| \langle 0|^{\otimes n} \mathcal{U}^\dagger(\mathbf{x}; \mathcal{E}) \mathcal{U}(\mathbf{x}'; \mathcal{E}) |0\rangle^{\otimes n} \right|^2. \tag{3}$$

The encoding strategy which is denoted as $\mathcal{E}$ is a description of the circuit structure, positions of $\mathbf{x}$ dependent gates (encoding gates), and preprocessing functions on the data $\mathbf{x}$. We decompose all encoding gates into $\mathbf{x}$-dependent single-qubit gates and non-parametrized two-qubit gates, followed by the diagonalization of all single-qubit gates. Now we can rewrite the $\mathcal{U}(\mathbf{x}; \mathcal{E})$ as alternating layers of diagonal, tensor-product encoding part and non-parametrized part,

$$\mathcal{U}(\mathbf{x}; \mathcal{E}) = \prod_{j=1}^{L} S_j(\mathbf{x}) \mathbf{W}_j, \qquad S_j(\mathbf{x}) := \left(\bigotimes_{k=1}^{n} e^{-i\phi_{jk}(\mathbf{x}) Z_k/2} \right) \tag{4}$$

We denoted pre-processing functions that depend on the $\mathcal{E}$ as ϕ, non-parametrized unitaries as $\mathbf{W}$, and Z_k denotes the Pauli-Z operator on kth qubit.

2.1 Quantum kernels in tensor network form

We use *parallelization* technique, where one can use diagrammatical calculation as in Fig. 1. We define

$$O' = \begin{cases} \bigotimes_{j=1}^{(L-1)/2} (W_{2j}^\dagger \otimes I) |\Phi\rangle \langle\Phi| (W_{2j} \otimes I) \otimes I, & \text{if L is odd} \\ \bigotimes_{j=1}^{L/2} (W_{2j}^\dagger \otimes I) |\Phi\rangle \langle\Phi| (W_{2j} \otimes I) \otimes I, & \text{if L is even} \end{cases} \tag{5}$$

$$\rho = \begin{cases} W_1 |0\rangle \langle 0| W_1^\dagger \otimes \bigotimes_{j=1}^{(L-1)/2} (I \otimes W_{2j+1}) |\Phi\rangle \langle\Phi| (I \otimes W_{2j+1}^\dagger), & \text{if L is odd} \\ W_1 |0\rangle \langle 0| W_1^\dagger \otimes \bigotimes_{j=1}^{(L/2-1)} (I \otimes W_{2j}) |\Phi\rangle \langle\Phi| (I \otimes W_{2j+1}^\dagger) \otimes |\Phi\rangle\langle\Phi|, & \text{if L is even} \end{cases} \tag{6}$$

as in Fig. **??**. Now we have

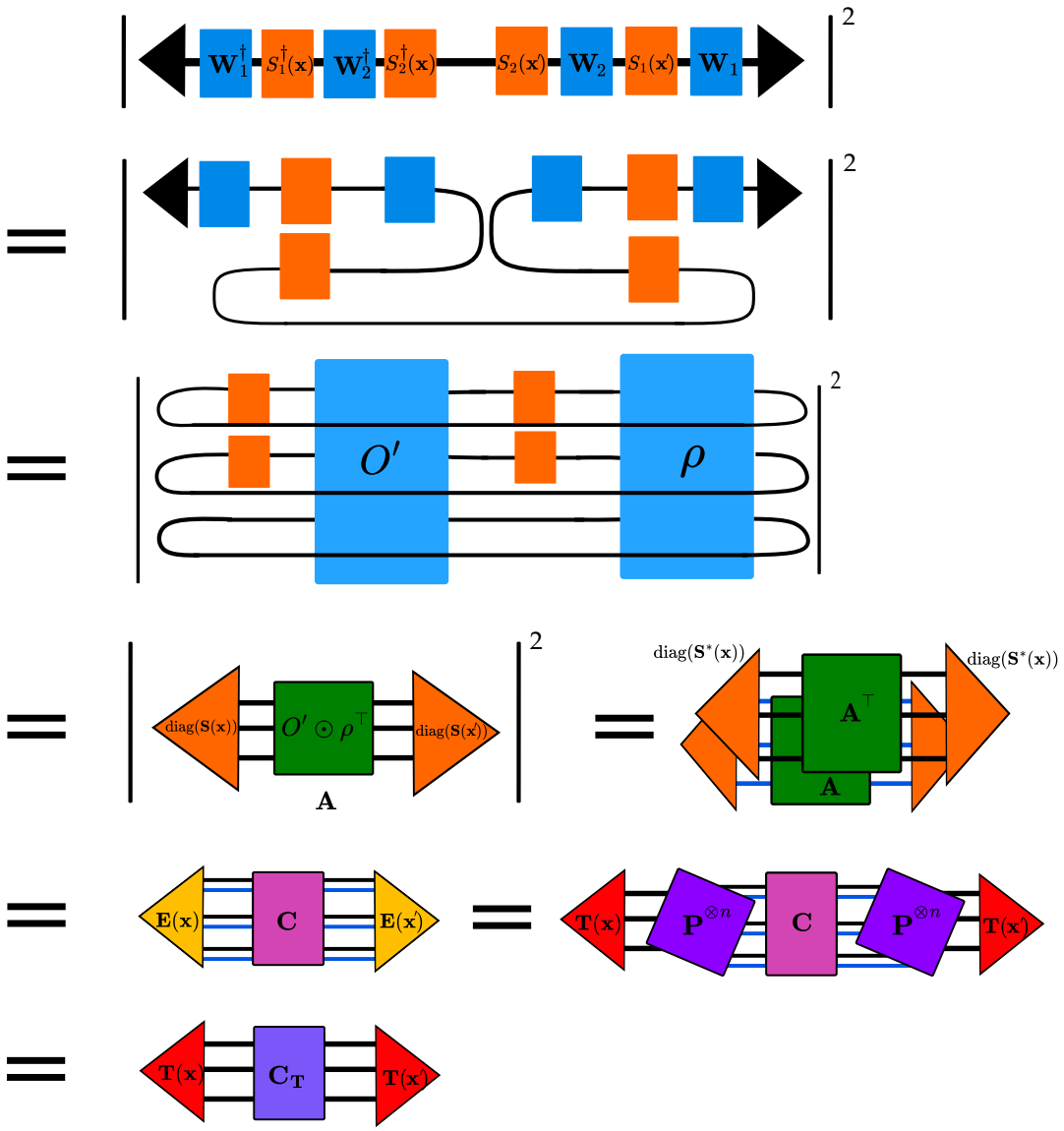
$$\mathcal{K}_Q = \mathrm{Tr}\Big\{ \rho \mathbf{S}^\dagger(x) O' \mathbf{S}(x') \Big\} \times (c.c) \tag{7}$$

We use the following equality

$$\mathrm{Tr}\Big\{ \mathrm{diag}(D)^\dagger \mathbf{A} \mathrm{diag}(D) \mathbf{B} \Big\} = \langle D| \left(\mathbf{A} \odot \mathbf{B}^\top \right) |D\rangle, \tag{8}$$

where $\odot$ represents the Hadamard product, D is a diagonal matrix and $\mathrm{diag}(D)$ denotes the diagonal matrix whose elements are entries of $|D\rangle$. With slight abuse of notation, we write a vector having elements of diagonal element of some diagonal matrix D as $|\mathrm{diag}(D)\rangle$. Using this, the quantum kernel becomes

$$\begin{aligned} \mathcal{K}_Q &= \langle \mathrm{diag}(\mathbf{S}(\mathbf{x}))| \left(O' \odot \rho^\top \right) |\mathrm{diag}(\mathbf{S}(\mathbf{x}'))\rangle \times (c.c) \\ &= \langle \mathrm{diag}(\mathbf{S}^*(\mathbf{x}))| \langle \mathrm{diag}(\mathbf{S}(\mathbf{x}))| \left(O' \odot \rho^\top \right)^\top \otimes \left(O' \odot \rho^\top \right) |\mathrm{diag}(\mathbf{S}^*(\mathbf{x}'))\rangle |\mathrm{diag}(\mathbf{S}(\mathbf{x}'))\rangle \\ &= \left(\bigotimes_{j=1}^{L} \left[\bigotimes_{k=1}^{n} \begin{pmatrix} 1 \\ e^{-i\phi_{jk}(\mathbf{x})} \\ e^{i\phi_{jk}(\mathbf{x})} \\ 1 \end{pmatrix} \right] \right)^\top (\mathbf{A}^\top \otimes_v \mathbf{A}) \bigotimes_{j=1}^{L} \left(\bigotimes_{k=1}^{n} \begin{pmatrix} 1 \\ e^{i\phi_{jk}(\mathbf{x}')} \\ e^{-i\phi_{jk}(\mathbf{x}')} \\ 1 \end{pmatrix} \right) \\ &:= \langle \mathbf{E}(\mathbf{x})| \mathbf{C} |\mathbf{E}(\mathbf{x}')\rangle, \end{aligned} \tag{9}$$



$$\mathbf{P} := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 1 & -i \\ 1 & 0 & 0 \end{pmatrix} \qquad O' := \qquad \rho :=$$

Figure 1: Diagramatical representation of getting tensor network form of quantum kernels. This shows the case when $L = 2$. Note the ordering of the 'vertical' tensor product $A^\top \otimes_v A$.

Where $\mathbf{C}$ has $2 \times 2nL$ legs, and satisfies

$$\mathbf{C}_{i_1 i_2 \ldots i_{2nL}; j_1 j_2 \ldots j_{2nL}} = \mathbf{A}^{\top}_{i_1 i_3 \ldots i_{2nL-1}; j_1 j_3 \ldots j_{2nL-1}} \times \mathbf{A}_{i_2 i_4 \ldots i_{2nL}; j_2 j_4 \ldots j_{2nL}}. \tag{10}$$

Diagramatically, one can think of $\mathbf{A}^{\top} \otimes_v \mathbf{A}$ as juxtaposing two tensors "vertically", thereby placing the same-qubit site indices be the nearest neighbors. The operator O' is a tensor product of identity and choi matrices of unitaries that are applied in the circuit, so it is a positive semidefinite (PSD). The operator $\rho^{\top}$ is also a PSD as it is a tensor product of (un-normalized) density matrices. Therefore, by the Schur product theorem, $\mathbf{A}$ and $\mathbf{C}$ are also PSD.

We observe that the core matrix $\mathbf{C}$ is complex-valued, and complex vector $|\mathbf{E}(\mathbf{x})\rangle\rangle$ possesses obvious redundant components incurred by repeated elements 1s. This can be dealt with introducing an isometry

$$\mathbf{P} := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 1 & -i \\ 1 & 0 & 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|I\rangle\rangle \langle 0| + |X\rangle\rangle \langle 1| + |Y\rangle\rangle \langle 2| \right), \tag{11}$$

where $|\mathbf{M}\rangle\rangle$ is the column-major vectorization of the matrix $\mathbf{M}$. From now on, for notational simplicity, we will set $N := nl$ and combine 'layer,qubit' index jk in to one index. This gives us the relation

$$\left|\mathbf{E}^{(k)}(\mathbf{x})\right\rangle\rangle = \begin{pmatrix} 1 \\ e^{i\phi_k(\mathbf{x})} \\ e^{-i\phi_k(\mathbf{x})} \\ 1 \end{pmatrix} = 2\mathbf{P} \left|\mathbf{T}^{(k)}(\mathbf{x})\right\rangle\rangle = \sqrt{2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 1 & -i \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \cos\phi_k(\mathbf{x}) \\ \frac{1}{\sqrt{2}} \sin\phi_k(\mathbf{x}) \end{pmatrix}. \tag{12}$$

We have set $\left\langle\left\langle \mathbf{T}^{(k)}(\mathbf{x}) \middle| \mathbf{T}^{(k)}(\mathbf{x}) \right\rangle\right\rangle = 1$, for normalization. Using an N tensor product of $\mathbf{P}$, we obtain

$$\begin{aligned} \mathcal{K}_Q &= \langle \mathbf{E}(\mathbf{x}) | \, \mathbf{C} \, | \mathbf{E}(\mathbf{x}') \rangle \\ &= \langle \mathbf{T}(\mathbf{x}) | \left(2^N \bigotimes_k \mathbf{P}^{\dagger} \right) \mathbf{C} \left(2^N \bigotimes_k \mathbf{P} \right) | \mathbf{T}(\mathbf{x}') \rangle \\ &:= \langle \mathbf{T}(\mathbf{x}) | \, \mathbf{C}_{\mathbf{T}} \, | \mathbf{T}(\mathbf{x}) \rangle, \end{aligned} \tag{13}$$

where tensors lose their superscripts, one should understand them as a N tensor product, such as $|\mathbf{T}(\mathbf{x})\rangle = \bigotimes_{k=1}^{N} \left|\mathbf{T}^{(k)}(\mathbf{x})\right\rangle$s, and $\mathbf{C}_{\mathbf{T}} := 4^N \left(\bigotimes_k \mathbf{P}^{\dagger} \right) \mathbf{C} \left(\bigotimes_k \mathbf{P} \right)$. Alternatively, we can also identify

$$(\mathbf{C}_{\mathbf{T}})_{\mathbf{ij}} = 4^N \times \frac{1}{2^N} \operatorname{Tr}\{\mathcal{P}_{\mathbf{i}} A \mathcal{P}_{\mathbf{j}} A\} \qquad \mathbf{i}, \mathbf{j} \in \{0,1,2\}^N, \tag{14}$$

where $\mathcal{P}_{\mathbf{i}}$ is the Pauli string. One can say that $\mathbf{C}_{\mathbf{T}}$ is a (truncated) re-scaled Pauli transfer matrix (PTM) of the linear map $\mathcal{A} : \mathbf{M} \mapsto A\mathbf{M}A$, and notice that it is also symmetric and now has real-valued elements. This process has a nice graphical description depicted in Fig. **??**.

Also, for PSD $\mathbf{C}$, $\mathbf{C}_{\mathbf{T}}$ is PSD as well. This is because for all $|v\rangle \in \mathbb{C}^{3^N}$, and PSD $\mathbf{C}$,

$$\begin{aligned} \frac{1}{4^N} \langle v | \, \mathbf{C}_{\mathbf{T}} \, | v \rangle &= \langle \tilde{v} | \, \mathbf{\Pi}_3 \mathbf{\Pi}_3 \mathbf{P}_{\mathbf{U}}{}^{\dagger} \mathbf{C} \mathbf{P}_{\mathbf{U}} \mathbf{\Pi}_3 \mathbf{\Pi}_3 \, | \tilde{v} \rangle \\ &= \langle \tilde{v} | \, \mathbf{\Pi}_3 \mathbf{C}' \mathbf{\Pi}_3 \, | \tilde{v} \rangle \geq 0, \end{aligned} \tag{15}$$

where $\Pi_3 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{\otimes N}$ is a projection and $\mathbf{P_U} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & i & 0 \\ 0 & 1 & -i & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}^{\otimes N}$, which is a unitary extension of $\mathbf{P}$ and $|\tilde{v}\rangle$ is an arbitrary extension of $|v\rangle$ to $\mathbb{C}^{4^n}$, which embed arbitrary elements to the extended dimension. Conjugation with unitary preserves PSD property, and $\mathbf{\Pi}_3 |\tilde{v}\rangle \in \mathbb{C}^{4^n}$, the last inequality follows.

2.2 Getting Mercer decomposition of quantum kernels

A Mercer decomposition of the kernel can provide a good understanding of its power. If $\mathbf{C_T}$ in Eq. (13) were diagonal, and all elements in $\mathbf{T}(\mathbf{x})$ were orthonormal, then it is done. However, this is not the case for general structures and general encoding strategies. Nevertheless, we can always transform this canonical form to Mercer decomposition form by orthonormalizing the components in $\mathbf{T}(\mathbf{x})$ and truncating and diagonalizing the core matrix.

First, we orthonormalize the set of components in $|\mathbf{T}(\mathbf{x})\rangle$, which are vectors in $L^2_\mu(\mathcal{X})$ space, $\{\mathbf{T}_j(\mathbf{x})\}_j$ by applying the Gram-Schmidt procedure on it. Through Gram-Schmidt, we get the set of orthogonal functions

$$\begin{aligned} u_k(\mathbf{x}) = \mathbf{T}_j(\mathbf{x}) - \sum_{j=1}^{k-1} \frac{\langle u_j, \mathbf{T}_k(\mathbf{x})\rangle}{\langle u_j, u_j\rangle} u_j(\mathbf{x}), \\ u_1(\mathbf{x}) = \mathbf{T}_1(\mathbf{x}) \end{aligned} \tag{16}$$

with $u_1(\mathbf{x}) = \mathbf{T}_i(\mathbf{x})$ and inner product is given as a $\langle u_i | u_j\rangle := \int_{\mathbf{x}\in\mathcal{X}} u_i^*(\mathbf{x}) u_j(\mathbf{x}) d\mu(\mathbf{x})$. Let us denote normalized vectors $u_k(\mathbf{x})/\|u_k\| := e_k(\mathbf{x})$, where $\|u_k\| = \sqrt{\langle u_k, u_k\rangle}$. Then one can see that

$$e_k(\mathbf{x}) = \sum_{j=1}^{k} \mathbf{L}_{kj} \mathbf{T}_j(\mathbf{x}), \tag{17}$$

where $\mathbf{L}$ is a lower triangular matrix and components satisfy the following recursive equation:

$$\begin{aligned} \mathbf{L}_{k,k-j} &= -\frac{1}{\|u_{k-j}\|} \sum_{l=0}^{j-1} \mathbf{L}_{k,k-l} \langle e_{k-j}, \mathbf{T}_{k-l}(\mathbf{x})\rangle, \\ \mathbf{L}_{k,k} &= \frac{1}{\|u_k\|} \end{aligned} \tag{18}$$

Using these constants as elements we can create lower triangular matrix $\mathbf{L}$, which satisfies

$$\mathbf{L} |\mathbf{T}(\mathbf{x})\rangle = \left|\bar{\mathbf{T}}(\mathbf{x})\right\rangle, \tag{19}$$

where

$$\left\langle \bar{\mathbf{T}}_i(\mathbf{x}), \bar{\mathbf{T}}_j(\mathbf{x}) \right\rangle = \delta_{ij} \qquad \text{if} \quad \bar{\mathbf{T}}_i(\mathbf{x}), \bar{\mathbf{T}}_j(\mathbf{x}) \neq 0. \tag{20}$$

The $L^2_\mu(\mathcal{X})$ space spanned by the elements of $\mathbf{T}(\mathbf{x})$ may have a dimension $K < 3^N$, in other words they might not form a linearly independent set. In such cases, certain components $\mathbf{T}_i(\mathbf{x})$s can be expressed as a linear combination of other components $\mathbf{T}_{j<i}(\mathbf{x})$s such as $\mathbf{T}_i(\mathbf{x}) = \sum_{j<i} \alpha_j \mathbf{T}_j(\mathbf{x})$. For these indices, we set the ith row of $\mathbf{L}$ as

$$\mathbf{L}_{ij} = \begin{pmatrix} -\alpha_1 & -\alpha_2 & \dots & -\alpha_{i-1} & 1 & 0 \dots 0 \end{pmatrix}. \tag{21}$$

In this way, we construct the matrix $\mathbf{L}$ which also satisfies the following property,

$$\bar{\mathbf{T}}_i(\mathbf{x}) = 0 \quad \text{if} \qquad \mathbf{T}_i(\mathbf{x}) = \sum_{j<i} \alpha_j \mathbf{T}_j(\mathbf{x}) \quad \text{for some } \alpha_j \in \mathbb{R}. \tag{22}$$

Note that $\mathbf{L}$ always has non-zero elements along its diagonal, so is always invertible.

Now general quantum kernel becomes

$$\begin{aligned} \langle \mathbf{T}(\mathbf{x}) | \, \mathbf{C_T} \, | \mathbf{T}(\mathbf{x}') \rangle &= \langle \mathbf{T}(\mathbf{x}) | \, \mathbf{L}^\top (\mathbf{L}^\top)^{-1} \mathbf{C_T} \mathbf{L}^{-1} \mathbf{L} \, | \mathbf{T}(\mathbf{x}') \rangle \\ &= \left\langle \bar{\mathbf{T}}(\mathbf{x}) \right| (\mathbf{L}^{-1})^\top \mathbf{C_T} \mathbf{L}^{-1} \left| \bar{\mathbf{T}}(\mathbf{x}') \right\rangle . \end{aligned} \tag{23}$$

Next, we truncate the vector $\left|\bar{\mathbf{T}}(\mathbf{x})\right\rangle$, by removing the 0 elements, thereby reducing it to a $(D \leq 3^N)$-dimensional vector. Let us represent truncated vector as $\left|\tilde{\mathbf{T}}(\mathbf{x})\right\rangle$. Similarly, we adjust the matrix $(\mathbf{L}^{-1})^\top \mathbf{C_T} \mathbf{L}^{-1}$ to a $D \times D$ matrix. This is achieved by discarding the rows and columns associated with the indices $\{i\}$ for which $\bar{\mathbf{T}}_i(\mathbf{x}) = 0$. Let us represent this truncated core matrix as $\tilde{\mathbf{C}}_\mathbf{T}$. Finally, we diagonalize this truncated core matrix,

$$\left\langle \tilde{\mathbf{T}}(\mathbf{x}) \right| \tilde{\mathbf{C}}_\mathbf{T} \left| \tilde{\mathbf{T}}(\mathbf{x}') \right\rangle = \left\langle \tilde{\mathbf{T}}(\mathbf{x}) \right| \mathbf{U}^\dagger \mathbf{D}_{\tilde{\mathbf{C}}_\mathbf{T}} \mathbf{U} \left| \tilde{\mathbf{T}}(\mathbf{x}') \right\rangle . \tag{24}$$

Because all the components in $\{\tilde{\mathbf{T}}_i(\mathbf{x})\}_{i=1}^D$ are orthonormal, so do components in $\mathbf{U}\left|\tilde{\mathbf{T}}(\mathbf{x})\right\rangle$, and this gives us the Mercer's decomposition of the given quantum kernel, with eigenvalues being diagonal entries of $\mathbf{D}_{\tilde{\mathbf{C}}_\mathbf{T}}$ and eigenvectors $\{\sum_{j=1}^D U_{ij} \tilde{\mathbf{T}}_j(\mathbf{x})\}_i$. We call this orthonormalized and truncated form of a quantum kernel as *Mercer form*. This procedure is not efficient at all, since all matrices above have the size of 3^N.

3 Entangled tensor kernels

Given two kernels $K_1 : \mathcal{X}_1 \times \mathcal{X}_1 \to \mathbb{R}$ and $K_2 : \mathcal{X}_2 \times \mathcal{X}_2 \to \mathbb{R}$, one can construct a new kernel K in the domain of $\mathcal{X}_1 \times \mathcal{X}_2$ with tensor product by defining

$$K((\mathbf{x}_1, \mathbf{x}_2), (\mathbf{x}_1', \mathbf{x}_2')) := K_1(\mathbf{x}_1, \mathbf{x}_1') K_2(\mathbf{x}_2, \mathbf{x}_2'). \tag{25}$$

This is one way of constructing a larger dimensional kernel out of smaller dimensional kernels. The Mercer decomposition of this new product kernel becomes

$$\sum_i^{d_1} \sum_j^{d_2} \gamma_i^{(1)} \gamma_j^{(2)} e_i^{(1)}(\mathbf{x}_1) e_j^{(2)}(\mathbf{x}_2) e_i^{(1)}(\mathbf{x}_1') e_j^{(2)}(\mathbf{x}_2'), \tag{26}$$

where $\gamma_i^{(1,2)}, e_i^{(1,2)}(\mathbf{x}_{1,2})$ are eigenvalues and eigenfunctions for respective kernel, and $d_{1,2}$ is the dimension of corresponding Hilbert space. One can notice that the eigenfunctions and eigenvalues of the product kernel are the products of those of the individual kernels.

However, if we have access to feature maps $\left|F^{(1,2)}(\mathbf{x}_{1,2})\right\rangle$ which satisfies $K_{1,2}(\mathbf{x}, \mathbf{x}') = \left\langle F^{(1,2)}(\mathbf{x}) \middle| F^{(1,2)}(\mathbf{x}') \right\rangle$, we can *entangle* feature maps or eigenfunctions of two kernels using $d_1 d_2 \times d_1 d_2$ PSD and symmetric (Hermitian if feature maps were complex) matrix $\mathbf{C}$, generating an *entangled tensor kernel* which

$$K_C((\mathbf{x}_1, \mathbf{x}_2), (\mathbf{x}_1', \mathbf{x}_2')) = \frac{\left\langle F^{(1)}(\mathbf{x}_1) \right| \left\langle F^{(2)}(\mathbf{x}_2) \right| \mathbf{C} \left| F^{(1)}(\mathbf{x}_1') \right\rangle \left| F^{(2)}(\mathbf{x}_2') \right\rangle}{\sqrt{\langle \mathbf{C} \rangle_{\mathbf{x}_1, \mathbf{x}_2}} \sqrt{\langle \mathbf{C} \rangle_{\mathbf{x}_1', \mathbf{x}_2'}}}. \tag{27}$$

Here

$$\langle \mathbf{C} \rangle_{\mathbf{x}_1,\mathbf{x}_2} := \left\langle F^{(1)}(\mathbf{x}_1) \right| \left\langle F^{(2)}(\mathbf{x}_2) \right| \mathbf{C} \left| F^{(1)}(\mathbf{x}_1) \right\rangle \left| F^{(2)}(\mathbf{x}_2) \right\rangle \tag{28}$$

is a normalization factor to ensure diagonal values be normalized. Now we see that the new feature map is

$$\frac{\mathbf{B} \left| F^{(1)}(\mathbf{x}_1) \right\rangle \left| F^{(2)}(\mathbf{x}_2) \right\rangle}{\left\| \mathbf{B} \left| F^{(1)}(\mathbf{x}_1) \right\rangle \left| F^{(2)}(\mathbf{x}_2) \right\rangle \right\|_2} = \frac{\mathbf{B}(\sqrt{\mathbf{\Gamma}_1} \otimes \sqrt{\mathbf{\Gamma}_2}) \left| e^{(1)}(\mathbf{x}_1) \right\rangle \left| e^{(2)}(\mathbf{x}_2) \right\rangle}{\left\| \mathbf{B} \left| F^{(1)}(\mathbf{x}_1) \right\rangle \left| F^{(2)}(\mathbf{x}_2) \right\rangle \right\|_2}, \tag{29}$$

where $\mathbf{C} = \mathbf{B}^\top \mathbf{B}$, and $\mathbf{\Gamma_{1,2}}$ denotes the diagonal matrix composed of eigenvalues of each kernel. One can notice that the orthonormal basis functions of each kernel are non-trivially mixed by $\mathbf{B}$, $\mathbf{\Gamma}$, and normalization factors, thereby creating *entangled* eigenfunctions where the name 'entangled tensor kernels' follows. Note that the usual product of kernels corresponds to the case where core tensor $\mathbf{C} = \mathbf{I}$.

This entangled tensor kernel can be generalized to multiple N kernels, and utilizing arbitrary PSD symmetric (Hermitian) matrix $\mathbf{C}$ that matches the dimensions of feature spaces,

$$K_{\mathbf{C}}(\mathbf{x}, \mathbf{x}') = \frac{\langle \mathbf{F}(\mathbf{x}) | \, \mathbf{C} \, | \mathbf{F}(\mathbf{x}') \rangle}{\sqrt{\langle \mathbf{C} \rangle_{\mathbf{x}}} \sqrt{\langle \mathbf{C} \rangle_{\mathbf{x}'}}}. \tag{30}$$

Now one can orthonormalize the functions in the new feature map vector, getting a Mercer's decomposition of it. One can also consider an unnormalized version of entangled tensor kernels,

$$K_{\mathbf{C}}(\mathbf{x}, \mathbf{x}') = \langle \mathbf{F}(\mathbf{x}) | \, \mathbf{C} \, | \mathbf{F}(\mathbf{x}') \rangle \, . \tag{31}$$

In this case, we can have a more direct Mercer decomposition, if all feature spaces are factorized, i.e., $\int \langle \mathbf{e}(\mathbf{x}) | \mathbf{e}(\mathbf{x}) \rangle \, d\mathbf{x} = \prod_{k=1}^{N} \int \langle \mathbf{e}(\mathbf{x}_k) | \mathbf{e}(\mathbf{x}_k) \rangle \, d\mathbf{x}_k$, making all functions in $|\mathbf{e}(\mathbf{x})\rangle$ are orthonormal.

$$\begin{aligned} K_{\mathbf{C}}(\mathbf{x}, \mathbf{x}') &= \langle \mathbf{e}(\mathbf{x}) | \left(\bigotimes_{k=1}^{N} \sqrt{\mathbf{\Gamma}_k} \right) \mathbf{C} \left(\bigotimes_{k=1}^{N} \sqrt{\mathbf{\Gamma}_k} \right) | \mathbf{e}(\mathbf{x}') \rangle \\ &= \langle \mathbf{e}(\mathbf{x}) | \, \mathbf{U}^\dagger \mathbf{D} \mathbf{U} \, | \mathbf{e}(\mathbf{x}') \rangle \, . \end{aligned} \tag{32}$$

Here $|\mathbf{e}(\mathbf{x})\rangle := \bigotimes_{k=1}^{N} \left| \mathbf{e}^{(k)}(\mathbf{x}) \right\rangle$. Therefore, eigenfunctions of different feature spaces become entangled by diagonalizing unitary of $\left(\bigotimes_{k=1}^{N} \sqrt{\mathbf{\Gamma}_k} \right) \mathbf{C} \left(\bigotimes_{k=1}^{N} \sqrt{\mathbf{\Gamma}_k} \right)$, and serve as eigenfunctions of the newly generated kernel.

3.1 Computational complexity

For simplicity, let all feature spaces' dimensions be d. To calculate $K_C(\mathbf{x}, \mathbf{x}')$, one needs $O(d^2 N)$ multiplications, which is exponential to the number of composing kernels. However, by recognizing that the feature map is a tensor product of N d-dimensional vectors, we can represent $\mathbf{C}$ with an N-site matrix product operator (MPO). The computational complexity of calculating K_C with $\mathbf{C}$ having a maximum bond dimension of χ is $O(d^2 \chi^2 N)$, implying that a low-bond dimensional MPO enables an efficient entangled tensor kernel.

3.2 Examples of entangled tensor kernels.

3.2.1 polynomial kernel

A polynomial kernel is given as

$$\mathcal{K}_N(\mathbf{x}, \mathbf{x}') = (c + \mathbf{x}^\top \mathbf{x}')^N, \tag{33}$$

for some constant c. One can immediately see that the feature map is given by

$$\mathbf{F}(\mathbf{x}) = \left([\sqrt{c},\ \mathbf{x}_1,\ \mathbf{x}_2,\ \ldots,\ \mathbf{x}_d]^\top\right)^{\otimes N}, \tag{34}$$

and $\mathbf{C} = I$.

3.2.2 Periodic shift-invariant kernel

Shift-invariant kernels, characterized as

$$\mathbf{K}(\mathbf{x}, \mathbf{x}') = \mathcal{K}(\mathbf{x} - \mathbf{x}'), \tag{35}$$

for some function $\mathcal{K}$, have cosine and sine functions as their eigenfunctions. For concreteness, we set the input domain to $[-\pi, \pi]$, and periodically extend the function $\mathcal{K}$. Then $\mathcal{K}$ allows the Mercer decomposition,

$$\mathcal{K}(x - x') = \sum_{j=1}^{\infty} \gamma_j \{\cos(jx)\cos(jx') + \sin(jx)\sin(jx')\}, \tag{36}$$

with $c_j \geq 0$ []. We can write this in a complex version as

$$\mathcal{K}(x - x') = \sum_{j=1}^{\infty} \gamma_j \{e^{-ij(x-x')} + e^{ij(x-x')}\}. \tag{37}$$

Now we truncate the frequencies to the N so that $j \in [N]$. This N dimensional periodic shift-invariant kernel can be represented with entangled tensor kernel using $O(log(N))$ feature maps. For example, choose feature maps

$$\left|\mathbf{F}^{(k)}(x)\right\rangle = \begin{pmatrix} e^{-i3^{k-1}x} \\ 1 \\ e^{i3^{k-1}x} \end{pmatrix}, \quad k \ \in [\log_3 N], \tag{38}$$

then one can confirm that

$$\mathbf{F}_h(x) = \exp\left(\sum_{k}^{\log_3 N} 3^{k-1}(h_k - 1)\right), \tag{39}$$

where $h \in \{0, 1, 2\}^{\log_3 N}$. Therefore by setting

$$\mathbf{C}_{\bar{h},\bar{h}} = \mathbf{C}_{h,h} = \gamma_{\left|\sum_k^{\log_3 N} 3^{k-1}(h_k - 1)\right|}, \tag{40}$$

where $\bar{h}$ is the tritstring where 2 and 0 are interchanged, one can obtain

$$\mathcal{K}(x - x') = \langle \mathbf{F}(x)| \, \mathbf{C} \, |\mathbf{F}(x')\rangle \,. \tag{41}$$

Note that if the diagonal matrix $\mathbf{C}$ had $O(log(N))$ bond dimension, one could calculate this N-dimensional kernel using only logarithmic number of arithmetics.

3.2.3 Efficiently MPS sampleable Random Fourier feature

The random Fourier feature (RFF) method allows using much smaller dimensional function space than that of the original kernel while ensuring a similar performance. Random Fourier features should be sampled from the Fourier transform of the original (shift-invariant) kernel function, and recently using RFF to dequantize variational quantum machine learning models has been suggested [4]. However, for efficient dequantizing classical models require efficiently sampleable Fourier frequencies, and probability distribution representable with poly-dimensional bond dimension MPS is suggested one of them. Here we show that efficient MPS sampleable RFF method can be seen as an efficient entangled tensor kernel. We are given the general N feature maps induced by the quantum circuit,

$$\left|\mathbf{F}^{(\mathbf{k})}(\mathbf{x})\right\rangle = \left(e^{-i\omega_M^{(k)}\mathbf{x}_k} \quad e^{-i\omega_{M-1}^{(k)}\mathbf{x}_k} \quad \dots \quad e^{-i\omega_1^{(k)}\mathbf{x}_k} \quad 0 \quad e^{+i\omega_1^{(k)}\mathbf{x}_k} \quad \dots \quad e^{+i\omega_{M-1}^{(k)}\mathbf{x}_k} \quad e^{+i\omega_M^{(k)}\mathbf{x}_k}\right)^\top, \tag{42}$$

and efficient MPS $\mathbf{p}$ that encodes the probability $p(\omega)$ of frequency vectors ωs satisfying

$$p(\omega_{h_1}^{(1)}, \omega_{h_2}^{(2)}, \dots, \omega_{h_N}^{(N)}) = \mathbf{p}_{(M-h_1)(M-h_2)\dots(M-h_N)} = \mathbf{p}_{(2M+1-h_1)(2M+1-h_2)\dots(2M+1-h_N)}, \tag{43}$$

where $h_j \in [0, M]$. Now we add redundant indices to $\mathbf{p}$, creating an efficient MPO of which diagonal entries are elements of $\mathbf{p}$. Setting this to the core tensor and take Eq. (42) feature maps as composing feature maps, we construct efficient entangled tensor kernels that RFF method tried to approximate originally.

4 Quantum kernels as entangled tensor kernels.

In Section 2.1, we observed that any quantum kernel can be represented in a tensor network form, as shown in Equation 13. Using this observation, we see that K_Q is an entangled tensor kernel constructed with feature maps:

$$\left|\mathbf{T}^{(k)}(\mathbf{x})\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ \cos\phi_k(\mathbf{x})\\ \sin\phi_k(\mathbf{x})\end{pmatrix}, \tag{44}$$

which produce kernels:

$$\mathcal{K}^{(k)}(\mathbf{x}, \mathbf{x}') = \left\langle \mathbf{T}^{(k)}(\mathbf{x}) \middle| \mathbf{T}^{(k)}(\mathbf{x}') \right\rangle = \frac{1}{2}\left[1 + \cos\left(\phi_k(\mathbf{x}) - \phi_k(\mathbf{x}')\right)\right], \tag{45}$$

and a quantum-circuit generated symmetric PSD $\mathbf{C_T}$. While this form is an unnormalized entangled tensor kernel, it is automatically normalized because $\mathcal{K}_Q(\mathbf{x}, \mathbf{x}) = |\langle 0|^{\otimes n} \mathcal{U}^\dagger(\mathbf{x}; \mathcal{E})\mathcal{U}(\mathbf{x}; \mathcal{E}) |0\rangle^{\otimes n}|^2 = 1$.

This leads to the unnormalized entangled tensor kernel family that includes all quantum kernels using the same number of encoding gates:

$$\langle \mathbf{T}(\mathbf{x})| \mathbf{C_C} |\mathbf{T}(\mathbf{x})\rangle, \tag{46}$$

where $\mathbf{C_C}$ is a PSD symmetric $3^N \times 3^N$ matrix. Since $\mathbf{C_T}$ is a subset of all PSD symmetric matrices of the same size, we conclude that a quantum kernel is a subclass of entangled tensor kernels. In other words, the quantum kernel method is a special way to construct a normalized entangled tensor kernel when feature maps like Eq. (44) are used. By leveraging the pre-processing functions $\phi_k(\mathbf{x})$, we use them as rotation angles for single-qubit Pauli-Z rotations. Alongside these data-dependent gates, we select non-parametrized quantum

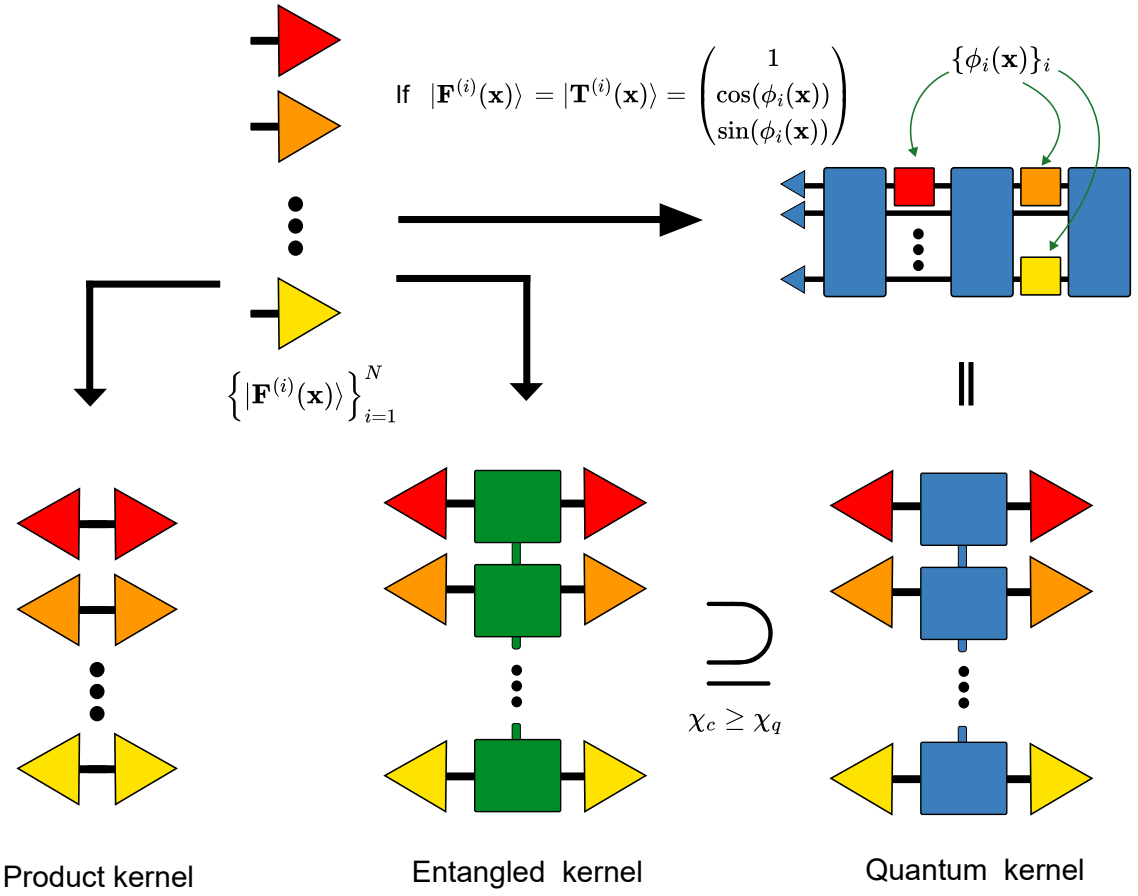


Figure 2: Quantum kernels are a subclass of entangled tensor kernels.

gates to construct a quantum circuit. Obtaining the expectation value of some observable gives us an entangled tensor kernel with $\mathbf{C_T}$ as defined in Eq. (13).

Classical entangled tensor kernels with polynomially scaling bond dimensions are efficiently calculable. Therefore, if the bond dimension of $\mathbf{C_T}$ is $O(poly(N))$, those quantum kernels can be efficiently replaced by classical kernels. However, it has been numerically confirmed that typical efficient quantum circuits—using only a polynomial number of quantum gates—can generate high bond dimensional $\mathbf{C_T}$ [3]. Thus, we expect that quantum kernels are efficient methods for generating highly entangled core tensors that are not tractable by classical means.

4.1 Generalization

We want to approximate the target function using as few samples as possible. Especially for the quantum kernels, we wish to use only $O(poly(N))$ samples where N is the number of qubits used. This is possible only when the largest eigenvalues scale as $O(1/poly(N))$ [2]. Moreover, only eigenvectors associated with $O(1/poly(N))$ scaling eigenvalues can be learned with $O(poly(N))$ samples [1] when $N \to \infty$. For quantum kernels,

$$\begin{aligned}\int \mathcal{K}_Q(\mathbf{x},\mathbf{x})p(\mathbf{x})d\mathbf{x} &= \int \left\langle \tilde{\mathbf{T}}(\mathbf{x})\right| \tilde{\mathbf{C}_\mathbf{T}} \left|\tilde{\mathbf{T}}(\mathbf{x})\right\rangle p(\mathbf{x})d\mathbf{x} \\ &= \mathrm{Tr}\Big\{\tilde{\mathbf{C}_\mathbf{T}} \int \left|\tilde{\mathbf{T}}(\mathbf{x})\right\rangle \left\langle \tilde{\mathbf{T}}(\mathbf{x})\right| p(\mathbf{x})d\mathbf{x}\Big\} \\ &= \mathrm{Tr}\Big\{\tilde{\mathbf{C}_\mathbf{T}}\mathbf{I}\Big\} \\ &= \sum_{i=1}^{D} (\mathbf{D}_{\tilde{\mathbf{C}_\mathbf{T}}})_{ii} = 1,\end{aligned} \tag{47}$$

implying that generalizable quantum kernels should have dimensions that scale only polynomially, $D = O(poly(N))$, or at least their eigenvalues should be largely concentrated on a polynomially scaling number of eigenfunctions, even though they have exponentially large function spaces. However, these generalizable quantum kernels can be approximated by

$$\tilde{\mathcal{K}}_Q(\mathbf{x},\mathbf{x}') := \sum_{j=1}^{D} \gamma_j \phi_j(\mathbf{x})\phi_j(\mathbf{x}'), \tag{48}$$

where the ϕ_js are the top D eigenfunctions of $\mathcal{K}_Q$. If these eigenfunctions were classically efficiently calculable, $\mathcal{K}_Q$ can be efficiently replaced by $\tilde{\mathcal{K}}_Q$. Therefore, we characterize useful (generalizable) yet classically hard quantum kernels as follows:

1. They utilize only a polynomially large effective function space.
2. Highly entangled eigenfunctions span the effective function space.

5 One-layer case

We look for the $L = 1$ case,

$$\begin{aligned}\mathcal{U}(\mathbf{x}) &= \left(\bigotimes_{k=1}^{N} e^{-i\phi_k(\mathbf{x})Z_k/2}\right)\mathbf{W} \\ &= \mathbf{S}(\mathbf{x})\mathbf{W}.\end{aligned} \tag{49}$$

For $L = 1$ case, we see that $O' = \mathbf{I}$, and $\rho = \mathbf{W}\,|0\rangle\langle 0|^{\otimes n}\,\mathbf{W}^\dagger := |\psi\rangle\langle\psi|$. Therefore,

$$\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') = \langle \mathrm{diag}(\mathbf{S}(\mathbf{x}))|\,(\mathbf{I} \odot |\psi\rangle\langle\psi|)\,|\mathrm{diag}(\mathbf{S}(\mathbf{x}'))\rangle \times (c.c). \tag{50}$$

When we apply the Hadamard product with the identity matrix $\mathbf{I}$, it selects the diagonal elements, leading to $(\mathbf{I} \odot |\psi\rangle\langle\psi|) = \mathrm{diag}(\psi^2)$, which is a diagonal matrix whose elements are the squared magnitudes of the components of $|\psi\rangle$. Therefore, from Eq. (13),

$$\begin{aligned}
\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') &= \langle \mathbf{E}(\mathbf{x})|\,\mathbf{C}\,|\mathbf{E}(\mathbf{x}')\rangle & (51)\\
&= \left(\bigotimes_{k=1}^{n} \begin{pmatrix} 1 \\ e^{-i\phi_k(\mathbf{x})} \\ e^{i\phi_k(\mathbf{x})} \\ 1 \end{pmatrix}\right)^\top (\mathrm{diag}(\psi^2) \otimes_v \mathrm{diag}(\psi^2)) \left(\bigotimes_{k=1}^{n} \begin{pmatrix} 1 \\ e^{i\phi_k(\mathbf{x}')} \\ e^{-i\phi_k(\mathbf{x}')} \\ 1 \end{pmatrix}\right) & (52)\\
&= \langle \mathbf{T}(\mathbf{x})| \left(\bigotimes_k \mathbf{P}^\dagger\right) 4^n (\mathrm{diag}(\psi^2) \otimes_v \mathrm{diag}(\psi^2)) \left(\bigotimes_k \mathbf{P}\right) |\mathbf{T}(\mathbf{x}')\rangle\,, & (53)
\end{aligned}$$

We will get a Mercer decomposition of it, and for further analysis, we restrict to the n-dimensional input case which employs $\phi_k(\mathbf{x}) = \mathbf{x}_k \in [-\pi, \pi]$. In other words, we are essentially utilizing a single encoding gate for each feature. In this scenario, core tensor $\mathbf{C}$ is diagonal and real. Moreover, all elements in $\bigotimes_{k=1}^{N}[1\ e^{-i\mathbf{x}_k}\ e^{i\mathbf{x}_k}]^\top$ become orthonormalized with respect to the inner product $\langle f|g\rangle = \prod_{k=1}^{N}\left(\frac{1}{2\pi}\int_{-\pi}^{\pi} f^*(\mathbf{x}_k)g(\mathbf{x}_k)d\mathbf{x}_k\right)$. With these properties, it is more convenient to work with $\mathbf{E}(\mathbf{x})$ rather than $\mathbf{T}(\mathbf{x})$. For orthogonalization of $\mathbf{E}_i(\mathbf{x})$s, we choose

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}^{\otimes N}, \qquad \mathbf{L}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^{\otimes N}. \tag{54}$$

which satisfies

$$\mathbf{L}\,|\mathbf{E}(\mathbf{x})\rangle = \begin{pmatrix} 1 \\ e^{-i\mathbf{x}_k} \\ e^{i\mathbf{x}_k} \\ 0 \end{pmatrix}^{\otimes N}. \tag{55}$$

Now

$$\begin{aligned}
\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') &= \left(\begin{pmatrix} 1 \\ e^{i\mathbf{x}_k} \\ e^{-i\mathbf{x}_k} \\ 0 \end{pmatrix}^\top\right)^{\otimes N} (\mathbf{L}^{-1})^\top \mathbf{C} \mathbf{L}^{-1} \begin{pmatrix} 1 \\ e^{-i\mathbf{x}'_k} \\ e^{i\mathbf{x}'_k} \\ 0 \end{pmatrix}^{\otimes N} & (56)\\
&:= \left\langle \bar{\mathbf{E}}(\mathbf{x}) \right| (\mathbf{L}^{-1})^\top \mathbf{C} \mathbf{L}^{-1} \left| \bar{\mathbf{E}}(\mathbf{x}') \right\rangle
\end{aligned}$$

Here elements of $\mathbf{C}$ are

$$\mathbf{C}_{i_1 i_2, \ldots, i_{2N}; i_1 i_2, \ldots, i_{2N}} = \psi^2_{i_1 i_3, \ldots, i_{2N-1}} \psi^2_{i_2 i_4, \ldots, i_{2N}}, \qquad i_{2k-1} i_{2k} \in \{00, 01, 10, 11\}. \tag{57}$$

Now we will consider the $2N$-length bit indices of $\mathbf{C}$ as a concatenation of 2-bit sequences. Conjugating $\mathbf{C}$ with $\mathbf{L}^{-1}$ does the following things.

- When the index of an element contains sequence of $i_{2k-1}i_{2k} = 11$, then add that elements to the $\mathbf{C}_{\mathbf{i}';\mathbf{i}'}$, where $\mathbf{i}' = i_1 i_2, \ldots, \underbrace{i_{2k-1}, i_{2k}}_{=00}, \ldots, i_{2N-1}i_{2N}$ for all $k \in [N]$.

  In other words, collects all elements containing 11 sequence in their indices, and sums them into the element containing 00 sequence at the same position of their 11-sequence positions.

- For indices not containing sequences of 00, nothing happens.

- From Eq. (57), we see that elements of $\mathbf{C}_{\mathbf{i};\mathbf{i}}$ are invariant under exchanging sequences 01 and 10 in their indices.

- Creates non-diagonal elements, and the associated indices contain 11 sequences.

The next thing we need to do is a truncation where $\bar{\mathbf{E}}_{\mathbf{i}}(\mathbf{x}) = 0$. The zero elements occur whenever there is a 11 sequence in the index, so we remove rows and columns where indices have 11 sequences, and this removes all the non-diagonal elements of $(\mathbf{L}^{-1})^\top \mathbf{C}\mathbf{L}^{-1}$, giving us

$$\begin{aligned}\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') &= \left(\begin{pmatrix} 1 \\ e^{i\mathbf{x}_k} \\ e^{-i\mathbf{x}_k} \end{pmatrix}^\top\right)^{\otimes N} \tilde{\mathbf{C}} \begin{pmatrix} 1 \\ e^{-i\mathbf{x}'_k} \\ e^{i\mathbf{x}'_k} \end{pmatrix}^{\otimes N} \\ &= \sum_{\alpha \in \{00,01,10\}^N} \tilde{\mathbf{C}}_{\alpha,\alpha} e^{-i\omega_\alpha \cdot (\mathbf{x}-\mathbf{x}')},\end{aligned} \tag{58}$$

where frequency vectors $\omega_\alpha \in \{-1, 0, 1\}^N$ are defined as

$$(\omega_\alpha)_k = \begin{cases} 0 & \text{if } \alpha_{2k-1}\alpha_{2k} = 00 \\ 1 & \text{if } \alpha_{2k-1}\alpha_{2k} = 01 \\ -1 & \text{if } \alpha_{2k-1}\alpha_{2k} = 10 \end{cases} \tag{59}$$

$$\tilde{\mathbf{C}}_{\alpha,\alpha} = \sum_{\alpha \in \mathcal{I}_\alpha} \psi^2_{\alpha_1\alpha_3,\ldots,\alpha_{2N-1}} \psi^2_{\alpha_2\alpha_4,\ldots,\alpha_{2N}}, \tag{60}$$

and $\mathcal{I}_\alpha$ is the set of all 2^N length bitstrings containing 00 and 11 sequences where $\alpha_{2k-1}\alpha_{2k} = 00$. For example, $\mathcal{I}_{0000} = \{0000, 0011, 1100, 1111\}$, $\mathcal{I}_{0001} = \{0001, 1101\}$, $\mathcal{I}_{0101} = \{0101\}$ and so on. There are several notes on diagonal matrix $\tilde{\mathbf{C}}$. First of all, it has a 'Hermiticity' property. Let $\bar{\alpha}$ be the index with 01 and 10 sequences interchanged. Then we have $\tilde{\mathbf{C}}_{\alpha,\alpha} = \tilde{\mathbf{C}}_{\bar{\alpha},\bar{\alpha}}$, and $\omega_\alpha = \omega_{\bar{\alpha}}$. Therefore, $\mathcal{K}_Q$ is indeed real and can be written in the form of

$$\mathcal{K}_Q(\mathbf{x}, \mathbf{x}') = \tilde{\mathbf{C}}_{\mathbf{0},\mathbf{0}} + \sum_{\alpha \in \Omega^+} 2\tilde{\mathbf{C}}_{\alpha,\alpha} \cos(\omega_\alpha \cdot (\mathbf{x} - \mathbf{x}')), \tag{61}$$

where Ω^+ is the set of indices containing only non-redundant ones. Secondly, we notice that eigenvalues concentrate more on indices having many 00 sequences. To be precisely, $|\mathcal{I}_\alpha| = 2^{|\alpha|_{00}}$, where $|\alpha|_{00}$ denotes the number of 00 sequences in α. Meanwhile $N - |\alpha|_{00}$ corresponds to the number of non-zero elements in the frequency vector ω_α, so eigenvalues tend to concentrate on the low-degree eigenfunctions. Let us assume all elements of $\psi^2 \otimes_v \psi^2$ are order of $(1/3)^N$, then the largest eigenvalue, associated with the constant function $\mathbf{1}$, scales $(2/3)^N$. The next largest eigenvalues scale as $1/2(2/3)^N$, and associated with the N degree-one frequencies $\{(1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$ and so on.

Conjugating with $\mathbf{L}$ is a local operation, so it does not increase the bond dimension of the original matrix. Therefore, when the Born probability of the pre-encoded state $|\psi\rangle = \mathbf{W}|\mathbf{0}\rangle$ can be represented with polynomially scaling bond-dimensional MPS, this quantum kernel corresponds to efficiently calculable entangled tensor kernels.

However, following the discussions from Sec. 4.1, generalizable models should utilize only polynomially large eigenfunctions. For one layer case we have discussed, this implies if the kernel were generalizable, only polynomially many $\tilde{\mathbf{C}}_{\alpha,\alpha}$s are relevant, so we can remove all other $O(1/exp(N))$ scaling values without causing much error. This results in poly-sparse $\tilde{\mathbf{C}}$, making it poly-dimensional MPO. That is, generalizable one-layer quantum kernels are vulnerable to dequantization.

6 Summary and Discussions

We introduced a method for obtaining Mercer decompositions of quantum kernels by representing them using tensor networks. Although this approach is inefficient, it allows us to separate the data-dependent and non-dependent parts, avoiding the need to integrate the data-dependent quantum state over the data space, as done in previous work [2]. Inspired by the tensor network form of quantum kernels, we introduced entangled tensor kernels generated by multiple kernels, a generalized version of the product of kernels. We assert that a quantum kernel is a method to create a new high-dimensional kernel from several kernels and efficiently generate highly entangled eigenfunctions. For quantum kernels to be advantageous over classical kernels, they should have small effective dimensions while their eigenfunctions should be highly entangled, making them resistant to efficient classical approximations. Finally, using the introduced technique we have analyzed the Mercer decomposition, generalizability, and possible dequantizability of one-layer quantum kernels, which is more general than previously studied tensor-product quantum kernels [2**?**].

DISCUSSIONS TO BE ADDED

A Product quantum kernels

If $\mathbf{W}$ were the product of single-qubit unitaries $\mathbf{W}^{(k)}$s, then everything simplifies, we get diagonal core tensor,

$$\tilde{\mathbf{C}_\mathbf{T}} = \bigotimes_{k=1}^{n} \begin{pmatrix} 1-2(\psi_1^{(k)}\psi_2^{(k)})^2 & 0 & 0 \\ 0 & (\psi_1^{(k)}\psi_2^{(k)})^2 & 0 \\ 0 & 0 & (\psi_1^{(k)}\psi_2^{(k)})^2 \end{pmatrix} \tag{62}$$

, where $\mathbf{W}^{(k)}|0\rangle = [\psi_1^{(k)}\ \psi_2^{(k)}]^\top$. Therefore the eigenfunctions are given as components of

$$\left|\tilde{\mathbf{T}}(\mathbf{x})\right\rangle = \bigotimes_{k=1}^{n} \begin{pmatrix} 1 \\ \sqrt{2}\cos\mathbf{x}_k \\ \sqrt{2}\sin\mathbf{x}_k \end{pmatrix}. \tag{63}$$

References

[1] Abdulkadir Canatar, Blake Bordelon, and Cengiz Pehlevan. Spectral bias and task-model alignment explain generalization in kernel regression and infinitely wide neural networks. *Nature Communications*, 12(1):2914, 2021.

[2] Jonas M Kübler, Simon Buchholz, and Bernhard Schölkopf. The Inductive Bias of Quantum Kernels. *arXiv*, 2021.
[3] Seongwook Shin, Yong Siah Teo, and Hyunseok Jeong. Dequantizing quantum machine learning models using tensor networks. *Phys. Rev. Res.*, 6:023218, May 2024.
[4] Ryan Sweke, Erik Recio, Sofiene Jerbi, Elies Gil-Fuster, Bryce Fuller, Jens Eisert, and Johannes Jakob Meyer. Potential and limitations of random fourier features for dequantizing quantum machine learning, 2023.

Characterizing the entanglement dimensionality vector in multipartite quantum states

Shuheng Liu[1 2 3 *] Qiongyi He[1] Marcus Huber[2 3] Matteo Fadel[4] Otfried Gühne[5] Giuseppe Vitagliano[2 3]

[1] *State Key Laboratory for Mesoscopic Physics, School of Physics, Frontiers Science Center for Nano-optoelectronics, and Collaborative Innovation Center of Quantum Matter, Peking University, Beijing 100871, China*
[2] *Vienna Center for Quantum Science and Technology, Atominstitut, TU Wien, 1020 Vienna, Austria*
[3] *Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, 1090 Vienna, Austria*
[4] *Department of Physics, ETH Zürich, 8093 Zürich, Switzerland*
[5] *Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, Siegen D-57068 Germany*

Abstract. Entanglement quantification is highly non-trivial and has become subject of intense investigation starting from the case of two particles of relatively small dimension, but reaches a daunting complexity when either or both the number of particles or the particles' dimensions increase. We first take inspiration from covariance matrix based techniques to derive a bipartite criterion for the entanglement dimensionality. It can be further bounded by the moments of randomized correlations, which are widely used in various experiments. We then derive a nonlinear criterion that can reveal both the level of multipartiteness and the dimensionality of the entanglement in the quantum states. We test our condition on paradigmatic classes of high-dimensional multipartite entangled states and find that, in comparison with other available criteria, our method provides a significant advantage.

Keywords: multipartite high-dimensional entanglement, entanglement dimensionality vector, entanglement quantification

1 Bipartite condition: bounding entanglement dimensionality from the covariance matrix [1]

High-dimensional entanglement has been identified as an important resource in quantum information processing, but also as a main obstacle for simulating classically a quantum system. In particular, the resource needed to reproduce the correlations in the quantum state can be quantified by the so-called entanglement dimensionality. Because of this, experiments aim at controlling larger and larger quantum systems and prepare them in high-dimensional entangled states. The question arising is then how to detect such entanglement dimensionality from experimental data, for example through specific entanglement witnesses. Most common methods involve very complex measurements, such as fidelities with respect to highly entangled states, which are often challenging and in some cases, like in ensembles of many atoms, completely inaccessible.

To overcome some of these difficulties, we focus here on quantifying entanglement dimensionality through covariances of global observables, which are typically measured in many-body experiments, such as those involving atomic ensembles in highly entangled spin-squeezed states. Concretely, we generalize well-known entanglement criteria based on covariance matrices of local observables and establish analytical bounds for different entanglement dimensionalities, which, when violated, certify what is the minimal entanglement dimensionality present in the system.

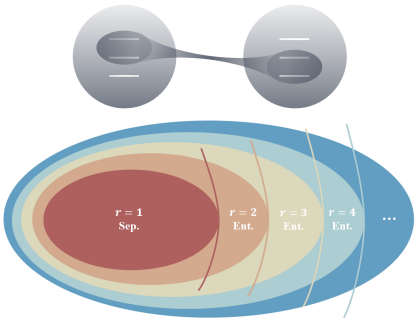


Figure 1: (Above) Entanglement between subsets of levels, signifying the entanglement dimensionality. (Below) Our nonlinear criterion for detecting different entanglement dimensionalities, as an improvement over linear witnesses. $r = 1$: separable states, $r \geq 2$: entangled states.

To show the practical relevance of our results, we derive criteria that require similar information as the existing methods in literature, yet can detect a wider set of states. We also consider paradigmatic criteria based on spin operators, similar to spin-squeezing inequalities, which would be very helpful for experimental detection of high-dimensional entanglement in cold atom systems.

Our work also opens interesting research directions and poses further intriguing theoretical questions, such as improving current methods to detect the entanglement dimensionality in multipartite states.

*liushuheng@pku.edu.cn

2 Bipartite condition: characterizing entanglement dimensionality from randomized measurements [2]

Bounding entanglement dimensionality is crucial for advancing quantum technologies. However, current methods require quite demanding measurement capabilities. Here we develop a method to rigorously detect the entanglement dimensionality with measurements in random directions. Such a method only needs local random unitary transformations and local measurements; therefore, it avoids the need of carefully tuning the measurement directions and bypasses even the requirement of a common reference frame.

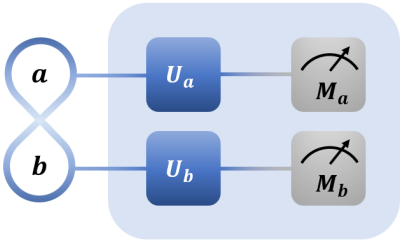


Figure 2: Scheme of randomized measurements.

Concretely, using the probability distribution of the correlations obtained from randomized measurements, we establish analytical boundaries for different entanglement dimensionalities. Any violation of these boundaries for a particular dimensionality suggests the existence of a higher dimensionality. We then show how our method works in practice, also considering a finite statistical sample of correlations, and we also show that it can detect more states than other entanglement-dimensionality criteria available in literature, thus providing a method that is both very powerful and potentially simpler in practical scenarios.

Our work provides an exciting research direction for implementing our method in many-body systems. Generalizing our results would allow for the detection of the full entanglement structure in multipartite states.

3 Multipartite condition: characterizing entanglement dimensionality vector [3]

For the case of more than two particles, multipartite entanglement is very complex to even characterize qualitatively, as considering all possible (infinitely many) pure-state decompositions of a density matrix is in general a very challenging task, leading to the NP-hardness of entanglement certification.

Hence, in order to properly characterize the genuinely multipartite nature of the entanglement in the state it is important not only to consider the full set of bipartitions, but also to take the worst-case scenario amongst all possible mixtures of states entangled differently across the different bipartitions. This translates into considering the vector of entropies of the reductions for all possible bipartitions. Our work focuses on the 0-entropy case,

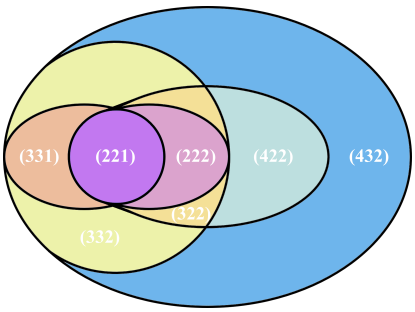


Figure 3: The structure of all possible Schmidt number vectors in a $4 \times 3 \times 2$ state space.

which extends the concept of the Schmidt number to multipartite states. This discrete measure is also a special case that allows for a better classification of the state as a resource, in contrast to continuous measures.

We present a new approach to find witnesses for the entanglement-dimensionality vector in multipartite systems, which is based on extending corollaries of the bipartite Covariance Matrix Criterion to the multipartite case. We have applied this idea explicitly to a known corollary of the CMC, which leads to a criterion that is strictly stronger than fidelity witnesses with respect to 1-uniform states such as the GHZ states, which represent in practice the most widely used witnesses.

Moreover, we have shown that this criterion also improves over known methods on a wide class of states, which include important paradigmatic examples useful for applications. Further developments of our approach can be obtained by finding new corollaries to the CMC, or in general nonlinear witnesses of the Schmidt number in the bipartite case, which thus represents a promising direction for further research in this topic.

References

[1] S. Liu, M. Fadel, Q. He, M. Huber, and G. Vitagliano, Bounding entanglement dimensionality from the covariance matrix, Quantum 8, 1236 (2024).

[2] S. Liu, Q. He, M. Huber, O. Gühne, and G. Vitagliano, Characterizing entanglement dimensionality from randomized measurements, PRX Quantum 4, 020324 (2023).

[3] S. Liu, Q. He, M. Huber, and G. Vitagliano, A nonlinear criterion for characterizing high-dimensional multipartite entanglement, arXiv:2405.03261 (2024).

Bayesian retrodiction of quantum supermaps

Ge Bai[1] *

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

Abstract. The Petz map has been established as a quantum version of the Bayes rule. We study a higher-order generalization of it by formulating the problem of quantum supermap retrodiction, namely update rules for the belief of a quantum channel given indirect observations on it. A list of axioms desired for supermap retrodiction are proposed in analogy with quantum Bayes rule. We give analytical solutions to families of supermaps and prior beliefs, and point out the difficulty of a general recipe to construct retrodiction supermaps.

Keywords: Quantum Bayes' rule, quantum supermaps, Petz recovery map

1 Introduction

The Bayes' rule lies in the centre of logical reasoning [1]. It tells how one updates one's belief of a random variable from indirect observations. In quantum generalizations of the Bayes' rule, the random variables correspond to quantum states, and the generalization is not straightforward due to operator non-commutativity. Various definitions of belief updates of quantum states has been proposed [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. Among those proposals, the Petz recovery map [13, 14] is the only update rule that satisfies a set of desired properties analogous to the classical Bayes rule [12].

The Petz map highlights a unification of conceptual retrodiction and a physical reverse process [15, 16]: Conceptually, it defines a retrodiction, which is an updated belief of the initial state of a process given observations on the final state; and operationally, it implements a reverse process that brings the final state back to the retrodicted initial state.

The Petz map seems to have given a satisfactory, if not the final, answer to the quantum Bayes' rule. However, we find that its generalization from quantum states to quantum channels turned out to be non-trivial. Consider a quantum process that contains a few steps. For some steps, we have their exact characterization, while others are unknown, and we only have an initial belief about their behaviour. The steps may be "hidden" in between other steps and are not directly accessible. We aim to answer the following question: given observations of the process as a whole, how can we update our information about the unknown steps that may not be directly accessible?

We focus on the case where one of the steps is unknown and formulate this question in the framework of quantum supermaps [17]. A quantum supermap can be imagined as a quantum circuit board with an empty slot into which a quantum process can be embedded, as shown on the left of Fig. 1. Such a circuit board, with all the exactly characterized steps soldered on board and leaving the unknown step as a slot, would be a supermap from the unknown step to the full quantum process.

Therefore, we call the problem of updating the belief of the unknown step "supermap retrodiction", in analogy to quantum channel retrodiction that updates the belief of its input quantum state.

An analogy can be made between the supermap retrodiction and updating conditional probabilities in a Bayesian network, as shown in Fig. 1.

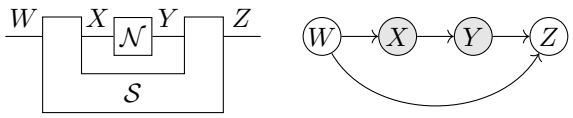


Figure 1: Quantum supermap retrodiction problem and its analogous Bayesian network. On the left, $\mathcal{S}$ is a supermap acting on a quantum channel $\mathcal{N}$. The supermap retrodiction aims to update one's belief on $\mathcal{N}$, namely the correlation between systems X and Y. On the right, it shows the Bayesian network connecting observed variables W, Z and latent variables X, Y with conditional probability distributions $P(X|W), P(Y|X), P(Z|YW)$. The supermap retrodiction is analogous to updating $P(Y|X)$ given observations on W and Z.

In this work, we propose axioms of retrodiction of supermaps, similar to those of the Petz map [12]. For a class of supermaps involving only classical-to-quantum channels, we give one solution satisfying all the axioms. For general supermaps, we reduce the problem into basic cases. However, even for the basic cases, finding a general solution satisfying all axioms turns out to be non-trivial. Nonetheless, we have found solutions for a few families of examples with analytical formulae to construct the retrodiction supermaps.

2 Problem formulation

We denote quantum systems with capital letters, and system X has Hilbert space $\mathcal{H}_X$ and dimension d_X. Let $S(\mathcal{H})$ be the set of density operators on Hilbert space $\mathcal{H}$. We denote the set of CPTP maps, namely quantum channels, from $S(\mathcal{H}_X)$ to $S(\mathcal{H}_Y)$ as $\mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y)$.

The Petz map [13, 14] gives a general recipe for the retrodiction of a quantum process $\mathcal{E} \in \mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y)$ and is defined as [15, 18, 12]:

$$\mathcal{R}^{\mathcal{E},\gamma}(\sigma) := \sqrt{\gamma}\mathcal{E}^\dagger\left(\mathcal{E}(\gamma)^{-1/2}\sigma\mathcal{E}(\gamma)^{-1/2}\right)\sqrt{\gamma}, \qquad (1)$$

where $\gamma \in S(\mathcal{H}_X)$ is a reference state, and the resulting map $\mathcal{R}^{\mathcal{E},\gamma}$ is in $\mathrm{CPTP}(\mathcal{H}_Y, \mathcal{H}_X)$.

*baige@nus.edu.sg

Quantum supermaps refer to transformations from one quantum process to another. In this paper, we consider supermaps deterministically realizable with quantum circuits, also known as superchannels, which are completely positive linear maps transforming CPTP maps to CPTP maps [17, 19, 20]. These objects are the higher-order counterparts of deterministic quantum processes, namely quantum channels.

Any superchannel $\mathcal{S} : \mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y) \to \mathrm{CPTP}(\mathcal{H}_W, \mathcal{H}_Z)$ acting on a CPTP map $\mathcal{N}$ can always be realized with the structure shown in Fig. 2 [17]. In the figure, A and B are ancillary systems, $\mathcal{I}_B$ is the identity channel on system $\mathcal{H}_B$, $\mathcal{V}_L \in \mathrm{CPTP}(\mathcal{H}_W, \mathcal{H}_X \otimes \mathcal{H}_B)$ is an isometric channel and $\mathcal{V}_R \in \mathrm{CPTP}(\mathcal{H}_Y \otimes \mathcal{H}_B, \mathcal{H}_Z \otimes \mathcal{H}_A)$ is a unitary channel (the dimensions satisfy $d_Y d_B = d_Z d_A$).

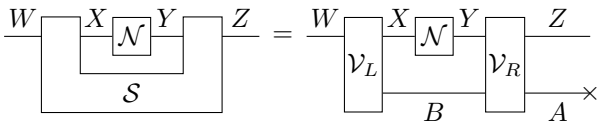


Figure 2: The decomposition of a superchannel.

Ref. [12] lists a set of axioms for retrodiction, which are all satisfied by the Petz map. We take the same set of axioms, replace the channels with superchannels, and list them as follows. For the retrodiction of superchannel $\mathcal{S} : \mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y) \to \mathrm{CPTP}(\mathcal{H}_Z, \mathcal{H}_W)$, the prior belief is a channel $\Gamma \in \mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y)$, and the retrodiction supermap aims to update the belief from the output of $\mathcal{S}$. We denote as $\mathcal{R}^{\mathcal{S},\Gamma} : \mathrm{CPTP}(\mathcal{H}_Z, \mathcal{H}_W) \to \mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y)$ the retrodiction supermap of $\mathcal{S}$ with prior Γ.

1. The retrodiction supermap is a superchannel, and thus can be realized with the structure in Fig. 2.

2. If the input of the retrodiction supermap is the propagated reference prior, it should recover the reference prior. Namely,

$$\mathcal{R}^{\mathcal{S},\Gamma}(\mathcal{S}(\Gamma)) = \Gamma. \tag{2}$$

   In other words, if the observation matches the prior belief exactly, no update will be made on the belief.

3. If the superchannel $\mathcal{S}$ is perfectly recoverable, namely there exists another superchannel $\mathcal{T}$ such that $\mathcal{T} \circ \mathcal{S}$ is the identity supermap, then the retrodiction supermap $\mathcal{R}^{\mathcal{S},\Gamma}$ also satisfies that $\mathcal{R}^{\mathcal{S},\Gamma} \circ \mathcal{S}$ is the identity supermap.

4. Involutive: If $\mathcal{R}^{\mathcal{S},\Gamma}$ is a retrodiction supermap for $\mathcal{S}$ with prior Γ, then $\mathcal{S}$ is a retrodiction supermap for $\mathcal{R}^{\mathcal{S},\Gamma}$ with prior $\mathcal{S}(\Gamma)$. Namely,

$$\mathcal{R}^{\mathcal{R}^{\mathcal{S},\Gamma},\mathcal{S}(\Gamma)} = \mathcal{S}. \tag{3}$$

5. Compositional: The retrodiction supermap for the composition of two superchannels $\mathcal{S}_2 \circ \mathcal{S}_1$ is the composition of their respective retrodiction supermaps in the reverse order, with priors properly propagated forward. Namely,

$$\mathcal{R}^{\mathcal{S}_2 \circ \mathcal{S}_1,\Gamma} = \mathcal{R}^{\mathcal{S}_1,\Gamma} \circ \mathcal{R}^{\mathcal{S}_2,\mathcal{S}_1(\Gamma)}. \tag{4}$$

6. Tensorial: The retrodiction supermap for the tensor product of two superchannels $\mathcal{S}_1 \otimes \mathcal{S}_2$ is the tensor product of their respective retrodiction supermaps:

$$\mathcal{R}^{\mathcal{S}_1 \otimes \mathcal{S}_2,\Gamma_1 \otimes \Gamma_2} = \mathcal{R}^{\mathcal{S}_1,\Gamma_1} \otimes \mathcal{R}^{\mathcal{S}_2,\Gamma_2}. \tag{5}$$

3 Partial Solution

Due to the Choi-Jamiołkowski isomorphism [21, 22], transformations on channels can be viewed as transformations on their Choi operators. Indeed, a superchannel $\mathcal{S} : \mathrm{CPTP}(\mathcal{H}_X, \mathcal{H}_Y) \to \mathrm{CPTP}(\mathcal{H}_W, \mathcal{H}_Z)$ defines a completely positive mapping between Choi operators [17]. We denote this map as $\mathcal{C}_\mathcal{S} \in \mathrm{CP}(\mathcal{H}_X \otimes \mathcal{H}_Y, \mathcal{H}_W \otimes \mathcal{H}_Z)$, $\mathcal{C}_\mathcal{S} : C_\mathcal{N} \mapsto C_{\mathcal{S}(\mathcal{N})}$, where CP denotes the set of completely positive maps.

One may think about defining the retrodiction supermap $\mathcal{R}^{\mathcal{S},\Gamma}$ via the retrodiction of $\mathcal{C}_\mathcal{S}$, such that $\mathcal{C}_{\mathcal{R}^{\mathcal{S},\Gamma}}$ is the Petz map of $\mathcal{C}_\mathcal{S}$ with prior C_Γ. Unfortunately, the Petz map does not always give a valid superchannel satisfying Axiom 1.

Nevertheless, the Petz map is helpful in some special cases. We consider a special case as in Fig. 3, where system W is classical, and $\mathcal{S}$ does the following when applied on $\mathcal{N}$:

1. Copy the value w of W and stores it into a classical memory W',

2. After applying $\mathcal{N}$, apply some channel $\mathcal{S}_w \in \mathrm{CPTP}(\mathcal{H}_Y, \mathcal{H}_Z)$ on system Y based on the stored value w.

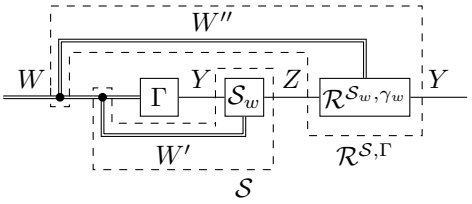


Figure 3: A diagram of $\mathcal{R}^{\mathcal{S},\Gamma}(\mathcal{S}(\Gamma))$. Double lines denote classical systems, and black dots denote copying the classical value. $\mathcal{S}$ copies the value of W, stores it into W' and applies $\mathcal{S}_w$ on system Y based on the stored value w. $\mathcal{R}^{\mathcal{S},\Gamma}$ copies the value of W to W'', and applies $\mathcal{R}^{\gamma_w}$ on the output side based on w.

To construct a retrodiction supermap for $\mathcal{S}$, the idea is to construct the Petz map of $\mathcal{S}_w$ for every w, and select the corresponding Petz map based on w. Specifically, define $\gamma_w := \Gamma(|w\rangle\langle w|)$, and let $\mathcal{R}^{\mathcal{S}_w,\gamma_w}$ be the usual Petz map of $\mathcal{S}_w$ with prior γ_w. The retrodiction superchannel $\mathcal{R}^{\mathcal{S},\Gamma}$ is then realized with the following steps:

1. Copy the value w of system W, and store it in a classical register W''.

2. Based on the stored value w, apply $\mathcal{R}^{\mathcal{S}_w,\gamma_w}$ on system Z.

A diagram showing $\Gamma, \mathcal{S}$ and $\mathcal{R}^{\mathcal{S},\Gamma}$ is in Fig. 3. Following the properties of the Petz map, we can show that this construction satisfies all axioms we desire, if we restrict W to be classical.

4 Examples for the general case

We have found families of cases where explicit solutions of retrodiction supermaps are available. It is desired that the solutions satisfy all axioms, but before a general recipe from Γ and $\mathcal{S}$ to $\mathcal{R}^{\mathcal{S},\Gamma}$ is present, it is difficult to verify Axioms 4 to 6 since they involve multiple retrodiction supermaps. Therefore, in the examples, we do not impose Axioms 4 to 6, and focus on solutions satisfying Axioms 1 and 2.

There is a trivial solution of retrodiction supermap satisfying Axioms 1 and 2, which is a superchannel mapping every channel to Γ. This is not what we desire since it does not update the prior belief at all. To find non-trivial solutions, we use an additional constraint inspired by the property of the Petz map.

We observe that the rank of the Petz map $\mathcal{R}^{\mathcal{E},\gamma}$ is never larger than that of the original map $\mathcal{E}$. We make a similar constraint here, by imposing the retrodiction superchannel $\mathcal{R}^{\mathcal{S},\Gamma}$ to have rank no larger than that of $\mathcal{S}$. When Γ and $\mathcal{S}(\Gamma)$ are full-rank, we show that this is the minimal rank of a superchannel that Axiom 2 may be satisfied. Intuitively, this minimal rank constraint requires the $\mathcal{R}^{\mathcal{E},\gamma}$ to keep the most information from the observation $\mathcal{S}(\mathcal{N})$.

Here, we present one of the examples. The reference channel is chosen as $\Gamma(\rho) = (D_p \circ \mathrm{CNOT})(\rho \otimes |0\rangle\langle 0|) \in \mathrm{CPTP}(\mathcal{H}_W, \mathcal{H}_Z \otimes \mathcal{H}_A)$, where D_p is a depolarizing channel defined as

$$D_p(\rho) := (1-p)\rho + p\mathbb{1}_{ZA}/d_{ZA},\ 0 \le p \le 1 \tag{6}$$

where $\mathbb{1}_{ZA}/d_{ZA}$ is the maximally mixed state in $S(\mathcal{H}_Z \otimes \mathcal{H}_A)$. The supermap is simply throwing away system A of the output.

We have found the solution of a retrodiction supermap for any p, and here we present the limiting case $p \to 0$ for simplicity. In this case, $\mathcal{R}^{\mathcal{S},\Gamma}$ can be implemented with the structure in Fig. 4 with $d_{M_1} = 4$ and $d_{M_2} = 2$, and the isometry U_L and unitary U_R are defined as

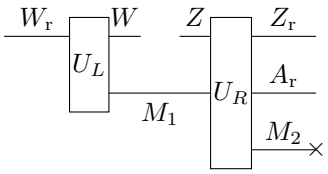


Figure 4: Structure of retrodiction supermaps.

$$U_L = \frac{|00\rangle + |11\rangle}{\sqrt{2}}\langle 0| + \frac{|02\rangle + |10\rangle}{\sqrt{2}}\langle 1|\,, \tag{7}$$

$$\begin{aligned} U_R = {} & |000\rangle\langle 00| + |101\rangle\langle 01| + |110\rangle\langle 02| + |011\rangle\langle 03| \\ & - |111\rangle\langle 10| - |001\rangle\langle 11| + |010\rangle\langle 12| + |100\rangle\langle 13|\,, \end{aligned} \tag{8}$$

where the ordering of systems is W, M_1, W_r for U_L and $Z_\mathrm{r}, A_\mathrm{r}, M_2, Z, M_1$ for U_R.

The obtained retrodiction supermap does not follow the pattern mentioned in Fig. 3. The first tooth is not "copying" system W but alters its value and entangle it with the memory system M_1.

5 Discussion

Our work gives a framework and a partial solution to the Bayesian retrodiction of quantum superchannels. For general cases, we have found analytical solutions to a few examples satisfying a set of properties analogous to Petz maps. The solutions are mysteriously exotic compared with the classical Bayes' rule and the Petz map.

The retrodiction of quantum superchannels, which is also the update rule for beliefs of quantum channels, is a basic component of quantum Bayesian networks [23, 5, 24, 25, 26]. A classical Bayesian network [1] is a connection of random variables with conditional probabilities. It is a machine learning model where the connections can be updated according to observations, and later used for making predictions. The quantum Bayesian network is a connection of quantum systems with quantum channels, where the channels can be updated according to observations and used for predictions. The Bayesian method may not be the optimal solution for certain tasks (for example, the Bayes' rule is not optimal for state retrieval [8]), but will hopefully be more consistent and scalable than numerical optimizations.

Compared with other proposals to update beliefs in quantum Bayesian networks [5, 25], our proposal of supermap retrodiction is both conceptually consistent with Bayes' rule and operationally realizable with a deterministic quantum circuit. This has the following benefits.

First, the retrodiction supermap can be used to recover errors of quantum operations. Here, the error model is a supermap capable of characterizing errors on the input, the output and unwanted side channel between them. This model is particularly suitable for accessing a remote process, such as cloud computing [27, 28, 29] and quantum illumination [30], where errors may occur at the transmission in both directions.

Second, the retrodiction can be applied to subsystems of a quantum process, and the quantum nature of our proposal makes it possible to preserve the entanglement between the subsystem of interest and its complement. In contrast, collecting the observations as classical data and making conceptual belief updates necessarily destroys entanglement.

Although we have found solutions of retrodiction supermaps for subclasses of superchannels and priors, a universal recipe is yet to be found. It remains unknown whether the aforementioned axioms can be all satisfied by a universal recipe. It is possible that some of them have to be compromised, for example, lifting Axiom 1 to allow for probabilistic supermaps [17] or virtual supermaps (weighted difference between to superchannels) [31]. They are still physical in the sense that they can be simulated with deterministic circuits and classical post-processing at the cost of more experimental repetitions.

References

[1] J. Pearl. *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Morgan Kaufmann, 1988.

[2] Masanao Ozawa. *Quantum state reduction and the quantum Bayes principle*. Springer, 1997.

[3] Christopher A Fuchs. Quantum foundations in the light of quantum information. *arXiv preprint quant-ph/0106166*, 2001.

[4] Ruediger Schack, Todd A Brun, and Carlton M Caves. Quantum bayes rule. *Physical Review A*, 64(1):014305, 2001.

[5] Manfred KK Warmuth. A bayes rule for density matrices. *Advances in neural information processing systems*, 18, 2005.

[6] Gerhart Lüders. Concerning the state-change due to the measurement process. *Annalen der Physik*, 518(9):663–670, 2006.

[7] Matthew S Leifer and Robert W Spekkens. Towards a formulation of quantum theory as a causally neutral theory of bayesian inference. *Physical Review A*, 88(5):052130, 2013.

[8] Jacopo Surace and Matteo Scandi. State retrieval beyond bayes' retrodiction. *arXiv preprint arXiv:2201.09899*, 2022.

[9] Mankei Tsang. Generalized conditional expectations for quantum retrodiction and smoothing. *Physical Review A*, 105(4):042213, 2022.

[10] Arthur J Parzygnat and Benjamin P Russo. A non-commutative bayes' theorem. *Linear Algebra and its Applications*, 644:28–94, 2022.

[11] Arthur J Parzygnat and James Fullwood. From time-reversal symmetry to quantum bayes' rules. *PRX Quantum*, 4(2):020334, 2023.

[12] Arthur J. Parzygnat and Francesco Buscemi. Axioms for retrodiction: achieving time-reversal symmetry with a prior. *Quantum*, 7:1013, May 2023.

[13] Denes Petz. Sufficient subalgebras and the relative entropy of states of a von neumann algebra. *Comm. Math. Phys.*, 105:123–131, 1986.

[14] Denes Petz. Sufficiency of channels over von Neumann algebras. *The Quarterly Journal of Mathematics*, 39(1):97–108, 03 1988.

[15] Francesco Buscemi and Valerio Scarani. Fluctuation theorems from bayesian retrodiction. *Phys. Rev. E*, 103:052111, May 2021.

[16] Clive Cenxin Aw, Francesco Buscemi, and Valerio Scarani. Fluctuation theorems with retrodiction rather than reverse processes. *AVS Quantum Science*, 3(4):045601, 2021.

[17] Giulio Chiribella, G Mauro D'Ariano, and Paolo Perinotti. Transforming quantum operations: Quantum supermaps. *Europhysics Letters*, 83(3):30004, 2008.

[18] Francesco Buscemi, Joseph Schindler, and Dominik Šafránek. Observational entropy, coarse-grained states, and the petz recovery map: information-theoretic properties and bounds. *New Journal of Physics*, 25(5):053002, may 2023.

[19] Giulio Chiribella, G Mauro D'Ariano, and Paolo Perinotti. Quantum circuit architecture. *Physical review letters*, 101(6):060401, 2008.

[20] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009.

[21] Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

[22] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[23] Robert R. Tucci. Quantum bayesian nets. *International Journal of Modern Physics B*, 09(03):295–337, 1995.

[24] Robert R Tucci. Factorization of quantum density matrices according to bayesian and markov networks. *arXiv preprint quant-ph/0701201*, 2007.

[25] Matthew S Leifer and David Poulin. Quantum graphical models and belief propagation. *Annals of Physics*, 323(8):1899–1946, 2008.

[26] Jonathan Barrett, Robin Lorenz, and Ognyan Oreshkov. Quantum causal models. *arXiv preprint arXiv:1906.10726*, 2019.

[27] Pablo Arrighi and Louis Salvail. Blind quantum computation. *International Journal of Quantum Information*, 4(05):883–898, 2006.

[28] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th annual IEEE symposium on foundations of computer science*, pages 517–526. IEEE, 2009.

[29] Tomoyuki Morimae and Keisuke Fujii. Blind quantum computation protocol in which alice only makes measurements. *Physical Review A*, 87(5):050301, 2013.

[30] Seth Lloyd. Enhanced sensitivity of photodetection via quantum illumination. *Science*, 321(5895):1463–1465, 2008.

[31] Chengkai Zhu, Yin Mo, Yu-Ao Chen, and Xin Wang. Reversing unknown quantum processes via virtual combs: for channels with limited information. *arXiv preprint arXiv:2401.04672*, 2024.

Angle Finding of Quantum Signal Processing for Matrix Inversion

Kenzo Makino[1] * Hiroaki Murakami[1] Yasunori Lee[2] Keita Kanno[2]
Kenji Minefuji[1] Tomonori Fukuta[1]

[1] *Mitsubishi Eelctric Corp. 2-7-3, Marunouchi, Chiyoda-ku, Tokyo 100-8310, Japan*
[2] *QunaSys Inc. Aqua Building, 9th Floor, 1-13-7 Hakusan, Bunkyo-ku, Tokyo 113-0001 Japan*

Abstract. Linear solvers have a wide range of applications and quantum algorithms provide them exponential speed-up, making them promising for quantum computers. Quantum singular value transformation (QSVT) algorithm is a strong candidate of a quantum linear solver. However, calculating rotation angles in QSVT is often unstable and a bottleneck. Various techniques have been proposed to address this, but the best combination of techniques was unclear. Our study found that using the Remez, Prony, and carving methods for angle finding in QSVT provided the best accuracy, achieving a computational accuracy of the error on the order of 10^{-13} in double-precision arithmetics.

Keywords: quantum computing, quantum algorithms, QSP, QSVT, matrix inversion

1 Introduction

Linear systems are core components in many fields of science, engineering, and optimization. Linear solvers have important industrial applications such as numerical solutions for differential equations, finite element methods, and machine learning. Since the first proposal of quantum algorithms for linear solvers by Harrow, Hassidim and Lloyd [1], several improvements have been proposed [2, 3, 4, 5]. Among them, quantum signal processing (QSP) and quantum singular value transformation (QSVT), which are algorithms that unify various quantum algorithms [5, 6], are able to perform matrix inversion with less computational complexity than the first proposal by avoiding quantum phase estimation. In QSVT, once the coefficient matrix A of linear equations is encoded in the block elements of the unitary matrix of a quantum circuit as a block encoding-operator, it is possible to construct a quantum circuit embedded with an approximate pseudo-inverse matrix of A in the block elements of the unitary matrix by using the block-encoding operators and Z-rotation gates. At that time, it is necessary to calculate the approximate polynomial of the inverse function x^{-1} and determine the angle sequence of the Z-rotation gates in the QSP circuit that represents the polynomial. However, the classical task of accurately calculating the angle sequence is often unstable and difficult in double-precision arithmetics on classical computers.

In previous studies on the matrix inversion with QSP, there are three options for approximating x^{-1} with a polynomial: direct method [3], Fourier-transform method [7], and iterative method with Remez algorithm [8]. In particular, the Remez algorithm is the best choice from an error perspective, as it provides the best approximate polynomial within the subspace of Chebyshev polynomials of a given degree.

On the other hand, there are various options for calculating the angle sequence of the QSP. Firstly, there are two approaches to angle finding: a factorization-based approach and an optimization-based approach [8]. The factorization-based approach consists of two substeps called completion and decomposition. There are two options for completion: root-finding method [9, 5, 10, 11] and Prony method [7, 12]. Also, there are two more options for decomposition: carving [5] and halving [10]. Various techniques have been proposed to avoid the numerical instabilities, but the best combination of the techniques was unclear.

In this work, we evaluate combinations of the various methods for the matrix inversion with QSVT, and report that by applying the Remez method to the polynomial approximation, Prony method and carving method to the angle finding, we were able to obtain the angle sequence with a QSP error on the order of 10^{-13} in double-precision arithmetics on a classical computer. This has advanced us one step further towards the application of quantum linear solvers.

2 Preliminary

Polynomial Approximation We assume that A is appropriately scaled by a factor such that $\|A\| \leq 1$, and let κ be the condition number of A. Let $p(x)$ be an d-degree odd polynomial with real coefficients. An inverse function $f(x) = (\beta x)^{-1}$ is approximated by $p(x)$ on $[\kappa^{-1}, 1]$, and its Chebyshev expansion is represented as follows,

$$f(x) \approx p(x) := \sum_{\substack{n:\text{odd} \\ 1 \leq n \leq d}} p_n T_n(x), \tag{1}$$

where $T_n(x) = \cos(n \cos^{-1} x)$ is the first-kind Chebyshev polynomials and the scale β is set such that $|p(x)| \leq 1$ for $^{\forall}x \in [-1, 1]$.

QSP There are two basic conventions for QSP, namely Wx and Wz conventions. In the Wx-convention QSP [5], the signal operator W_X, the signal processing operator S_Z, and the QSP operator sequence $U_X(x, \mathbf{\Phi})$ for $\mathbf{\Phi} := (\phi_0, \ldots, \phi_d) \in \mathbb{R}^{d+1}$ are defined as follows,

*makino.kenzo@dw.mitsubishielectric.co.jp

Definition 1 Wx-convention QSP

$$W_X(x) := e^{itX} = \begin{pmatrix} \cos t & i\sin t \\ i\sin t & \cos t \end{pmatrix} \tag{2}$$

$$S_Z(\phi) := e^{i\phi Z} = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix} \tag{3}$$

$$U_X(x, \mathbf{\Phi}) := S_Z(\phi_0) \prod_{n=1}^{d} W_X(\theta) S_Z(\phi_n) \tag{4}$$

where $t := \cos^{-1} x$ for $x \in [-1, 1]$ and X, Z are Pauli-X, Pauli-Z matrices. In the Wz-convetion QSP [11, 6], $U_Z(x, \mathbf{\Phi})$ is defined similarly to U_X but with X and Z swapped, where $W_Z(t) := e^{itZ}$ and $S_X(\phi) := e^{i\phi X}$. Since X and Z are similar with respect to the Hadamard transform, they have the relationship $U_X(x, \mathbf{\Phi}) = HU_Z(x, \mathbf{\Phi})H$.

In QSVT, given the angle sequence $\mathbf{\Phi}$ such that $p(x) = \mathrm{Re}[\langle 0| U_X(x, \mathbf{\Phi}) |0\rangle]$, it is possible to construct a QSVT circuit encoding the pseudo-inverse of A, by using the block encoding operators of $A^\dagger$ and Z-rotation gates [5].

3 Setup

In this study, we performed angle findings by combining the various methods mentioned above, and evaluated the QSP errors and the calculation runtime with respect to the polynomial degree d. The d corresponds to the number of queries of the block-encoding operators.

As shown in Figure 1, the angle finding consists of the polynomial approximation (referred to as truncation), calculation of the polynomial G (referred to as completion), which will be menthoned later, and the calculation to decompose U_X into W_X, S_Z (referred to as decomposition). For comparison, we also performed the angle findings with the optimization method [8].

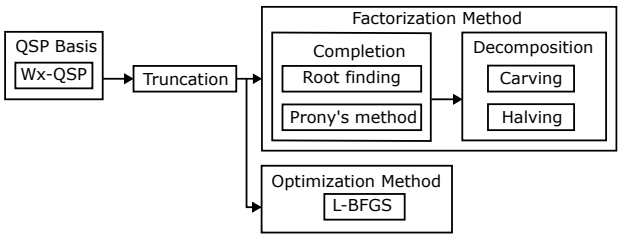


Figure 1: Flow chart of angle finding for QSVT.

Firstly, in the truncation step, we utilized the Remez algorithm to find the polynomial $p(x)$ with odd parity and a given degree d over the domain $[\kappa^{-1}, 1]$. Then, by transforming $t = \cos^{-1} x, \omega = e^{it}$, we converted $p(x)$ into a Laurent polynomial $\tilde{p}(\omega)$ with odd parity and degree d as follows,

$$p(x) = \sum_{\substack{n:\mathrm{odd} \\ -d \le n \le d}} \frac{1}{2} p_{|n|} \omega^n =: \tilde{p}(\omega). \tag{5}$$

Note that $\tilde{p}(\omega)$ is reciprocal, i.e. $\tilde{p}(\omega) = \tilde{p}(\omega^{-1})$. The scale β was set according to κ and n so that $x \in [-1, 1], |p(x)| \le 0.3$.

Secondly, in the completion step, we calculated on the Wz-QSP instead of the Wx-QSP for simplicity. In the Wz-QSP, the QSP operator sequence U_Z is written by U_{FG} as

$$U_{FG} = \begin{pmatrix} F(\omega) & iG(\omega) \\ iG(\omega^{-1}) & F(\omega^{-1}) \end{pmatrix}, \tag{6}$$

where $F, G \in \mathbb{R}[\omega, \omega^{-1}]$, $\deg(F) \le d$, $\deg(G) \le d$, $\mathrm{Parity}(F) = \mathrm{Parity}(G) = d \bmod 2$, $|F(\omega)|^2 + |G(\omega)|^2 = 1$ [10, 6]. For numerical stability, we added anti-reciprocal signal of $\frac{\gamma}{2}(\omega^d - \omega^{-d})$ as $F(\omega) = \tilde{p}(\omega) + \frac{\gamma}{2}(\omega^d - \omega^{-d})$, referred to as capitalization [11, 7]. Then, we calculated $G(\omega)$ with two options: the root-finding method and Prony method. The capitalization amplitude was set to $\gamma = 0.4$.

In the decomposition step, we had two more options, the carving [5] and halving [10], to decompose U_{FG} and calculated the angle sequence $\mathbf{\Phi}$ respectively.

Furthermore, for comparison, we performed angle findings by the numerical optimization method [8]. Using the L-BFGS method, we searched for the angle sequence $\mathbf{\Phi}$ that minimizes the following loss function,

$$L(\mathbf{\Phi}) = \frac{1}{\tilde{d}} \sum_{j=1}^{\tilde{d}} |\mathrm{Re}\,\langle 0| U_X(x_j, \mathbf{\Phi}) |0\rangle - p(x_j)|^2, \tag{7}$$

where $\tilde{d} = \lceil \frac{n+1}{2} \rceil$, $x_j = \cos\left(\frac{(2j-1)\pi}{4\tilde{d}}\right)$.

For verification, we evaluated the errors of the QSP results $\hat{p}(x) := \mathrm{Re}[\langle 0|U_X(x, \Phi)|0\rangle]$. The error was defined as follows,

$$\epsilon := \frac{\|\hat{p}(x) - f(x)\|_\infty}{\|f(x)\|_\infty}. \tag{8}$$

Also, for reference, we evaluated the residual errors of the truncation results $p(x)$ in the same way.

All of the above calculations were performed using Python 3.10.12 and the numpy library 1.26.3, with a laptop with a 3.4 GHz 16-Core Intel Core i7-13700K CPU.

4 Results

We evaluated the degree dependence of the QSP errors ϵ and CPU runtime for each method by changing κ to 10, 20, 30, 40, and 50. As a representative example, we show the results of $\kappa = 10$ in Figure 2(a, b). We set the degree d to $11, 21, 31, \cdots$ in 10 steps and calculated the approximate polynomial up to $d = 311$. The combination of Prony method and carving (Wx.P.C) performed the best, with the smallest error of $\epsilon = 5.0 \times 10^{-13}$ for $d = 311$, and shortest computation time for degrees above 50. It overlapped with the truncation error, which is the best approximation of the inverse function. The combination of Prony method and halving (Wx.P.H) as well as the optimization method (Wx.O) had errors comparable to (Wx.P.C), with the the smallest error of $\epsilon = 1.3 \times 10^{-12}$ and 3.0×10^{-12}, respectively. But they resulted in longer computation times in our implementation. The root-finding method and either the halving or carving method (Wx.RF.C, Wx.RF.H) resulted in the smallest error of $\epsilon = 1.2 \times 10^{-10}$ and 1.3×10^{-10}, respectively.

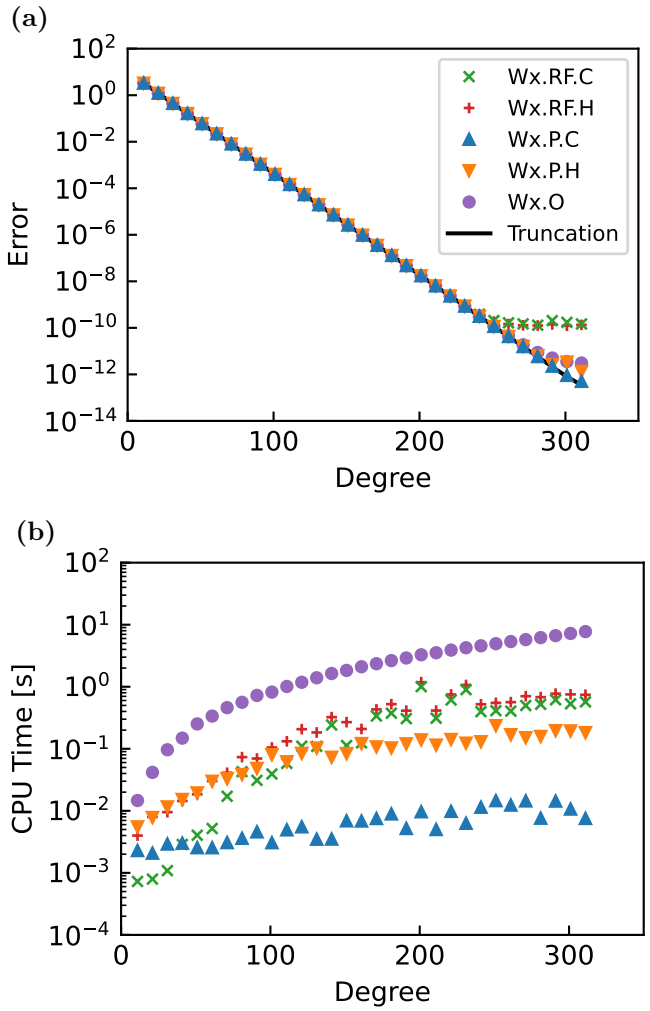


Figure 2: Angle finding of QSP for matrix inversion of $\kappa = 10$. (a) QSP errors ϵ, (b) Runtimes of factorization method and optimization method.

5 Summary

As a result of comparing the angle findings for matrix inversion of QSVT by various methods on a double precision arithmetics, it was found that the combination of Prony method and carving was the best in terms of both angle accuracy and computation time. In our poster presentation, we will also report on the results of changing the condition number κ.

References

[1] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, Vol. 103, No. 150502, 2009.

[2] Andris Ambainis. Variable time amplitude amplification and quantum algorithms for linear algebra problems. In *29th International Symposium on Theoretical Aspects of Computer Science (STACS 2012)*, Vol. 14 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pp. 636–647, 2012.

[3] Andrew M. Childs, Robin Kothari, and Rolando D. Somma. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, Vol. 46, No. 6, 10.1137/16M1087072, 2017.

[4] Leonard Wossnig, Zhikuan Zhao, and Anupam Prakash. Quantum Linear System Algorithm for Dense Matrices. *Physical Review Letters*, Vol. 120, No. 50502, 2018.

[5] 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 2019, p. 193–204, New York, NY, USA, 2019. Association for Computing Machinery.

[6] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. Grand Unification of Quantum Algorithms. *PRX Quantum*, Vol. 2, No. 040203, 2021.

[7] Lexing Ying. Stable factorization for phase factors of quantum signal processing. *Quantum*, Vol. 6, p. 842, 2022.

[8] Yulong Dong, Xiang Meng, K. Birgitta Whaley, and Lin Lin. Efficient phase-factor evaluation in quantum signal processing. *Physical Review A*, Vol. 103, No. 042419, 2021.

[9] Guang Hao Low, Theodore J. Yoder, and Isaac L. Chuang. Methodology of resonant equiangular composite quantum gates. *Physical Review X*, Vol. 6, No. 041067, 2016.

[10] Jeongwan Haah. Product decomposition of periodic functions in quantum signal processing. *Quantum*, Vol. 3, No. 190, 2019.

[11] Rui Chao, Dawei Ding, Andras Gilyen, Cupjin Huang, and Mario Szegedy. Finding Angles for Quantum Signal Processing with Machine Precision. arXiv:2003.02831v2 [quant-ph], 2020.

[12] Shuntaro Yamamoto and Nobuyuki Yoshioka. Robust Angle Finding for Generalized Quantum Signal Processing. arXiv:2402.03016 [quant-ph], 2024.

Directly Estimating Mixed-State Entanglement with Bell Measurement Assistance

Gong-Chu Li[1] * You Zhou[2] † Geng Chen[1] ‡ Chuanfeng Li [1] §

[1] *University of Science and Technology in China*
[2] *Fudan University*

Entanglement, a key feature of quantum mechanics, lies at the heart of quantum information processing. Determining the degree of entanglement in a mixed quantum state (a probabilistic blend of pure states) is a significant challenge. We introduce a novel approach, Few-Shot Randomized Measurement (FSRM) enhanced with Bell measurements, that directly estimates entanglement in mixed states using random unitary evolution and Bell measurements. This method is efficient, robust, and scalable, making it practical for real-world applications.

Traditional methods for entanglement quantification often rely on prior knowledge about the quantum state or use complex, indirect measures. Other common measures like negativity are highly nonlinear making **direct** evaluation difficult.

We focus on direct estimation because it enables us to analyze its unbiasedness, efficiency, and other statistical properties. This paper aims to build an unbiased estimator for mixed-state entanglement that suits even very few shots.

Recent advancements in randomized measurements (RM) and classical shadow (CS) have provided promising pathways to directly estimate various quantum properties. However, traditional RM schemes using only local unitary evolution have limitations in estimating entanglement, especially in mixed states. We overcome these limitations by introducing Bell measurements, which allow for direct access to entanglement information.

Our approach, FSRM, leverages the power of random unitaries and Bell measurements. FSRM requires only a few measurements per setting, significantly reducing experimental overhead. Moreover, compared with CS methods, it is robust to errors in the implementation of random unitaries, making it suitable for noisy quantum systems. The combination of Bell measurements with FSRM allows us to directly estimate entanglement, bypassing the need for indirect measures.

We experimentally demonstrate the effectiveness of our BM-enhanced FSRM scheme using entangled photon pairs. We generate both pure and mixed states, accurately estimating the negativity of each. Our results show significant improvement in robustness compared to traditional shadow estimation, highlighting the advantages of our approach.

Table 1: Comparisons Among the schemes

	robust to channel error	few shot	least design number	type of predictor	post-processing
CS	✗	✓	2	universal	intensive
RM	✓	✗	k	special	a little
FSRM	✓	✓	k	special	almost no

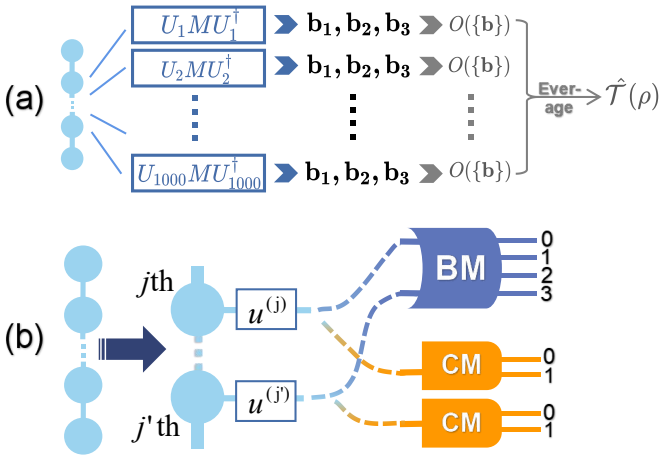


Figure 1: (a)*Demonstation of the FSRM.* With constraints of resources, we choose a more versatile measurement setting with less repeat per setting. We take $N = 1000$ and $k = 3$ for an example. (b) *Demonstration of the BM-enhanced FSRM* We randomly implement Bell measurement onto randomly chosen qubit-pairs.

Our work provides a practical and efficient method for directly characterizing mixed-state entanglement. This research significantly advances the field of randomized measurements by demonstrating the effectiveness of BM-enhanced FSRM for direct mixed-state entanglement quantification. Our approach offers a powerful tool for characterizing quantum systems, contributing to the development of robust and scalable quantum technologies.

*lgc1997@mail.ustc.edu.cn
†you_zhou@fudan.edu.cn
‡chengeng@ustc.edu.cn
§cfli@ustc.edu.cn

Optimal demonstration of generalized quantum contextuality

Soumyabrata Hazra[1] Subhankar Bera[2] * Anubhav Chaturvedi[3 4] Debashis Saha[5] A. S. Majumdar[2]

[1] *International Institute of Information Technology, Gachibowli, Hyderabad 500032, India*
[2] *S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India*
[3] *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland*
[4] *International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk, 80-308 Gdańsk, Poland*
[5] *School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Kerala 695551, India*

Abstract. The notion of general quantum contextuality encompasses preparation as well as measurement contextuality. Our methodology proposes a generalized noncontextual polytope that maintains constant dimension despite variations in measurements and outcomes, ensuring a consistent approach to noncontextual polytope construction. Our constructed polytope's facet inequalities, serve as necessary conditions for generalized noncontextuality, can be obtained computationally efficiently. We illustrate the efficacy of our methodology through several distinct contextuality scenarios involving up to six preparations and three measurements, obtaining the maximum quantum violations of our derived noncontextuality inequalities. Our investigation uncovers many novel non-trivial noncontextuality inequalities and reveals intriguing aspects and applications of quantum contextual correlations.

Keywords: Quantum Contextuality, Non-Contextual Polytopes, Semi- definite hierarchy.

Reference - arXiv:2406.09111v1

Introduction.—One of the most striking features of quantum theory is that its predictions resist generalized noncontextual or "Leibnizian" realist explanations [1, 2, 3, 4, 5, 6, 7, 8]. The notion of noncontextuality embodies the Leibnizian methodological principle that attributes identical realist descriptions to operationally equivalent or indistinguishable experimental procedures. The phenomenon of generalized contextuality of quantum theory constitutes a fundamental nonclassical feature of the quantum formalism that underlies other characteristic nonclassical predictions of quantum theory [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23]. Even though contextuality has roots in the realist camp, it is as relevant to the operationalists since it fuels quantum-over-classical advantage in a broad range of information processing tasks, such as quantum computation, state discrimination, randomness certification, oblivious communication and communication complexity [24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37].

Preparation noncontextuality attributes identical epistemic states to preparation procedures, which are indistinguishable, i.e., all measurements yield identical statistics on such preparation procedures. Inequalities that hold in all theories satisfying preparation noncontextuality can be violated in quantum theory, revealing the contextuality of preparation or simply *preparation contextuality*. Similarly, measurement noncontextuality attributes identical response schemes to measurement procedures that are operationally indistinguishable, i.e., give rise to identical empirical statistics on all possible preparations. However, measurement noncontextuality alone is compatible with quantum theory [1].

Generalized noncontextuality is the logical conjunction of preparation and measurement noncontextuality in contextuality scenarios associated with prepare and measure experiments. Analogous to Bell inequality, generalized noncontextuality implies empirical inequalities, referred to as (generalized) noncontextuality inequalities (NCI). Quantum theory prescribes preparations and measurements, which, while satisfying the operational indistinguishable conditions, violate NCI. A contextuality scenario is specified by the number of preparations, measurements, and measurement outcomes, as well as the operational indistinguishability conditions between preparation and measurement procedures corresponding to their distinct convex mixtures, respectively. Given a contextuality scenario, finding a set of empirical criteria fulfilled by any noncontextual theory is a demanding task of both foundational and operational importance.

The set of empirical statistics possessing noncontextual explanations forms a convex polytope, and consequently, the inequalities representing the facets of that polytope combine to provide the necessary and sufficient criteria for noncontextuality [4]. However, the noncontextual polytope is a product of two polytopes, one for preparations and the other for measurements. To obtain the facet inequality of the noncontextual polytope, one needs to compute the extremal points of a D_P-dimensional polytope associated with the preparations to find the extremal epistemic states, which are probability distributions over the ontic state space and the extremal points of a D_T-dimensional polytope associated with product polytope. It turns out, typically, D_P increases polynomially with the number of measure-

*berasanu007@gmail.com

ments, and D_T increases polynomially with the square of the number of measurements, owing to the polynomial increase in the number of distinct ontic states one needs to consider.

The motivation of the present work is to address this fundamental aspect in the study of contextuality, as to: *when is a given scenario sufficient to exhibit quantum contextuality?* As mentioned above, the computational technique to retrieve all the facet inequalities applicable to arbitrary contextuality scenarios is computationally challenging. Therefore, it is highly desirable to seek efficient methods to find a set of empirical conditions depicting the generalized non-contextuality framework. In the present study, our aim is to formulate statistical inequalities that are necessarily satisfied by noncontextual theories.

Specifically, here we introduce a novel and efficient method to retrieve noncontextuality inequalities in any contextuality scenario, where only a single ontic state is needed to characterize the polytope for preparations. As a result, in contrast to the conventional method [4], in our approach, one needs to compute only the extremal points of a polytope whose dimension remains constant, irrespective of the number of measurements and their outcomes. The formalism proposed here enables us to obtain a polytope containing the noncontextual polytope considerably faster. The facet inequalities of this polytope constitute noncontextuality inequalities necessarily satisfied by all noncontextual theories. Violation of the obtained inequalities thus provides us with sufficient conditions for guaranteeing generalized quantum contextual correlations.

As an upshot of our formalism, through the present analysis we are able to investigate efficiently various contextuality scenarios and uncover new applications of quantum contextuality in those scenarios, such as certification of non-projective measurements, certification of dimensionality, and quantum advantage in oblivious communication.

Generalized notion of contextuality.— A prepare-and-measure experiment uses distinct preparation and measurement procedures to predict outcomes. Two preparation procedures, P_x and $P_{x'}$, are operationally equivalent or indistinguishable (denoted as $P_x \sim P_{x'}$) if they yield identical outcome statistics $\{p(z|x,y)\}$ for all measurements, where $p(z|x,y)$ indicates the probability of obtaining outcome z when the measurement specified by y is performed on the preparation specified by x. Similarly, two measurement procedures $M_{z|y}$ and $M_{z'|y'}$ are operationally equivalent or indistinguishable (denoted as $M_{z|y} \sim M_{z'|y'}$) if they produce identical outcome statistics for all possible preparations.
In a prepare and measure experiment, n_x distinct preparations and n_y different measurements are conducted, each with n_z possible outcomes. A set of hypothetical preparations is realized by taking convex mixtures of these preparations, resulting in indistinguishable mixed preparations. These mixed preparations are labeled by the variable $s \in \{0,\dots,n_s\}$ and realized by the convex coefficients $\{\alpha_{x|s}\}$. The indistinguishability conditions imply that $\sum_x \alpha_{x|s} P_x \sim \sum_x \alpha_{x|s'} P_x$ for all s, s'. Similarly, if $t \in \{0,\dots,n_t\}$, is the labeling and $\{\beta_{z,y|t}\}$ are the convex coefficients of indistinguishable measurement procedures, then indistinguishability conditions on measurements are expressed as $\sum_{z,y} \beta_{z,y|t} M_{z|y} \sim \sum_{z,y} \beta_{z,y|t'} M_{z|y}$ for all z, y, t. Here convex coefficients $\{\alpha_{x|s}\}$ and $\{\beta_{z,y|t}\}$ both satisfy the positivity and normalization conditions. These indistinguishability conditions on preparations and measurements are considered independent, requiring the vectors $\vec{u}_s := \left(\alpha_{0|s}, \alpha_{1|s}, \cdots, \alpha_{n_x-1|s}\right)$ and $\vec{v}_t := \left(\beta_{0|t}, \beta_{1|t}, \cdots, \beta_{n_y-1|t}\right)$ respectively, of these convex coefficients to form an independent set of vectors. The number of preparations, measurements, and measurement outcomes, along with the set of independent indistinguishability conditions, defines a *contextuality scenario*.

In quantum theory, preparations are described by density operators ρ_x, and measurements are described by positive semi-definite operators $M_{z|y}$. The probability of obtaining an outcome when performing a measurement on preparation P_x is given by $p(z|x,y) = \mathrm{Tr}(\rho_x \mathbb{M}_{z|y})$. Quantum preparations and measurements satisfy the indistinguishability conditions if and only if $\sum_x \alpha_{x|s}\, \rho_x = \sum_x \alpha_{x|s'}\, \rho_x\ ,\ \ \forall s, s'$ and $\sum_{z,y} \beta_{z,y|t} \mathbb{M}_{z|y} = \sum_{z,y} \beta_{z,y|t'} \mathbb{M}_{z|y}\ ,\ \forall t, t'$.
An ontological model offers an explanation for the prediction of an operational theory by considering the state of the system as an objective reality, denoted by $\lambda \in \Lambda$, where Λ is an arbitrary measurable space referred to as the ontic state space. A preparation procedure P_x prepares the system in an ontic state λ with probability $\mu(\lambda|x)$, while the probability of obtaining the outcome when a measurement is performed on the ontic state λ is given by the response function $\xi(z|\lambda,y)$. The indistinguishability conditions in any noncontextual ontological model imply $\sum_x \alpha_{x|s}\ \mu(\lambda|x) = \sum_x \alpha_{x|s'}\ \mu(\lambda|x)\ ,\ \ \forall s, s'$ and $\sum_{z,y} \beta_{z,y|t} \xi(z|\lambda,y) = \sum_{z,y} \beta_{z,y|t'} \xi(z|\lambda,y)\ ,\ \ \forall t, t'$, regarding every λ.

Comparison with the method for finding the facets of exact noncontextual polyotpe:- Method to find the exact noncontextual polytope was provided by Schmid *et al.* [4]. The polytope presented in this work is notably larger than this exact noncontextual polytope. Consequently, the violation of the inequalities we derive here serves as a sufficient criterion (though not necessary) for operational certification of generalized contextuality. However, our approach presents a two-folded and substantial advantage over the method for identifying the exact noncontextual polytope in terms of efficiency.

We recall that n_x, n_y, and n_z refer to the number of preparations, measurements, and outcomes, respectively, in a contextuality scenario. Say, the number of extremal points obtained for the variables $\{\xi(z|y)\}$ satisfying indistinguishability conditions is r. According to the method in [4], the total number of ontic states λ

sufficient to characterize the preparations is $n_x \cdot r$. However, owing to the normalization conditions and the independent indistinguishability conditions, n_x and $r \cdot n_s$ number of variables are eliminated, respectively. As a result, the dimension of the polytope characterizing the preparations becomes $(n_x - n_s)r - n_x$ [38].

In contrast, our method involves a fixed number of independent variables for characterizing the preparations, which is $n_x - n_s$ irrespective of the settings of the measurement side. Therefore, the difference between the dimensions of the two polytopes, whose extremal points are computed in the two different methods, is given by

$$\Delta_P = (n_x - n_s)r - 2n_x + n_s.$$

Furthermore, the method in [4] involves $r \cdot n_y \cdot n_z$ number of variables $\{\xi(z|y,\lambda)\}$ that describe the measurements. And, owing to the normalization conditions and the independent indistinguishability conditions, we can eliminate $r \cdot n_y$ and $r \cdot n_t$ number of variables, respectively. As a result, the dimension of the polytope characterizing the measurements becomes $r(n_y n_z - n_y - n_t)$. One needs to compute the extremal points of the product of the two polytopes involving the variables $\{\mu(\lambda|x)\}$ and $\{\xi(z|y,\lambda)\}$ by multiplying the extremal points of these two polytopes. The product polytope has a dimension of $(n_x - n_s)r - n_x + r(n_y n_z - n_y - n_t)$, which follows from the fact that the dimension of a product polytope is the sum of the dimensions of the individual polytopes [38]. On the other hand, the product polytope, for which we compute the facet inequalities in our method, possesses a dimension of $n_x - n_s + n_y n_z - n_y - n_t$. Hence, the difference in dimensions between these two product polytopes, whose extremal points are computed through these two methods is given by

$$\Delta_T = (r-1)(n_x + n_y n_z - n_s - n_y - n_t) - n_x.$$

Discussion.– Deriving a set of empirical criteria applicable to any operational theory that satisfies the generalized notion of contextuality is an arduous task of both foundational and operational significance. The conventional method [4] of extracting facet inequalities from the pertinent noncontextual polytope is computationally demanding due to the polynomial growth in the dimension of the polytope describing the preparations with the number of measurements. In this work, we introduce an innovative approach for constructing a polytope that encompasses the actual noncontextual polytope while ensuring that the complexity of the method remains minimal. The facet inequalities resulting from the intersection of our extended polytope with the normalization polytope constitute necessary conditions for noncontextuality.

We demonstrate the efficacy of our proposed method by applying it here to three scenarios comprising of four to seven preparations and two to three measurements. Consequently, we retrieve a large number of novel NCI, violations of which serve as sufficient conditions for demonstrating quantum contextuality in these scenarios. To obtain the maximum violations of these NCI, we employ two semi-definite programming techniques introduced in [7]. The see-saw technique retrieves lower bounds on the maximum quantum violations with the quantum states and measurements of specific Hilbert space dimensions. On the other hand, the second technique, inspired by the Navascués–Pironio–Acín hierarchy for nonlocal correlations [39], provides a dimension independent upper bound on the maximum quantum violation of the NCI. We further study the robustness to experimental noise of the quantum violations. Our investigation uncovers novel non-trivial noncontextuality inequalities and reveals intriguing aspects of quantum contextual correlations, including applications in information processing tasks such as oblivious communication, dimension witness, certification of non-projective measurements and randomness generation.

The present study has focused on sets of indistinguishability conditions regarding preparations and measurements, respectively, to render them indistinguishable from each other. It is possible to consider scenarios with more than one set of indistinguishability conditions for a given scenario, each corresponding to convex decompositions of mixed preparations or measurements [7]. Extending our method to cover such scenarios could be explored more thoroughly in future research. The inherently contextual nature of quantum theory offers several distinct advantages in cryptographic and computational tasks. Our present analysis should motivate future endeavours to leverage newfound instances of quantum contextuality for information theoretic applications.

Example:- *Quantum advantage in oblivious communication.*— We consider a scenario, which consists of four preparations and three binary outcome measurements, defined with preparation indistinguishability conditions, as

$$\frac{1}{3}(P_0 + P_1 + P_2) \sim \frac{1}{2}(P_0 + P_3). \tag{1}$$

with $x \in \{0,1,2,3\}$, $y \in \{0,1,2\}$, $z \in \{0,1\}$. Using our approach, a large number of NCI are obtained [40], among which, a non-trivial inequality (with $p_{x,y} := p(0|x,y)$) is

$$\mathcal{I}_2 = -p_{0,0} + 2p_{1,0} + p_{0,1} - 2p_{2,1} \leqslant 2, \tag{2}$$

whose lower quantum bound is determined to be 2.645. We provide the strategy for obtaining the highest quantum bound 2.732.

The oblivious information transfer task is crucial in information theory, with numerous applications in cryptography [41, 42, 43, 44]. Quantum violations of NCIs with preparation indistinguishability lead to quantum advantage in oblivious communication [29]. The optimal classical encoding strategy for the sender in the oblivious communication task with respect to $\mathcal{I}_2$ is bounded by 2, and from our derived NCI, it follows that quantum advantage ensues whenever $\mathcal{I}_2 > 2$.

References

[1] R. W. Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Phys. Rev. A*, 71:052108, May 2005.

[2] Yeong-Cherng Liang, Robert W. Spekkens, and Howard M. Wiseman. Specker's parable of the overprotective seer: A road to contextuality, nonlocality and complementarity. *Physics Reports*, 506(1):1–39, 2011.

[3] Michael D Mazurek, Matthew F Pusey, Ravi Kunjwal, Kevin J Resch, and Robert W Spekkens. An experimental test of noncontextuality without unphysical idealizations. *Nature communications*, 7:11780, 2016.

[4] David Schmid, Robert W. Spekkens, and Elie Wolfe. All the noncontextuality inequalities for arbitrary prepare-and-measure experiments with respect to any fixed set of operational equivalences. *Phys. Rev. A*, 97:062103, Jun 2018.

[5] Matthew F. Pusey. Robust preparation noncontextuality inequalities in the simplest scenario. *Phys. Rev. A*, 98:022112, Aug 2018.

[6] Zhen-Peng Xu, Debashis Saha, Hong-Yi Su, Marcin Pawłowski, and Jing-Ling Chen. Reformulating noncontextuality inequalities in an operational approach. *Phys. Rev. A*, 94:062103, Dec 2016.

[7] Anubhav Chaturvedi, Máté Farkas, and Victoria J Wright. Characterising and bounding the set of quantum behaviours in contextuality scenarios. *Quantum*, 5:484, June 2021.

[8] Costantino Budroni, Adán Cabello, Otfried Gühne, Matthias Kleinmann, and Jan-Åke Larsson. Kochen-specker contextuality. *Rev. Mod. Phys.*, 94:045007, Dec 2022.

[9] Robert W. Spekkens. Negativity and contextuality are equivalent notions of nonclassicality. *Phys. Rev. Lett.*, 101:020401, Jul 2008.

[10] Anubhav Chaturvedi and Debashis Saha. Quantum prescriptions are more ontologically distinct than they are operationally distinguishable. *Quantum*, 4:345, October 2020.

[11] Anubhav Chaturvedi, Marcin Pawłowski, and Debashis Saha. Quantum description of reality is empirically incomplete, 2021.

[12] Matthew F. Pusey. Anomalous weak values are proofs of contextuality. *Phys. Rev. Lett.*, 113:200401, Nov 2014.

[13] Matteo Lostaglio. Quantum fluctuation theorems, contextuality, and work quasiprobabilities. *Phys. Rev. Lett.*, 120:040602, Jan 2018.

[14] David Schmid and Robert W. Spekkens. Contextual advantage for state discrimination. *Phys. Rev. X*, 8:011015, Feb 2018.

[15] David Schmid, John H. Selby, Matthew F. Pusey, and Robert W. Spekkens. A structure theorem for generalized-noncontextual ontological models, 2020.

[16] David Schmid, John H. Selby, and Robert W. Spekkens. Unscrambling the omelette of causation and inference: The framework of causal-inferential theories, 2020.

[17] Lorenzo Catani, Matthew Leifer, David Schmid, and Robert W. Spekkens. Why interference phenomena do not capture the essence of quantum theory. *Quantum*, 7:1119, September 2023.

[18] Lorenzo Catani, Matthew Leifer, Giovanni Scala, David Schmid, and Robert W. Spekkens. What is nonclassical about uncertainty relations? *Phys. Rev. Lett.*, 129:240401, Dec 2022.

[19] John H. Selby, Elie Wolfe, David Schmid, and Ana Belén Sainz. An open-source linear program for testing nonclassicality, 2022.

[20] Lorenzo Catani, Matthew Leifer, Giovanni Scala, David Schmid, and Robert W. Spekkens. Aspects of the phenomenology of interference that are genuinely nonclassical. *Phys. Rev. A*, 108:022207, Aug 2023.

[21] Matteo Lostaglio and Gabriel Senno. Contextual advantage for state-dependent cloning. *Quantum*, 4:258, April 2020.

[22] Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Roope Uola, and Alastair A. Abbott. Bounding and simulating contextual correlations in quantum theory. *PRX Quantum*, 2:020334, Jun 2021.

[23] Victoria J. Wright and Máté Farkas. Invertible map between bell nonlocal and contextuality scenarios. *Phys. Rev. Lett.*, 131:220202, Nov 2023.

[24] Robert W. Spekkens, D. H. Buzacott, A. J. Keehn, Ben Toner, and G. J. Pryde. Preparation contextuality powers parity-oblivious multiplexing. *Phys. Rev. Lett.*, 102:010401, Jan 2009.

[25] André Chailloux, Iordanis Kerenidis, Srijita Kundu, and Jamie Sikora. Optimal bounds for parity-oblivious random access codes. *New Journal of Physics*, 18(4):045003, apr 2016.

[26] V. Veitch J. Emerson M. Howard, J. Wallman. Contextuality supplies 'magic' for quatum computation. *Nature*, 510:351, 2014.

[27] Otfried Gühne, Costantino Budroni, Adán Cabello, Matthias Kleinmann, and Jan-Åke Larsson. Bounding the quantum dimension with contextuality. *Phys. Rev. A*, 89:062107, Jun 2014.

[28] Debashis Saha and Anubhav Chaturvedi. Preparation contextuality as an essential feature underlying quantum communication advantage. *Phys. Rev. A*, 100:022108, Aug 2019.

[29] Debashis Saha, Paweł Horodecki, and Marcin Pawłowski. State independent contextuality advances one-way communication. *New J. Phys.*, 21(9):093057, sep 2019.

[30] Alley Hameedi, Armin Tavakoli, Breno Marques, and Mohamed Bourennane. Communication games reveal preparation contextuality. *Phys. Rev. Lett.*, 119:220402, Nov 2017.

[31] Jaskaran Singh, Kishor Bharti, and Arvind. Quantum key distribution protocol based on contextuality monogamy. *Phys. Rev. A*, 95:062333, Jun 2017.

[32] Shouvik Ghorai and A. K. Pan. Optimal quantum preparation contextuality in an n-bit parity-oblivious multiplexing task. *Phys. Rev. A*, 98:032110, Sep 2018.

[33] Andris Ambainis, Manik Banik, Anubhav Chaturvedi, Dmitry Kravchenko, and Ashutosh Rai. Parity oblivious d-level random access codes and class of noncontextuality inequalities. *Quantum Information Processing*, 18(4):111, Mar 2019.

[34] David Schmid, Haoxing Du, John H. Selby, and Matthew F. Pusey. Uniqueness of noncontextual models for stabilizer subtheories. *Phys. Rev. Lett.*, 129:120403, Sep 2022.

[35] Kieran Flatt, Hanwool Lee, Carles Roch I Carceller, Jonatan Bohr Brask, and Joonwoo Bae. Contextual advantages and certification for maximum-confidence discrimination. *PRX Quantum*, 3:030337, Sep 2022.

[36] Carles Roch i Carceller, Kieran Flatt, Hanwool Lee, Joonwoo Bae, and Jonatan Bohr Brask. Quantum vs noncontextual semi-device-independent randomness certification. *Phys. Rev. Lett.*, 129:050501, Jul 2022.

[37] Zhen-Peng Xu Adan Cabello A. S. Majumdar Shashank Gupta, Debashis Saha. Quantum contextuality provides communication complexity advantage. *Phys. Rev. Lett.*, 130:080802, February 2023.

[38] Martin Henk, Jürgen Richter-Gebert, and Günter M Ziegler. Basic properties of convex polytopes. In *Handbook of discrete and computational geometry*, pages 383–413. Chapman and Hall/CRC, 2017.

[39] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007.

[40] Anubhav Chaturvedi Debashis Saha Soumyabrata Hazra, Subhankar Bera and A. S. Majumdar. Optimal demonstration of generalized quantum contextuality by relaxing of the noncontextual polytope. *Phys. Rev. A*.

[41] Claude Cr´epeau Charles H. Bennett, Gilles Brassard and Marie-H´el'ene Skubiszewsk. Practical quantum oblivious transfer. *Advances in Cryptology – CRYPTO'91*, page 351.

[42] Armando N. Pinto Manuel B. Santos, Ana C. Gomes and Paulo Mateus. Private computation of phylogenetic trees based on quantum technologies. *IEEE Access*, 10:38065, 2022.

[43] Armando N. Pinto Manuel B. Santos, Paulo Mateus. Quantum oblivious transfer: a short review. 2022.

[44] Masahito Hayashi and Seunghoan Song. Two-server oblivious transfer for quantum messages. *Advanced Quantum Technologies*, 2024.

Efficient Parameter-Shift Rule Implementation for Computing Gradient on Quantum Simulators

Vu Tuan Hai[1] * Le Vu Trung Duong[1] Pham Hoai Luan[1] Yasuhiko Nakashima[1]

[1] *Nara Institute of Science and Technology, 8916–5 Takayama-cho, Ikoma, Nara 630-0192, Japan*

Abstract. Quantum computing is an active research interest in the new computational area with various applications. In the quantum machine learning field, the parameterized quantum circuit is a core learnable model; this model is updated iteratively by the general Parameter-Shift Rule (PSR) technique. In many qubits and parameter scenarios, using PSR consumes significant computational resources, particularly in the quantum simulator. Therefore, this research proposes a method to perform the PSR more efficiently for matrix multiplication and state-based quantum simulators. The results show that our method is faster than baseline matrix multiplication-based **12** times and baseline state-based **39** times on average experiment.

Keywords: quantum simulator, quantum machine learning, quantum gradient

1 Introduction

Quantum machine learning (QML) is the intersection of quantum computing and artificial intelligence, which presents an exciting new frontier with transformative potential across various research fields, from combinatorial optimization and machine learning to simulation [1]. By combining principles from quantum mechanics and machine learning algorithms, QML promises novel approaches to propose new efficient learning models where the Parameterized Quantum Circuit (PQC) is the core part [2]. As a learning model, a PQC minimizes the cost value by updating its parameters, which are phase values in rotation gates. Accordingly, a lot of optimizers for the PQC have been proposed, from zero-order optimizers such as COBYLA [3] and finite difference [4] to quantum optimizers such as quantum nature gradient [5]. Recently, the general Parameter-Shift Rule (PSR) has been proposed in Ref. [6] and combined with first optimizer optimizers to provide an exact first-order gradient form for the PQC. After proving the efficiency versus other methods [7], this PSR has been integrated into quantum simulators including Matrix Multiplication (MM)-based simulators such as Pennylane [8] and Cirq [9], as well as state-based (stabilizer frame and wave function) like Qiskit [10] simulators.

Unfortunately, computing gradients by PSR requires lots of quantum evaluation, *which consumes huge computational resources in large scenarios and limits the application range of PSR in the above simulators.* To solve this problem, two possible solutions are proposed, including zero-order optimizer and self-optimizing PSR. The first solution uses the above zero-order optimizer for saving execution time with lower accuracy than the first-order optimizer, whereas the second solution uses self-optimizing PSR by reducing the number of quantum evaluations (#QE) [11, 12]. However, the efficiency of self-optimizing PSR still does not meet the requirements of quantum simulators. In this paper, we focus on enhancing the second solution to compute the unique elements of all QEs. Particularly, duplicate elements in QEs can be eliminated to avoid unnecessary computations. As a result, the PSR's efficiency is significantly enhanced, *leading to increases in the performance of the quantum simulator.* To the best of our knowledge, this is the first proposed method for both MM-based and state-based simulators.

*vu.tuan_hai.vr7@naist.ac.jp

2 Background

2.1 Parameterized Quantum Circuit (PQC)

Consider a n-qubits variational circuit $U(\boldsymbol{\theta})$ parametrized by $\boldsymbol{\theta} \equiv [\theta_0 \ \theta_1 \ \theta_2 \ \dots \ \theta_{m-1}]^\intercal$, which is also known as a PQC, can be written as a product of sub-circuit, where each sub-circuit contain only one parameter, as $U(\boldsymbol{\theta}) = U_{m-1}(\theta_{m-1}) \dots U_1(\theta_1) U_0(\theta_0)$. The target of using PQC is to find optimal $\boldsymbol{\theta}^*$ to achieve the minimal cost value $C(\boldsymbol{\theta}) = \langle\psi|U^\dagger(\boldsymbol{\theta})\hat{B}U(\boldsymbol{\theta})|\psi\rangle$, where $\hat{B}$ is the measurement operator and $|\psi\rangle$ is the reference quantum state. This task is solved by computing a gradient term as Eq. (1) and using classical optimizers such as SGD and Adam to update until $\boldsymbol{\theta} \approx \boldsymbol{\theta}^*$:

$$\nabla_{\boldsymbol{\theta}} C(\boldsymbol{\theta}) = \langle\psi|\nabla_{\boldsymbol{\theta}}(U^\dagger(\boldsymbol{\theta})\hat{B}U(\boldsymbol{\theta}))|\psi\rangle \tag{1}$$

2.2 Parameter-Shift Rule (PSR)

For rotation gates R_i, two-term PSR formula has been proposed in Ref. [13] as Eq. (2):

$$\frac{\partial C(\boldsymbol{\theta})}{\partial_{\theta_j}} = r[C(\boldsymbol{\theta}_j^{+\epsilon}) - C(\boldsymbol{\theta}_j^{-\epsilon})], \tag{2}$$

where $\boldsymbol{e}_j$ is the m-dimensional j^{th} unit vector, $\epsilon = \pi/2$, $r = 1/2$. For greater convenient, we denote $U(\boldsymbol{\theta}) \equiv U$, $\theta_j^{\pm\epsilon} \equiv \theta_j \pm \epsilon$ and $\boldsymbol{\theta}_j^{\pm\epsilon} \equiv \boldsymbol{\theta} \pm \epsilon \boldsymbol{e}_j$. In general, we have $2R$ - term PSR for any kind of parameterized gate, which is known as general PSR with $R \geq 2$ as the number of distinct eigenvalues of gate's generator [6]:

$$\frac{\partial C(\boldsymbol{\theta})}{\partial_{\theta_j}} = \sum_{k=1}^{R} d_k \left[C\left(\boldsymbol{\theta}_j^{+\epsilon_k}\right) - C\left(\boldsymbol{\theta}_j^{-\epsilon_k}\right)\right] \tag{3}$$

The fixed #QE is $(2 \times R) \times m$ for m parameters, then, number of matrix multiplications (#MM) for simulating

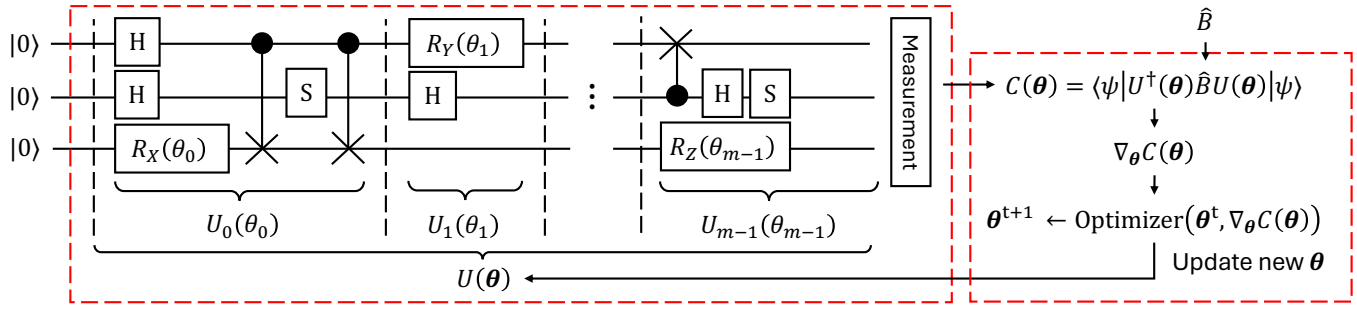


Figure 1: (Left) An example 3-qubits PQC ($U(\boldsymbol{\theta})$) is propose to split into sub-circuits $\{U_j(\theta_j)\}_{j\in[0,m-1]}$. Each sub-circuit has only one parameter. (Right) The output is used for computing gradient, then back to update PQC's parameters by the classical optimizer.

Eq. (3) sequentially is $(2 \times R \times m) \times (m-1)$. *As a result, these calculations will be enormous if the number of parameters is high.* Note that #MM is quite different if U is split in another way.

3 Proposed method

As mentioned in Sec. 2.2, there is a large #QE for baseline PSR that needs to be optimized. Because reducing #QE has been conducted in other research [11, 12], our proposed method will aim to compute these QE faster by considering U object, note that $\hat{B}$ and $|\psi\rangle$ are constant so it can be ignored. First, U is separated as $\{U_j\}$, then unique elements and duplicate elements are determined. In Sec. 3.1, we apply this idea to the MM-based simulator; the state-based simulator requires evaluating $|\psi_{m-1}\rangle = U|0\rangle$ that is quite different and will be discussed in Sec. 5. After that, unique elements are sorted and saved in a Look Up Table (LUT) presented in Sec. 3.2.

3.1 Application for MM-based simulator

We use the notation $\mathcal{U}_{i:j}$ as Eq. (4) for following content:

$$\mathcal{U}_{i:j} = \begin{cases} U_j U_{j-1} \dots U_i \text{ if } i < j \\ U_i \text{ if } i = j \\ \mathbb{I}_{2^n} \text{ if } i > j \end{cases} . \tag{4}$$

For each group $\{U(\boldsymbol{\theta}_j^{\pm\epsilon_k})\}_{k\in[1,R]}$, there are duplicate MMs from (1) computing $\mathcal{U}_j^{\text{head}} := \mathcal{U}_{0:j-1}$ and $\mathcal{U}_j^{\text{tail}} := \mathcal{U}_{j+1:m-1}$ in terms: $U(\boldsymbol{\theta}_j^{\pm\epsilon_k}) = \mathcal{U}_j^{\text{tail}} U_j(\theta_j^{\pm\epsilon_k}) \mathcal{U}_j^{\text{head}}$ and (2) between $\{\mathcal{U}_j^{\text{head}}, \mathcal{U}_{j+1}^{\text{head}}\}$ and $\{\mathcal{U}_j^{\text{tail}}, \mathcal{U}_{j-1}^{\text{tail}}\}$. The duplicate MMs can be eliminated by reusing $\mathcal{U}_j^{\text{head}}$ and $\mathcal{U}_j^{\text{tail}}$ for computing $\mathcal{U}_{j+1}^{\text{head}} = U_j \mathcal{U}_j^{\text{head}}$ and $\mathcal{U}_{j-1}^{\text{tail}} = \mathcal{U}_j^{\text{tail}} U_{j-1}$ as Eq. (5), respectively:

$$\begin{aligned} U(\boldsymbol{\theta}_{j+1}^{\pm\epsilon_k}) &= \mathcal{U}_j^{\text{tail}} U_{j+1}(\theta_{j+1}^{\pm\epsilon_k}) \mathcal{U}_{j+1}^{\text{head}}, \\ U(\boldsymbol{\theta}_{j-1}^{\pm\epsilon_k}) &= \mathcal{U}_{j-1}^{\text{tail}} U_{j-1}(\theta_{j-1}^{\pm\epsilon_k}) \mathcal{U}_{j-1}^{\text{head}}. \end{aligned} \tag{5}$$

For analyzing the efficiency of the application for MM-based simulator, the #MM for $\{\mathcal{U}_j^{\text{head}}, \mathcal{U}_j^{\text{tail}}\}$ is discussed here. For example if $j = 2$, we need to compute $\{\mathcal{U}_{0:2}, \mathcal{U}_{1:2}, U_2\}$, where $\mathcal{U}_{1:2} = U_2 U_1$ and $\mathcal{U}_{0:2} = \mathcal{U}_{1:2} U_0$, totally cost only two MMs. In general:

$$\begin{aligned} \#\text{MM}_{(\text{Proposed})} &= \sum_{j=0}^{m-1} j + 4R = m \times (m-1)/2 + 4R \\ \#\text{MM}_{(\text{Baseline})} &= (4R) \times (m \times (m-1)/2), \end{aligned} \tag{6}$$

where $\#\text{MM}_{(\text{Proposed})}$ and $\#\text{MM}_{(\text{Baseline})}$ is the #MM in the proposed method and baseline method, respectively. $4R(2 \times 2R)$ in term $\#\text{MM}_{(\text{Proposed})}$ is for $2R$ evaluations, where each evaluation consumes two MMs. One between $\{\mathcal{U}_j^{\text{head}}, U_j(\theta_j^{\pm\epsilon_k})\}$ and one between $\{\mathcal{U}_j^{\text{tail}}, U_j(\theta_j^{\pm\epsilon_k}) \mathcal{U}_j^{\text{head}}\}$. Obviously, the $\#\text{MM}_{(\text{Proposed})}$ is less than $\#\text{MM}_{(\text{Baseline})} (\forall m, R \in \mathbb{N}^+, R \geq 2)$ at least **8** (4×2) times for derivative at R_i gates, **16** (4×4) times for derivative at Control-R_i gates and more for more complex gates.

3.2 Memory for the Look Up Table (LUT)

As discussed in the above section, $\{\mathcal{U}_j^{\text{head}}, \mathcal{U}^{\text{tail}}, U_j\}$ are unique elements. By using a LUT, we offer a trade-off between execution-time and memory for saving those elements as $m \times (m+1)/2$ $2^n \times 2^n$-matrices. Thus, for MM-based simulator, we only save maximum $(1 + m + m)$ elements for one $\mathcal{U}^{\text{head}}$, m different $\mathcal{U}_j^{\text{tail}}$ and m different U_j, respectively. Note that $\mathcal{U}_j^{\text{head}}$ and $\mathcal{U}_j^{\text{tail}}$ can be eliminated since computing term $U(\boldsymbol{\theta}_{j+1}^{+\epsilon_0})$. In state-based simulator, it needs $(m + m)$ elements for m different U_j and m different $|\psi_j\rangle$. Especially, the LUT is not dependent on R and n, which means the proposed PSR can scale for high-order gradients and the large number of qubit circuits.

4 Experiment

The simulations are implemented in Python and run on the Intel i7-13700K 24-core CPU. Our method is verified on compact random quantum circuit datasets, where each circuit has a maximum number of gates with a given depth (d). Next, each circuit is divided into m sub-circuits by converting the quantum circuit from Qiskit object to QASM 2.0 format. Then, sub-circuits data is put into three different processing functions including MM-based (Proposed), MM-based (Baseline), and state-based (Baseline). The execution time is measured from the moment the program receives the sub-circuits to

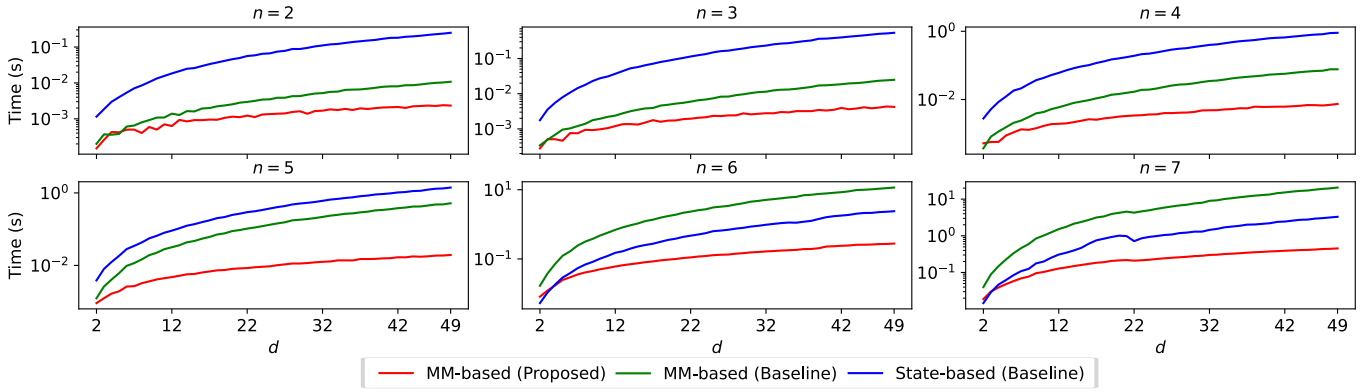


Figure 2: Execution time (y-axis) from 2 to 7-qubit quantum circuit in log scale, with (x-axis) is depth value from 2 to 49.

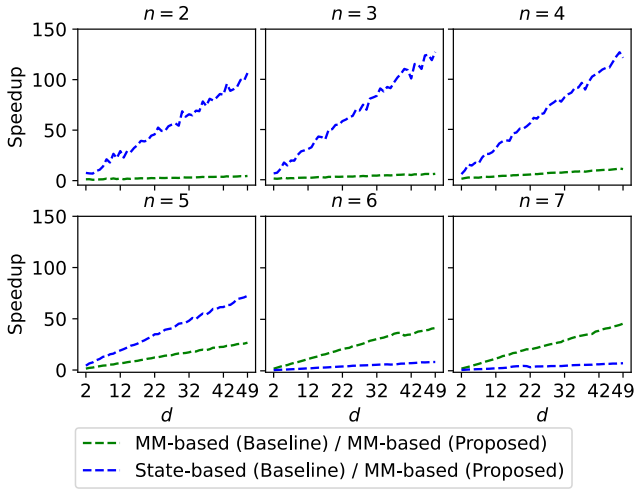


Figure 3: Speedup (y-axis) compare between proposed method and baselines, from 2 to 7-qubit quantum circuit, with (x-axis) is depth value from 2 to 49.

when the processing functions return the gradient value. Each case $\{n, d\}$ is evaluated by computing the gradient for 100 different circuits in the dataset and then returning the average.

The main results are shown in Fig. 2. Baseline PSR and Proposed PSR in MM-based methods are implemented from scratch when we use Qiskit's method named `from_instruction(.)` from module `qiskit.quantum_info.Statevector` to extract $|\psi_l\rangle$ for simulating state-based simulator (stabilizer frames). Stabilizer frames only keep a quantum state, which ensures a very short execution time compared with MM-based.

The result in Fig. 3 shows that our proposed method is faster than both baselines and more efficient in higher depth. In a higher #qubit, the speedup increases with the MM baseline and decreases with the state-based baseline, as Fig. 3. In the smallest case (2 qubits with a depth of 2), our method is faster than baseline PSR MM-based **1.3** times and baseline PSR state-based **7.6** times. In the largest case (7 qubits with a depth of 49), our method is faster than baseline PSR MM-based **45.7** times and baseline PSR state-based **7.2** times.

5 Discussion: Application for state-based simulator

For different quantum simulators such as wave function [14] and stabilizer frame [15], the proposed PSR can be applied with reverse computation path compared with baseline PSR MM-based . With $|\psi_j\rangle = \mathcal{U}_j^{\text{head}}|\mathbf{0}\rangle$, we have already known $|\psi_{j+1}\rangle = U_{j+1}|\psi_j\rangle$ which can be rewritten as $\hat{n}_{j+1}$ steps $\left(G_{j+1,\hat{n}_{j+1}-1}\ldots\left(G_{j+1,1}\left(G_{j+1,0}|\psi_j\rangle\right)\right)\right)$. Similar with MM-based, we create a 1-dimensional LUT to store $\{|\psi_j\rangle, U_j\}_{j\in[0,m-1]}$. The number of total steps for stabilizer formalism is $(2\times R\times m)\times\left(\sum_{j=0}^{m-1}\hat{n}_j\right)$. In proposed method, we consume m matrix-vector multiplication for preparing $\{|\psi_j\rangle\}_{j\in[0,m-1]}$ and $(2\times R)\times(\sum_{j=0}^{m-1}\sum_{l=j}^{m-1}\hat{n}_l)$ steps for stabilizer formalism, which reduced about half number of steps.

6 Conclusion

Reducing the cost of computing gradient in simulation is a crucial problem for QML applications. By eliminating the duplicate element in the PSR technique, the execution time can be significantly reduced, it can be decreased more if applying our proposal in parallel. This method can work with different kinds of existing quantum simulators such as Qiskit, Pennylane, and Qulacs. Further experiments in different datasets and simulators will be conducted and compared in future works.

Appendix

Appendix 1: Algorithms

The algorithm for the baseline PSR MM-based simulator and proposed PSR MM-based simulator can be referred to Algorithm. 1 and Algorithm. 2, respectively.

Appendix 2: High-order gradient

In this appendix, we discuss about higher-order gradient. Because Eq. (2) is the analytic derivative, we can apply it again to get the higher-order, such as second-order derivative with respect to any parameters $\{\theta_j, \theta_{j'}\}$: $\partial_{\theta_j\theta_{j'}}C(\boldsymbol{\theta}) = \partial_{\theta_{j'}}(\partial_{\theta_j}C(\boldsymbol{\theta}))$. For general $\mathcal{K}$-order derivative with $\mathcal{K} > 0$:

Algorithm 1 Two-term PSR ($R = 2$) for MM-based simulator

Input: $U(\boldsymbol{\theta}), \hat{B}$
Output: $\nabla_{\boldsymbol{\theta}} C$

state$^+ \leftarrow [1\ 0\ ...\ 0]^\intercal$; state$^- \leftarrow [1\ 0\ ...\ 0]^\intercal$
$\nabla_{\boldsymbol{\theta}} C \leftarrow [0\ 0\ \dots\ 0]^\intercal$
$Us \leftarrow$ splitter(U) {Divide U into $\{U_0, U_1, \dots, U_{m-1}\}$}
for i in $[0, \dots, m-1]$ **do**
  for j in $[0, \dots, m-1]$ **do**
    $\theta_j \leftarrow \boldsymbol{\theta}[j]$
    if $j = i$ **then**
      state$^+ \leftarrow Us[j](\theta_j^{+\epsilon}) \times$ state$^+$
      state$^- \leftarrow Us[j](\theta_j^{-\epsilon}) \times$ state$^-$
    else
      state$^+ \leftarrow Us[j](\theta_j) \times$ state$^+$
      state$^- \leftarrow Us[j](\theta_j) \times$ state$^-$
    end if
  end for
  $\mathrm{C}^+ \leftarrow \left((\text{state}^+)^\dagger\right)^\intercal \times \hat{B} \times \text{state}^+$
  $\mathrm{C}^- \leftarrow \left((\text{state}^-)^\dagger\right)^\intercal \times \hat{B} \times \text{state}^-$
  $\nabla_{\boldsymbol{\theta}} C[i] \leftarrow r \times (\mathrm{C}^+ - \mathrm{C}^-)$
end for
return $\nabla_{\boldsymbol{\theta}} C$

Algorithm 2 Proposed two-term PSR ($R = 2$) for MM-based simulator

Input: $U(\boldsymbol{\theta}), \hat{B}$
Output: ∇C

$\mathbf{0} \leftarrow [1\ 0\ ...\ 0]^\intercal$; $\nabla C \leftarrow [0\ 0\ \dots\ 0]^\intercal$
$Us \leftarrow$ splitter(U); {Divide U into $\{U_0, U_1, \dots, U_{m-1}\}$}
$\mathcal{U}s^{\text{tail}} \leftarrow [\mathbb{I}_{2^n}]$; $\mathcal{U}^{\text{tail}} \leftarrow \mathbb{I}_{2^n}$
for j in $[m-1, \dots, 2, 1]$ **do**
  $\mathcal{U}^{\text{tail}} \leftarrow \mathcal{U}^{\text{tail}} \times Us[j]$
  $\mathcal{U}s^{\text{tail}}$.append($\mathcal{U}^{\text{tail}}$)
end for
$\mathcal{U}^{\text{head}} \leftarrow \mathbb{I}_{2^n}$; $\mathcal{U}s^{\pm} \leftarrow [\,]$;
for j in $[0, 1, \dots, m-1]$ **do**
  $U(\boldsymbol{\theta}_j^{+\epsilon}) \leftarrow \mathcal{U}s^{\text{tail}}[m-1-j] \times Us[j](\theta_j^{+\epsilon}) \times \mathcal{U}^{\text{head}}$
  $U(\boldsymbol{\theta}_j^{-\epsilon}) \leftarrow \mathcal{U}s^{\text{tail}}[m-1-j] \times Us[j](\theta_j^{-\epsilon}) \times \mathcal{U}^{\text{head}}$
  $\mathcal{U}^{\text{head}} \leftarrow Us[j] \times \mathcal{U}^{\text{head}}$
  $\mathcal{U}s^{\pm}$.append($[U(\boldsymbol{\theta}_j^{+\epsilon}), U(\boldsymbol{\theta}_j^{-\epsilon})]$)
end for
for j in $[0, 1, \dots, m-1]$ **do**
  $[U(\boldsymbol{\theta}_j^{+\epsilon}), U(\boldsymbol{\theta}_j^{-\epsilon})] \leftarrow \mathcal{U}s^{\pm}[j]$
  $\mathrm{C}^+ \leftarrow \left((U(\boldsymbol{\theta}_j^{+\epsilon}) \times \mathbf{0})^\dagger\right)^\intercal \times \hat{B} \times \left(U(\boldsymbol{\theta}_j^{+\epsilon}) \times \mathbf{0}\right)$
  $\mathrm{C}^- \leftarrow \left((U(\boldsymbol{\theta}_j^{-\epsilon}) \times \mathbf{0})^\dagger\right)^\intercal \times \hat{B} \times \left(U(\boldsymbol{\theta}_j^{-\epsilon}) \times \mathbf{0}\right)$
  $\nabla C[j] \leftarrow r \times (\mathrm{C}^+ - \mathrm{C}^-)$
end for
return ∇C

$$\partial_{\theta_1\theta_2\dots\theta_{\mathcal{K}}} C(\boldsymbol{\theta}) = \frac{\Sigma_{\boldsymbol{s}\in\mathbf{S}_{\pm1,\pm2,\dots,\mathcal{K}}} P(\boldsymbol{s}) C(\boldsymbol{\theta}+\boldsymbol{s})}{2^{\mathcal{K}}(\prod_{j=1}^{\mathcal{K}} \sin(\epsilon_j))},$$

where:

$$\mathbf{S}_{\pm1,\pm2,\dots,\mathcal{K}} = [\pm\epsilon_0 \boldsymbol{e}_0\ \pm\epsilon_1 \boldsymbol{e}_1\ \dots\ \pm\epsilon_k \boldsymbol{e}_k]^\intercal$$

$$\text{and } P(\boldsymbol{s}) = \operatorname{sgn}\left(\prod_{j=0}^{k} \epsilon_j \boldsymbol{e}_j\right).$$

Following the above equations, a single $\mathcal{K}$-order derivative requires evaluating $2^{\mathcal{K}}$ elements in the sum. As the analysis in Ref. [16], the derivative tensor of order $\mathcal{K}$ is symmetric, so the actual #QE equals the number of distinct elements, which is less than $2^{\mathcal{K}}$, $\binom{m+\mathcal{K}-1}{\mathcal{K}} \approx \mathcal{O}(m^{\mathcal{K}})$ if $m \gg \mathcal{K}$. As a result, the #MM for our proposed PSR will be $m \times (m-1)/2 + (2 \times \mathcal{K} \times R)$ while the LUT is the same as the first-order derivative.

References

[1] Jacob Biamonte et al. "Quantum machine learning". In: *Nature* 549.7671 (Sept. 2017), pp. 195–202. ISSN: 1476-4687. DOI: 10.1038/nature23474. URL: https://doi.org/10.1038/nature23474.

[2] K. Mitarai et al. "Quantum circuit learning". In: *Phys. Rev. A* 98 (3 Sept. 2018), p. 032309. DOI: 10.1103/PhysRevA.98.032309. URL: https://link.aps.org/doi/10.1103/PhysRevA.98.032309.

[3] M. J. D. Powell. "Direct search algorithms for optimization calculations". In: *Acta Numerica* 7 (1998), pp. 287–336. DOI: 10 . 1017 / S0962492900002841.

[4] Gian Giacomo Guerreschi and Mikhail Smelyanskiy. "Practical optimization for hybrid quantum-classical algorithms". In: *arXiv preprint arXiv:1701.01450* (2017).

[5] James Stokes et al. "Quantum Natural Gradient". In: *Quantum* 4 (May 2020), p. 269. ISSN: 2521-327X. DOI: 10.22331/q-2020-05-25-269. URL: https://doi.org/10.22331/q-2020-05-25-269.

[6] David Wierichs et al. "General parameter-shift rules for quantum gradients". In: *Quantum* 6 (Mar. 2022), p. 677. ISSN: 2521-327X. DOI: 10.22331/q-2022-03-30-677. URL: https://doi.org/10.22331/q-2022-03-30-677.

[7] Marco Wiedmann et al. "An Empirical Comparison of Optimizers for Quantum Machine Learning with SPSA-Based Gradients". In: *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*. Vol. 01. 2023, pp. 450–456. DOI: 10.1109/QCE57702.2023.00058.

[8] Ville Bergholm et al. "Pennylane: Automatic differentiation of hybrid quantum-classical computations". In: *arXiv preprint arXiv:1811.04968* (2018).

[9] Sergei V Isakov et al. “Simulations of quantum circuits with approximate noise using qsim and cirq”. In: *arXiv preprint arXiv:2111.02396* (2021).

[10] Ali Javadi-Abhari et al. “Quantum computing with Qiskit”. In: *arXiv preprint arXiv:2405.08810* (2024).

[11] Vu Tuan Hai and Le Bin Ho. “Lagrange Interpolation Approach for General Parameter-Shift Rule”. In: *Quantum Computing: Circuits, Systems, Automation and Applications*. Ed. by Himanshu Thapliyal and Travis Humble. Cham: Springer International Publishing, 2024, pp. 1–17. ISBN: 978-3-031-37966-6. DOI: 10.1007/978-3-031-37966-6_1. URL: https://doi.org/10.1007/978-3-031-37966-6_1.

[12] Hanrui Wang et al. “QOC: quantum on-chip training with parameter shift and gradient pruning”. In: *Proceedings of the 59th ACM/IEEE Design Automation Conference*. DAC ’22. San Francisco, California: Association for Computing Machinery, 2022, pp. 655–660. ISBN: 9781450391429. DOI: 10.1145/3489517.3530495. URL: https://doi.org/10.1145/3489517.3530495.

[13] Maria Schuld et al. “Evaluating analytic gradients on quantum hardware”. In: *Phys. Rev. A* 99 (3 Mar. 2019), p. 032331. DOI: 10.1103/PhysRevA.99.032331. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.032331.

[14] Yasunari Suzuki et al. “Qulacs: a fast and versatile quantum circuit simulator for research purpose”. In: *Quantum* 5 (Oct. 2021), p. 559. ISSN: 2521-327X. DOI: 10.22331/q-2021-10-06-559. URL: https://doi.org/10.22331/q-2021-10-06-559.

[15] Jingyi Mei, Marcello Bonsangue, and Alfons Laarman. “Simulating Quantum Circuits by Model Counting”. In: *arXiv preprint arXiv:2403.07197* (2024).

[16] Andrea Mari, Thomas R. Bromley, and Nathan Killoran. “Estimating the gradient and higher-order derivatives on quantum hardware”. In: *Phys. Rev. A* 103 (1 Jan. 2021), p. 012405. DOI: 10.1103/PhysRevA.103.012405. URL: https://link.aps.org/doi/10.1103/PhysRevA.103.012405.

Measurement-Induced Magic Resources

Gong-Chu Li[1] * You Zhou[2] † Geng Chen[1] ‡ Chuanfeng Li [1] § Alioscia Hamma [3] ¶

[1] *University of Science and Technology in China*
[2] *Fudan University*
[3] *Università degli Studi di Napoli Federico II Dipartimento di Fisica Ettore Pancini*

Keywords: Magic state, Measurement-based Quantum Computation, Resource Theory

The final target of universal quantum computation, capable of tackling problems beyond the reach of classical computers, hinges on a crucial element: "magic." Magic refers to special quantum states namely T states and H states. Clifford with the help of magic states/gates become universal and hard to simulate in classical computers. Traditionally, these magic states are carefully prepared beforehand and injected into the quantum system. However, we delve into a groundbreaking approach: **generating magic through measurement**.

Measurement-based Quantum Computation (MQC) presents a unique framework for universal quantum computation. It begins with intricately entangled states, known as graph states. Instead of directly manipulating these states with standard quantum operations, MQC achieves computation by performing adaptive single-qubit measurements within the entangled network and final correction with the measurement results. From the view of magic resources, graph state brings zero magic resources and correction part won't change the magic resources as well, thus, all the magic resources were injected though the middle measurement part. We quantificationally reveal a surprising and powerful outcome: these measurements can effectively inject "magic" into the system, significantly boosting its computational power.

To understand how measurements generate magic, we introduce two novel concepts: invested magic resources and potential magic resources. Invested magic quantifies the amount of magic "invested" through the measurement process, akin to measuring the fuel used to power a journey. This provides a tool for analyzing the magic required for specific computations, serving as a **sufficient condition and upper bound** for realizing specific quantum operations. The greater the invested magic, the more complex the quantum tasks that can be achieved.

Potential magic, on the other hand, captures the maximum magic achievable within a given graph state, regardless of the measurement sequence. This concept highlights that not all entangled states are equally capable of generating magic. We demonstrate that simple graph structures, like linear chains or GHZ states, have

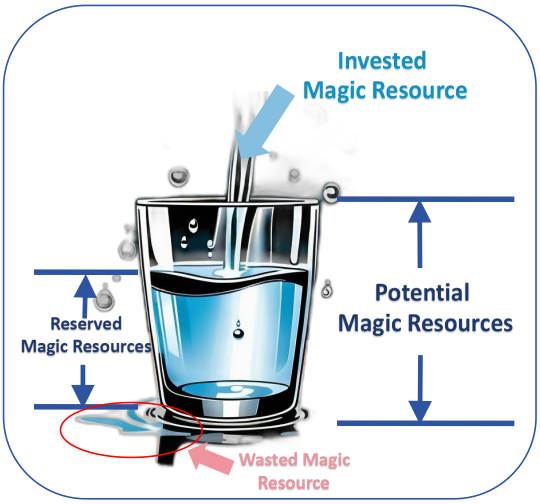


Figure 1: *Relationship among invested magic resources, potential magic resources, and the reserved magic resources.*

the potential magic of a mere 1T (1T is the maximum magic resource for 1 qubit) regardless of the number of qubits, restricting their utility for universal computation. That provides an information-theoretical explanation of the university of linear and GHZ states.

We also implement an experiment of MQC of 1D and 2D graphs with a high-quality 4-photon experiment. We scrutinize the invested and reserved magic resources step by step. Experimental results confirm the efficiency of MQC in generating magic compared to the conventional Magic State Injection (MSI) method. MQC can achieve higher magic content with fewer physical qubits, leading to significant space efficiency for building practical quantum computers. This advantage makes MQC a promising approach for developing smaller, more efficient quantum computers.

We also delve into the magic resource cost of QFT, a powerful algorithm with applications in cryptography and other fields. Using the concept of invested magic, We demonstrate that the magic requirements for QFT scale linearly with the number of qubits, $O(n)$. In the previous paper, at least $O(n \log n)$ of magic resources are needed. This finding opens the door to resource-efficient implementations of QFT, particularly through the use of truncated versions focusing on low-frequency compo-

*lgc1997@mail.ustc.edu.cn
†you_zhou@fudan.edu.cn
‡chengeng@ustc.edu.cn
§cfli@ustc.edu.cn
¶alioscia.hamma@unina.it

nents, potentially reducing computational complexity.

This research signifies a significant leap forward in our understanding and utilization of magic resources in quantum computation. The ability to generate magic through measurement opens up a new path for magic distillation with measurement distillation, leading to more powerful and versatile quantum algorithms. Furthermore, the concepts of invested and potential magic provide a powerful framework for analyzing and quantifying magic in general, potentially leading to more sophisticated resource theories and analysis techniques.

Realization of a Noisy-resilient Wavefunction Ansatz on a Cloud Based Quantum Hardware

Xiongzhi Zeng[1] Huili Zhang[2]

[1] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China.*
[2] *Hefei National Research Center for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei, 230026,China.*

Abstract. Quantum computing holds great potential for simulating chemical systems. In this study, we propose an efficient protocol for simulations of chemical systems, enabling accurate chemical reaction modeling on quantum hardware. In this protocol, we combine a correlation energy-based selection to define the active space, the driven similarity renormalization group (DSRG) method to account for the electron correlation effect, and a noise-resilient wavefunction ansatz to mitigate errors. This combination provides a quantum resource-efficient way to accurately simulate chemical systems. Additionally, modeling a Diels-Alder (DA) reaction using this protocol is performed on a cloud-based superconducting quantum computer. These results represent an important step forward in realizing quantum utility in the NISQ era.

Keywords: Driven similarity renormalization group(DSRG), hardware adaptable ansatz(HAA), variational quantum eigensolver(VQE), quantum cloud, quantum error mitigation

1 Introduction

In the rapidly evolving field of quantum computing, recent advancements have highlighted significant quantum advantages offered by various quantum platforms[1, 2], positioning quantum chemistry as a prime area for the application of this technology[3]. It is crucial to develop hybrid quantum-classical algorithms that require only a dozen qubits and shallow quantum circuits for quantum simulations of practical chemical systems. The choice of the active space is a longstanding problem in the context of both classical and quantum computational chemistry. Especially, in case of the theoretical predication of chemical reaction barriers, selecting the active space should be consistent for both the initial state and the transition state in order to obtain reliable relative energies. The effective Hamiltonian scheme[4, 5] that utilizes quantum computers only to diagonalize the effective Hamiltonian is preferred. One typical example is the driven similarity renormalization group (DSRG) method[6], which introduces a driving term to decouple interactions in a Hamiltonian and thus build a similarity-transformed Hamiltonian within a small active space for accurately treating electron correlation. As a promising application, the quantum DSRG method has been employed to study the bicyclobutane isomerization reaction using only a single qubit[7]. It is interesting to assess the quantum DSRG for simulating practical chemical reactions.

In this work, a novel strategy for automatically selecting active orbitals is first proposed based on orbital correlation energy. The quantum DSRG method is employed to generate the effective Hamiltonian, which is diagonalized using the varitional quantum eigensolver (VQE) with a hardware-adaptable ansatz[8]. We apply this protocol to simulate the Diels-Alder (DA) reaction[9, 10] on cloud-based superconducting quantum computer, achieving high accuracy in predicting the reaction barrier. Meanwhile, we demonstrate that the hardware-adaptable ansatz is more noise-resilient than the hardware-efficient ansatz.

2 Methods

The effective Hamiltonian theory has been posited as an innovative method to lessen the qubit requirement[11, 12] by "downfolding" the system Hamiltonian into an effective Hamiltonian in a small active space. As such, a complex many-body problem is significantly simplified into a manageable one that still capture the essence of the quantum system's behavior. In this work, we employ the DSRG method[13, 14] to build the effective Hamiltonian as

$$\hat{H}(s) = \hat{U}^\dagger(s) H \hat{U}(s) = e^{-\hat{A}(s)} H e^{\hat{A}(s)} \tag{1}$$

where $\hat{H}(s)$ is a similarity-transformed Hamiltonian and $\hat{U}(s)$ is a unitary transformation with a continuous parameter s defined in the range $[0, \infty)$. $\hat{A}(s)$ is an anti-Hermitian operator, written as

$$\hat{A}(s) = \hat{T}(s) - \hat{T}^\dagger(s). \tag{2}$$

$\hat{T}(s)$ is the cluster operator, which is represented as a sum of single, double, ..., excited operators $\hat{T}_k(s)$.

In the DSRG, the similarity-transformed Hamiltonian is driven by the source operator $\hat{R}(s)$, according to the following equation:

$$\left[\hat{H}(s)\right]_{od} = \left[e^{-\hat{A}(s)} H e^{\hat{A}(s)}\right]_{od} = \hat{R}(s) \tag{3}$$

The equation is augmented with an appropriate boundary condition for the operator. For $s = 0$, the non-diagonal component of the Hamiltonian is identical to the bare Hamiltonian $\left[\hat{H}(0)\right]_{od} = H_{od}$, which corresponds to $\hat{A}(0) = 0$. For $s \to \infty$, the DSRG flows decouple excitation configurations from the reference, driving the off-diagonal part of $\hat{H}(s)$ to zero, namely $\left[\hat{H}(\infty)\right]_{od} = 0$.

Although the DSRG method can significantly reduce the number of qubits required for simulating chemical

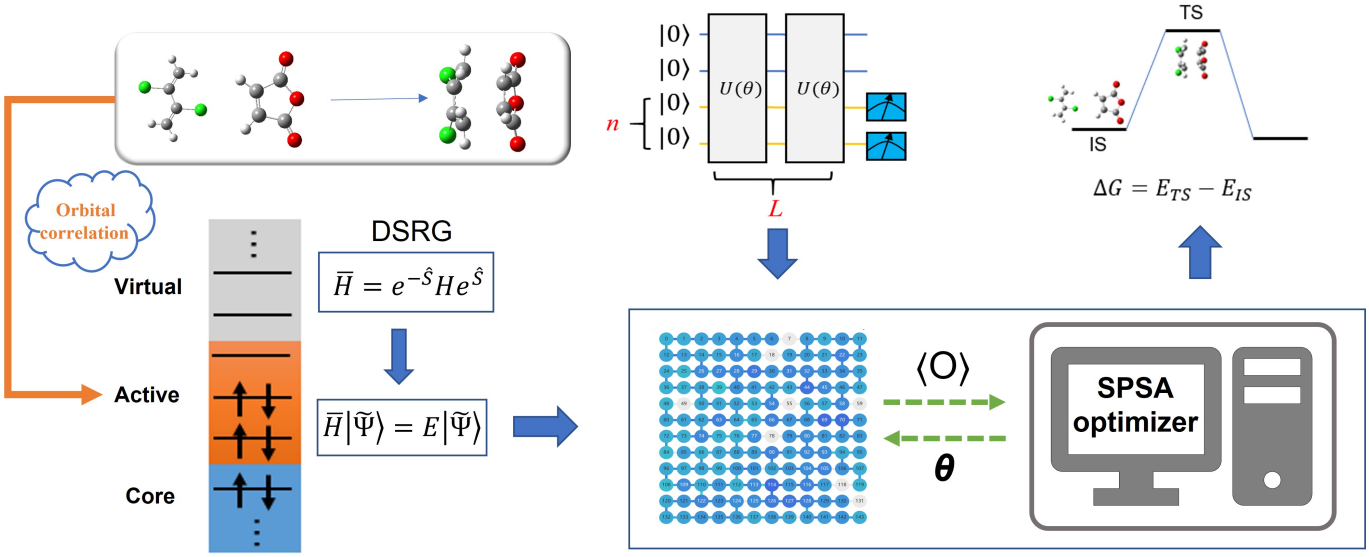


Figure 1: The workflow of the hybrid quantum-classical algorithm, which is composed of three main components: an automatic orbital selection procedure for determining the active space, the DSRG procedure for constructing an effective Hamiltonian, and the VQE procedure for estimating the total energies of chemical compounds.

systems, short coherence time and noise make us difficult to obtain reliable results on current NISQ hardware[3]. Therefore, it is essential to design an appropriate wave function ansatz or quantum circuit to reduce circuit depth in order to avoid error accumulation[15]. Circuit-friend wave function Ansätze, such as hardware efficient ansatz (HEA)[16] and the qubit coupled-cluster method[17], are able to ensure shallow circuits while advanced error mitigation techniques are still necessary. Recently, Zeng et al. suggested a hardware adaptable ansatz (HAA) [8], inspired by quantum neural networks. The corresponding quantum channel of HAA is defined as

$$\rho^{out} = tr_{anc}(U(\rho^{in} \bigotimes \rho^{anc})U^{\dagger}), \tag{4}$$

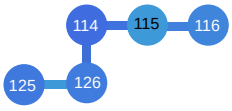
$$U = \prod_{l=1}^{L} \prod_{i=1}^{N} U_i^l(\theta_i^l) \tag{5}$$

where ρ^{in} and ρ^{anc} are the input density matrices of the system and ancilla qubits, respectively. ρ^{out} is the output density matrix of the system. $\rho^{in}/\rho^{anc} = |00..0><0..00|$. The operation tr_{anc} means the partial trace over the ancilla qubits. N is the number of ancilla qubits and L is the number of entangled layers.

3 Results

The quantum experiment is performed on Baqis's cloud-based hardware *Quafu Baiwang*[18, 19]. Baiwang consists of 136 superconductiong qubits, as shown in Fig. 1. The avaerge single qubit gate fidelity is 99.7% and the CZ gate fidelity is 94.6%. In this experiment, we select five qubits, the topology and information of the qubits and gates are shown in Fig. 2.

The Hamiltonian of electrons in the active space is encoded into 9 terms using Bravyi-Kitaev transformation.



Qubit Number	116	115	114	126	125
Single qubit gate fidelity (%)	99.979	99.990	99.991	99.976	99.984
CNOT gate fidelity (%)	98.8		98.6		
		99.3		97.2	
T1 (μs)	43.9	33.3	48.0	52.2	44.2
T2 Ramsey(μs)	14.40	18.44	11.79	24.64	25.57

Figure 2: The information of qubits used in experiment.

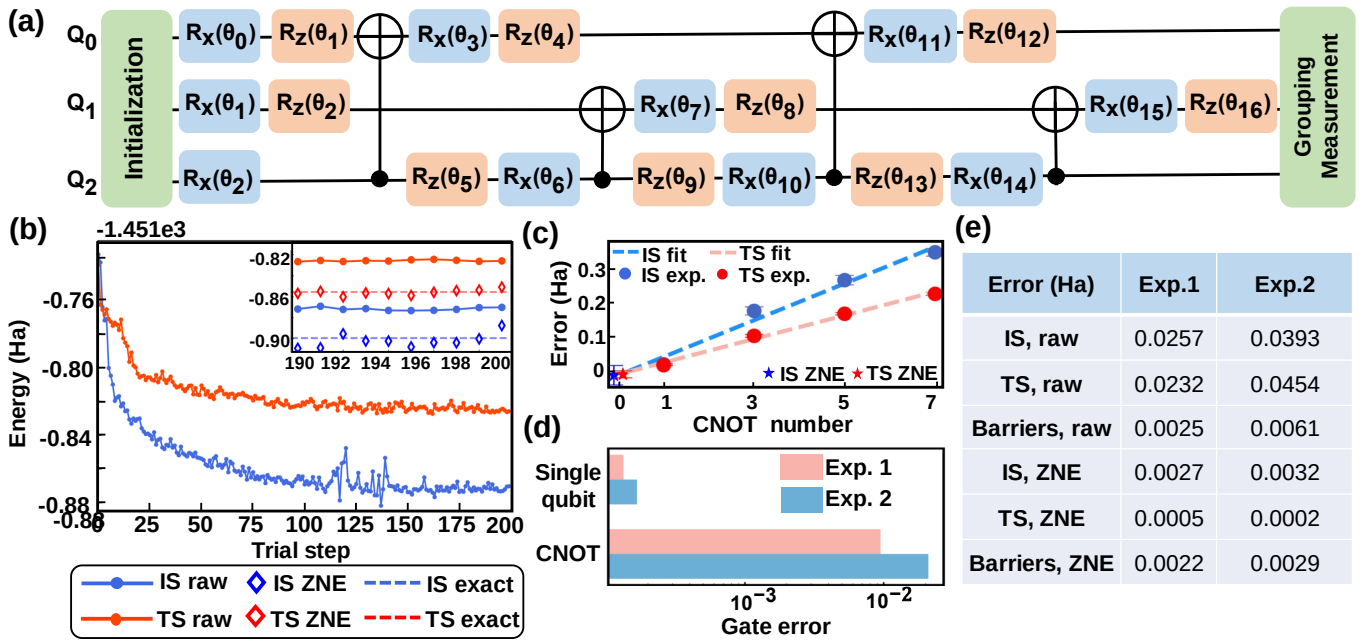
Then, the total energy can be reformulated as

$$E_{IS/TS} = \sum_{i=1}^{9} c_i \langle O_i \rangle, \tag{6}$$

where the coefficients c_i are obtained from the combination of one- and two-electron integrals.

The circuit utilized for minimizing the ground state energy of initial and transition states are designed by HAA, which includes 19 adjustable rotation gates along Z axis and X axis with 17 parameters and 4 CNOT gates,as shown in Figure 3(a). After iteration, we apply zero-noise extrapolation (ZNE) [20, 21, 22] approach to suppress experimental errors. In our ZNE approach, each single CNOT gate in the circuit is replaced by N copies of itself, while the single qubit gates are in consistent with the gates in corresponding trial steps. The final energy is obtained by linear extrapolating the averaged energy of 10 steps to the noiseless limit N = 0.

To minimize the energy, we apply the simultaneous perturbation stochastic approximation (SPSA) optimizer[23] on the classical computer to search the single gate parameters in quantum circuits. At the kth iteration step, the energy gradient $\boldsymbol{g}_k(\boldsymbol{\theta}_k)$ is calculated by adding the perturbation $\pm\boldsymbol{\epsilon}$ of the input parameter $\boldsymbol{\theta}_k$[24, 25], then the parameter is updated by the formula $\boldsymbol{\theta}_{k+1} = \boldsymbol{\theta}_{k+1} + a_k \boldsymbol{g}_k(\boldsymbol{\theta}_k)$, where a_k is the learning rate.



Error (Ha)	Exp.1	Exp.2
IS, raw	0.0257	0.0393
TS, raw	0.0232	0.0454
Barriers, raw	0.0025	0.0061
IS, ZNE	0.0027	0.0032
TS, ZNE	0.0005	0.0002
Barriers, ZNE	0.0022	0.0029

Figure 3: (a) The quantum circuit of hardware adaptable ansatz. The single qubit rotation angles $\theta_i, i \in [0, 16]$ are parameters to be optimized in the experiment. (b) The minimization procedure of the energy for the initial state (IS) energy (blue) and transition state (TS) energy (red). The inset shows the raw energy and energy after error mitigation using the zero-noise extrapolation (ZNE) technique for the final 10 steps. (c) The linear fitting of the averaged IS energy errors and TS energy errors of the final 10 steps, with each CNOT gate replaced with 1,3,5, and 7 CNOT gates, respectively. The correlation coefficients for the linear fittings are 0.9738 (IS) and 0.9916 (TS). (d) Average single qubit gate errors and CNOT gate errors of two qubit groups in experiments. (e) Comparison of the energy errors for HAA experiments using two groups of qubits on the quantum device.

The cost function in the optimizer is the total energy in experiment. In our experiment, we set the learning rate and perturbation to be 0.1 rad and 0.05 rad, respectively. For each measurement, the energy is obtained from 5120 shots on quantum devices. The calculated energy for each iteration step is shown in Fig. 3(b).

Zero-noise extrapolation (ZNE) method is widely used in quantum computation experiments[20, 21], which was first introduced by Li et al.[26] and Temme et al.[27] at 2017. This method amplifies circuit noise uniformly by gradually inserting gates into the circuit, and the desired (zero-noise) result is achieved through such as exponential function fitting. In the experiment, we take the energy from the final 10 steps of optimization process. In our ZNE approach, each single CNOT gate in the circuit is replaced by N copies of itself, while the single qubit gates are in consistent with the gates in corresponding trial steps. For each CNOT gate number and each step, we obtain the energy with 5 repetitions of 5120 shots in experiment, the result is shown in Fig. 3c. The final energy is obtained by linear extrapolating the averaged energy of 10 steps to the noiseless limit $N = 0$, as shown in 3b. After ZNE, the error of the energy can be suppressed below 2×10^{-3}, closing to the threshold of chemistry accuracy.

We also carry out the experiment using another group of qubits with lower gate quality on the same chip. The error rates of average single qubit gates and CNOT gates in two experiments are shown in Figure 3d. The difference of energy errors between two experiments shown in Figure 3e demonstrates that the HAA circuit is accurate even when the average CNOT gate error rate exceeds 1%, further attesting to HAA's noise resistance against noisy quantum circuits.

4 Conclusion

We propose a unique hybrid quantum algorithm. By selecting active orbitals based on the MBECAS scheme, we ensure that only the most important orbitals are involved in quantum simulations, thereby reducing quantum resource requirement. Next, using the DSRG method to build an effective Hamiltonian, enabling us to accurately capture both static and dynamic correlation effect in chemical reactions. Additionally, we introduce a hardware-adaptive wavefunction ansatz, further enhancing the algorithm's compatibility and efficiency on actual quantum hardware. By validating this algorithm on real quantum computing hardware, we demonstrated its feasibility, showcasing its efficiency and accuracy in handling specific chemical reactions. These results indicate that this new algorithm has the potential to become an important tool in chemistry and materials science as quantum computing technology matures.

References

[1] Arute, F. *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).

[2] Zhong, H.-S. *et al.* Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).

[3] McArdle, S., Endo, S., Aspuru-Guzik, A., Benjamin, S. C. & Yuan, X. Quantum computational chemistry. *Reviews of Modern Physics* **92**, 015003 (2020).

[4] Motta, M. *et al.* Quantum simulation of electronic structure with a transcorrelated hamiltonian: improved accuracy with a smaller footprint on the quantum computer. *Physical Chemistry Chemical Physics* **22**, 24270–24281 (2020).

[5] Bauman, N. P. *et al.* Downfolding of many-body hamiltonians using active-space models: Extension of the sub-system embedding sub-algebras approach to unitary coupled cluster formalisms. *J. Chem. Phys.* **151**, 014107 (2019).

[6] Evangelista, F. A. A driven similarity renormalization group approach to quantum many-body problems. *J. Chem. Phys.* **141**, 054109 (2014).

[7] Huang, R., Li, C. & Evangelista, F. A. Leveraging small-scale quantum computers with unitarily downfolded hamiltonians. *PRX Quantum* **4**, 020313 (2023).

[8] Zeng, X., Fan, Y., Liu, J., Li, Z. & Yang, J. Quantum neural network inspired hardware adaptable ansatz for efficient quantum simulation of chemical systems. *Journal of Chemical Theory and Computation* **19**, 8587–8597 (2023).

[9] Liepuoniute, I. *et al.* Simulation of a diels-alder reaction on a quantum computer. *arXiv preprint arXiv:2403.08107* (2024).

[10] Houk, K. Generalized frontier orbitals of alkenes and dienes. regioselectivity in diels-alder reactions. *Journal of the American Chemical Society* **95**, 4092–4094 (1973).

[11] Yanai, T. & Chan, G. K. Canonical transformation theory for multireference problems. *The Journal of chemical physics* **124** (2006).

[12] White, S. R. Numerical canonical transformation approach to quantum many-body problems. *The Journal of chemical physics* **117**, 7472–7482 (2002).

[13] Evangelista, F. A. A driven similarity renormalization group approach to quantum many-body problems. *The Journal of chemical physics* **141** (2014).

[14] Li, C. & Evangelista, F. A. Multireference theories of electron correlation based on the driven similarity renormalization group. *Annual Review of Physical Chemistry* **70**, 245–273 (2019).

[15] Cao, Y. *et al.* Quantum chemistry in the age of quantum computing. *Chemical reviews* **119**, 10856–10915 (2019).

[16] Kandala, A. *et al.* Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *nature* **549**, 242–246 (2017).

[17] Ryabinkin, I. G., Yen, T.-C., Genin, S. N. & Izmaylov, A. F. Qubit coupled cluster method: a systematic approach to quantum chemistry on a quantum computer. *Journal of chemical theory and computation* **14**, 6317–6326 (2018).

[18] Group, B. Q. Quafu-rl: The cloud quantum computers based quantum reinforcement learning (2024). 2305.17966.

[19] Group, B. Q. Quafu-qcover: Explore combinatorial optimization problems on cloud-based quantum computers (2023). 2305.17979.

[20] Kim, Y. *et al.* Evidence for the utility of quantum computing before fault tolerance. *Nature* **618**, 500–505 (2023).

[21] Kim, Y. *et al.* Scalable error mitigation for noisy quantum circuits produces competitive expectation values. *Nature Physics* **19**, 752–759 (2023).

[22] Foss-Feig, M. *et al.* Entanglement from tensor networks on a trapped-ion quantum computer. *Phys. Rev. Lett.* **128**, 150504 (2022). URL https://link.aps.org/doi/10.1103/PhysRevLett.128.15

[23] Kandala, A. *et al.* Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature* **549**, 242–246 (2017).

[24] Spall, J. Implementation of the simultaneous perturbation algorithm for stochastic optimization. *IEEE Transactions on Aerospace and Electronic Systems* **34**, 817–823 (1998).

[25] Spall, J. Multivariate stochastic approximation using a simultaneous perturbation gradient approximation. *IEEE Transactions on Automatic Control* **37**, 332–341 (1992).

[26] Li, Y. & Benjamin, S. C. Efficient variational quantum simulator incorporating active error minimization. *Phys. Rev. X* **7**, 021050 (2017).

[27] Temme, K., Bravyi, S. & Gambetta, J. M. Error mitigation for short-depth quantum circuits. *Phys. Rev. Lett.* **119**, 180509 (2017).

Asymptotic teleportation scheme bridging between standard and port-based teleportation

Ha Eum Kim [1] * Kabgyun Jeong [2 3] †

[1] *Department of Physics, Korea University, Seoul 02841, Korea*
[2] *Research Institute of Mathematics, Seoul National University, Seoul 08826, Korea*
[3] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*

Abstract. To address experimental constraints and specific application requirements in quantum teleportation, various schemes have been proposed. We introduce a novel approach that interconnects these schemes to overcome their limitations and leverage their unique advantages. In this study, we bridge standard teleportation and port-based teleportation through a new asymptotic teleportation scheme requiring classical selection followed by quantum correction. Specifically, we categorize and analytically investigate protocols within this scheme for qubit systems. We extend our analysis to higher-dimensional systems and discuss the potential application of a protocol from one of these groups as a universal programmable processor.

Keywords: Quantum teleportation, port-based teleportation, quantum communication, square-root measurement

1 Introduction

Quantum teleportation, initially proposed by Bennett *et al.* [1] and also known as standard teleportation (ST), represents one of the most intriguing predictions of quantum mechanics, allowing for the transmission of an unknown quantum state across spatially separated locations without the physical transfer of particles. This paradigm-shifting protocol exploits the non-local properties of quantum entanglement, a phenomenon that Albert Einstein famously critiqued as "spooky action at a distance." Such innovations underscore the protocol's critical role in enabling secure and efficient quantum networks [2, 3, 4], paving the way for the realization of a future quantum internet [5, 6].

However, the implementation of quantum communication encounters various challenges in the real world, leading to the proposal of different modified teleportation protocols to overcome these impediments. For example, catalytic quantum teleportation was theoretically proposed to overcome inevitable practical noise in resource states, utilizing entanglement states that are not consumed or degraded during the process [7]. Lipka-Bartosik *et al.* [8] proved that this protocol could achieve teleportation fidelity equal to that of noiseless teleportation. Recent experimental approaches to overcome noise include the use of multipartite hybrid entanglement to protect against dephasing noise in a linear optical framework [9]. Additionally, quantum error correction codes [10, 11] and weak measurements [12] are implemented in the quantum teleportation protocol. Moreover, based on linear optics, the maximum probability of successfully distinguishing Bell states is limited to 50%, significantly reducing the efficiency of teleportation [13]. Through the use of ancillary photons, the teleportation scheme proposed by Knill, Laflamme, and Milburn (KLM) enables asymptotically perfect state transmission[14], while other experiment have recently demonstrated Bell-state measurements exceeding this limit [15].

An asymptotic teleportation scheme that allows the receiver to make selections without performing quantum corrections has been proposed, known as port-based teleportation (PBT) [16]. This approach provides a universal programmable processor in a simple and natural manner. With its application potential in cryptography [17], holography [18], and quantum computing [19, 20], PBT contributes significantly to quantum communication. It also sheds light on the non-local measurements of multipartite states and advances understanding of communication complexity [21] and quantum channels [22]. Current research efforts are focused on modifying and optimizing PBT [23, 24, 25, 26], expressing it as efficient quantum circuits [27], and analysing its performance against noise [28].

Accordingly, various quantum teleportation schemes have been proposed and developed with the aim of surmounting experimental constraints or targeting specific applications. Such individuality and diversity prompt us to ask the ensuing question: 'Is it feasible to transition between different teleportation schemes through incremental adjustments of their parameters?' Exploring this possibility could unveil underlying connections between seemingly disparate teleportation mechanisms, offering a unified perspective on quantum communication. Our investigation seeks to not only validate the theoretical feasibility of such transitions but also to understand potential enhancements to teleportation efficiency and flexibility. In this work, we take the first steps by starting with an analysis of the effects of altering joint positive operator-valued measure (POVM) elements.

2 Model and Results

Drawing upon the insights from the PBT protocol, we introduce an asymptotic teleportation scheme rooted in our scenario. To understand this scheme, we revisit the

*hekim007@korea.ac.kr
†kgjeong6@snu.ac.kr

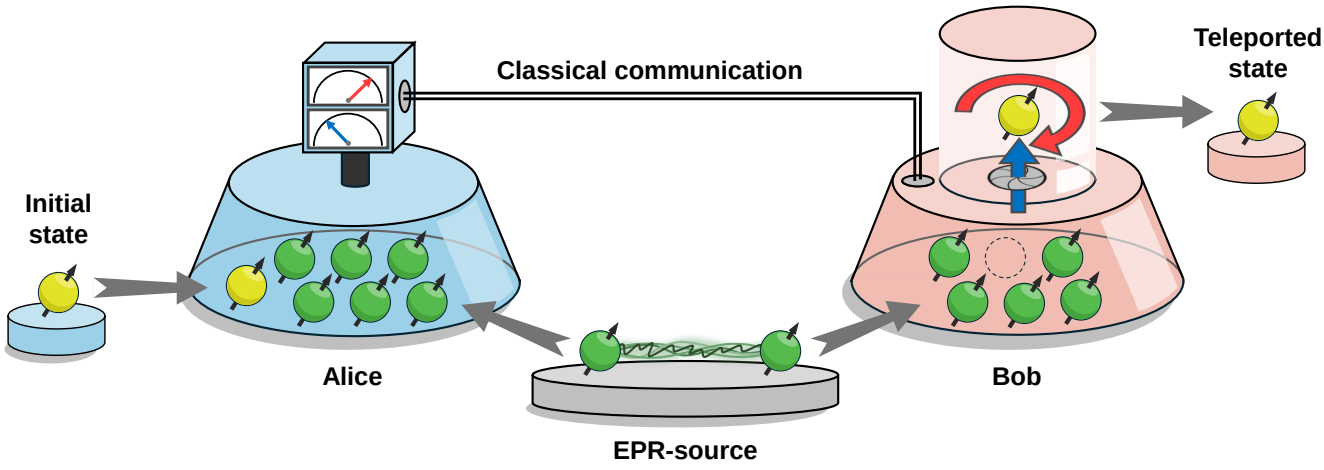


Figure 1: The scheme for port-based quantum correction teleportation (PBQCT). Alice wishes to teleport a quantum state, encoded in her yellow qudit, to Bob. They share N copies of maximally entangled pair of particles, shown as green qudits, originating from an EPR source. Alice then conducts a joint POVM, inspired from PBT protocol, on her yellow qudit and her bundles of green qudits. The measurement leads to two types of outcomes that convey classical and quantum correction information. She gets two type of outcomes, indicating classical and quantum correction information. Upon receiving these outcomes via classical communication, Bob selects the corresponding qudit and applies a quantum operation to reconstruct Alice's initial state. In the asymptotic limit of large N, the initial state is perfectly teleported.

PBT protocol, which is characterized by its requirement for only classical corrections for port-selection without the need for any quantum operations. This distinctive feature of PBT stems from its signal state configuration. In the asymptotic limit as N approaches infinity, the joint POVM elements converge directly to the signal states. Furthermore, we only needs to consider each single qubit of Alice and Bob's resource states upon observing the outcome. Thus, the state, storing the unknown state, and the Bob's qubit collapse to a Bell state, identical to the POVM element. This implies that once a port is selected, state transmission is ensured solely through a projection onto a prepared Bell state, rendering Bob's operation essentially an identity operation. Building upon this foundation, we extend the signal set used in PBT to include teleportation protocols that necessitate not only port-selection but also additional quantum corrections. We refer to this generalized measurement approach as port-based quantum correction teleportation, abbreviated as PBQCT.

Originating from PBT, our scheme inherits the characteristic of achieving perfect fidelity in the asymptotic limit, which we have proven in this work. Furthermore, given that PBQCT protocols utilize the expanded signal set of PBT, they can be systematically organized and interconnected based on the number of POVM elements. Specifically, for qubit systems, figure 2 demonstrates a diagram of asymptotic teleportation scheme transitions with changes in the number of ports and POVM elements. The area highlighted in blue represents the domain where PBQCT protocols are applicable. The range begins with the minimum number of POVM elements, where the count matches the number of ports and includes PBT, plotted by red dots. It extends to the maximum, with the count reaching the square of the dimension. This transition evolves into parallel ST functioning as independent protocols across ports, as represented by gray dots. Therefore, the PBQCT scheme ensures the preservation of asymptotic perfect fidelity, permitting a fluid transition between both protocols by gradually modifying the signal set.

In figure 2, the two yellow dots signify the linear optics teleportation protocol that employs a single EPR pair. Due to constraints in present Bell-state measurement techniques within linear optics, only two of the four Bell states are identifiable. Owing to these constraints, the teleportation protocol can be interpreted in two different ways: as deterministic protocols with two and three POVM elements. Considering the two indistinguishable Bell states as a single independent element of a POVM, the protocol operates through a three-element POVM. Conversely, if the space projected by these two states is regarded as null space, it results in a protocol utilizing a two-element POVM. Each protocol can be extended into PBQCT-2 and PBQCT-3 by doubling and tripling the number of ports, respectively. These protocols are indicated by blue open and closed dots in figure 2.

In our initial exploration of PBQCT, we investigate signal sets that remain invariant under the action of any permutation on the Alice's qubits, following the approach in PBT. This implies that every qubit is treated uniformly, without any particular distinction. Furthermore, we impose the condition that all signal states become one of the generalized Bell states when the identity part is traced out. This constraint is motivated by the fact that SRM is recognized as a highly effective measurement, approaching optimality, particularly for signal sets

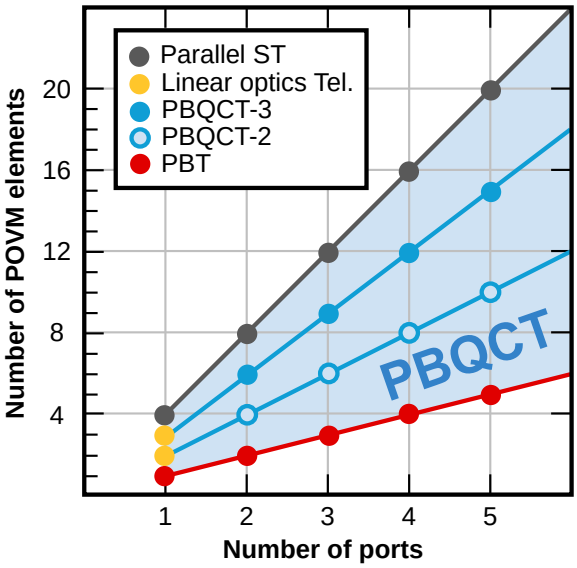


Figure 2: Asymptotic teleportation scheme diagram for qubit systems with respect to the number of ports and POVM elements. The blue shaded region depicts the PBQCT scheme. Protocols with the minimum number of POVM elements, including port-based teleportation (PBT) protocol, are denoted by red dots. The upper boundary of the domain, corresponding to the parallel standard teleportation (ST) protocol, is indicated with gray dots. For a single port, teleportation via linear optics is interpreted as two distinct PBQCT protocols, shown as yellow dots, depending on the approach to POVM. Incrementing the number of ports extends the protocols into PBQCT-2 and PBQCT-3 protocols, indicated by open and closed blue dots, respectively.

with orthogonal states. Moreover, this constraint enables the scheme to achieve asymptotic perfect teleportation fidelity. We summarize our investigations and findings for both two-dimensional and higher-dimensional systems in this work as follows:

- We proved that every PBQCT protocol provides perfect entanglement fidelity in the asymptotic limit for any type and dimension.
- We catagorized PBQCT into four groups, named as PBT, PBQCT-2, PBQCT-3 and parallel-ST, according to entanglement fidelity for qubit systems. Protocols within the same group have same size of POVM, and can be transformed with local unitary transformation at POVM and quantum correction operators.
- We analytically evaluated the POVM elements and entanglement fidelity of every PBQCT protocol in qubit systems.
- We generalized PBQCT-2 to higher dimensions, and analytically evaluated the POVM elements and entanglement fidelity.
- We numerically investigated PBQCT for qudit systems and found that the fidelities are enhanced as the size of the signal set increases.

3 Conclusions

The PBQCT protocols with SRM induced by two signal states for each port, denoted as PBQCT-2, show potential applicability for finding experimentally feasible teleportation schemes such that quantum correction is unnecessary. The first proposed PBT protocol has many difficulties in implementing it because the SRM elements are diagonalized to the Shur basis. On the other hand, PBQCT-2 appears to have greater implementation potential in that it is block diagonalized for computational total number and has a simple block form. Additionally, given that the null space where teleportation fails is the same as the KLM protocol, it is expected that it will be possible to express it with linear optics. Due to the necessity of Pauli correction in PBQCT-2, it cannot be classified as a protocol possessing identical functionality to PBT. The required quantum correction can be overcome by applying a simple two-bit concatenated code. If we apply a more generalized error code to PBQCT, we expect to be able to find protocols that can be utilized as a universal programmable processor that is also protected from various errors.

For high-dimensional applications, the generalized PBQCT-2 protocol retains all characteristics of PBQCT across higher dimensions. This opens new avenues for creating universal programmable processors utilizing qudit systems, offering significant advancements in quantum computing. Besides being a valuable and effective guide in finding nonnecessary quantum correction teleportation, PBQCT promises to be a good map for classifying existing asymptotic quantum teleportation. Just as ST and PBT have been linked through modification of POVM measurements, we expect that other teleportation protocols, like KLM protocol and catalytic teleportation, may also be classified as one of the PBQCT protocols if additional variations such as different forms of resource state, LOCC, and noise are allowed.

References

[1] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels *Phys. Rev. Lett.* **70** 1895

[2] Liao S-K, C W-Q and Handsteiner J *et al.* 2018 Satellite-Relayed Intercontinental Quantum Network *Phys. Rev. Lett.* **120** 030501

[3] Daiss S, Langenfeld S, Welte S, Distante E, Thomas P, Hartung L, Morin O and Rempe 2021 A quantum-logic gate between distant quantum-network modules *Science* **371** 614

[4] Pompili M, Hermans S L N, Baier S, Beukers H K C, Humphreys P C, Schouten R N, Vermeulen R F L, Tiggelman M J, L. dos Santos Martins, Dirkse B,

Wehner S and Hanson R 2021 Realization of a multinode quantum network of remote solid-state qubits *Science* **372** 259

[5] Kimble H 2008 The quantum internet *Science* **453** 1023

[6] Wehner S, Elkouss D and Hanson R 2018 Quantum internet: A vision for the road ahead *Science* **362** eaam9288

[7] Jonathan D and Plenio M B 1999 Entanglement-Assisted Local Manipulation of Pure Quantum States *Phys. Rev. Lett.* **83** 3566

[8] Lipka-Bartosik P and Skrzypczyk P 2021 Catalytic Quantum Teleportation *Phys. Rev. Lett.* **127** 080502

[9] Liu Z -D, Siltanen O and Kuusela T, Miao R -H, Ning C -X, Li C -F, Guo G -C and Piilo J 2024 Overcoming noise in quantum teleportation with multipartite hybrid entanglement *Sci. Adv.* **9** eadj3435

[10] Luo Y -H, Chen M -C and Erhard M *et al.* 2021 Quantum teleportation of physical qubits into logical code spaces *Proc. Natl Acad. Sci.* **118** e2026250118

[11] Ryan-Anderson C, Brown, N C and Baldwin C H *et al.* 2024 High-fidelity and Fault-tolerant Teleportation of a Logical Qubit using Transversal Gates and Lattice Surgery on a Trapped-ion Quantum Computer *arXiv:2404.16728*

[12] Harraz S, Cong S and Nieto J J 2022 Enhancing quantum teleportation fidelity under decoherence via weak measurement with flips *EPJ Quantum Technol.* **9** 15

[13] Calsamiglia J and Lütkenhaus N 2001 Maximum efficiency of a linear-optical Bell-state analyzer *Appl. Phys.* B **72** 67-71

[14] Knill E, Laflamme R, and Milburn G 2001 A scheme for efficient quantum computation with linear optics *Nature* **409** 46-52

[15] Bayerbach M J, D'Aurelio S E, van Loock P, and Barz S 2023 Bell-state measurement exceeding 50% success probability with linear optics *Sci. Adv.* **9** eadf4080

[16] Ishizaka S and Hiroshima T 2008 Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor *Phys. Rev. Lett.* **101** 240501

[17] Beigi S and König R 2011 Simplified instantaneous non-local quantum computation with applications to position-based cryptography *New. J. Phys.* **13** 093036

[18] May A 2022 Complexity and entanglement in non-local computation and holography *Quantum* **6** 864

[19] Sedlák M, Bisio A and Ziman M 2019 Optimal Probabilistic Storage and Retrieval of Unitary Channels *Phys. Rev. Lett.* **122** 170502

[20] Quintino M T, Dong Q, Shimbo A, Soeda A and Murao M 2019 Reversing Unknown Quantum Transformations: Universal Quantum Circuit for Inverting General Unitary Operations *Phys. Rev. Lett.* **123** 210502

[21] Buhrman H, Czekaj Ł, Grudka A, Horodecki M, Horodecki P, Markiewicz M, Speelman F and Strelchuk S 2016 Quantum communication complexity advantage implies violation of a Bell inequality *Proc. Natl. Acad. Sci. U.S.A.* **113**, 3191

[22] Pirandola S, Laurenza R, Lupo C and Pereira J L 2019 Fundamental limits to quantum channel discrimination *npj Quantum Inf.* **5** 50

[23] Mozrzymas M, Studziński M, Strelchuk S and Horodecki M 2018 Optimal port-based teleportation *New. J. Phys.* **20** 053006

[24] Jeong K, Kim J and Lee S 2020 Generalization of port-based teleportation and controlled teleportation capability *Phys. Rev.* A **102** 012414

[25] Studziński M, Mozrzymas M, Kopszak P and Horodecki M 2022 Efficient Multi Port-Based Teleportation Schemes *IEEE Trans. Inf. Theory* **68** 7892

[26] Strelchuk S and Studziński M 2023 Minimal port-based teleportation *New. J. Phys.* **25** 063012

[27] Grinko D, Burchardt A, Ozols M 2023 Efficient quantum circuits for port-based teleportation arXiv:2312.03188

[28] Kim H E and Jeong K 2024 Port-based entanglement teleportation via noisy resource states *Phys. Scr.* **99** 035105

High-dimensional Reconciliation for Continuous-Variable Quantum Key Distribution over a Free-Space Optical Channel

Kadir Gümüş[1] * João dos Reis Frazão[1] Vincent van Vliet[1] Sjoerd van der Heide[1]
Menno van den Hout[1] Gabriele Liga[2] Yunus Can Gültekin[2] Aaron Albores-Mejia[1 3]
Thomas Bradley[1] Alex Alvarado[2 3] Chigo Okonkwo[1 3]

[1] *High-capacity Optical Transmission Laboratory, Eindhoven University of Technology, The Netherlands*
[2] *Information and Communication Theory lab, Eindhoven University of Technology, The Netherlands*
[3] *CUbIQ Technologies, De Groene Loper 19, Eindhoven, The Netherlands*

Abstract. One of the most important aspects of continuous-variable quantum key distribution (CV-QKD) is the reconciliation step, which significantly impacts the performance of the CV-QKD system. We simulate the impact of discrete modulation on the reconciliation efficiency and consider the use of d-dimensional reconciliation with $d > 8$ to mitigate this impact, improving reconciliation efficiencies by up to 3.4%. We validate our results by experimentally demonstrating CV-QKD over a turbulent FSO link and demonstrate SKR gains by up to 165%.

Keywords: Continuous-variable Quantum Key Distribution, Reconciliation, Error Correction, Free-space Optics

1 Introduction

Quantum key distribution (QKD), first proposed in [1], has attracted considerable attention in recent years as concerns for information security grow. Using Shor's algorithm [2], it would be possible to break current public-key cryptography protocols, assuming that sufficiently capable quantum computers can be developed. With continuous advances in quantum computing [3], these concerns are expected to become a reality in the future. A potential solution to these issues is QKD, as it allows for the sharing of secret keys without a potential eavesdropper (Eve) with infinite computational power being able to recover the keys.

QKD can be broadly categorised into two different variants: discrete-variable (DV) [1] and continuous-variable (CV) [4]. DV-QKD involves the transmission of single photons for the distillation of secret keys and thus requires single photon detectors. Conversely, in CV-QKD quantum random numbers are modulated on the in-phase and quadrature components of coherent light and standard fibre optical telecommunication components which allows for a more cost-effective implementation, as opposed to DV-QKD [5]. The downside, however, is that post-processing is more challenging for CV-QKD. An important part of the post-processing is the reconciliation, where Alice and Bob try to share bits using error correction.

During reconciliation, the two involved parties, Alice and Bob, use their transmitted and measured quantum states, respectively, to exchange bits for secret key distillation. Alice generates the quantum states using either Gaussian modulation [6], in which she randomly generates a symbol based on a Gaussian distribution or discrete modulation [7], where she uses a finite-size constellation and randomly picks one of the constellation points. Although Gaussian modulation allows for longer distance QKD, practical implementation is difficult, as it is impossible to obtain a perfect Gaussian distribution using electro-optical modulators and digital-to-analog converters with finite resolution [8]. A system using discrete modulation formats mitigates this issue by approximating Gaussian modulation using probabilistically shaped quadrature amplitude modulation (PS-QAM) [9]. Analysis of different discrete modulation formats for CV-QKD has been performed in, e.g., [10], [11].

A commonly used protocol for reconciliation is multi-dimensional reconciliation, first introduced in [12]. Multi-dimensional reconciliation involves the use of multiplications and divisions of ($d = \{1, 2, 4, 8\}$-) dimensional numbers constructed using the Cayley-Dickson construction [13] in an attempt to construct a virtual channel. The constructed virtual channel is similar to a binary-input additive white Gaussian noise (BI-AWGN) channel. As shown in [14], The higher the dimensionality d of the reconciliation, the more closely the virtual channel resembles a BI-AWGN channel, hence, higher reconciliation efficiencies can be achieved as the capacity of the virtual channel increases.

In [12], [15] multi-dimensional reconciliation with $d > 8$, which we will refer to as high-dimensional reconciliation from this point forward, has been proposed and analysed. Instead of using multiplications and divisions, a mapping matrix is used. This high-dimensional reconciliation shows significant gains compared to when $d \leq 8$. This method involves the continuous generation of orthogonal random matrices, which will be used for constructing the mapping matrix. A new mapping matrix needs to be constructed for each set of d symbols for security reasons [12].

In this work, we investigate how the use of discrete modulation formats impacts the performance of error correction over a wide range of code rates. We consider the use of high-dimensional reconciliation to improve the reconciliation efficiency, showing improvements in reconciliation efficiencies β, especially for short- and mid-range CV-QKD systems, by up to 3.4%. Furthermore, we experimentally demonstrate high-dimensional reconciliation with CV-QKD transmission over a turbulent FSO channel and show that we can increase secret key rates (SKRs) by up to 165% compared to conventional multi-dimensional reconciliation.

*k.gumus@tue.nl

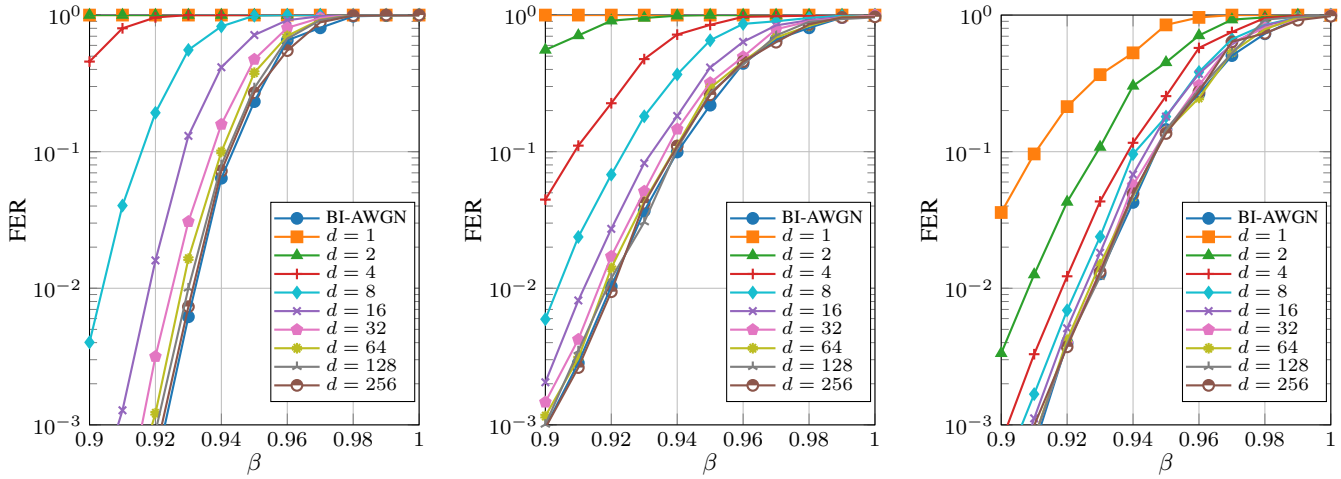


Figure 1. Simulated FER vs. β for different rate (Left: $R = \frac{1}{5}$, Middle: $R = \frac{1}{10}$, Right: $R = \frac{1}{50}$) TPB-LDPC codes for different d.

2 High-dimensional Reconciliation

To analyse the effect of the multi-dimensional reconciliation on the performance of the error correction, we have simulated the frame error rate (FER) curves for three type-based protograph (TBP) LDPC codes with rates $R = \frac{1}{5}$, $R = \frac{1}{10}$, $R = \frac{1}{50}$ [16] corresponding to short- ($\sim$ 20 km), mid- ($\sim$ 40 km), and long-range ($\sim$ 100 km) CV-QKD links for a large range of values of d. The quasi-cyclic parity check matrices for these codes were generated using progressive edge-growth [17], with cyclant sizes of 200, 200, and 500, and blocklengths of 10^5, 10^5, and 10^6 respectively. Gaussian modulation was used to generate the quantum states. The maximum amount of decoding iterations was set to 500.

The results of these simulations are shown in Fig. 1. The performance of the reconciliation depends on both d and R. For $R = \frac{1}{5}$, there is a significant gap in performance between $d = 8$ and $d = 128$, namely 2.7% β for an FER of 10%. When the rate of the code decreases, this gap diminishes, with a 1.6% difference for $R = \frac{1}{10}$, and 0.5% for $R = \frac{1}{50}$. We conjecture that this is because in the lower signal-to-noise ratio regime the decrease in channel capacity of the virtual channel compared to the quantum channel, caused by using a finite d in multi-dimensional reconciliation, is smaller. It is still worth considering using high-dimensional reconciliation for long-distance CV-QKD links, as the increase in complexity is negligible compared to the complexity of the decoding while offering an increase in β. However, it is mostly useful for short to mid-distance links, as this increase in β can lead to significant increases in SKR, as will be shown later.

We also simulated how different modulation formats impact the multi-dimensional reconciliation. The modulation formats are PS-QAM constellations, designed according to [10]. As shown in Fig. 2, the modulation format has a slight impact on the error correction performance. QPSK modulation performs the best because all symbols have equal power, and therefore, the virtual channel created during reconciliation corresponds to a BI-AWGN channel regardless of what d is. When increasing the cardinality of the constellation, the performance of the error correction code worsens when $d = 8$. This is especially clear for $R = \frac{1}{5}$, but for $R = \frac{1}{10}$ and $R = \frac{1}{50}$ the modulation formats are closer in performance. When we choose a high d, the error correction curves almost completely overlap for all of the codes for the different modulation formats.

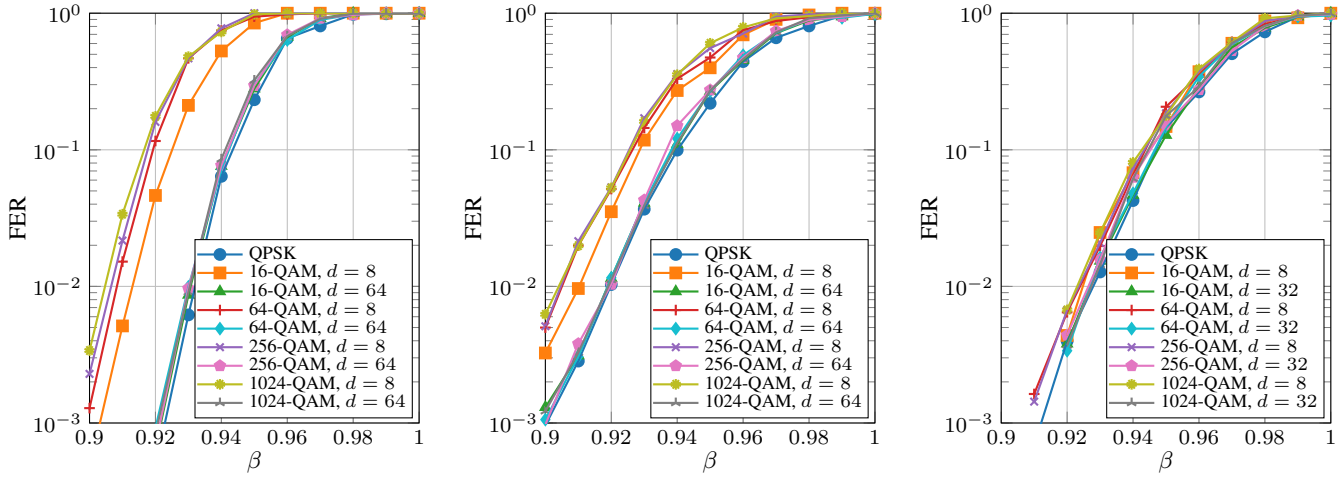


Figure 2. Simulated FER vs. β for different rate (Left: $R = \frac{1}{5}$, Middle: $R = \frac{1}{10}$, Right: $R = \frac{1}{50}$) TPB-LDPC codes for different d and modulation formats.

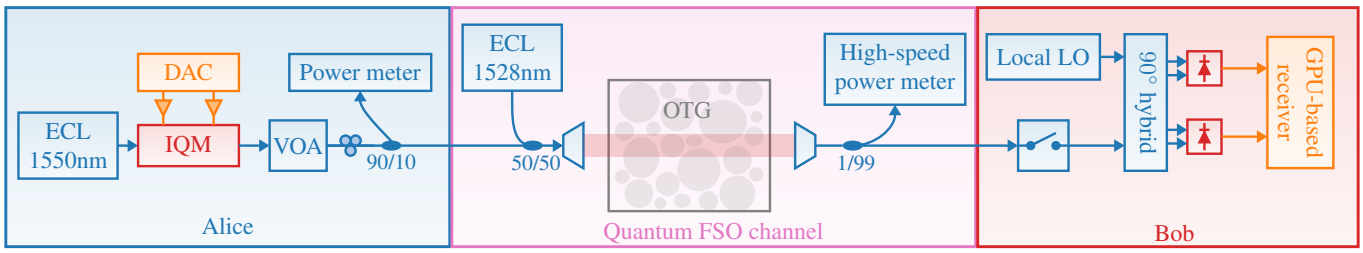


Figure 3. The CV-QKD setup for transmission over an FSO channel with an optical turbulence generator.

3 Experimental Results

Fig. 3 shows the experimental setup employed for CV-QKD transmission validation over a free-space optical (FSO) channel. On Alice's side, we deploy a <100 kHz linewidth external cavity laser (ECL) tuned to 1550 nm, a digital-to-analogue (DAC) converter, and an optical IQ-modulator (IQM) to transmit a PS-256QAM constellation with a symbol rate of 250 MBaud. A variable optical attenuator (VOA) and a power meter are used to attenuate the signal to an average power of 7.44 shot noise units (SNU) (−69.2 dBm). We combine a second tone produced by a second ECL for turbulence characterisation placed at 1528 nm with the attenuated 1550 nm quantum signal and coupled to free space using a collimator. The light then traverses an optical turbulence generator (OTG) [18], [19], which can mimic FSO channels with various turbulence strengths. We split off 1% of the light to a high-speed power meter for FSO channel characterisation. For our setup, we have measured a turbulence strength generated by the OTG with scintillation indices $\sigma_I = 0.001$ and pointing jitter $\beta_{jitter} = 123.8$ respectively, which can be classified as weak fluctuations [20].

The remaining 99% of light is directed to Bob's side, where for the 90° optical hybrid, a local ECL is used as a local local oscillator (LLO), after which the outputs are digitised. Calibration and recovery of the quantum signal is done using digital signal processing [21]. During the parameter estimation, the mutual information I_{AB}, the excess noise ξ_{Bob}, and the Holevo information χ_{BE} are estimated, taking into account finite-size effects [22]. Parameters for the system are a quantum efficiency of 40%, privacy amplification block size of $6.8 \cdot 10^6$, a clearance of 10 dB, an average ξ_{Bob} of 0.0045 SNU, and an average transmittance T of 0.41.

We use 128-dimensional reconciliation. Furthermore, we use the $R = 0.2$ expanded TBP-LDPC code punctured to $R \approx 0.3$, around the average I_{AB} of the system, for error correction. We choose a block length $N = 1.024 \cdot 10^5$ with a maximum of 500 decoding iterations. For the calculation of the secret key rate we use the following equation: $\text{SKR} = (1 - \text{FER})(\beta I_{AB} - \chi_{BE})$.

Figure 4 shows both the FER (left) and the SKR (right) of the experimental results. As expected, the FER of the 128-dimensional reconciliation is close in performance to the BI-AWGN, and at an FER of 10% there is an increase in β of approximately 3.4% compared to the 8-dimensional case. This is slightly more gain compared to the results in Fig. 2 because of the higher code rate. As a result, the SKR increases by 165%, where the optimal SKR is achieved at $\beta = 94\%$.

4 Conclusion

In this work, we have investigated the use of high-dimensional reconciliation for CV-QKD. We have analysed how the different modulation formats impact the reconciliation, and using experimental results, we show SKR gains by up to 165%. Future works could focus on a more extensive study on reconciliation in different experimental settings.

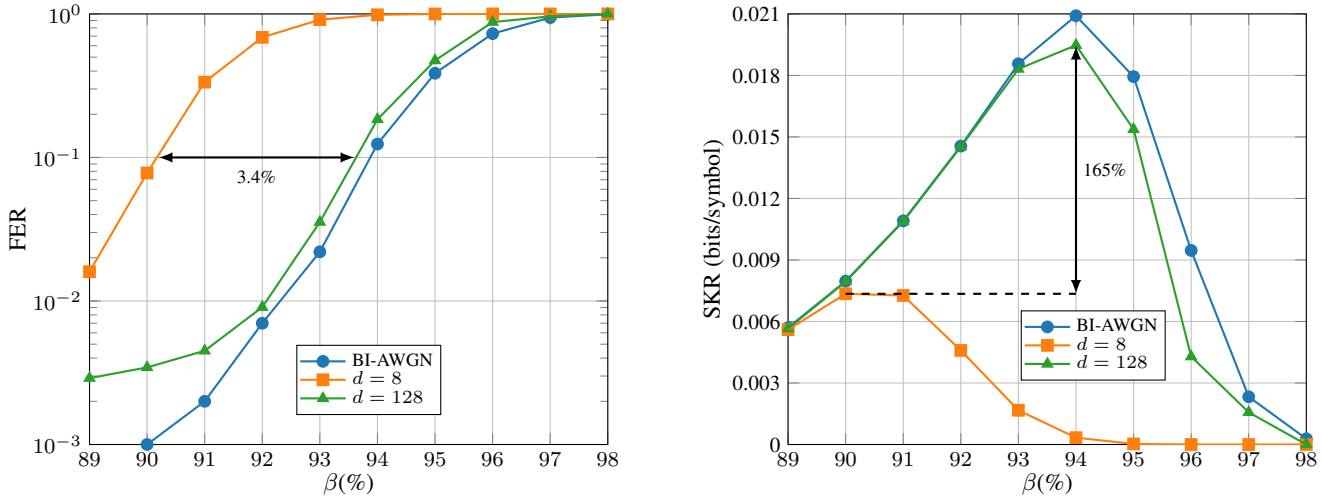


Figure 4. Experimental results. The FER (Left) and SKR (Right) of the $R = \frac{1}{5}$ expanded TBP-LDPC code when punctured to $R = 0.3$ for different d compared to the BI-AWGN channel for CV-QKD transmission over the FSO channel.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, ISSN: 0304-3975.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[3] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, 2019.

[4] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057 902, 5 2002.

[5] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, 2018.

[6] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[7] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Physical Review X*, vol. 9, no. 2, p. 021 059, 2019.

[8] E. Kaur, S. Guha, and M. M. Wilde, "Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 103, p. 012 412, 1 2021.

[9] J. Cho and P. J. Winzer, "Probabilistic constellation shaping for optical fiber communications," *Journal of Lightwave Technology*, vol. 37, no. 6, pp. 1590–1607, 2019.

[10] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, 2021.

[11] M. N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì, and M. Secondini, "Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel," *IEEE Transactions on Communications*, vol. 72, no. 1, pp. 375–386, 2024, ISSN: 1558-0857.

[12] A. Leverrier, R. Allé aume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Physical Review A*, vol. 77, no. 4, 2008.

[13] L. E. Dickson, "On quaternions and their generalization and the history of the eight square theorem," *Annals of Mathematics*, pp. 155–171, 1919.

[14] Y. Zhou, X.-Q. Jiang, W. Liu, T. Wang, P. Huang, and G. Zeng, "Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation," *Chinese Physics B*, vol. 27, no. 5, p. 050 301, 2018.

[15] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Physical Review A*, vol. 84, no. 6, 2011.

[16] K. Gümüş and L. Schmalen, "Low rate protograph-based LDPC codes for continuous variable quantum key distribution," *Proc. ISWCS 2021*, 2021.

[17] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE transactions on information theory*, vol. 51, no. 1, pp. 386–398, 2005.

[18] V. van Vliet, "Optical Turbulence Generator for Lab-based Experimental Studies of Atmospheric Turbulence in Vertical Optical Communication Links," M.S. thesis, TU/e, 2022.

[19] V. van Vliet, M. van den Hout, S. van der Heide, and C. Okonkwo, "Design, Characterisation, and Demonstration of a Hot-Air-Based Optical Turbulence Generator," in *Proceedings of the 26th Annual Symposium of the IEEE Photonics Benelux Chapter*, 26th Annual Symposium of the IEEE Photonics Benelux Chapter, 2022.

[20] K. Kiasaleh, "On the probability density function of signal intensity in free-space optical communications systems impaired by pointing jitter and turbulence," *Optical Engineering*, vol. 33, 1994.

[21] S. van der Heide, J. Frazão, A. Albores-Mejía, and C. Okonkwo, "Receiver noise stability calibration for CV-QKD," *Proc. OFC 2023*, 2023.

[22] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," *Physical Review A*, vol. 86, no. 3, 2012.

Leveraging Different Boolean Function Decompositions to Reduce T-Count in LUT-based Quantum Circuit Synthesis

David Clarino[1] * Naoya Asada[2] † Atsushi Matsuo[2] ‡ Shigeru Yamashita[1] §

[1] *Ritsumeikan University, Graduate School of Information Science and Engineering*
[2] *IBM Research, Tokyo*

Abstract. Lookup Table (LUT) based synthesis methods have recently been proposed as a way to synthesize quantum Boolean circuits in a qubit-constrained environment. Other recent research has demonstrated the possibility of using *relative phase* quantum circuits when compute/uncompute logic is used in tandem, reducing T-count in quantum Boolean circuits in the fault-tolerant quantum computing paradigm. Because LUT-based synthesis methods use compute/uncompute pairs on ancilla qubits, this suggests that implementing the arbitrary Boolean logic that make up the individual Boolean logic network nodes in a relative phase manner could reduce the T-count. To generate such arbitrary Boolean functions, we utilize Shannon's decomposition, Davio expansions, as well as alternating balanced and unbalanced relative phase circuits. Experimental results demonstrate that our method can reduce the T-count to an average of 24% of the existing method.

Keywords: relative-phase Toffoli gates (RTOF), circuit optimization, LUT, quantum circuit synthesis

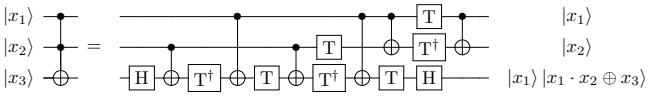


Figure 1: A Toffoli gate in Clifford+T basis

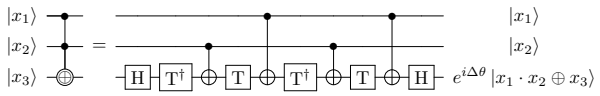


Figure 2: An relative phase Toffoli (RTOF) gate in Clifford+T basis

1 Introduction and Preliminary Knowledge

Quantum Boolean circuits [6] implement Boolean operations as quantum circuits and are common components of many quantum algorithms. To realize such quantum Boolean circuits, a Toffoli gate, which implements the Boolean AND, is an essential logic primitive in a universal gate set. These Toffoli gates have to be, in turn, composed of physically realizable gates, such as NOT, CNOT, and T gates (e.g., the Clifford + T [2] basis gate set). However, in the fault-tolerant paradigm, T-gates incur much higher cost than the NOT and CNOT gates. It is therefore useful to consider ways to reduce this *T-count*, which is the number of both the T-gates and their inverse the $T^\dagger$ in the circuit.

One of the methods that has been proposed to reduce the T-count is to implement Boolean functions only up to a *relative phase* [2], which is an input dependent phase on the output. We display a Relative Phase Toffoli gate (RTOF) in Fig. 2, which has a T-count of 4, compared to a T-count of 7 with the normal Toffoli gate. However, because quantum Boolean circuits are often used as subroutines inside larger quantum algorithms, the introduced relative phase is, in general, problematic. It can only be used inside applications where the relative phase on the output is erased before the output is used elsewhere.

A Boolean function is implemented with several smaller quantum Boolean circuits, there is often a need to make these smaller quantum Boolean circuits act on ancilla qubits. However, when a circuit acts on (*compute*) an ancilla qubit, there is a need to reverse its effects on the ancilla. This means there is a need to apply the same quantum Boolean circuit twice to the same qubit to reverse the effects. When we reverse these states we say we *uncompute* them. One of the results from [4] is that these pairs of compute/uncompute logic can be implemented only up to a relative phase in order to save on T-count, without changing the overall function. This is because when we generate the compute logic only up to a relative phase, we can also generate the uncompute logic to implement the same Boolean function, but with the opposite relative phase.

Recent attempts to synthesize quantum circuits using LUT (Lookup Table) based methods [5] generalize the decomposition of larger quantum Boolean circuits. Just like before, there is a need to use ancilla in the decomposition. This creates structures with compute/uncompute logic, just like in [4]. This means that we can see further reduction in T-count if the compute and uncompute halves were created with relative phases that cancel each other out. However, because LUT-based methods have arbitrary Boolean functions for the compute logic, there is a need to generate arbitrary Boolean functions up to a relative phase. Knowing this, we now detail the proposed contributions of our work:

Our Contribution. We propose a method that reduces the number of T-gates in a LUT-based synthesized quantum Boolean circuit by generating relative phase quantum circuits. Among our contributions:

- A method to generate arbitrary Boolean functions up to a relative phase using Shannon's Decomposition and Davio Expansions, as well as balanced and unbalanced constructions of relative phase gates
- A method to generate a quantum Boolean circuit from a Boolean logic network representation leveraging the above method to reduce T-count

*dizzy@ngc.is.ritsumei.ac.jp
†accel@ngc.is.ritsumei.ac.jp
‡matsuoa@jp.ibm.com
§ger@cs.ritsumei.ac.jp

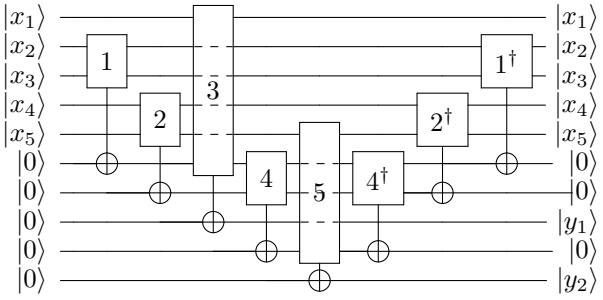


Figure 3: A quantum circuit implementing a Boolean logic network using LHRS

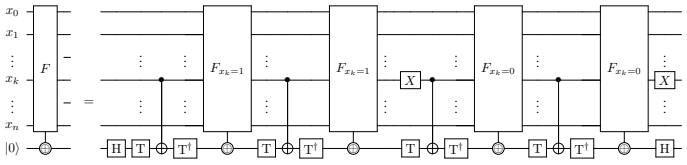


Figure 4: Balanced Shannon's Decomposition

2 LUT-based Quantum Circuit Synthesis

Previous research [5] has detailed a method to use Boolean Logic Networks to generate quantum circuits in a manner similar to classical LUT-based logic synthesis. In this paradigm, each of the nodes is interpreted as a lookup table, where the inputs are interpreted as indices, and the outputs are entries, according to its truth table. As a quantum circuit, they are implemented as an F-controlled NOT (FCNOT) gate, which is a gate that inverts its target qubit if the Boolean function F it is supposed to implement is true.

The result of the method is shown in Fig. 3. To get from a Boolean logic network to Fig. 3, first, we take as input a Boolean logic network synthesized from a Boolean expression using existing Boolean logic network decomposition methods. Then this Boolean logic network is parsed by the algorithm to create a quantum circuit of FCNOT gates. Any intermediate node is decomposed as two FCNOTs: one to compute, and the other to uncompute, acting on the same dirty ancilla. Any node that acts only on output qubits (output node) is given only one FCNOT.

Because the FCNOT gates act on ancilla, there is a need to uncompute them, so the flow next produces uncompute logic. This produces the compute/uncompute pair that a relative-phase based construction of the function can take advantage of. If we have a function that implements, for example, gate 1 and $1^\dagger$ as relative phase functions with opposite phase, we can realize a T-count reduction. We detail how we can create such a method in the following section.

3 Realizing Arbitrary Boolean Functions Up To A Relative Phase

3.1 Relative Phase Shannon's Decomposition and Davio Expansions

Recall Shannon's decomposition $F(x_n, \cdots, x_k, \cdots, x_1) = x_k \cdot F(x_n, \cdots x_k = 1, \cdots, x_1) + \overline{x_k} \cdot F(x_n, \cdots x_k = 0, \cdots, x_1)$. We can implement it using Fig. 4, recursively using the same deconstruction to implement the FCNOT gates

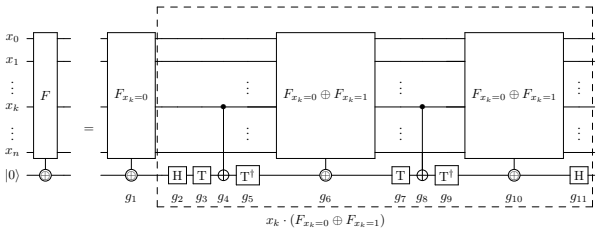


Figure 5: Balanced positive Davio Expansion

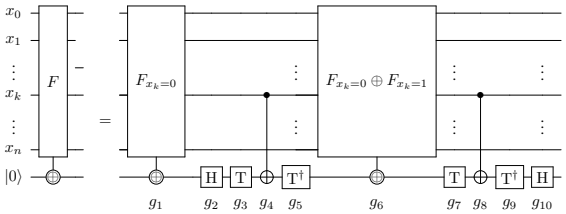


Figure 6: Unbalanced positive Davio Expansion

inside it.

However, observe from Fig. 4, that there is significant cost associated with doing the Boolean AND. Each multiplication costs at least 4 T-gates, along with the associated cost of the decomposed function. Therefore, it is useful to consider a method that takes advantage of *Exclusive Sum of Products* (ESOP) expressions to reduce the number of multiplications in the decomposition multiplication cost. Recall the positive Davio Expansion $F = F_0 \oplus x_k \cdot F_2$ and the corresponding negative Davio expansion $F = F_1 \oplus \overline{x_k} \cdot F_2$ where F is Boolean function of variables $\{x_n, \cdots, x_k, \cdots, x_0\}$, $F_0 = F(x_k = 0)$,$F_1 = F(x_k = 1)$, and $F_2 = F_0 \oplus F_1$. These expansions have the advantage that, at every level, only one multiplication takes place, which already reduces the maximum possible T-gate use at any node from 8 to 4. We demonstrate how a positive Davio Expansion can be implemented in Fig. 5.

3.2 Using Balanced and Unbalanced Relative Phase Functions

To realize a further savings in T-count, we again observe the the part of Fig. 5 that calculates $x_k \cdot (F_{x_k=0} \oplus F_{x_k=1})$, indicated by the dashed box. In this construction, note that the gates g_6 and g_{10} calculate identical Boolean functions. Gate g_{10} serves to uncompute the effects of g_6 on the state, leaving only the phase. We call this type of construction *balanced*. In a balanced construction, the cost of the decomposition doubles the cost of implementing the decompositions below it in the hierarchy. This means that even in the best case, T-count is proportional to $2^{(n-1)}$.

We can remove g_{10} and get the construction in Fig. 6. Here, we calculate the same Boolean function but without the cost of the decomposition in the recursive levels below x_k. We call this type of construction *unbalanced*. These types of constructions can only be used in a restricted manner when doing the Boolean AND however [1]. We summarize the limitations of the use of the unbalanced construction in our application with the following statement: unbalanced constructions can be used to implement FCNOTs used in the Boolean AND of two functions only when done in a balanced construction. Therefore we devise a method to use balanced and unbalanced constructions at alternating levels of the hierarchy. In doing so, we

Table 1: Experimental Results

Circuit	No Relative Phase				Shannon-Only				Proposed method			
	LUT6 (T-count)	LUT5	LUT4	LUT3	LUT6	LUT5	LUT4	LUT3	LUT6	LUT5	LUT4	LUT3
priority_size_2022	98664	0.56	0.32	0.26	0.27	0.51	0.19	0.16	0.14	0.08	0.06	**0.05**
int2float_size_2022	22592	1.14	0.49	0.38	0.94	0.94	0.4	0.35	0.27	0.17	0.1	**0.06**
i2c_size_2022	89288	0.69	0.4	0.27	0.94	0.68	0.31	0.23	0.61	0.27	0.18	**0.13**
dec_size_2018	57344	0.5	0.41	0.2	1	0.41	0.31	0.16	1	0.39	0.3	**0.15**
ctrl_size_2022	7560	1.17	0.84	0.68	0.99	1.12	0.51	0.41	0.99	0.88	0.35	**0.24**
cavlc_size_2022	116896	0.8	0.49	0.41	0.63	0.6	0.3	0.29	0.13	0.1	0.07	**0.06**
bar_size_2015	176400	0.94	0.03	**0.03**	7.15	1.4	0.21	0.21	0.15	0.21	0.07	0.07
arbiter_size_2022	175640	0.68	0.42	0.28	0.35	0.63	0.27	0.17	0.21	0.13	0.11	**0.05**
adder_size_2022	4992	9.75	6.38	1.94	1	7.16	4.06	2.54	1	1.91	1.95	1.66
Per LUT Average		1.80	1.08	0.49	0.5	0.46	0.35	0.27	1.47	1.49	0.73	0.50
Average		1.13			0.72				0.24			

can reduce the dependency from $2^{(n-1)}$ to $2^{\frac{n-1}{2}}$. While still exponential, this has quite a significant reduction in the regime we are working with.

Additionally, observe that in a Davio Expansion, one of the terms does not use the Boolean AND. We are therefore free to implement this term that does not use the AND using an unbalanced construction. This dispenses with the need to double the cost of the decomposition's recursion level below it, providing us with further reduction in T-count.

4 Proposed Method

We now integrate Sec 3.1 and Sec 3.2 into a synthesis algorithm to implement a Boolean function up to a relative phase. We use this relative phase algorithm as a subroutine in the following process.

We query a node traversal algorithm to get the next node. We then check if this node is an output node or an intermediate node. If it is an intermediate node, we generate the compute logic as an FCNOT with a relative phase, and then invert that circuit to generate the uncompute logic, which generates a relative phase FCNOT with the opposite relative phase. We set the two gates to act on ancilla. If the node is an output node, we generate the FCNOT without relative phase and add it to the circuit. We continue until there are no more nodes to process from the node traversal algorithm and terminate.

5 Experimental Results

We find that using our method, we generate quantum Boolean circuits with an average of 24% of the T-count of the case without relative phase. We also compare our proposed method to a simplified method using only Shannon's Decomposition and balanced compositions. We find that this simplified method (Shannon-Only) has corner cases which have higher T-count than the non-relative phase case. This is because Shannon's Decomposition and balanced constructions create FCNOT gates that have a large T-count. Introducing Davio Expansions and unbalanced constructions allows the proposed method to take care of these cases. In fact, the full proposed method has an absolute advantage over this simplified method.

6 Conclusion

This paper proposed the use of Shannon's Decomposition, Davio expansions and alternating balanced/unbalanced relative phase constructions to optimize relative phase constructions in their usage in LUT-based quantum circuit synthesis. The experimental results showed a clear advantage over the naive case, and Davio Expansions and balanced/unblanced constructions prove effective at dealing with corner cases that hinder the Shannon-Only case. There remains one interesting exception where the proposed method underperforms the naive method, however, and it relates to a special form of Boolean logic network which consists of independent output gates.

The results of this paper show a clear advantage to using our proposed method, as well as possible further avenues of inquiry for related research. As the experimental results show, there remain many variables to control to optimize in this method, and researching those further could prove fruitful.

References

[1] Matthew Amy and Neil J. Ross. Phase-state Duality in Reversible Circuit Design. *Phys. Rev. A*, 104:052602, Nov 2021.

[2] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary Gates for Quantum Computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.

[3] Brett Giles and Peter Selinger. Exact Synthesis of Multiqubit Clifford+t Circuits. *Phys. Rev. A*, 87:032332, Mar 2013.

[4] Dmitri Maslov. Advantages of Using Relative-phase Toffoli Gates with an Application to Multiple Control toffoli Optimization. *Physical Review A*, 93(2):022311, 2016.

[5] Mathias Soeken, Martin Roetteler, Nathan Wiebe, and Giovanni De Micheli. LUT-based Hierarchical Reversible Logic Synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 38(9):1675–1688, 2018.

[6] Shigeru Yamashita, Shinichi Minato, and D Michael Miller. DDMF: An Efficient Decision Diagram Structure for Design Verification of Quantum Circuits Under a Practical Restriction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 91(12):3793–3802, 2008.

Expressivity of deterministic quantum computation with one qubit

Yujin Kim[1] * Daniel K. Park[1 2] †

[1] *Department of Statistics and Data Science, Yonsei University, Seoul 03722, Republic of Korea*
[2] *Department of Applied Statistics, Yonsei University, Seoul 03722, Republic of Korea*

Abstract. A deterministic quantum computation with one qubit (DQC1) is a subuniversal model of quantum computation that operates with a single qubit initialized in non-zero polarization, along with uniformly random bits. This model is of both theoretical and practical interest because it can offer computational advantages for certain problems. We introduce parameterized DQC1 as a quantum machine learning model. We demonstrate that the gradient of model can be computed directly using DQC1 protocol. We then analyze the expressivity of model, and show that DQC1-based ML is as powerful as quantum neural networks based on universal computation.

Keywords: Quantum Machine Learning, DQC1, Expressivity, Fourier Analysis

1 Introduction

Quantum machine learning (QML) leverages the information processing capabilities of quantum systems to redefine the boundaries of machine learning (ML) and data analysis. As the development of universal and fault-tolerant quantum computers remains a long-term prospect, exploring the ML capabilities of less powerful but more realistic quantum devices is of significant importance.

Expressivity characterizes the complexity of the family of functions generated by the parametric function and is a crucial property of an ML model. In QML, the laws of physics dictate the breadth of function classes that can be represented by the quantum processor. Previous research has investigated the family of functions learnable under the circuit model of universal quantum computation [1, 2]. However, it remains unclear how this scenario changes when quantum computation is constrained to subuniversal models.

In this work, we analyze the expressivity of the deterministic quantum computation with one qubit (DQC1) model. DQC1 is a subuniversal model of quantum computation where only one quantum bit with non-zero purity can be prepared and measured, while the computation can utilize uniformly random bits. Nevertheless, it can outperform classical computers in solving certain computational problems. Therefore, understanding the ML capabilities of DQC1 in terms of expressivity is crucial for advancing both the theory and practicality of QML.

2 DQC1

DQC1 is a model of quantum computation equipped with a single signal qubit initialized with a non-zero polarization denoted by α, along with n uniformly random bits, the capability to apply arbitrary unitary transformations, and the ability to measure the expectation of the Pauli obervables on the signal qubit [3]. It is subuniversal in the sense that only one quantum bit, which is not necessarily pure, can be prepared and measured. The uniformly random bits are typically realized by a quantum system prepared in a maximally mixed state. Although less powerful compared to universal quantum computers, it is conjectured that DQC1 can solve certain computational problems exponentially faster than classical computers [3, 4, 5]. An outstanding example of this is the problem of estimating the normalized trace of an n-qubit unitary operator, U, for which the quantum advantage can be achieved if U can be implemented using $O(\mathrm{poly}(n))$ elementary quantum gates.

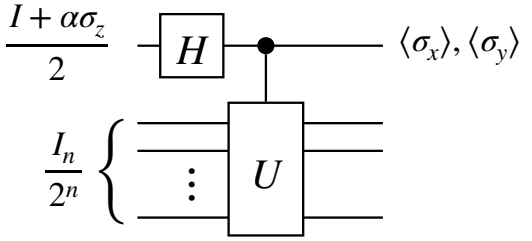


Figure 1: A quantum circuit representation of a DQC1 protocol for estimating the trace of n-qubit unitary operator U. The signal qubit (the first qubit from the top) is prepared with non-zero purity ($\alpha > 0$).

To estimate the trace using DQC1, the following protocol is employed. The process first applies a Hadamard gate to the signal qubit initialized in $(I + \alpha\sigma_z)/2$, where I denotes the 2×2 identity matrix and σ_i is the Pauli operator with $i \in \{x, y, z\}$. Then the controlled unitary gate $|0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes U$ is applied to the signal qubit and n uniformly random bits, where I_n denotes the $2^n \times 2^n$ identity matrix and the signal qubit acts as the control qubit. This operation prepares the following state: $\rho = \frac{1}{2^{n+1}} \left(I_{n+1} + \alpha \left(|0\rangle\langle 1| \otimes U^\dagger + |1\rangle\langle 0| \otimes U \right) \right)$.

The protocol concludes by measuring the expectation values of Pauli X and Y observables (σ_x and σ_y) on the signal qubit, resulting in

$$\langle\sigma_x\rangle = \frac{\alpha}{2^n} \mathrm{Re}\left(\mathrm{tr}\left(U\right)\right), \quad \langle\sigma_y\rangle = \frac{\alpha}{2^n} \mathrm{Im}\left(\mathrm{tr}\left(U\right)\right). \tag{1}$$

The quantum circuit of the DQC1 protocol is depicted in Fig. 1. Repeating the protocol $O(\log(1/\delta)/(\alpha\epsilon)^2)$ times

*k.yujin2228@yonsei.ac.kr
†dkd.park@yonsei.ac.kr

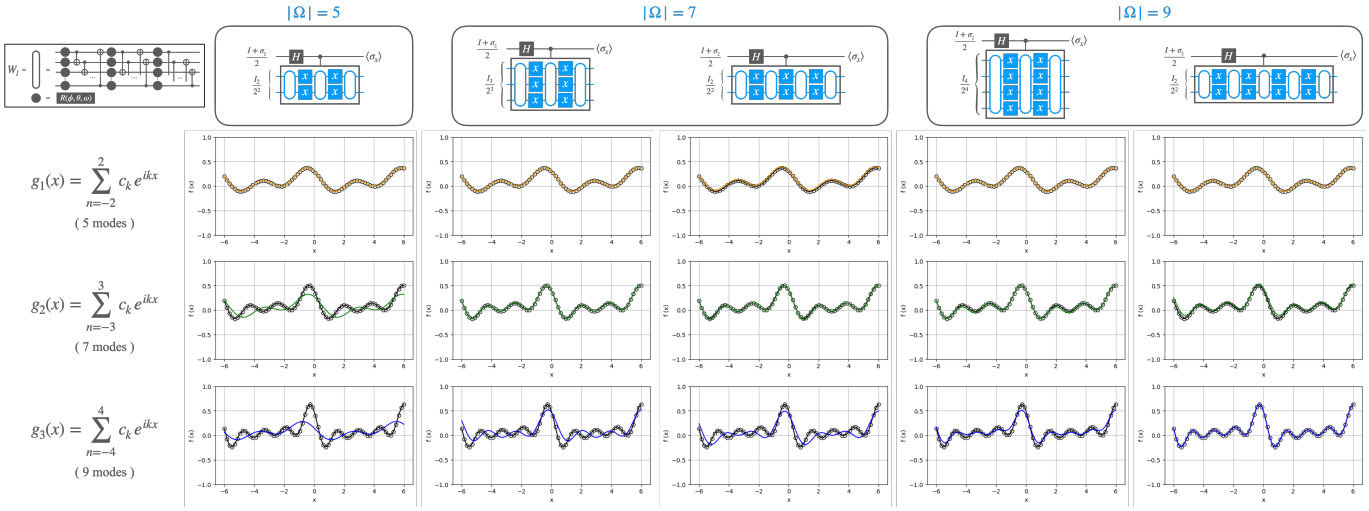


Figure 2: Training results of DQC1-based ML model $f(\boldsymbol{x}, \boldsymbol{\theta})$ (green and blue lines). Target functions are $g_1(x) = \sum_{-2}^{2} c_k\, e^{ikx}$, $g_2(x) = \sum_{-3}^{3} c_k\, e^{ikx}$ and $g_3(x) = \sum_{-4}^{4} c_k\, e^{ikx}$ (black line and open circles) with $c_0 = 0.1\,, c_k = 0.05 + 0.05\,i\,(k \neq 0)$, consisting of 5, 7 and 9 modes respectively. The training unitary $W_l(\boldsymbol{\theta})$ chosen in this example is depicted on the top-left. The open circles represent 70 data samples used for training, with a batch size of 25. All simulations are iterated 200 times with Adam optimizer at learning rate 0.15 using Pennylane.

facilitates the estimation of the expectation values within ϵ with a probability of error δ [6].

3 DQC1 for ML

Let us denote the set of functions that be expressed by a DQC1 protocol as $\mathcal{F}$ and an element of the set as $f(\boldsymbol{x}, \boldsymbol{\theta})$. In general, a DQC1-based ML model with n uniformly random bits can be defined as

$$f(\boldsymbol{x}, \boldsymbol{\theta}) \in \mathcal{F} = \left\{ \frac{1}{2^n} \mathrm{tr}\left(U(\boldsymbol{x}, \boldsymbol{\theta})\right) : U \in U(2^n), \boldsymbol{\theta} \in \boldsymbol{\Theta} \right\}, \tag{2}$$

where $U(N)$ is the unitary group of degree N and $\boldsymbol{\Theta} \subseteq \mathbb{R}^{4^n}$ denotes the parameter space. Specifically, we consider the unitary operator in the form of

$$U(\boldsymbol{x}, \boldsymbol{\theta}) = \prod_{l=1}^{L} W_l(\boldsymbol{\theta}_l) V_l(\boldsymbol{x}_l). \tag{3}$$

The trainable unitary $W_l(\boldsymbol{\theta}_l)$ can be written as

$$W_l(\boldsymbol{\theta}_l) = \prod_{k=1}^{k'} \exp(-i(\boldsymbol{\theta}_l)_k H_{lk}) T_{lk}, \tag{4}$$

where H_{lk} is an $2^n \times 2^n$ Hermitian operator that commutes with itself and T_{lk} is an unparametrized unitary. This form of $U(\boldsymbol{x}, \boldsymbol{\theta})$ is a reasonable choice since an n-qubit Pauli operator, $\sigma_k \in \mathcal{P}_n = \{I, \sigma_x, \sigma_y, \sigma_z\}^{\otimes n}$, commutes with itself and $\{\exp(-i(\boldsymbol{\theta}_l)_k \sigma_k) : \sigma_k \in \mathcal{P}_n\}$ forms a universal gate set.

Using the fact that H_{lk} commutes with itself, the partial derivative of the model function with respect to a parameter can be computed as

$$\begin{aligned} \frac{\partial f(\boldsymbol{x}, \boldsymbol{\theta})}{\partial (\boldsymbol{\theta}_l)_k} = \frac{-i}{2^n} \mathrm{tr} \Bigg(H_{lk} \left(\prod_{j=k}^{k'} e^{-i(\boldsymbol{\theta}_l)_j H_{lj}} T_{lj} \right) V_l(\boldsymbol{x}_l) \\ \times \left(\prod_{j=l+1}^{L} W_j(\boldsymbol{\theta}_j) V_j(\boldsymbol{x}_j) \right) \left(\prod_{j=1}^{l-1} W_j(\boldsymbol{\theta}_j) V_j(\boldsymbol{x}_j) \right) \\ \times \prod_{j=1}^{k-1} e^{-i(\boldsymbol{\theta}_l)_j H_{lj}} T_{lj} \Bigg). \end{aligned} \tag{5}$$

Therefore, if H_{lk} is a unitary (e.g. $H_{lk} \in \mathcal{P}_n$), the gradient of $f(\boldsymbol{x}, \boldsymbol{\theta})$ with respect to $\boldsymbol{\theta}$ can be obtained via DQC1, and the gradient-based optimization techniques can be employed for training the model.

4 Expressivity of DQC1

The trace of an n-qubit unitary operator $\mathrm{tr}(U(\boldsymbol{x}, \boldsymbol{\theta}))$ can be expressed as Fourier-type sums

$$\sum_{\omega \in \Omega} c_\omega(\boldsymbol{\theta})\, e^{i\,\omega(\boldsymbol{x})} \quad (\omega = \omega(\boldsymbol{x}))\,, \tag{6}$$

where $\omega(\boldsymbol{x})$ is an element of the frequency spectrum Ω determined by the data-encoding part of $U(\boldsymbol{x}, \boldsymbol{\theta})$, and $c_\omega(\boldsymbol{\theta})$ is the corresponding coefficient controlled by the trainable unitary part.

Given $U(\boldsymbol{x}, \boldsymbol{\theta})$ in form of Eq. (3), the data encoding unitary $V_l(\boldsymbol{x}_l)$ can be constructed by single-qubit rotation gates $V_l(\boldsymbol{x}_l) = \prod_{q=1}^{n} \exp(-i(\boldsymbol{x}_l)_q \sigma_k^{(q)}/2)$, where $\sigma_k^{(q)}$ is a Pauli operator acting on the qth qubit. This form is appropriate since all fixed gates involved in data-encoding can be absorbed to W terms before and after V_l. The data-encoding circuit can be further simplified to

$V_l(\boldsymbol{x}_l) = \prod_{q=1}^{n} \exp(-i(\boldsymbol{x}_l)_q \sigma_z^{(q)}/2)$ by absorbing the gates for diagonalizing the Pauli operator to the W terms.

Then, we can rewrite Eq. (6) as

$$\mathrm{tr}(U(\boldsymbol{x},\boldsymbol{\theta})) = \mathrm{tr}\left(\prod_{l=1}^{L} W_l(\boldsymbol{\theta}_l) V_l(\boldsymbol{x}_l)\right), \tag{7}$$

with the index $k_i \in [2^n] = \{1, 2, 3, \cdots, 2^n\} (i = 1, 2, \cdots, L)$ for

$$e^{i\,\omega(\boldsymbol{x})} = e^{i\left((\Sigma_1)_{k_1 k_1} + (\Sigma_2)_{k_2 k_2} + \cdots + (\Sigma_L)_{k_L k_L}\right)}, \tag{8}$$

$$c_\omega(\boldsymbol{\theta}) = (W_1(\boldsymbol{\theta}_1))_{k_L k_1} (W_2(\boldsymbol{\theta}_2))_{k_1 k_2} \cdots (W_L(\boldsymbol{\theta}_L))_{k_{L-1} k_L}. \tag{9}$$

The diagonalized matrix Σ_i is defined as $\Sigma_i \equiv -\sum_{q=1}^{n} (\boldsymbol{x}_i)_q \, \sigma_z^{(q)}/2$ which contains up to 2^n unique eigenvalues of each Σ_i.

Therefore, the cardinality of frequency spectrum Ω is

$$|\Omega| \leq 2^{nL}. \tag{10}$$

This is the number of orthogonal basis functions of a Fourier series, indicating the degrees of complexity of the quantum model. Equation (10) implies that scaling up the number of qubits (parallel) yields the same level of complexity as increasing the circuit depth (serial).

In comparison, the quantum neural network [7] based on universal computation with n qubits yields the following set of functions:

$$f_{\mathrm{u}}(\boldsymbol{x},\boldsymbol{\theta}) \in \left\{\langle \mathbf{0}_n | U^\dagger(\boldsymbol{x},\boldsymbol{\theta}) M U(\boldsymbol{x},\boldsymbol{\theta}) | \mathbf{0}_n \rangle : M^\dagger = M\right\},$$

where $|\mathbf{0}_n\rangle = |0\rangle^{\otimes n}$ and $U(\boldsymbol{x},\boldsymbol{\theta})$ takes the same form as in Eq. 3. The cardinality of the frequency spectrum produced by this model is $|\Omega| \leq 2^{2nL}$ [1]. This shows that DQC1 can generate as many orthogonal Fourier basis functions as the universal model simply by increasing the number of qubits or the circuit depth by a factor of two.

5 Machine Learning Examples

Figure 2 demonstrates that DQC1-based ML model $f(\boldsymbol{x},\boldsymbol{\theta})$ defined in Eq. (2) can express a target function $g(x)$ by optimizing variables $\boldsymbol{\theta}$ with a classical optimizer.

For simplicity, we assumed a univariate x for $U(\boldsymbol{x},\boldsymbol{\theta})$ in Eq. (3) and encoded x using only single-qubit σ_x rotation gates for $V_l(x)$, with $V_{L+1} = I_{2^n}$. Consequently, the diagonal matrix $\Sigma_i \, (i = 1, \cdots, L)$ has $(n+1)$ unique eigenvalues corresponding to $-\frac{n}{2}, -\frac{n-2}{2}, \cdots, \frac{n}{2}$. Subsequently, an L-layer circuit makes $(nL+1)$ unique frequencies, $-\frac{nL}{2}, -\frac{nL-2}{2}, \cdots, \frac{nL}{2}$, satisfying

$$|\Omega| = nL + 1. \tag{11}$$

The simulation results confirm that DQC1-based ML models achieve sufficient expressive power to learn the target function, provided the circuit employs the number of qubits and data-encoding layers specified by Eq. (10).

6 Conclusions

In this work, we introduced the DQC1-based ML model and analyzed its expressive power. Our theoretical analysis and numerical simulations demonstrate that this subuniversal model of quantum computation is equally capable as the universal model in generating the Fourier basis. Since the DQC1 protocol is well-suited for ensemble quantum information processors such as those with spin ensembles and magnetic resonance, our findings broadens the range of feasible quantum computing hardware platforms for QML.

References

[1] 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.

[2] Ben Jaderberg, Antonio A. Gentile, Youssef Achari Berrada, Elvira Shishenina, and Vincent E. Elfving. Let quantum neural networks choose their own frequencies. *Phys. Rev. A*, 109:042421, Apr 2024.

[3] E. Knill and R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81:5672–5675, Dec 1998.

[4] Animesh Datta, Steven T. Flammia, and Carlton M. Caves. Entanglement and the power of one qubit. *Phys. Rev. A*, 72:042316, Oct 2005.

[5] Peter W. Shor and Stephen P. Jordan. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Info. Comput.*, 8(8):681–714, September 2008.

[6] P. J. Huber. *Robust Statistics*. Wiley, New York, 1981.

[7] Jarrod R. McClean, Sergio Boixo, Vadim N. Smelyanskiy, Ryan Babbush, and Hartmut Neven. Barren plateaus in quantum neural network training landscapes. *Nature Communications*, 9(1):4812, 2018.

Quantum frequency conversion experiment with a PPLN waveguide resonator

Shoichi Murakami[1 2 *] Toshiki Kobayashi[1 2] Shigehito Miki[3] Hirotaka Terai[3]
Tsuyoshi Kodama[3 4] Tsuneaki Sawaya[4] Akihiko Ohtomo[4] Hideki Shimoi[4]
Takashi Yamamoto[1 2] Rikizo Ikuta[1 2]

[1] *Graduate School of Engineering Science, Osaka Univ., Osaka 560-8531, Japan*
[2] *Center for Quantum Information and Quantum Biology, Osaka Univ., Osaka 560-0043, Japan*
[3] *Advanced ICT Research Institute, NICT, Hyogo 651-2492, Japan*
[4] *Hamamatsu Photonics K.K., Shizuoka , Japan*

Abstract. We present the QFC experiment of a heralded single photon at 780 nm generated via a spontaneous parametric down-conversion (SPDC) process to a 1540 nm photon with PPLN waveguide resonator. In addition to the experimental result of QFC, we show the details of the noise characteristics and the effect of the cavity enhancement of the QFC.

Keywords: quantum frequency conversion, quantum communication, quantum internet

1 Introduction

In recent years, there has been remarkable progress in the development of quantum computers [1]. In connection with this background, research on quantum internet and quantum interconnects [2, 3], which connect quantum computers, are actively explored. The wavelengths of photons interacting with these quantum computers and other quantum systems depend on physical systems such as atoms, ions, semiconductors, and so on. Therefore, for quantum internet/interconnect based on optical fiber communication, it is crucial to develop the technologies of quantum frequency conversion (QFC) [4] that converts the wavelengths of emitted photons from the various quantum systems to the telecommunication band without disturbing quantum information. One of the challenges of QFC is to reduce background noises due to the Raman scattering originating from the high-power pump light required for QFC [5]. In previous QFC experiments, a narrowband frequency filter system was conducted by combining etalons and bandpass filters to achieve a high signal-to-noise ratio (SNR) after QFC [6, 7]. In this study, we conducted QFC experiments based on a periodically poled lithium niobate waveguide resonator (PPLN-WR), which confines only the converted light but does not confine the signal and pump light[8]. In this experiment, the wavelength of a heralded single photon generated via a spontaneous parametric down-conversion (SPDC) process converted from 780 nm to 1540 nm. We investigated the frequency and pump light power dependence of the Raman noise in this process.

2 Theory

We describe the theory of QFC with a cavity for the converted mode, according to Ref. [8]. In this model, the frequency-converted mode inside the cavity is coupled to two external modes like the two-sided cavity. One of the external modes is the signal mode of QFC, and the other is the converted mode outside the cavity. They are coupled to the cavity mode with coupling constants $|\xi|$ proportional to the pump power $\sqrt{P}$ and $\sqrt{\gamma_{\rm r}}$ related to the reflectance of the end mirror of the cavity. The complex amplitudes of unconverted and conversion efficiencies are written as:

$$t_{\rm ss} = \frac{\frac{1}{2}(1-\tilde{C}) - i\tilde{\Delta}_{\rm c}}{\frac{1}{2}(1+\tilde{C}) - i\tilde{\Delta}_{\rm c}}, \tag{1}$$

$$r_{\rm rs} = \sqrt{\tilde{\gamma}_{\rm r}}\frac{e^{-i\phi}\sqrt{\tilde{C}}}{\frac{1}{2}(1+\tilde{C}) - i\tilde{\Delta}_{\rm c}}, \tag{2}$$

where ϕ is the phase of pump light, $\tilde{\gamma}_{\rm r} = \gamma_{\rm r}/\gamma_{\rm all}$, and $\tilde{C} = |\xi|^2/\gamma_{\rm all}$. Here, $\gamma_{\rm all} = \gamma_{\rm r} + \gamma_{\rm int}$ is the total loss determined by $\gamma_{\rm r}$ and internal loss of the cavity $\gamma_{\rm int}$.

In QFC experiments, the strong pump light is used for not only QFC but also other unwanted nonlinear optical processes. For the wavelength configuration of our QFC experiments, it is widely known that the pump light generates anti-Stokes (AS) photons as noise photons contaminating the converted mode. We treat the generation process of the AS photons as the singly-resonant SPDC process [9] with a pair of AS photons inside a cavity and non-resonant phonons. Based on the treatment, we discuss the SNR of the cavity-enhanced QFC. The amount of photons generated by singly resonant SPDC is the same as that without a cavity for the detection bandwidth comparable to the FSR of the cavity [9]. On the other hand, the conversion efficiency of QFC is enhanced by a factor of $F_{\rm cold}/\pi$ [10], where $F_{\rm cold}$ is the finesse of the cavity without QFC. As a result, if a BPF with a bandwidth comparable to FSR is used for QFC, the SNR will be improved by a factor of $F_{\rm cold}/\pi$ compared with the QFC without a cavity.

When frequency up-conversion process of the generated AS photons is induced by the pump light used for QFC, the up-conversion efficiency is the same as the efficiency of QFC. From the fact and Eq. (2), the amount

*smurakami@qi.mp.es.osaka-u.ac.jp

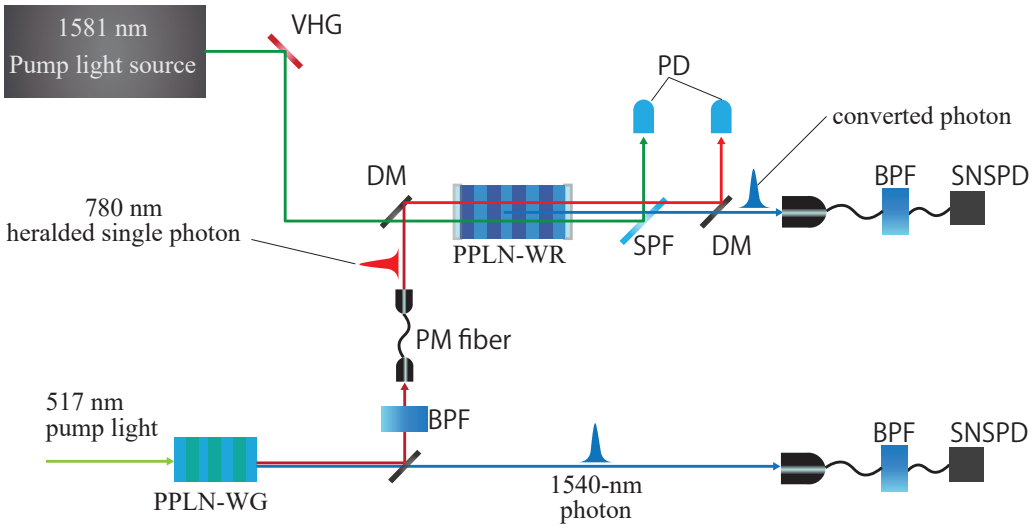


Figure 1: The experimental setup. VHG: volume holographic gratings, BPF: bandpass filter, PM fiber: polarization maintaining fiber, PD: photodetector, SPF: short pass filter, DM: dichroic mirror, SNSPD: superconducting nanostrip single photon detector

of the AS photons is described as,

$$N_{\mathrm{noise}} = \alpha_{\mathrm{noise}} P \left(1 - \frac{\tilde{\gamma}_{\mathrm{r}} \tilde{C}}{1+\tilde{C}}\right), \tag{3}$$

where α_{noise} is the constant of proportionality of the number of anti-Stokes photons to the pump power P.

3 Experiments

3.1 Experimental setups

Fig. 1 shows our experimental setup. We first characterized the performance of the cavity-enhanced frequency conversion process using laser light. For this, we used a tunable laser for the pump light at the center wavelength of 1600 nm. The pump light and 780 nm laser light were coupled to the PPLN-WR. The PPLN-WR satisfies the type-0 quasiphase-mathing condition and the length was 14 mm which corresponds to the FSR of 5 GHz. After the frequency conversion process, the pump light and unconverted signal light were separated from converted light at 1522 nm by a short pass filter (SPF) and the dichroic mirror (DM) respectively. The pump, the signal, and the converted light were measured by photodetectors (PDs).

For the QFC of a single photon at 780 nm, we used 1579 nm laser light as pump light. The spectrum of the pump light was cleaned up by the volume holographic grating (VHG). We prepared a 780-nm single photon using a non-degenerate SPDC process which generates a 780-nm signal photon and a 1542-nm idler photon. This idler photon passed through a bandpass filter with the bandwidth of 0.03 nm and then was detected by a superconducting nanostrip single photon detector (SNSPD) [11] developed by NICT and Hamamatsu Photonics. This detection was used for heralding a 780-nm single photon. The heralded photon entered the PPLN-WR after passing through the bandpass filter with the bandwidth of 0.4 nm and was converted to a 1540 nm photon. After coupling to a single-mode fiber, the converted photon passed through the bandpass filter with the bandwidth of 0.03 nm and was detected by another SNSPD. Using the coincidence events, we observed cross-correlation function $g^{(2)}_{\mathrm{c,i}}$ between the converted mode and idler mode.

3.2 Experimental result

Fig. 2 (a) shows the relationship between the internal conversion efficiency in the PPLN-WR and the pump power P. From this data, it was estimated that the maximum conversion efficiency was achieved at $P = 137$ mW. In the previous QFC experiment [12] using a 20-mm PPLN waveguide without cavity structure, 700-mW pump power was required for the maximum conversion efficiency. We thus confirmed the cavity enhancement of the conversion process. Fig. 2 (b) shows the relationship between the bandwidth of QFC and P. As predicted by Eqs (1) and (2), the bandwidth of the QFC increases in proportion to P.

Fig. 3 (a) and (b) show the observed coincidence between the idler mode and the signal mode. From this measurement, the cross-correlation function $g^{(2)}_{\mathrm{c,i}}$ between the converted mode and the idler mode was 2.25, surpassing the classical limit 2, while the cross-correlation function $g^{(2)}_{\mathrm{s,i}}$ between the signal mode and the idler mode was 7.15. In this experiment, we used the heralded photons with the bandwidth of 0.03 nm corresponding to $\sim$ 76 % of the FSR. This gives a good agreement with the estimation that the 10 % input signal photons were converted. Nonetheless, we achieved the successful QFC due to the SNR improvement by the cavity effect. If we could prepare a sufficiently narrow photon, such as from neutral atoms, $g^{(2)}_{\mathrm{c,i}}$ would be improved to ~ 5.4 [13].

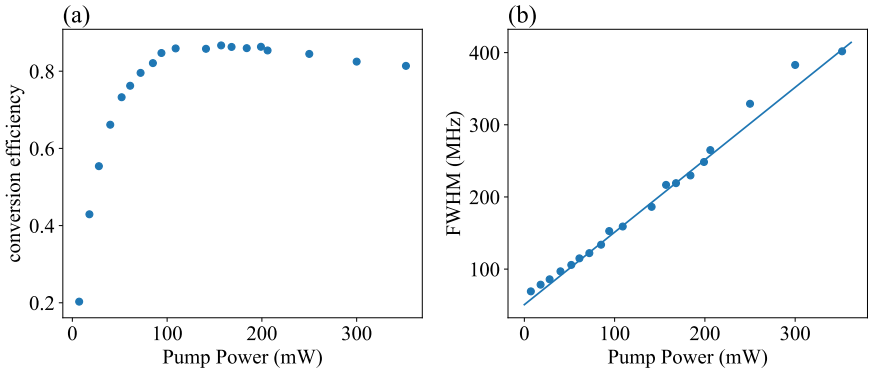


Figure 2: The pump power dependency of (a) the internal conversion efficiency in the PPLN-WR and (b) the bandwidth of QFC.

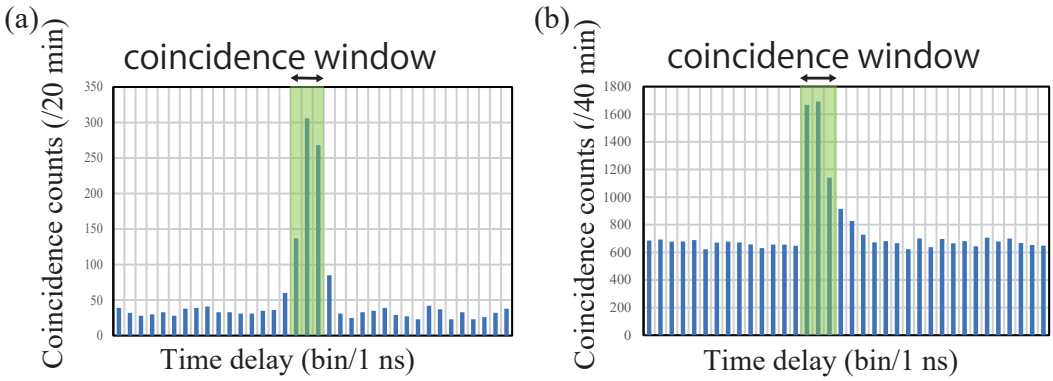


Figure 3: (a) The observed coincidence counts in 20 min between the signal mode and the idler mode. (b) The observed coincidence counts in 40 min between the converted mode and the idler mode with $P \sim 106$ mW.

4 Conclusion

We conducted the QFC of a 780-nm heralded photon using the PPLN waveguide resonator. The observed cross-correlation function between the converted mode and the idler mode was 2.25 which surpasses the classical limit 2, even though we used heralded photons whose bandwidth was much wider than that of the cavity. If we used a sufficiently narrow photon, $g^{(2)}_{\mathrm{s,i}}$ would be improved up to ~ 5.4.

Our result suggests the potential for frequency conversion while maintaining the quantum statistics of a signal photon even without narrowband filters. This will help the realization of the photonic quantum network.

4.1 Acknowledgments

This work was supported by Moonshot R & D, JST JPMJMS2066, JST JPMJMS226C; FOREST Program, JST JPMJFR222V; R & D of ICT Priority Technology Project JPMI00316, Asahi Glass Foundation, JSPS JP22J20801, and Program for Leading Graduate Schools: Interactive Materials Science Cadet Program.

References

[1] Nathalie P. de Leon and *et. al.,* Materials challenges and opportunities for quantum computing hardware. Science **372**(6539) (2021).

[2] S. Wehner and *et. al.,* Quantum internet: A vision for the road ahead. Science **362**(6412) (2018).

[3] H. J. Kimble The quantum internet. Nature, **453**(7198), 1023–1030 (2008).

[4] P. Kumar Quantum frequency conversion Opt. Letters, **15**(24), 1476–1478 (1990).

[5] J. S. Pelc, *et. al.,* Long-wavelength-pumped upconversion single-photon detector at 1550 nm: performance and noise analysis Opt. express **19**(22), 21445–21456 (2011).

[6] R. Ikuta, *et. al.,* Polarization insensitive frequency conversion for an atom-photon entanglement distribution via a telecom network Nat. Commun. **9**(1), 1997 (2018).

[7] T. v. Leent, *et. al.,* Long-Distance Distribution of Atom-Photon Entanglement at Telecom Wavelength Phys. Rev. Lett., **124**(1), 010510 (2020)

[8] R. Ikuta, *et. al.,* Optical Frequency Tweezers Phys. Rev. Applied **17** 034012 (2022)

[9] Y. Jeronimo-Moreno, *et. al.,* Theory of cavity-enhanced spontaneous parametric downconversion Laser physics **20**, 1221-1233. (2010)

[10] R. Ikuta, *et. al.,* Cavity-enhanced broadband photonic Rabi oscillation Phys. Rev. A **103**(3), 033709 (2018).

[11] S. Miki, *et. al.,* Stable, high-performance operation of a fiber-coupled superconducting nanowire avalanche photon detector. Opt. Lett. **25**(6), 6796-6804 (2017).

[12] R. Ikuta, *et. al.,* Wide-band quantum interface for visible-to-telecommunication wavelength conversion Nat. Commun. **2**, 537 (2011).

[13] B. Albrecht, *et. al.,* A waveguide frequency converter connecting rubidium-based quantum memories to the telecom C-band Nat. Commun. **5**, 3376 (2014).

Zero-Noise Extrapolation with Indirect-Control System

Arijit Das[1] * Masaki Owari[1] †

[1] *Department of Information Science and Technology, Graduate School of Science and Technology, Shizuoka University, Japan*

Abstract. In the indirect-control method, the whole quantum system is completely controlled by a combination of free time-evolution of the many-body Hamiltonian and quantum operations on a small control unit. Employing this method reduces the number of externally accessed qubits and minimizes the noise entering the quantum device. Recently, Anan *et al.* proposed a way to implement the variational quantum eigensolver by indirect-control. Based on this research, in this paper, we explore error mitigation by zero-noise extrapolation (ZNE) using indirect-control.

Keywords: Quantum error mitigation, quantum control, zero-noise extrapolation (ZNE)

1 Introduction

Recently, significant advancements in noisy intermediate-scale quantum (NISQ) devices have been witnessed [1]. The current state of the art quantum device has enabled us to achieve *quantum supremacy* by outperforming classical supercomputer [2]. However the NISQ devices are susceptible to noise, which reduces their reliability. It is impossible to entirely eliminate noise from a quantum system. As the size of the system grows, the noise also increases. Quantum error correction code (QEC) is a solution to any error arises due to the noise [3], which can lead to fault-tolerant quantum computers. However, error correction demands a significantly higher number of physical qubits, which is not feasible in the NISQ era. Quantum error mitigation (QEM) serves as an immediate improvement to quantum information processing with existing hardware limit. Instead of correcting the error, QEM aims to minimize the noise induced bias in the expectation value of an observable by post-processing the data directly derived from noisy hardware [4]. There are different strategies of error mitigation such as zero-noise extrapolation (ZNE), probabilistic error cancellation, and Clifford regression to name a few.

Another way to deal with noise is to reduce the number of pathways through which noise can enter the quantum device from the outside. In current NISQ devices, the entire quantum system is controlled by direct access to individual qubits. On the other hand, this external access also causes an additional noise in the NISQ device. Therefore, if the number of externally accessed qubits can be reduced, the noise could be reduced as well. It is known that in a typical quantum many-body system such as the XY-model, universal quantum computation on the whole system is possible by accessing only a few qubits (control unit). This method of controlling the whole quantum system by a combination of free time-evolution of the many-body Hamiltonian and quantum operations on a small control unit is called indirect-control [5].

When indirect-control is used, we need to repeatedly apply various quantum operations on the control unit at specific timings to compute the desired unitary to the whole system. However, it is difficult to find these operations and timings which are necessary to implement a desired unitary operation. Recently, however, Anan *et al.* showed that this difficulty does not arise in implementing a variational quantum eigensolver (VQE), where the circuit is optimised using a classical computer. VQE can be implemented on spin chains such as the XY-model using indirect-control [6]. If this indirect-control VQE and error mitigation are used simultaneously, achieving even less noisy calculations may be possible. However, no known method of performing error mitigation using indirect-control has existed. In this paper, we show that in the case of VQE using indirect-control on a one-dimensional XY-spin chain, error mitigation can be implemented by the ZNE method if, in addition to unitary operations on the control unit, Y-gate operations are allowed on the odd-numbered qubits including the inaccessible part.

2 Preliminaries

In this section, we briefly review the two key concepts of our paper: VQE in an indirect-control and error mitigation by ZNE.

2.1 Indirect-control VQE

A variational quantum eigensolver (VQE) is a classical-quantum optimization algorithm tailored for NISQ devices that estimates the ground state energy, or minimum eigenvalue, of a target Hamiltonian [7]. For a given target Hamiltonian H_T, the minimum eigenvalue E_0 can be derived as a solution of the following variational problem $E_0 = \min_{|\Psi\rangle} \langle\Psi| H_T |\Psi\rangle$. VQE approximates E_{VQE} to E_0 which is described by the following optimization problem:

$$E_{VQE} = \min_{\boldsymbol{\xi}} E(\boldsymbol{\xi}), \tag{1}$$

$$E(\boldsymbol{\xi}) = \langle \mathbf{0}| \mathbf{U}^\dagger(\boldsymbol{\xi}) H_T \mathbf{U}(\boldsymbol{\xi}) |\mathbf{0}\rangle , \tag{2}$$

where, $|\mathbf{0}\rangle$ is a typical initial state, $\mathbf{U}(\boldsymbol{\xi})$ is a generic parameterized unitary, and $\boldsymbol{\xi}$ is a vector-parameter. Using

*a.das.23@shizuoka.ac.jp
†masakiowari@inf.shizuoka.ac.jp

a series of qubit gates one defines a parametric ansatz circuit that prepares $\mathbf{U}(\boldsymbol{\xi})$. H_T can be written in a weighted sum of Pauli operations, which can be directly measured on a quantum computer. Thus, $E(\boldsymbol{\xi})$ can be calculated by the ansatz circuit with parameter $\boldsymbol{\xi}$ on a quantum computer, and E_{VQE} can be derived by minimizing $E(\boldsymbol{\xi})$ with respect to $\boldsymbol{\xi}$ via classical post-processing.

In an indirect-control system, the whole system consists of two subsystems: a control unit where we perform unitary operators and an inaccessible part where we cannot perform any active operations. The whole system undergoes free time-evolution with the system Hamiltonian H_S. To implement an ansatz circuit in such system, we instantaneously operate a parameterized unitary operator $V_n(\vec{\theta}_n)$ on the control unit at time t_n for $n = 1, 2, 3, \cdots, L$ with $t_n < t_{n+1}$. Then, an ansatz circuit which is given by the time evolution of the whole system can be described as

$$\mathbf{U}(\boldsymbol{\xi}) := \Pi_{n=1}^{L} U(t_n, t_{n+1}) V_n(\vec{\theta}_n) \tag{3}$$

Here, the parameter of the circuit $\boldsymbol{\xi}$ consists of the time parameters $\{t_n\}_{n=1}^{L}$ and the angular parameters $\{\vec{\theta}_n\}_{n=1}^{L}$. In Eq.(3), $U(t_n, t_{n+1}) := \exp(-iH_S(t_{n+1} - t_n))$ is a time-evolution operator acting on the whole system from time t_n to time t_{n+1}.

In [6], the first two qubits of 1-D XY-spin chain are chosen as a control unit, and two-qubits unitary V_n consist of X and Y rotation gates R_X, R_Y and control-Z gates CZ as

$$\begin{aligned} &V_n(\vec{\theta}_n) \\ =&R_Y(\theta_{4n-2})R_X(\theta_{4n-3}) \otimes R_Y(\theta_{4n})R_X(\theta_{4n-1}) \cdot CZ \end{aligned} \tag{4}$$

Further, the system Hamiltonian H_S is chosen as the 1-D XY-model Hamiltonian H_{XY}:

$$\begin{aligned} &H_{XY} \\ =&\sum_{k=1}^{N-1} c_k[(1+\gamma)X_kX_{k+1} + (1-\gamma)Z_kZ_{k+1}] + \sum_{k=1}^{N} b_kZ_k, \end{aligned} \tag{5}$$

where N is the number of qubits, c_k are the coupling constants, b_k are the strength of the local magnetic fields, and γ is an anisotropy parameter. Figure 1 depicts the n-th layer of the indirect-control VQE ansatz. In [6], Anan *et al.* showed that the performance of VQE using the above indirect-control parametric circuit is not so different from that of using standard parametric circuits.

2.2 Zero-noise extrapolation with a vector noise scaling factor

Zero-noise extrapolation (ZNE) mitigates errors by extrapolating data to the zero-noise limit via classical post-processing [8]. Let us consider a realistic situation where our system has noise while implementing an ansatz circuit. In this case, the output of VQE, which will be written as $E'_{VQE}(\lambda)$, depends on the noise level λ of the ansatz circuit, and in general, is not equal to E_{VQE} defined by Eq.(1). By definition, E_{VQE} is equal to

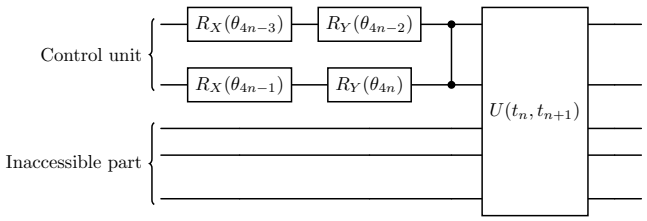


Figure 1: An n-th layer of an ansatz circuit for VQE on a 5-qubit indirect-control XY-model given by Eqs.(3) and (4).

$E'_{VQE}(\lambda)$ with $\lambda = 0$. Although it is difficult to decrease the noise level λ to 0 in a real quantum device, we can increase the noise level of the ansatz circuits λ by various methods. Thus, by calculating $E'_{VQE}(\lambda)$ for various different λ and extrapolating the function $E'_{VQE}(\lambda)$ to $\lambda = 0$, we can achieve a good estimated value of E_{VQE}.

The paper [9] treated the parameterized circuits with a vector noise scaling factor $\vec{\lambda}$, where an estimate of E_{VQE} can be derived by extrapolating the expectation value of the target Hamiltonian $E'_{VQE}(\vec{\lambda})$ to $\vec{\lambda} = \vec{0}$. This extrapolation can be applied by adopting the multivariate framework of Richardson extrapolation.

3 ZNE in indirect-Control Systems

The purpose of our paper is to apply ZNE to the indirect-control VQE. For this purpose, we need to increase the noise level of the indirect-control ansatz like the one given in Figure 1. Here, we cannot implement any active operation on the accessible part, and the known methods to increase the noise level, like identity insertion and pulse stretching [8], may never work in this situation. Hence, in this paper, we slightly relax the constraint of indirect-control and try to find a minimum requirement to implement a ZNE on the indirect-control ansatz on a 1-D XY-model given by Figure 1.

To boost the noise in the ansatz circuit, we used the identity scaling technique [8] where, for an arbitrary noisy gate G, we insert the $G^\dagger G$ noisy identity in the circuit. We refer to such a circuit with identities as a *redundant circuit*. However, since our ansatz circuit (Figure 1) has time-evolution gates $U(t_n, t_{n+1})$, the identity $U^\dagger U$ demands negative time evolution $U^\dagger(t_n, t_{n+1}) = U(t_{n+1}, t_n)$, which is not physical.

Nonetheless, it is possible to show that $U^\dagger(t_n, t_{n+1})$ can be implemented by simply adding an ability to perform Y gates on odd-numbered qubits including the inaccessible part under the condition that the system Hamiltonian is H_{XY} given by Eq.(5) with $b_k = 0$. This is due to the symmetry of 1-D XY-model Hamiltonian H_{XY} without local magnetic fields given by $\Pi_{j=0}^{M} Y_{2j+1} \cdot H_{XY} \cdot \Pi_{j=0}^{M} Y_{2j+1} = -H_{XY}$ when $N = 2M + 1$; the similar equation also holds when $N = 2M$. This equation leads

$$\Pi_{j=0}^{M} Y_{2j+1} \cdot U(t_n, t_{n+1}) \cdot \Pi_{j=0}^{M} Y_{2j+1} = U^\dagger(t_n, t_{n+1}) \tag{6}$$

Hence, for an arbitrary n-qubit XY time-evolution gate $U(t_n, t_{n+1})$, the $U^\dagger(t_n, t_{n+1})$ gate can be achieved by setting $b_k = 0$ and applying Y gates on the odd-numbered

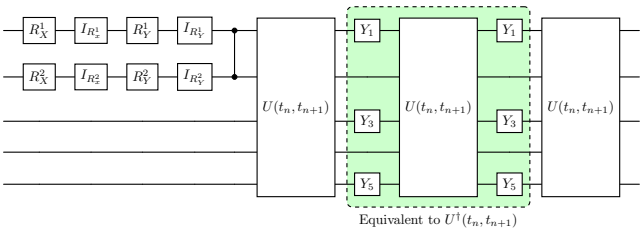


Figure 2: The n-th layer of a 5-qubit indirect-control *redundant* circuit is depicted, where $I_{R_x^1}$ is an abbreviation of $R_X^\dagger R_X$ on the 1st-qubit, etc. The highlighted section corresponds to $U^\dagger(t_n, t_{n+2})$. Depending on the number of identities, we define the noise levels n_R, n_T, and n_Y, where each value is equal to or proportional to the numbers of rotational gates, time-evolution gates, and Y gates respectively. In this specific figure, if we define n_R as the total number of rotation gates, n_T as the number of U and $U^\dagger$ gates, and n_Y as half the number of Y gates, then the layer has $(n_R, n_T, n_Y) = (12, 3, 3)$.

qubit before and after the time-evolution, as depicted in the highlighted part of Figure 2 for a 5-qubit time-evolution gate. Utilizing the identity scaling technique, we construct various redundant circuits corresponding to different noise levels.

To increase noise, we add noisy identities $G^\dagger G$, with G representing rotational, time-evolution, or Y gates, forming a redundant circuit. Note that no $C_z^\dagger C_z$ has been used. We denote noise levels as $\vec{\lambda} = (n_R, n_T, n_Y)$ for single-qubit rotation, time-evolution, and Y gates, respectively. The values of (n_R, n_T, n_Y) can be chosen to the amount of noise caused by the corresponding gates in some unit and are, therefore, proportional to the number of corresponding noisy gates in each layer. The multivariate Richardson extrapolation uses three independent variables (n_R, n_T, n_Y) and one dependent variable, the energy expectation value.

We studied 7-qubit system at various fixed noise probabilities at a depth of 30 layers by inserting depolarizing channels after each gate for all qubits. We chose the parameters of our system Hamiltonian, that is 1-D XY-model, as $\gamma = 0$, $b_k = 0$, $c_k = 1/2$. The target Hamiltonian H_T is chosen as the transverse field Ising model Hamiltonian given by Eq.(5) with $\gamma = 1$, $b_k = 1$, $c_k = 1/2$. We used a probabilistic optimization algorithm to calculate $E'_{VQE}(\vec{\lambda_0})$ for $\vec{\lambda_0}$ corresponding to the noise level of non-redundant circuits given by Figure 1. We ran the optimization 10 times independently and derived the mean and the standard deviation for $E'_{VQE}(\vec{\lambda_0})$, and 10 distinct sets of optimized parameters. These parameter-sets were then employed in redundant circuits to calculate $E'_{VQE}(\vec{\lambda})$ for $\vec{\lambda} > \vec{\lambda_0}$. Finally, 10 independent estimations of ZNE values $E'_{VQE}(\vec{0})$ are derived using the multivariate Richardson extrapolation with various polynomial degrees. In Figure 3, each graph displays mean ZNE values $E'_{VQE}(\vec{0})$ at different polynomial degrees alongside the mean $E'_{VQE}(\vec{\lambda_0})$ calculated by noisy circuits for noise probabilities of 0.001 and 0.0001, as well as the mean E_{VQE} calculated by noise-free circuits. For both cases,

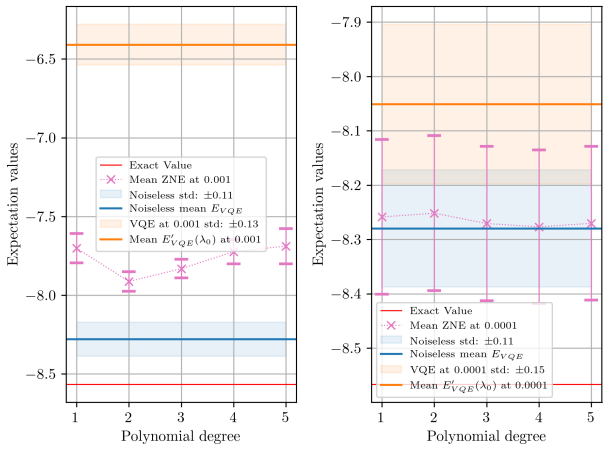


Figure 3: Mean ZNE values for a 7-qubit, 30-layered system using multi-variate Richardson extrapolation. No constraints on time parameters were applied. Mean and standard deviation at a given noise probability were calculated using 10 independent samples of VQEs.

we can observe that the mean $E'_{VQE}(\vec{\lambda}_0)$ is outside of the region of the standard deviation of the mean noiseless E_{VQE}, and also the mean ZNE values are much smaller than the mean $E'_{VQE}(\vec{\lambda}_0)$ and close to the mean noiseless E_{VQE}, which guarantees the successful implementation of the error mitigation.

References

[1] M. AbuGhanem and H. Eleuch, "Nisq computers: A path to quantum supremacy," *arXiv:2310.01431*, 2023.

[2] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, p. 505–510, 2019.

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[4] 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," *Reviews of Modern Physics*, vol. 95, Dec. 2023.

[5] K. Maruyama and D. Burgarth, *"Gateway Schemes of Quantum Control for Spin Networks" in "Electron Spin Resonance (ESR) Based Quantum Computing"*, pp. 167–192. Springer New York, 2016.

[6] T. Anan *et al.*, "Implementation of variational quantum eigensolver with indirect control," *48th Quantum Information Technology Workshop (QIT48)*, May 2023.

[7] J. Tilly *et al.*, "The variational quantum eigensolver: A review of methods and best practices," *Physics Reports*, vol. 986, p. 1–128, Nov. 2022.

[8] Giurgica-Tiron *et al.*, "Digital zero noise extrapolation for quantum error mitigation," in *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, IEEE, Oct. 2020.

[9] V. Russo and A. Mari, "Quantum error mitigation by layerwise richardson extrapolation," *arXiv:2402.04000*, 2024.

Reducing T Gate Count by Combining Two Types of MCT Gate Decomposition Techniques

Taketo Yamaguchi[1] Shigeru Yamashita[2]

[1] *Graduate School of Information Science and Engineering Ritsumeikan University*

Abstract. For fault-tolerant quantum compilation, reducing the T-gate count is crucial. Using LUT-based synthesis, a MCT (Multiple Control Toffoli) gate is applied based on the input information of the LUT node. This gate targets an initialized ancilla bit. In quantum circuits, states other than the qubits used for calculating the output must be returned to their initial state. Considering the decomposition of the MCT gate, there are redundant gates, and there is a room to reduce the number of T gate. By defining decomposition constraints and exploring appropriate combinations, we achieved up to 8.7% reduction in T-gate count through experiments.

Keywords: Quantum circuit, T-gate count, MCT gate

1 Introduction

Quantum computers [1] are computers that perform calculations using the superposition states of qubits, and they are attracting attention for having algorithms that can solve certain problems faster than existing computers.

Quantum circuits that realize quantum algorithms consist of two parts, circuits specific to quantum algorithms and circuits that compute Boolean functions. A hierarchical logic synthesis using Look Up Tables (LUTs) has been proposed as an efficient method to synthesize quantum circuits that compute Boolean functions [2].

The synthesis using LUTs first applies Multiple Control Toffoli (MCT) gates [3] to ancilla bits initialized to 0, based on the input information held by the nodes of the LUT. If the value of the LUT node is not an output bit, an MCT gate that performs uncomputation is placed. Next, the MCT gates are decomposed and mapped to Clifford + T gates [4] to generate directly executable Boolean quantum circuits. Since the T gates are more costly compared to other gates, reducing the number of T gates used is important.

In this paper, we propose a method to reduce the number of T gates by combining two types of MCT gate decomposition techniques. The first decomposition technique takes into account paired MCT gates. In quantum circuits, due to the nature of applying the same MCT gate twice for computation and uncomputation, there exist pairs of computation and uncomputation gates with the same inputs. Therefore, redundant gates are reduced.

The second decomposition technique reduces the number of ancilla bits initialized to 0 required for decomposition by splitting an MCT gate into three MCT gates. The technique that considers paired MCT gates requires auxiliary bits initialized to 0, and when decomposed, the value of the auxiliary bits becomes uninitialized. As a result, it becomes impossible to store the computed values. By devising ways to decompose MCT gates, we aim to reduce the number of qubits that cannot store values, thus increasing the number of instances where the first technique can be applied. Then, under the constraint of not increasing the number of qubits, we generate an initial solution by combining the two decomposition techniques. Using Simulated Annealing, we heuristically explore ways to increase the number of instances where the two ideas can be applied. As the result, the number of T gates reduced up to 8.7% compared to existing methods.

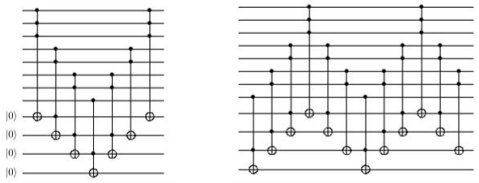


Figure 1: MCT decomposition

2 Background

The Multiple Control Toffoli (MCT) gate is a quantum gate that has k control bits ($k \leq 3$) and one target bit. The MCT gate outputs the exclusive OR of the logical product of all control bits and the value of the target bit to the target bit. Since the MCT gate is not directly executable, it needs to be decomposed into executable gates such as Clifford + T gate. In this chapter, we explain the method that uses the fewest T gates and auxiliary bits for decomposition [3]. The decomposition of the MCT gate is performed using auxiliary bits, and the methods differ depending on whether the auxiliary bits are initialized or not. After this point, auxiliary bits initialized to 0 are referred to as clean ancilla, while those not initialized as such are called dirty ancilla. Leftside of Figure1 shows the decomposition using clean ancilla. The MCT gate is decomposed into Toffoli gates and MCT gates with three control bits. Since intermediate values are stored in the clean ancilla during the decomposition, gates for uncomputation are placed on all but the output bits. Rigtside of Figure1 shows the decomposition using dirty ancilla. When using dirty ancilla, values cannot be directly stored in them. Therefore, as shown in rightside of Figure 1, it is necessary to apply the MCT gate twice to the same auxiliary bit. The gates acting on the output bits are replaced by Toffoli gates, while the others are replaced by MCT

Table 1: T-count and ancilla required for decomposing an MCT gate

control bits	T-count	ancilla	ancilla status
$k = 3$	15	1	$\|0\rangle$
$k = 3$	16	1	$\|x\rangle$
$k >= 4$	$8k - 9$	$\lceil \frac{k-2}{2} \rceil$	$\|00..00\rangle$
$k >= 4$	$8k - 8$	$\lceil \frac{k-2}{2} \rceil$	$\|xx..xx\rangle$

gates with three control bits. Next, each gate is replaced by a Relative Phase Toffoli (RTOF) gate, which approximates a phase-applied Toffoli gate. The RTOF can be implemented without auxiliary bits in the case of three control bits and can be implemented with fewer T gates than the Toffoli gate. Table 1 summarizes the number of T gates and auxiliary bits used for the decomposition of the MCT gate.

3 The Proposed Method

In this chapter, a method to reduce the number of T gates by combining two types of MCT gate decomposition methods is proposed. The reduction is achieved by considering the decomposition of paired MCT gates and using a method that decomposes into three MCT gates, thereby reducing the number of clean ancilla required for decomposition. Simulated Annealing is then used heuristically to explore the cases where the decomposition method can be applied more frequently.

3.1 Method for Decomposing an MCT Gate

3.1.1 To decompose the method considering paired MCT gates

In some cases, MCT gates have pairs with the same control and target bits. In quantum circuit design, it is necessary to uncompute for values unrelated to the output, applying the same MCT gate twice to auxiliary bits. Considering the decomposition of the MCT gate, it can be seen that there are four gates with the same control bits. In reftside of Figure 2, the gates enclosed in red are computational gates used to create the uncomputational gates. These four gates with the same control bits consist of computational gates and uncomputational gates. Performing the computation and uncomputation twice is redundant. Therefore, by not performing uncomputation of the intermediate state of the MCT gate, the number of redundant gates is reduced, and the necessary number of T gates is decreased. In leftside of Figure 2, the gates enclosed in red, yellow, and blue are gates that perform uncomputation and recomputation of the intermediate state and can be reduced. Rightside of Figure 2 shows the circuit diagram where the MCT gate is reduced and the intermediate state is not uncomputated. To decompose paired MCT gates, clean ancilla are required. Therefore, there is a constraint condition related to the number of clean ancilla. Let be the number of clean ancilla that can be used by the t-th MCT gate, n is the number of MCT gates between the forward and reverse computation gates and y be the number of clean ancilla required for the decomposition of the MCT gate. The constraint condition can be written as follows in equation(1)

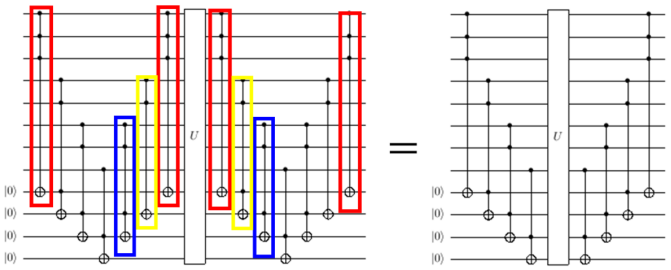


Figure 2: Example of considering paired MCT gates

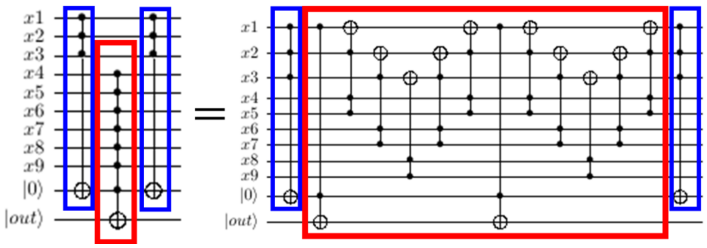


Figure 3: Example of method to reduce clean ancilla required for decomposition by decomposing into three MCT gates

$$y \leq \mathrm{MIN}(x_t, x_{t+1} ....x_{t+n}) \tag{1}$$

3.1.2 A method to reduce the number of clean ancilla required for decomposition by decomposing into three MCT gates

In this section, we explain a method to reduce the number of clean ancilla used in the decomposition of MCT gates. First, we decompose MCT gates using clean ancilla. When the number of control bits of the MCT gate is k, we split the MCT gate into one with x control bits and one with $k - x + 1$ control bits where x is the minimum integer that satisfies $x \leq \lceil \frac{k-2-x}{2} \rceil$. The decomposition of MCT gates is done in three steps. First, we decompose the MCT gate with x control bits using clean ancilla. Next, we consider the MCT gate with $k - x + 1$ control bits as having already decomposed x control bits and dirty ancilla, and decompose it accordingly. Finally, we perform the inverse computation of the MCT gate with x control bits. By decomposing the MCT gate into three parts, the number of clean ancilla can be reduced to $\lceil \frac{x-2}{2} \rceil$ where x is the minimum integer that satisfies $x \leq \lceil \frac{k-2-x}{2} \rceil$. x represents the condition that the number of auxiliary bits required for the decomposition of the MCT gate, indicated by the blue box, exceeds the number of control bits of the MCT gate, indicated by the red box in Figure 3. The number of T gates contained in an MCT gate is $8k - 8$. The number of T gates in the decomposed MCT gate using auxiliary bits is $8(x - 1)$, and the number of T gates when control bits are considered as auxiliary bits in the decomposition is $8(k - x + 1 - 1)$. Therefore, the total number of T gates in the MCT gate is $8(x - 1) + 8(k - x + 1 - 1)$, which is equal to $8(k - 1)$.

Table 2: T-count and ancilla required for decomposing an MCT gate propsed way

	control bits	T-count	clean ancilla
existing	$k >= 4$	$8k - 9$	1
proposed	$k >= 4$	$8k - 8$	$\lceil \frac{x-2}{2} \rceil \{x \mid \lceil \frac{k-2-x}{2} \rceil \leq x\}$

Although the number of T gates increases by one compared to decomposition using clean ancilla, the number of auxiliary bits used is significantly reduced.

Applying the decomposition method described in this section can reduce the number of clean ancilla. Therefore, when combined with the decomposition method proposed in Section 3.1.1 to address the paired MCT gates suggested, the conditions for applying the decomposition method proposed in Section 3.1.1 (equation 1) are met, resulting in an increase in the number of MCT gates that can be reduced on the Boolean quantum circuit. On the other hand, combining the decomposition methods proposed in Sections 3.1.1 and 3.1.2 results in control bits changing their values, rendering them unusable for computation. Therefore, when combining the decomposition methods proposed in Sections 3.1.1 and 3.1.2, they can only be applied to gates where control bits are not used during the computation from MCT gate computation to uncomputation.

3.2 Application of decomposition method using combinatorial optimization

Due to the limited availability of qubits in quantum circuits, not all MCT gates can satisfy the condition of Equation 1. Therefore, to maximize the reduction in the number of T gates, it is necessary to consider combinations of MCT gates that apply the proposed decomposition. Figure 3.2 illustrates an example circuit demonstrating the combinations of MCT gates where the reduction effect is most significant. The MCT gates surrounded by blue, yellow, and red rectangles represent gates that do not perform uncomputation of intermediate states. The blue, yellow, and red arrows indicate the intervals where the corresponding MCT gates, corresponding to the colors, occupy auxiliary bits. The number of T gates can be reduced from 216 to 184, making this quantum circuit have fewer T gates. By greedily applying MCT gates starting from those with early uncomputations, it is possible to find combinations with even fewer T gates. When greedily searching, obtaining the optimal solution is not guaranteed. Moreover, when decomposing considering paired MCT gates, it is difficult to explore the optimal combinations to apply on large-scale Boolean quantum circuits. Therefore, using the results of greedy search as initial solutions, heuristic exploration is performed with the Simulated Annealing algorithm to further reduce the number of T gates by changing answer randomly.

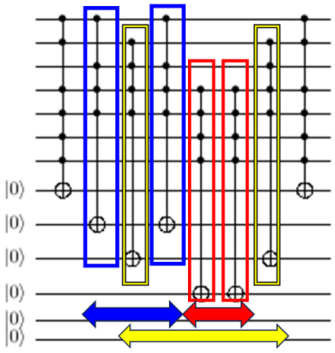


Figure 4: Example of greedy combinations

Table 3: experimental result

benchmarks	esop based	proposed	$\Delta T(\%)$
arbiter	477453	445453	6.7
i2c	41490	38242	7.8
mem_ctrl	2154898	19731380	8.4
priority	52821	50517	4.3
router	6546	5970	8.7
ctrl	2647	2615	1.2
intfloat	9433	9018	3.7
voter	420630	420630	0.0
square	359824	359776	0.0
adder	18504	18488	0.0

4 Experimental Result

The proposed method was implemented using C++. Using the open-source tool [5] that can create LUTs, benchmarks composed of And-inverter graphs were converted into LUT networks with an LUT size of 6. Boolean quantum circuits were created based on the LUT networks. The Boolean functions represented by the LUT nodes were converted into ESOP (Exclusive-Sums-Of-Products) using the EFPL logic library [6], and MCT gates corresponding to the ESOP were placed. Then, based on the number of clean ancilla, the proposed method was used to search and determine the number of T gates that could be reduced. Since the number of quantum bits available in quantum computers is limited, in this experiment, we did not provide any surplus clean ancilla that do not store the values of LUT nodes.
As a result of the experiment, the number of T-gates was reduced by up to 8.7% and by an average of 4%.

5 Conclusion

This papaer proposes Method for reducing T gate count by combining two types of MCT gate decomposition techniques. Using a greedy search and the Simulated Annealing algorithm, we efficiently searched for combinations where the decomposition method could be effectively applied, demonstrating that there exist Boolean quantum circuits where the number of T gates can be reduced.

References

[1] Charles H. Bennett and David P. DiVincenzo *Quantum information and computation.* Nature volume 404, p247-255,2000.

[2] Mathias Soeken, Martin Roetteler, Nathan Wiebe, and Giovanni De Micheli *LUT Based Hierarchical Reversible Logic Synthesis.* IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (Volume:38,Issue:9,September 2019)

[3] Dmitri Maslov. On the advantages of using relative phase Toffolis with an application to multiple control Toffoli optimization. Phys. Rev. A 93, 022311, 2016.

[4] Xinlan Zhou and Debbie W. Leung and Isaac L. Chuang. Methodology for quantum logic gate construction. Phys. Rev. A 62, 052316, 2000.

[5] Mathias Soeken. A toolkit for reversible circuit design https://github.com/msoeken/cirkit.

[6] Mathias Soeken, Heinz Riener, Winston Haaswijk, Eleonora Testa, Bruno Schmitt, Giulia Meuli, Fereshte Mozafari, Siang-Yun Lee, Alessandro Tempia Calvino, Dewmini Sudara Marakkalage, Giovanni De Micheli Integrated Systems Laboratory, EPFL, Lausanne, Switzerland. The EPFL Logic Synthesis Libraries https://doi.org/10.48550/arXiv.1805.05121, 2016.

Error mitigated digital quantum simulation with auxiliary parameter

Sangjin Lee[1] Youngseok Kim[2] Seung-Woo Lee[1]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea*

[2] *IBM Quantum, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA*

Abstract. Digital quantum simulation potentially offers an advantage in modeling quantum many-body systems beyond the capabilities of classical computation. However, Trotter errors significantly degrade the performance, which are unavoidable due to the decomposition of the unitary evolution of the Hamiltonian into finite number of Trotter steps. In this work, we introduce a cost-efficient quantum error mitigation scheme to reduce Trotter errors in digital quantum simulation by using an auxiliary parameter. The auxiliary parameters can be easily adjustable in experimental settings to effectively address Trotter errors up to a target precision without increasing the required gates. We demonstrate that our scheme achieves comparable precision in simulation results while significantly reducing the number of gates used compared to previously proposed Trotter-error mitigation strategies.

Keywords: Trotter-error mitigation, Quantum simulation

1 Introduction

A quantum simulator is a natural-born tool for an exploration to complex and many-body physics in which conventional computation techniques such as an exact diagonalization suffers from exponentially large Hilbert space. Concerning large Hilbert space, a numbers of constructed quantum simulators even with small number of qubits already start to benchmark standard known results: energy levels of molecules, phase diagram of lattice gauge theories[1, 2]. Even though many quantum simulations have been already working, we still need an efficient algorithm to be implemented to existing quantum simulation platforms because of restricted resources and practical errors.

Regarding to quantum simulations, there are two types of quantum simulations: analog and digital quantum simulations. Those two types of quantum simulations have pros and cons respectively. In spite of its advantage in controllability, digital quantum simulation is inevitably contaminated by so-called Trotter errors. The Trotter errors, in principle, can be arbitrary reduced if the number of Trotter steps is sufficiently large. However, in the presence of physical errors caused by such as decoherence or gating errors, the performance of digital quantum simulation is also significantly reduced. Therefore, in the realistic simulation, an efficient strategy to control both the Trotter errors and physical errors is essential.

In efforts to control of algorithmic errors originated from quantum simulation, especially Trotter errors, there were two types approaches: developing well-designed series of quantum gates to reduce Trotter error and post-processing of errored simulated data. In ideal situation, Trotter errors can be handled up to arbitrary precision by Suzuki formula with the cost of exponentially large numbers of quantum gates. Even though Suzuki formula is mathematically correct but it is costly to be implemented. Therefore, as an alternative to Suzuki formula based approach, it seems to be plausible to develop a post-processing algorithm that extracts out ideal quantum simulation data from the classical data obtained from quantum simulator to mitigate *Trotter errors*. Treating classical data is relatively easier to deal with than quantum data which is contaminated by external noises and Trotter errors.

In this work, we propose a cost-efficient quantum error mitigation scheme that efficiently mitigates Trotter errors with auxiliary parameters. The auxiliary parameters can be easily adjustable in experimental settings to effectively address Trotter errors up to a target precision without increasing the required gates. We demonstrate that our scheme achieves comparable precision in simulation results while significantly reducing the number of gates used compared to previously proposed quantum error mitigation strategies [3]. We note that fewer numbers of quantum gates used in our scheme also lowers the effects of physical errors from quantum operation to achieve better error bounds in real implementations.

2 Extrapolation based approach

We start with a brief introduction of the previous work, which estimates ideal data by using extrapolation [3]. Suppose we want to investigate time-evolution of an observable $\mathcal{O}$ described by an time-independent Hamiltonian $H = \sum_\mu H_\mu$. Exact time-evolution operator should be $U(t) = e^{-iHt}$ and an ideally simulated observable $\mathcal{O}(t)$ is

$$\langle \mathcal{O} \rangle_U = \langle \psi | U^\dagger(t) \mathcal{O} U(t) | \psi \rangle, \tag{1}$$

with respect to an initial state $|\psi\rangle$.

In practical quantum circuit, $U(t)$ is approximately realized by $V(t)$ composed of a sequence of quantum gates such as $V(t) = \prod_\mu e^{-itH_\mu}$. In general, elements of $\{H_\mu\}$ do not commute, which generates the Trotter error,

$$V(t) = U(t) + \sum_{s=p} E_s t^s. \tag{2}$$

This sequence of quantum gates is called a p-th order Trotter formula, and simulated observable $\langle \mathcal{O}(t) \rangle_V =$

$\langle\psi|V^\dagger(t)\mathcal{O}V(t)|\psi\rangle$ deviates from the ideal result by

$$\langle\mathcal{O}(t)\rangle_V = \langle\mathcal{O}(t)\rangle_U + \sum_{s=p}\epsilon_s t^s. \tag{3}$$

Note that for fixed time t, one can easily show that

$$\lim_{n\to\infty} V^n\left(\frac{t}{n}\right) = U(t), \tag{4}$$

and an associated simulated data also approaches to ideal result.

From the observations, we can reinterpret a quantum error mitigation scheme for quantum simulation proposed by the previous work [3] as follows.

1. For a positive integer m, conduct quantum simulation with m-units of given Trotter formula, $V_m = \left(V\left(\frac{t}{m}\right)\right)^m$ and obtain time-evolved observable $\langle\mathcal{O}(t)\rangle_{V_m}$.
2. Do the similar experiments with various m and collect pairs of data $\{(m, \langle\mathcal{O}\rangle_{V_m})\}$.
3. With the obtained data, extrapolate by using a polynomial form to the infinite m that estimates $\langle\mathcal{O}(t)\rangle_U$.

The procedure described above can be summarized as in Figure 1. Technical details can be found in [3].

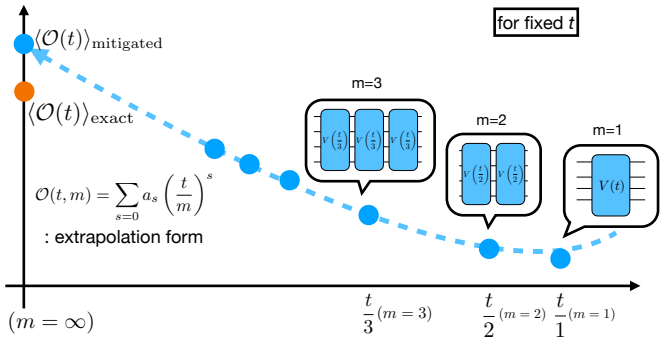


Figure 1: A scheme proposed in [3]. With various circuit depths and fixed time t, quantum simulations of an observable give blue dots. From a set of collected data, one can extrapolate to estimate behaviors of $\langle\mathcal{O}(t)\rangle_{V_m}$ at infinite m which should be the ideally simulated value, $\langle\mathcal{O}(t)\rangle_U$.

We note that the proposed scheme costs $\mathcal{O}\left(q^2\right)$ units of p-th order Trotter formula to achieve $\mathcal{O}\left(t^{p+q}\right)$ precision. It may be harmful in real situations because physical errors will be piled up as increasing the depth of quantum circuits, which eventually degrades the overall performance of quantum simulation.

3 Our proposal: error-profiling from auxiliary parameter

We now propose a quantum error mitigation scheme with auxiliary parameter for digital quantum simulation, which requires less number of quantum gates compared to previous methods. For that, we consider two-units of p-th order Trotter formula circuit, $V(t)$ and their composition such as

$$\begin{aligned} V_r(t) &= V(rt)V\left((1-r)\,t\right), \\ &= U(t) + \sum_{s=p}\bar{E}_s(r)t^s. \end{aligned}$$

Here, we introduced an auxiliary parameter r that probes the landscape of error.

For the given composition $V_r(t)$, one can compute errors of given observable simulated by $V_r(t)$. For example,

$$\begin{aligned} \langle\mathcal{O}(t)\rangle_{V_r} &= \langle\psi|V_r^\dagger(t)\mathcal{O}V_r(t)|\psi\rangle, \\ &= \langle\mathcal{O}(t)\rangle_U + \langle E_p^\dagger\mathcal{O} + h.c.\rangle(r^p + (1-r)^p)t^p + \mathcal{O}\left(t^{p+1}\right), \end{aligned}$$

where $\langle\ \bullet\ \rangle \doteq \langle\psi|\ \bullet\ |\psi\rangle$. In theory, it could be difficult to calculate directly the matrix element $\langle E_p^\dagger\mathcal{O} + h.c.\rangle$ for arbitrary large quantum system. However, for fixed t, one can estimate a coefficient of the function $r^p + (1-r)^p$, which is the matrix element, by observing the profile of $\langle\mathcal{O}(t)\rangle_{V_r}$ as a function of r up to $\mathcal{O}\left(t^{p+1}\right)$.

After reading off $\langle E_p^\dagger\mathcal{O} + h.c.\rangle$, the ideal time evolution of $\mathcal{O}$ is mitigated as

$$\langle\mathcal{O}(t)\rangle_U \simeq \langle\mathcal{O}(t)\rangle_{V_r} - \langle E_p^\dagger\mathcal{O} + h.c.\rangle(r^p + (1-r)^p)t^p, \tag{5}$$

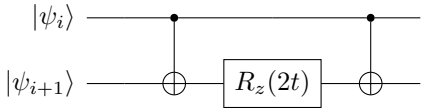
which is correct up to $\mathcal{O}\left(t^{p+1}\right)$.

We sketch our proposal to compare it with previous methods as follows:

1. Prepare two-units of a Trotter formula that elapses rt and $(1-r)\,t$ respectively, and obtain functional forms of the observable regarding to the given composition up to coefficient.
2. For fixed time t, conduct quantum simulation of the observable with various r and collect a set of data, $\{(r, \langle\mathcal{O}\rangle_{V_r})\}$.
3. By comparing $\{(r, \langle\mathcal{O}\rangle_{V_r})\}$ to the functional form of step 1., fix down undetermined coefficients.
4. From obtained erroneous terms in step 3., extract out $\langle\mathcal{O}(t)\rangle_U$ from $\langle\mathcal{O}(t)\rangle_{V_r}$.

The procedure is illustrated in Figure 2.

Finally, we want to remark on our proposals with few things. First, conducting experiments with various r is relatively easy to implement than to increase the number of unit Trotter formula layer, since time-evolution operator, say $V(t)$ is essentially realized in terms of quantum gates as phase rotations gates. For example, $e^{-itZ_iZ_{i+1}}$ can be realized as



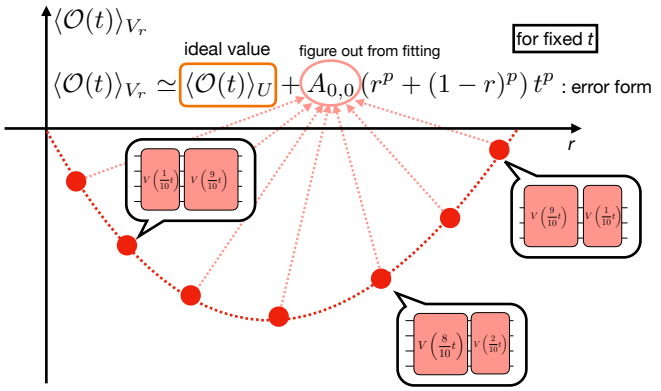


Figure 2: By observing profile of $\langle \mathcal{O}(t) \rangle_{V_r}$ as an function of auxiliary parameter r, one can estimate erroneous terms from fitting form, $\langle \mathcal{O}(t) \rangle_{V_r} \simeq \langle \mathcal{O}(t) \rangle_U + A_{0,0}\,(r^p + (1-r)^p)\, t^\alpha$. As a result, one can read off $A_{0,0}$ by fitting, which finally allow us deduce the ideal value, $\langle \mathcal{O}(t) \rangle_U$.

Therefore, our proposal is essentially replacing the cost of quantum gates to the number of measurements which is plausible with quantum computing platforms currently working on. Secondly, in a similar spirit with previous comment, the scheme we proposed requires only two-units of Trotter formula, which makes robust to the corruption of quantum simulation by physical noise. Therefore, we expect our proposal may improve the quality of quantum simulation with the same cost of resources.

References

[1] S. McArdle, S. Endo, A. Aspuru-Guzik, S. C. Benjamin, & X. Yuan, Quantum computational chemistry, *Rev. Mod. Phys.* **92**, 015003 (2020).

[2] L. Lumia, P. Torta, G. B. Mbeng, G. E. Santoro, E. Ercolessi, M. Burrello, & M. M. Wauters, Two- Dimensional $\mathbb{Z}_2$ Lattice Gauge Theory on a Near-Term Quantum Simulator: Variational Quantum Optimization, Confinement, and Topological Order, *PRX Quantum.* **3**, 020320 (2022)

[3] A. Carrera Vazquez, D. J. Egger, D. Ochsner, and S. Woerner, Well-conditioned multi-product formulas for hardware-friendly Hamiltonian simulation

Quantum **7**, 1067 (2023).

Reducing Quantum Cost by Decomposing Two MCT Gates as a Pair

Takaki Hasegawa[1] * Shigeru Yamashita[1] †

[1] *Graduate School of Information Science and Engineering, Ritsumeikan University*

Abstract. There exists a method for reducing basic quantum gates when decomposing Multiple-Control Toffoli (MCT) gates in quantum circuits. This method involves decomposing a single MCT gate into four MCT gates with fewer control bits and four Controlled-V (CV) gates, repeating this process until only basic quantum gates remain, and removing redundant gates using a labeling method. However, this method applies to a single MCT gate and does not consider decomposing multiple MCT gates. We propose a decomposition method that reduces quantum gates by reordering MCT gates and canceling out MCT and CV gates that appear after decomposing adjacent MCT gates.

Keywords: MCT gate, CV gate

1 Introduction

Quantum circuits are represented by combining quantum gates that perform quantum computations. In quantum circuit design, Multiple-Control Toffoli (MCT) gates can be used to implement any logical function. However, MCT gates are significantly more costly to implement compared to other quantum gates. Therefore, decomposition methods for MCT gates are being studied to design more efficient quantum circuits.

A method proposed by Kole et al. involves decomposing a single MCT gate into four MCT gates with fewer control bits and four Controlled-V (CV) gates, repeatedly performing this operation. This decomposition method recursively decomposes the resulting MCT gates, eventually generating a quantum circuit composed solely of gates with a quantum cost of 1.Furthermore, since the generated circuit contains redundant gates, a labeling method is used to remove these redundant gates. However, since this decomposition method is applied to a single MCT gate, it does not account for the decomposition of multiple MCT gates within a quantum circuit.Thus, we propose a decomposition method for MCT gates that further reduces quantum gates by reordering MCT gates and canceling out MCT and CV gates that appear when decomposing adjacent MCT gates.

2 Proposed Method

2.1 Classification of MCT Gate Pair Types

When decomposing two MCT gates as a pair, the decomposition method applied to the MCT gates varies depending on the relations between their control bits and target bits. The relations categorizes MCT gate pairs into four types. The relations between the control bits and target bits of the two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ when decomposed as a pair are as follows. Here, $A \supset B$ indicates that B is a proper subset of A.

A. $C_p = C_q, t_p = t_q$

B. $C_p \supset C_q$ or $C_p \subset C_q, t_p \neq t_q$

C. $C_p \cap C_q \neq \emptyset, C_p \neq C_q, t_p = t_q$

D. $C_p \cap C_q \neq \emptyset, C_p \not\supset C_q, C_p \not\subset C_q, t_p \neq t_q$

Relations A indicates that all control bits and target bits of the two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ are identical. An example of relations A is shown in Fig. 1. Relations B indicates that all control bits of one MCT gate match some of the control bits of the other MCT gate, while the target bits are different. However, this excludes cases where all control bits of the two MCT gates are identical. An example of relations B is shown in Fig. 2. Relations C indicates that some control bits of the two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ match, and their target bits are also identical. This excludes cases where all control bits of the two MCT gates are identical. An example of relations C is shown in Fig. 3. Relations D indicates that some control bits of the two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ match, while the target bits are different. This excludes cases where all control bits of one MCT gate match some of the control bits of the other MCT gate. An example of relations D is shown in Fig. 4.

2.2 How to Select Two MCT Gates to Decompose as a Pair

When selecting two MCT gates to decompose as a pair, we select a pair that match the types of MCT gate pairs described previously. In this process, it is necessary to establish a priority order for pairing MCT gates. The priority should be set such that pairs of MCT gates that can achieve greater reductions in quantum cost are given higher priority. The priorities and conditions for selecting two MCT gates to decompose as a pair with $M_p(C_p; t_p)$ are as follows. Here, $M_q(C_q; t_q)$ and $M_r(C_r; t_r)$ represent candidate MCT gates for pairing with $M_p(C_p; t_p)$.

1. A pair in relations A
2. A pair in relations B where $\frac{|C_p|}{2} \leq |C_q| \leq 2|C_p|$
   - Among $|C_q|$ and $|C_r|$, a pair with the smaller difference from $|C_p|$
   - If $|C_q|$ and $|C_r|$ have the same difference from $|C_p|$, a pair with the larger number of control bits

*tofu@ngc.is.ritsumei.ac.jp
†ger@cs.is.ritsumei.ac.jp

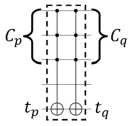


Figure 1: An example of a pair in relations A

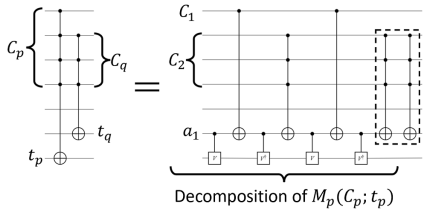


Figure 2: An example of a pair in relations B

3. A pairs in relations C or D where $\frac{|C_p|}{2} \leq |C_p \cap C_q|$ and $\frac{|C_q|}{2} \leq |C_p \cap C_q|$

- Among $|C_q|$ and $|C_r|$, a pair with the smaller difference from $|C_p|$
- If $|C_q|$ and $|C_r|$ are the same, a pair in relations C

Priority 1 represents a pair of two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ in relations A in the types of MCT gate pairs. In the case of relations A, the two MCT gates can cancel each other out, making this the highest priority for pairing.

Priority 2 represents a pair of two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ in relations B, where the number of control bits of one gate is at least half and at most twice the number of control bits of the other gate. In the case of relations B, the MCT gate with fewer control bits can be removed, giving this a high priority, second only to Priority 1. Additionally, if the pair $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ and the pair $M_p(C_p; t_p)$ and $M_r(C_r; t_r)$ are both priority 2, the pair where the difference in the number of control bits from $M_p(C_p; t_p)$ is smaller is prioritized. If the difference is the same, the MCT gate with the larger number of control bits is prioritized.

Priority 3 represents a pair of two MCT gates $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ in either relations C or D, where the number of matching control bits between the two MCT gates is at least half of the control bits of each gate. In the case of either relations C or D, some gates can be removed after decomposing into four MCT gates and four CV gates, giving this a high priority, next after Priority 2. Additionally, if the pair $M_p(C_p; t_p)$ and $M_q(C_q; t_q)$ and the pair $M_p(C_p; t_p)$ and $M_r(C_r; t_r)$ are both priority 3, the pair where the difference in the number of control bits from $M_p(C_p; t_p)$ is smaller is prioritized. If the number of control bits is the same for $M_q(C_q; t_q)$ and $M_r(C_r; t_r)$, the pair in relations C is prioritized.

MCT gates that cannot be paired under any of the priorities 1 to 3 are decomposed using the previous method for decomposing a single MCT gate.

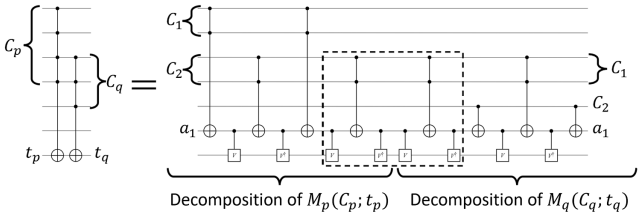


Figure 3: An example of a pair in relations C

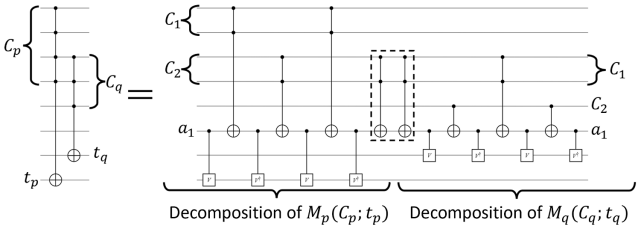


Figure 4: An example of a pair in relations D

2.3 Decompose Two MCT Gates as a Pair

The order in which MCT gates in a quantum circuit are decomposed as a pair is as follows.

Step 1. Creating pairs among commutative gates

Step 2. Decomposing according to the types of pairs as shown in Figures 1 to 4

Step 3. Replacing with elementary quantum gates

Step 4. Removing redundant gates

In Step 1, pairs of MCT gates are created based on the priority order described above. First, the MCT gate at the left end of a given quantum circuit Q is defined as $M_p(C_p; t_p)$. Next, the MCT gate with the highest priority when pairing $M_p(C_p; t_p)$ with each of the MCT gates other than $M_p(C_p; t_p)$ is defined as $M_r(C_r; t_r)$. Then, $M_p(C_p; t_p)$ and $M_r(C_r; t_r)$ are saved as a pair and deleted from the quantum circuit Q. If no MCT gate that reduces cost when paired with $M_p(C_p; t_p)$ is found, we preserve $M_p(C_p; t_p)$ as a single MCT gate and remove it from quantum circuit Q. we repeat this process until no gates remain in quantum circuit Q.

In Step 2, we apply the decomposition methods corresponding to the types of MCT gate pairs described above to the pairs of MCT gates preserved in Step 1. This operation is applied to all preserved MCT gate pairs.

In Steps 3 and 4, we apply the previous decomposition method to the MCT gates. First, in Step 3, we decompose the MCT gate pairs from Step 2 and the single MCT gates preserved in Step 1 into quantum circuits composed solely of elementary quantum gates. Then, in Step 4, we use the labeling method to remove redundant gates from these quantum circuits composed solely of elementary quantum gates. This process is applied to all MCT gates. Finally, we combine all resulting quantum circuits into a single quantum circuit R, thus completing the process of decomposing MCT gates into pairs in the quantum circuit Q.

3 Experimental Results

We evaluated the proposed method by comparing the quantum cost of quantum circuits after applying both Kole's method and the proposed method to the same quantum circuits. In this experiment, we used the RevLib benchmark circuits. The experimental results of applying Kole's method and the proposed method to the benchmark circuits are shown in Table 1. The meaning of each item in this table is as follows:

- Benchmark
  - Circuit Name: The name of the RevLib benchmark circuit
  - Number of Gates: The number of MCT gates contained in the benchmark circuit before applying the methods
- Quantum Cost
  - Previous Method: The number of elementary quantum gates in the benchmark circuit after applying Kole's method
  - Proposed Method: The number of elementary quantum gates in the benchmark circuit after applying the proposed method
- Reduction Rate(%):$(1 - \frac{\text{Proposed Method}}{\text{Kole's Method}}) \times 100$

The experimental results indicate that we reduced more quantum gates in all benchmark circuits compared to the previous method. Therefore, decomposing two MCT gates as a pair when decomposing quantum circuits is effective in achieving quantum circuits with lower quantum cost.

Table 1: Comparison of quantum cost between the previous method and the proposed method

Benchmark		Quantum Cost		Reduction
Circuit Name	Number of Gates	Previous Method	Proposed Method	Rate (%)
dk27_225	24	226	180	20.3540
wim_266	25	199	133	33.1658
cu_219	40	1028	804	21.7899
z4_268	48	568	416	26.7606
cm150a_210	53	958	818	14.6138
dc2_222	75	1664	1156	30.5288
decod_217	80	1458	880	39.6433
apla_203	80	3096	2104	32.0413
root_255	99	2445	1713	29.9387
life_238	107	2959	2561	13.4505
9symml_195	129	3961	3493	11.8152
mlp4_245	131	3286	2434	25.9282
alu2_199	157	4319	3675	14.9109
clip_206	174	4973	3919	21.1945
dist_223	185	5378	3902	27.4451
sym10_262	194	7023	6271	10.7077
add6_196	229	5667	4219	25.5514
hwb8_114	614	9792	8398	14.2361
hwb8_113	637	11474	10158	11.4694
hwb9_119	1544	32021	28217	11.8797

References

[1] S. YAMASHITA, S.-i. MINATO, and D. M. MILLER. Ddmf: An efficient decision diagram structure for design verification of quantum circuits under a practical restriction. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E91-A, No. 12, p. 3793–3802, December 2008.

[2] D. Michael Miller, Robert Wille, and Zahra Sasanian. Elementary quantum gate realizations for multiple-control toffoli gates. In *2011 41st IEEE International Symposium on Multiple-Valued Logic*, pp. 288–293, 2011.

[3] Abhoy Kole and Kamalika Datta. Improved ncv gate realization of arbitrary size toffoli gates. In *2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems (VLSID)*, pp. 289–294, 2017.

[4] Sasanian Zahra and D. Michael Miller. Reversible and quantum circuit optimization: A functional approach. *Reversible Computation*, pp. 112–124, 2013.

[5] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Series A*, Vol. 400, No. 1818, pp. 97–117, July 1985.

[6] Ming-Cu Li and Ai-Xi Chen. Elementary quantum gates between long-distance qubits mediated by a resonator. *Information Processing*, Vol. 19, No. 10, p. 365, September 2020.

[7] Zhiqiang Li, Xiaoyu Song, Marek Perkowski, Hanwu Chen, and Xiaoxia Feng. Realization of a new permutative gate library using controlled-kth-root-of-NOT quantum gates for exact minimization of quantum circuits. *International Journal of Quantum Information*, Vol. 12, No. 5, p. 1450034, October 2014.

[8] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, Vol. 52, No. 5, p. 3457–3467, November 1995.

[9] R. Wille, D. Große, L. Teuber, G. W. Dueck, and R. Drechsler. RevLib: An online resource for reversible functions and reversible circuits. In *Int' l Symp. on Multi-Valued Logic*, pp. 220–225, 2008. RevLib is available at http://www.revlib.org.

Rydberg-EIT based electrometry in a vapor cell

In-Ho Bae[1] * Jisoo Hwang[1] Jae-Keun Yoo[1] Heejin Lim[2]

[1] *Division of Physical Metrology, Korea Research Institute of Standards and Science, Daejeon 34113, Korea*
[2] *Quantum Technology Institute, Korea Research Institute of Standards and Science, Daejeon 34113, Korea*

Abstract. We introduce Rydberg atom-based electromagnetically induced transparency (EIT) in a hot Rb vapor cell. Two external cavity diode lasers (ECDLs) resonating at lower transition and upper transition can be used as a probe and a coupling lasers, respectively. After adjusting the frequencies of the two ECDLs, highly excited Rydberg atomic states in the vapor cell can be constructed. We are developing an electrometer capable of RF-to-THz measurements using Rydberg atoms, and we will discuss its potential as a quantum electrometer.

Keywords: Rydberg atom, electromagnetically induced transparency, quantum electrometer

1 Introduction

In recent years, atomic electric field sensor based on the EIT effect is actively studied for potential applications in radio-frequency (RF) communications and THz imaging [1, 2, 3, 4, 5, 6, 7, 8, 9]. The concept of EIT sensor is quite different from that of a traditional electric field sensor, especially for the medium as a receiver. The EIT-based quantum sensor using highly excited Rydberg states is utilized as a quantum receiver, which can detect the incident RF field. This method can be achieved by forming a well-known ladder-type EIT scheme [1, 2].

Many outstanding achievements and progress have been reported in the field of communications [3, 4, 5, 6, 7, 8]. In particular, Rydberg atom-based quantum electric field sensor reveals a variety of applications such as electric field measurement standards [3], portable electric field sensor [4], phase measurements [5], angle-of-arrival (AOA) measurements [6], music recording [7], and even recently video streaming [8]. Electric field imaging is a research field that has begun to receive attention more recently [9].

Here we present theoretical calculations based on quantum defect theory, and experimental schematics of Rydberg-EIT. Additionally, we will discuss the quantum sensing applications using highly sensitivie electric field detection.

2 Schematics and Results

Figure 1 shows the (a) energy level diagram of Rydberg-EIT and (b) experimental schematic of Rydberg-EIT based on Rb vapor cell. The probe and coupling ECDLs propagate in the opposite direction to create ladder-type EIT. The atomic vapor cell prepared for the experiment was natural gas cells containing 72% and 28% of ^{85}Rb and ^{87}Rb, respectively. While performing the experiment, dichroic mirrors are used to couple and split the probe and the coupling ECDLs.

We performed theoretical calculation based on quantum defect theory, as shown in Fig. 2. A detailed explanation of the calculation can be found in the reference paper [10]. From the calculation, we confirmed that

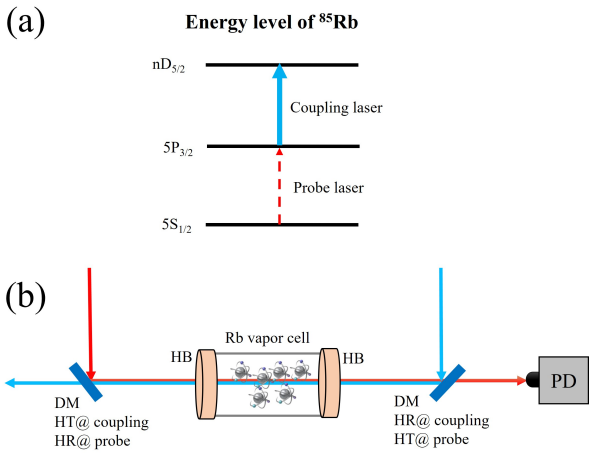


Figure 1: (a) Schematic diagram of the atomic system in the $5S_{1/2}$-$5P_{3/2}$-$nD_{5/2}$ transition of ^{85}Rb atom. (b) Simplified experimental setup for Rydberg-EIT in a Rb vapor cell. DM: dichroic mirror; HB: heating band; HR: High reflectance; HR: High transmittance.

the RF-to-THz frequencies with Rydberg state of ^{85}Rb are available from GHz to frequencies above 1 THz. As shown in the Fig. 2, although not all frequencies are continuous, a wide band can be covered depending on the quantum number.

Figure 3 shows the Rydberg-EIT signal resulted from the balaced detection, which allows removal of Doppler background noise. Upper spectrum is saturated absorption signal and lower spectrum is Doppler-free Rydberg-EIT spectrum based on balanced detection, respectively. Considering Doppler background noise, it can be expected that frequency calibration will be difficult without balanced measurement.

3 Discussions

In this paper, Rydberg-EIT based electrometer was introduced for future applicaions on the quantum electric field sensing. We reported the balanced signal of Rydberg-EIT with simple cancellation of Doppler background. From the calculation results based on quan-

*inhobae@kriss.re.kr

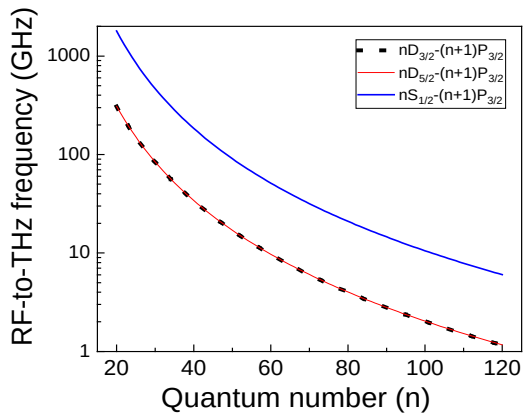


Figure 2: Theoretical calculations for estimating frequency of the RF-to-THz transitions as a function of principal quantum number n. We confirmed that the RF transitions with Rydberg state of atoms are available from GHz to frequencies above THz.

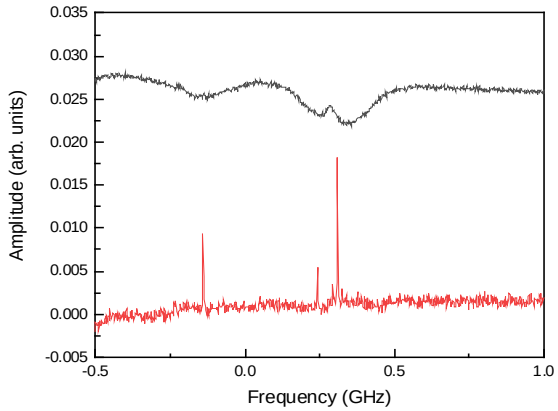


Figure 3: Rydberg-EIT signal resulted from the balanced detection.

tum defect theory, it was also suggested that measurements from RF to THz range can be achievable by using Rydberg-EIT system. We believe that atom-based electrometer will be a good candidate for solving antenna size problems depending on the frequency band. Additionally, because Rydberg-based sensor is known to have excellent sensitivity, it is expected that our system can be used in quantum sensor fields that require extreme sensitivity and broadband coverage.

4 Acknowledgement

This work was supported by Korea Research Institute for Defense Technology Planning and Advancement (KRIT) - Grant funded by Defense Acquisition Program Administration(DAPA) (22-405-A00-004).

References

[1] J. A. Sedlacek, A. Schwettmann, H. Kübler, R. Löw, T. Pfau and J. P. Shaffer Microwave electrometry with Rydberg atoms in a vapour cell using bright atomic resonances. *Nat. Phys.*, 8:819–824, 2012.

[2] J. A. Sedlacek, A. Schwettmann, H. Kübler, and J. P. Shaffer Atom-Based Vector Microwave Electrometry Using Rubidium Rydberg Atoms in a Vapor Cell. *Phys. Rev. Lett.*, 111(6):063001, 2013.

[3] C. L. Holloway, J. A. Gordon, S. Jefferts, A. Schwarzkopf, D. A. Anderson, S. A. Miller, N. Thaicharoen, G. Raithel Broadband Rydberg atom-based electric-field probe for SI-traceable, self-calibrated measurements. *IEEE Trans. Ant.*, 62(12):6169, 2014.

[4] Matt T. Simons, Joshua A. Gordon, and Christopher L. Holloway Fiber-coupled vapor cell for a portable Rydberg atom-based radio frequency electric field sensor. *Appl. Optics*, 57(22):6456–6460, 2018.

[5] M. T. Simons, A. H. Haddab, J. A. Gordon, C. L. Holloway A Rydberg atom-based mixer: measuring the phase of a radio frequency wave. *Appl. Phys. Lett.*, 114:114101, 2019.

[6] A. K. Robinson, N. Prajapati, D. Senic, M. T. Simons, and C. L. Holloway Determining the angle-of-arrival of a radio-frequency source with a Rydberg atom-based sensor. *Appl. Phys. Lett.*, 118(11):114001, 2021.

[7] C. L. Holloway, M. T. Simons, A. H. Haddab, C. J. Williams, and M. W. Holloway A real-time guitar recording using Rydberg atoms and electromagnetically induced transparency: quantum physics meets music. *AIP Adv.*, 9(6):065110, 2019.

[8] N. Prajapati, A. P. Rotunno, S. Berweger, M. T. Simons, A. B. Artusio-Glimpse, S. D. Voran, and C. L. Holloway TV and video game streaming with a quantum receiver: A study on a Rydberg atom-based receiver's bandwidth and reception clarity. *AVS Quantum Sci.*, 4:035001, 2022.

[9] L. A. Downes, A. R. MacKellar, D. J. Whiting, C. Bourgenot, C. S. Adams, and K. J. Weatherill Full-Field Terahertz Imaging at Kilohertz Frame Rates Using Atomic Vapor. *Phys. Rev. X*, 10(1):011027, 2020.

[10] M. Mack, F. Karlewski, H. Hattermann, S. Höckh, F. Jessen, D. Cano, and J. Fortágh Measurement of absolute transition frequencies of 87Rb to nS and nD Rydberg states by means of electromagnetically induced transparency. *Phys. Rev. A*, 83(5):052515, 2011.

Demonstration of Quantum Sparse Matrix Inversion based on Quantum Singular Value Transformation

Yasunori Lee[1] * Keita Kanno[1] Kenzo Makino[2] Hiroaki Murakami[2]

[1] *QunaSys Inc., 1-13-7 Hakusan, Bunkyo, Tokyo 113-0001 Japan*
[2] *Mitsubishi Electric Corp., 2-7-3 Marunouchi, Chiyoda, Tokyo 100-8310 Japan*

Abstract. Quantum singular value transformation (QSVT) is an ingenious quantum algorithm for (including but not limited to) matrix arithmetics. However, its *practical* power has not been assessed thoroughly to date due to its complexity. Here, we explicitly construct the full quantum circuit for the QSVT-based matrix inversion for simple examples and estimate the *actual* cost.

Keywords: fault-tolerant quantum computation (FTQC), block encoding, quantum singular value transformation (QSVT), matrix inversion

Quantum computers are expected to afford the performance of computational tasks which might be too expensive for classical computers. One of the leading candidates for such task is computations involving large matrices, especially sparse matrix inversion, whose wide range of application attest to their importance.

On one hand, there is a well-known algorithm of *Harrow-Hassidim-Lloyd* (HHL) [1] for this task which in theory runs exponentially faster (in terms of the matrix size) than any known classical algorithms. However, its actual implementation is difficult, if not impossible, since it requires

- exponentiation of the target matrix, which further relies on the use of black-box *oracles* encoding the information of the matrix, and
- a certain controlled-rotation gate inverting the eigenvalues of the target matrix,

whose gate-level implementations are rather subtle. On the other hand, a novel algorithm based on *block encoding* of the target matrix and *quantum singular value transformation* (QSVT) [2] has been proposed, but while it succeeds in circumventing the most of the subtleties encountered in the HHL algorithm, it still makes heavy use of oracles as black boxes, and the actual cost of the algorithm as a whole is somewhat obscured.

In this study, we take sparse Toeplitz matrices as the target matrix to be inverted, and explicitly construct the oracle quantum circuits for their block encoding based on [3]. By feeding the block-encoding unitary into the corresponding QSVT circuit, we estimate the quantum-computational costs of the matrix inversion including the number of necessary non-Clifford gates and the actual runtime, and thereby evaluate the feasibility and the exponential advantage over classical counterpart beyond the level of (asymptotic) query complexity.

$$A_{8\times 8} = \begin{pmatrix} 3 & 2 & 1 & 0 & \cdots & 0 \\ 4 & 3 & 2 & 1 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 1 \\ \vdots & & \ddots & \ddots & \ddots & 2 \\ 0 & \cdots & \cdots & 0 & 4 & 3 \end{pmatrix}$$

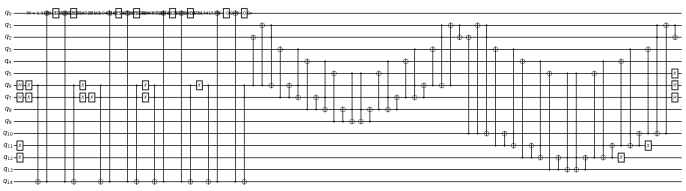


Figure 1: An example of a (sparse) Toeplitz matrix and its block-encoding unitary quantum circuit.

*lee.y@qunasys.com

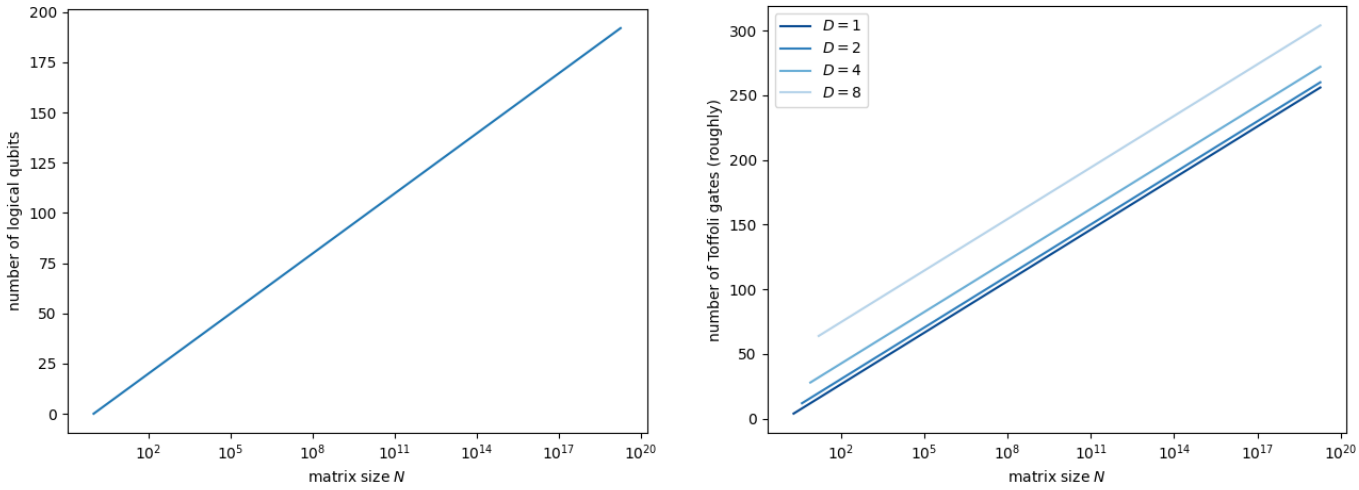


Figure 2: The numbers of logical qubits (left) and Toffoli gates (right) required to block-encode a generic Toeplitz matrix of size N and band-width D, on which the overall estimation of the cost is based.

References

[1] A. Harrow, A. Hassidim, S. Lloyd. *Quantum algorithm for solving linear systems of equations.* Physical Review Letter 103, 150502, 2009. arXiv:0811.3171 [quant-ph].

[2] A. Gilyén, Y. Su, G. H. Low, N. Wiebe. *Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics.* Proceedings of the 51st ACM STOC (2019) pp. 193-204, arXiv:1806.01838 [quant-ph].

[3] C. Sünderhauf, E. Campbell, J. Camps. *Block-encoding structured matrices for data input in quantum computing.* Quantum 8, 1226 (2024), arXiv:2302.10949 [quant-ph].

[4] K. Makino, H. Murakami, Y. Lee, K. Kanno, K. Minefuji, T. Fukuta. *Angle Finding of Quantum Signal Processing for Matrix Inversion.* To appear.

NNA Circuit Synthesis Method by SMT Solver Considering Bit Reduction

Tatsuya Nakao[1] * Shigeru Yamashita[1] † Kyouhei Seino[1] ‡

[1] *Graduate School of Information Science and Technology, Ritsumeikan University*

Abstract. When implementing quantum circuits on actual quantum computers, there exists a constraint known as the Nearest Neighbor Architecture (NNA) constraint. which states that CNOT gate can act only between neighboring quantum bits. Typically, quantum circuits are constructed ignoring NNA constraint and then converted into circuits that satisfy NNA constraint before execution on a quantum computer. However, the number of CNOT gates increases in most cases when a circuit is converted to satisfy NNA constraint, and the increase in the number of CNOT gates leads to an increase in the error rates, it is essential to convert circuits to satisfy NNA constraint while minimizing the increase of the number of CNOT gate. A quantum circuit that satisfies NNA constraint is called an NNA circuit. This paper describes about the constraint equations that the converted NNA circuit must satisfy are expressed as constraint represented as constraint equations given to an SMT solver. Following this, the more optimal NNA circuit is synthesized from the solution obtained from MT solver. This paper also introduces a method for converting larger-scale quantum circuits into NNA circuits.

Keywords: Nearest Neighbor Architecture (NNA) constraint, CNOT gate, SMT solver, necessary_set

1 Introduction

There exists a method proposed by Jingwen[1] et al. for converting quantum circuits to satisfy NNA constraint. In their approach, the quantum circuit is first divided at positions of T gates or H gates, extracting sub-circuits composed solely of multiple CNOT gates, as shown in Figure 1. Subsequently, for each sub-circuit, they generate a quantum circuit satisfying NNA constraint while maintaining equivalent outputs using an SMT solver. However, a significant issue arises with exponential increases in computation time when converting large-scale circuits using SMT solver.
Therefore, the proposed method aims to reduce both CNOT gates and computation time. To achieve this goal, two modifications are introduced. Firstly, since T gate desn't directly affect the observation result of quantum bit, during circuit dividing, the circuit is divided at positions of H gates, extracting sub-circuits composed of multiple CNOT gates and T gates, as shown in Figure SuggestSep. Secondly, select logic functions computable with combination of six or fewer quantum bits from necessary_set and find a circuit outputs their logic function using while satisfying NNA constraint using SMT solver. This secondly modification step is repeated until the converted circuit can compute all logic functions of necessary.

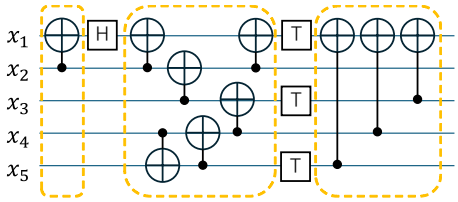


Figure 1: Circuit division by Jingwen's method

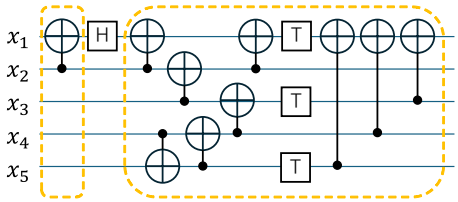


Figure 2: Circuit division by suggested method

2 Method

2.1 Variables on quantum circuit

During the conversion of quantum circuits, it is necessary to formulate the four constraint equations that the converted circuit must satisfy as an integer programming problem and input these constraint equations into an SMT solver. To achieve this, the following variables are introduced.

- $Necessary\_set_d$
- NNA_i
- $F_{i,j}$
- $f_{i,j}$

$Necessary\_set_d$ represents the set of logical functions output by the d-th quantum sub-circuit. In circuit conversion, it is essential that the outputs of the circuit before and after conversion are equal. Therefore, the outputs of the circuit before conversion are represented as a set called necessary_set. For example, in Figure 3, $necessary\_set$ is represented as $necessary\_set = \{x_1 \oplus x_3\}, \{x_2 \oplus x_3\}, \{x_3 \oplus x_5\}, \{x_5\}, \{x_4 \oplus x_5\}$.

NNA_i refer to the set of quantum bits are adjacents to q_i on quantum architecture. For example, in Figure 4, q_3

*eleven@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp
‡seino0702@gmail.com

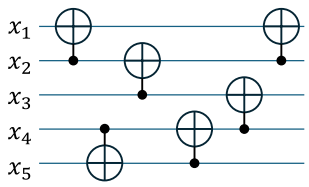


Figure 3: Sub-circuit constructed only CNOT gates

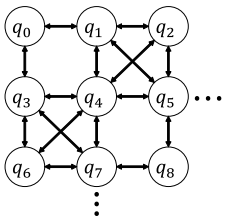


Figure 4: Quantum architecture

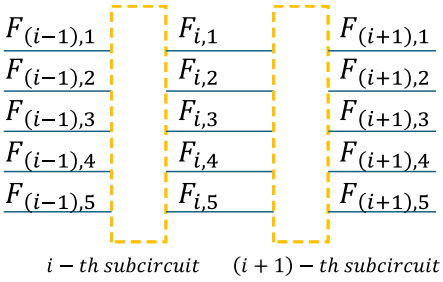


Figure 5: Relationships of logic functions between the sub-circuits

is adjacent to q_1, q_4, q_6 and q_7, so NNA_3 is represented as $NNA_3 = \{1, 4, 6, 7\}$.

The $F_{i,j}$ represents the output of each sub-circuit after dividing the entire circuit. An example is shown in Figure 5.

The $f_{i,j}$ refer to the transition of the state of each quantum bit within the sub-circuit. An example is shown in Figure 6.

2.2 Four constraint equations for the SMT solver

1 A single CNOT gate can be represented using two types of variables, $T_{i,j}$ and $C_{i,j}$. $T_{i,j}$ indicates whether the j-th quantum bit is treated as the target bit in the i-th CNOT gate. Similarly, $C_{i,j}$ indicates whether the j-th quantum bit is treated as the control bit in the i-th CNOT gate. As an example, the variables $T_{i,j}$ and $C_{i,j}$ in Figure 3 are shown as

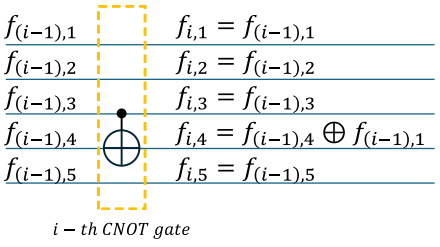


Figure 6: Transition about the state of quantum bits within the sub-circuits

Eq. 1 and Eq. 2 respectively.

$$C_{i,j} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{1}$$

$$T_{i,j} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{2}$$

Furthermore, using these variables, it is necessary to express with constraint equations that there is exactly one control bit and one target bit for each CNOT gate like Eq. 3 and Eq. 4.

$$\begin{aligned} &(C_{i,1} \wedge \neg C_{i,2} \wedge \cdots \wedge \neg C_{i,n}) \\ &\vee (\neg C_{i,1} \wedge C_{i,2} \wedge \cdots \wedge \neg C_{i,n}) \\ &\vee \cdots \vee (\neg C_{i,1} \wedge \neg C_{i,2} \wedge \cdots \wedge C_{i,n}) \end{aligned} \tag{3}$$

$$\begin{aligned} &(T_{i,1} \wedge \neg T_{i,2} \wedge \cdots \wedge \neg T_{i,n}) \\ &\vee (\neg T_{i,1} \wedge T_{i,2} \wedge \cdots \wedge \neg T_{i,n}) \\ &\vee \cdots \vee (\neg T_{i,1} \wedge \neg T_{i,2} \wedge \cdots \wedge T_{i,n}) \end{aligned} \tag{4}$$

2 In addition to the representation of CNOT gate described Eq. 3 and Eq. 4, it is necessary to have the constraint equation such that the quantum bit serving as the control bit and the quantum bit serving as the target bit are adjacent to each other. Therefore, create constraint equations about relationship between CNOT gate and quantum bit using NNA as shown in Eq. 5 and Eq. 6.

$$f_{CNOT}(i, j, k) = (C_{i,k} \wedge T_{i,j}) \wedge (j \neq k) \wedge k \in NNA_j \tag{5}$$

$$\bigwedge_{i=0}^{q} \bigwedge_{j=0}^{n} \bigwedge_{k=0}^{n} f_{i,j} = \begin{cases} F_{(d-1),j} & \text{if } (i = 0) \\ f_{(i-1),k} \oplus f_{(i-1),j} & \text{else if } f_{CNOT} \\ f_{(i-1),j} & \text{otherwise} \end{cases} \tag{6}$$

3 It is allowed that the positions of quantum bits for each logic functions output from the circuit before conversion are differ from the positions of each logic functions are outputted from circuit after conversion. Therefore, a constraint equation is required to ensure that the logic functions in necessary_set are reproduced somewhere within the converted circuit.

$$\bigwedge_{o \in necessary\_set_d} (o = f_{q,1}) \vee (o = f_{q,2}) \vee \cdots \vee (o = f_{q,n}) \tag{7}$$

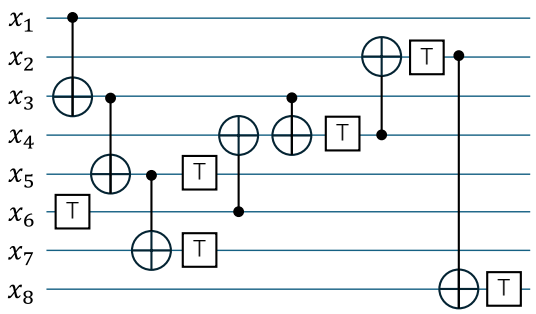


Figure 7: An 8 quantum bits circuit

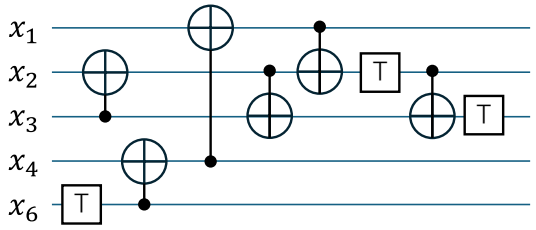


Figure 8: A converted circuit from the one as shown in Fig. 7

4 To avoid the situation where the logic functions cannot be reproduce in the subsequent sub-circuit that uses the outputs of current circuit, a constraint equation is needed such that all logic functions output from converted circuit are included from the output of sub-circuit before

$$\bigwedge_{i=0}^{n} F_{d,i} \in necessary\_set_d \tag{8}$$

3 Idea for reducing the number of quantum bits

There is a key issue with SMT solver is that converting circuits with 7 bits or more becomes infeasible within a realistic computation time. Therefore, we propose a method that focuses the logic functions computable with six or fewer quantum bits within sub-circuit and performs partial converting using SMT solver iteratively. This approach allows for the step-by-step conversion of the circuit while reduce the number of quantum bits used to SMT solver.

As an example, we apply and explain the proposed method to the quantum circuit shown in Figure 7. At the quantum circuit, necessary_set is $\{x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_6\}, \{x_1 \oplus x_3 \oplus x_4 \oplus x_6\}, \{x_1 \oplus x_3 \oplus x_5\}, \{x_6\}, \{x_1 \oplus x_3 \oplus x_5 \oplus x_7\}, \{x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_8\}$. The logic functions computable with six or fewer quantum bits in necessary_set is $\{x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_6\}, \{x_1 \oplus x_3 \oplus x_4 \oplus x_6\}, \{x_6\}$ The circuit converted by SMT solver to reproduce the set of these logical functions is shown in Figure 8.

As a result of recalculating the remaining necessary_set based on the output of this circuit, the updated necessary_set are $\{x_3 \oplus x_4 \oplus x_5\}, \{x_3 \oplus x_4 \oplus x_5 \oplus x_7\}\{x_2 \oplus x_8\}$, which can also be solved using SMT solver as partial quantum circuits with 7 bits or fewer.

The proposed method achieves an average reduction of 58.11

References

[1] Jingwen Ding and Shigeru Yamashita. Exact synthesis of nearest neighbor compliant quantum circuits in 2-d architecture and its application to large-scale circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(5):1045–1058, 2019.

[2] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[3] Gushu Li, Yufei Ding, and Yuan Xie. Tackling the qubit mapping problem for nisq-era quantum devices. In *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 1001–1014, 2019.

[4] Philipp Niemann, Chandan Bandyopadhyay, and Rolf Drechsler. Combining swaps and remote toffoli gates in the mapping to ibm qx architectures. In *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 200–205. IEEE, 2021.

[5] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[6] Soh Takehid, Mutsunori Banbara, Naoya Tamura, and Hidetomo Nabeshima. Recent trends and utilization techniques in sat solvers. *computer software*, 35(4):72–92, 2018.

[7] Robert Wille, Aaron Lye, and Rolf Drechsler. Optimal swap gate insertion for nearest neighbor quantum circuits. In *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 489–494. IEEE, 2014.

[8] Robert Wille, Nils Quetschlich, Yuma Inoue, Norihito Yasuda, and Shin-ichi Minato. Using dds for nearest neighbor optimization of quantum circuits. In *International Conference on Reversible Computation*, pages 181–196. Springer, 2016.

An Efficient Erasure Decoder and Quantum Multiplexing using Hypergraph Product Codes

Nicholas Connolly[1 2 *] Shin Nishio[3 1 4] Vivien Londe[5] Nicolò Lo Piparo[1]
William John Munro[1 4] Thomas Rowan Scruby[1] Anthony Leverrier[2]
Nicolas Delfosse[6 7] Kae Nemoto[1 4]

[1] *Okinawa Institute of Science and Technology Graduate University, Onna-son, Kunigami-gun, Okinawa, Japan*
[2] *INRIA, Paris, France*
[3] *SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan*
[4] *National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan*
[5] *Microsoft, Paris, France*
[6] *IonQ, College Park, Maryland, USA*
[7] *Microsoft Quantum, Redmond, Washington 98052, USA*

Abstract. We propose a decoder for the correction of erasure errors with hypergraph product (HGP) codes, a popular family of quantum low-density parity-check (LDPC) codes. Our simulations show that this decoder provides a close approximation of the maximum likelihood decoder that can be implemented in $O(N^2)$ bit operations where N is the length of the quantum code. We also consider a practical application of this decoder to quantum multiplexing using HGP codes. In multiplexed quantum communication, multiple qubits of information are encoded in a single photon. By adapting the qubit-photon assignment strategy to our new decoder, we show how physical resources can be reduced without sacrificing decoder performance.

Keywords: Quantum Error Correction, Erasure Channel, Decoder, Hypergraph Product Codes, LDPC Codes, Quantum Communication, Quantum Multiplexing

Introduction

Due to the high noise rate of quantum hardware, extensive quantum error correction is necessary to scale quantum devices into the regime of practical applications. The surface code [4, 6] is one of the most popular quantum error correcting codes for quantum computing architectures but it comes with an enormous qubit overhead because each qubit must be encoded into hundreds or thousands of physical qubits. Quantum Low-Density Parity-Check (LDPC) codes [7, 13] such as the hypergraph product (HGP) code [21] promise a significant reduction of this qubit overhead [8, 5]. Simulations with circuit noise show a 15× reduction of the qubit count in the large-scale regime [22].

Decoders are used to detect and correct errors in information transmission, but decoders must be fast for applications to utilize fault-tolerant quantum computation (FTQC). In this work, we propose an efficient decoding algorithm for the correction of erasure errors or detectable qubit loss in the special case of HGP codes. Decoding of erasures is practically relevant because this is the dominant source of noise in photonic systems, for which photon loss can be interpreted as an erasure, or neutral atoms [9, 1, 24]. Furthermore, in the classical case, many of the ideas that led to the design of capacity-achieving classical LDPC codes over binary symmetric channels were first discovered by studying the correction of erasures [11, 18].

To show a practical application of our new decoder, we consider a scenario involving quantum multiplexing [16, 15], which refers to the encoding of multiple qubits of information onto a single photon. A single photon has multiple degrees of freedom such as polarization [23], time bin [2, 14, 20], path (dual rail) [10], and frequency-bin [19, 17], each of which can be used to store quantum information. Although multiplexing can reduce the number of required physical resources, losing a single photon corresponds to the erasure of all encoded qubits. The choice of how qubits are assigned to photons has a large effect on the performance of quantum communication using multiplexing. In the case of HGP codes, our simulation results show that performance degradation due to multiplexing can be mitigated by using decoder-aware photon assignment strategies.

Erasure Channel and Peeling Decoder

Our erasure decoder for HGP codes is a generalization of a classical algorithm known as the *peeling decoder* [12]. To explain this algorithm, we briefly review the setting of the classical erasure channel. Recall that for a classical linear code of length n, information is transmitted via codewords with n bits. Erasure errors correspond to the loss of a known subset of bits in the transmitted codeword. An erasure correction problem can be converted into an error correction one by assigning the erased bits the values 0 and 1 at random, and then making a syndrome measurement. Unlike standard error correction, we make the additional assumption that non-erased bits do not have errors.

The peeling decoder [12] is a linear-time algorithm for correcting erasure errors in classical codes. To explain this algorithm, it is helpful to think of a code in terms of its *Tanner graph* $T(H)$: the bipartite graph obtained

*nicholas.connolly@oist.jp

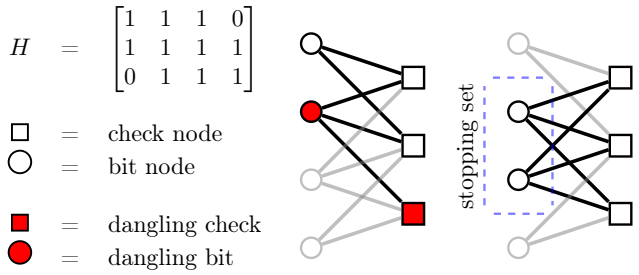


Figure 1: Two examples of an erasure-induced subgraph for a simple Tanner graph $T(H)$. Non-erased nodes are grayed-out and excluded from the subgraph.

using the parity check matrix H as an adjacency matrix. An erasure induces a subgraph of $T(H)$ corresponding to the subset of erased bit-nodes and any adjacent check-nodes (see Fig. 1). Check-nodes which have degree 1 in this subgraph are said to be *dangling checks*. The peeling algorithm identifies dangling checks in this subgraph and uses these to correct the adjacent *dangling bits*, hence "peeling" the erasure subgraph. The algorithm terminates either when all erasure errors have been corrected by peeling, or it becomes stuck in a *stopping set*: a subgraph with no remaining dangling checks.

Erasure correction for a quantum code is modeled similarly to the classical case, with an erasure error on a codeword corresponding to the loss of a known subset of qubits. As in the classical case, erasure correction can be converted into error correction, with the modified rule that erased qubits are assigned Pauli errors in $\{I, X, Y, Z\}$ at random in the quantum case. For a CSS code, errors can be corrected by applying the peeling algorithm two times, once using the classical Tanner graph for H_Z and once again for H_X.

Hypergraph Product Codes

We briefly review the construction for hypergraph graph product codes due to [21]. HGP codes are a special class of CSS code defined using any two classical linear codes. Given classical partiy check matrices H_1 and H_2, we may define the matrices H_X and H_Z of a CSS code via the formulas

$$H_X = (H_1 \otimes I | I \otimes H_2^T) \quad (1)$$
$$H_Z = (I \otimes H_2 | H_1^T \otimes I). \quad (2)$$

These matrices satisfy the condition $H_X H_Z^T = 0$ by construction and hence define a valid CSS code HGP(H_1, H_2). When H_1 and H_2 define LDPC codes, H_X and H_Z will also define LDPC codes.

HGP codes have a geometrically rich Tanner graph structure which can be visualized as the cartesian product of the Tanner graphs for the two input classical codes as shown in Fig. 2. The subgraph corresponding to each row and column in this Tanner graph block structure can be understood as the classical Tanner graph for one of the classical codes. As shown in the figure, the HGP Tanner graph can be divided into quadrants, each representing a different component of the code.

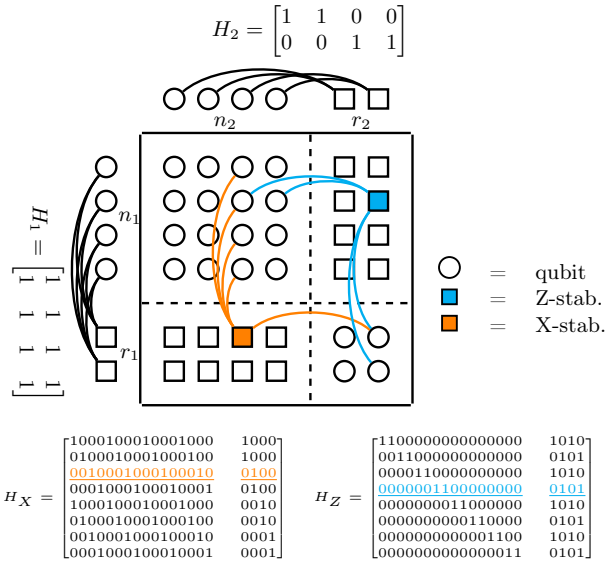


Figure 2: Example of the Tanner graph for a simple HGP code HGP(H_1, H_2) constructed from two classical codes with parity check matrices H_1 and H_2. This is the cartesian product of the two classical Tanner graphs.

Pruned Peeling + VH Decoder

Although the classical peeling decoder is not maximum-likelihood (ML), it is very efficient and works well for codes with sparse Tanner graphs such as LDPC codes. However, it performs very poorly when applied to quantum CSS codes, including LDPC codes. This is explained by the existence of stopping sets unique to quantum codes that have no classical analogue. Our proposed decoder [3] is a generalization of the classical peeling algorithm to HGP codes based on identifying and correcting the most common types of stopping sets.

A *stabilizer stopping set* occurs when the erasure pattern covers the qubit support of an X- or Z-type stabilizer. The *pruned peeling decoder* is a modified version of the classical decoder which attempts to fix these by removing a qubit from the erasure, thus "breaking" the stabilizer support and possibly allowing the peeling algorithm to become unstuck. This exploits a feature of stabilizer codes and can be applied to any CSS code.

Classical stopping sets are unique to HGP codes; these are patterns of erased qubits supported entirely on a single row or column in the HGP Tanner graph block structure of Fig. 2. Any stopping set for a HGP code can be decomposed into a union of components of this form. The *VH decoder* algorithm attempts to order and efficiently solve each of these classical stopping sets in sequence using Gaussian elimination. Although Gaussian elimination is too slow in general (cubic complexity), by restricting its application to classical stopping sets, the overall complexity of the VH decoder is quadratic in the code length. However, the decoder can still fail for certain configurations of classical stopping sets.

The decoder we propose for HGP codes in [3] combines all three techniques (peeling + pruned peeling + VH de-

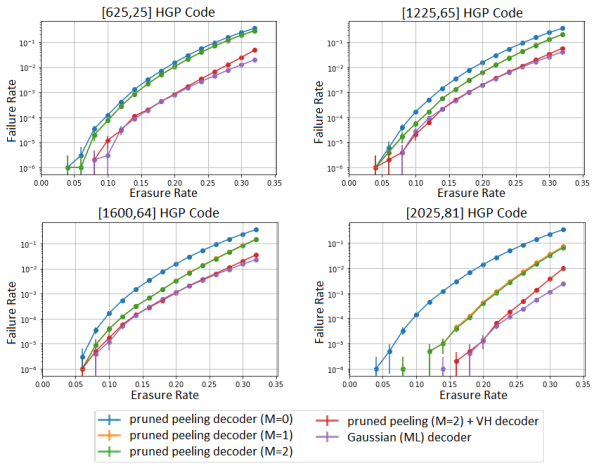


Figure 3: Numerical simulations showing the performance of the combined decoder for several HGP codes.

coder). Although not ML, the combined decoder shows close to ML performance at low erasure rate (see Fig. 3), making it useful in the regime of practical interest.

Application to Quantum Multiplexing

We conclude with an application showing how the pruned peeling + VH decoder can be used for multiplexed quantum communication [15]. We assume a photonic system, wherein each photon encodes m qubits of information; $m = 1$ corresponds to no-multiplexing. Hence, the loss of a single photon corresponds to the simultaneous erasure of m qubits. The choice of how physical qubits are assigned to photons thus introduces a correlation in the types of erasure errors. This correlation can have a significant effect on the decoding performance, motivating our search for good assignment strategies adapted to the decoder.

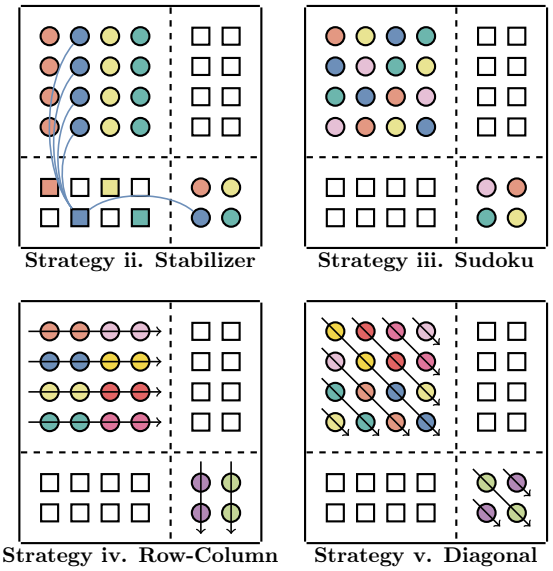


Table 1: Examples of four different photon assignment strategies for the simple HGP code shown in Fig. 2.

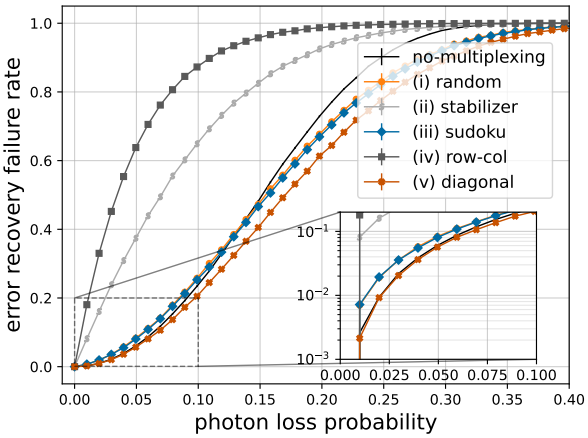


Figure 4: Multiplexing decoder performance for a ⟦320,82⟧ HGP code at fixed $m = 8$. In this example, strategy (v) diagonal outperforms all other strategies.

We introduce a number of strategies for assigning to photons groups of m qubits in a HGP code.

i. **Random:** qubits assigned to photons at random.

ii. **Stabilizer:** photons correspond to the qubit-support of X and Z-type stabilizer generators.

iii. **Sudoku:** qubits of a given photon come from different rows or columns in the Tanner graph.

iv. **Row-Column:** qubits of a given photon come from the same row or column in the Tanner graph.

v. **Diagonal:** qubits of a given photon come from the same diagonal slice in the Tanner graph.

The first strategy is independent of the choice of code or decoder, but the remaining four are designed with the pruned peeling + VH decoder in mind and are summarized in visually in Table 1. Strategy ii. seeks to create stabilizer stopping sets, which are fixed by pruned peeling. Strategies iii. and v. seek to minimize classical stopping sets and hence decoder failures. Strategy iv. does the opposite, maximizing classical stopping sets, which can be thought of as a worst case scenario.

Fig. 4 shows our numerical simulations using each of these five strategies with a fixed HGP code. A strategy is considered good if its performance is close to the no-multiplexing case. Our results show that a decoder-aware strategy can even outperform the no-multiplexing case.

The speed-up gained by our proposed decoder can offset new errors that might arise with a slower ML decoder. In addition to achieving close to optimal performance with reduced complexity, our simulations show how the performance of the pruned peeling + VH decoder can be further improved through the use of quantum multiplexing. Furthermore, given the practical information throughput advantage that HGP codes have over surface codes, our new efficient decoder is a significant result.

References

[1] S. Bartolucci, P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, et al. Fusion-based quantum computation. *arXiv preprint arXiv:2101.09310*, 2021.

[2] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594, 1999.

[3] N. Connolly, V. Londe, A. Leverrier, and N. Delfosse. Fast erasure decoder for a class of quantum ldpc codes. *arXiv preprint arXiv:2208.01002*, 2022.

[4] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.

[5] 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)*, pages 743–754. IEEE, 2018.

[6] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3):032324, 2012.

[7] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962.

[8] D. Gottesman. Fault-tolerant quantum computation with constant overhead. *Quantum Information & Computation*, 14(15-16):1338–1372, 2014.

[9] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816):46–52, 2001.

[10] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of modern physics*, 79(1):135, 2007.

[11] S. Kudekar, T. Richardson, and R. L. Urbanke. Spatially coupled ensembles universally achieve capacity under belief propagation. *IEEE Transactions on Information Theory*, 59(12):7761–7813, 2013.

[12] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Efficient erasure correcting codes. *IEEE Transactions on Information Theory*, 47(2):569–584, 2001.

[13] D. J. MacKay, G. Mitchison, and P. L. McFadden. Sparse-graph codes for quantum error correction. *IEEE Transactions on Information Theory*, 50(10):2315–2330, 2004.

[14] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin. Femtosecond time-bin entangled qubits for quantum communication. *arXiv preprint quant-ph/0205144*, 2002.

[15] S. Nishio, N. Connolly, N. L. Piparo, W. J. Munro, T. R. Scruby, and K. Nemoto. Multiplexed quantum communication with surface and hypergraph product codes. *arXiv preprint quant-ph arXiv:2406.08832*, 2024.

[16] N. L. Piparo, W. J. Munro, and K. Nemoto. Quantum multiplexing. *Physical Review A*, 99(2):022337, 2019.

[17] S. Ramelow, L. Ratschbacher, A. Fedrizzi, N. Langford, and A. Zeilinger. Discrete tunable color entanglement. *Physical review letters*, 103(25):253601, 2009.

[18] T. Richardson and R. Urbanke. *Modern coding theory*. Cambridge university press, 2008.

[19] Y. Shih and A. Sergienko. Observation of quantum beating in a simple beam-splitting experiment: Two-particle entanglement in spin and space-time. *Physical Review A*, 50(3):2564, 1994.

[20] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Physical Review A*, 66(6):062304, 2002.

[21] J.-P. Tillich and G. Zémor. Quantum ldpc codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2013.

[22] M. A. Tremblay, N. Delfosse, and M. E. Beverland. Constant-overhead quantum error correction with thin planar connectivity. *arXiv preprint arXiv:2109.14609*, 2021.

[23] A. B. U'Ren, K. Banaszek, and I. A. Walmsley. Photon engineering for quantum information processing. *arXiv preprint quant-ph/0305192*, 2003.

[24] Y. Wu, S. Kolkowitz, S. Puri, and J. D. Thompson. Erasure conversion for fault-tolerant quantum computing in alkaline earth rydberg atom arrays. *arXiv preprint arXiv:2201.03540*, 2022.

Fast erasure decoder for a class of quantum LDPC codes

Nicholas Connolly,[1] Vivien Londe,[2] Anthony Leverrier,[1] and Nicolas Delfosse[3]
[1] *Inria, Paris, France*
[2] *Microsoft, Paris, France*
[3] *Microsoft Quantum, Redmond, Washington 98052, USA*
(Dated: March 8, 2023)

We propose a decoder for the correction of erasures with hypergraph product codes, which form one of the most popular families of quantum LDPC codes. Our numerical simulations show that this decoder provides a close approximation of the maximum likelihood decoder that can be implemented in $O(N^2)$ bit operations where N is the length of the quantum code. A probabilistic version of this decoder can be implemented in $O(N^{1.5})$ bit operations.

Introduction – Due to the high noise rate of quantum hardware, extensive quantum error correction is necessary to scale quantum devices to the regime of practical applications. The surface code [1, 2] is one of the most popular quantum error correction code for quantum computing architectures but it comes with an enormous qubit overhead because each qubit must be encoded into hundreds or thousands of physical qubits.

Quantum Low-Density Parity-Check (LDPC) codes [3, 4] such as hypergraph product (HGP) codes [5] promise a significant reduction of this qubit overhead [6, 7]. Numerical simulations with circuit noise show a 15× reduction of the qubit count in the large-scale regime [8]. For applications to quantum fault toleance, HGP codes must come with a *fast* decoder, whose role is to identify which error occurred. In this work, we propose a fast decoder for the correction of erasures or qubit loss. Our numerical simulations show that our decoder achieves a logical error rate close to the maximum likelihood decoder.

Our motivation for focusing on the decoding of erasures is twofold. First it is practically relevant and it is the dominant source of noise in some quantum platforms such as photonic systems [9, 10] for which a photon loss can be interpreted as an erasure, or neutral atoms [11]. Second, many of the ideas that led to the design of capacity-achieving classical LDPC codes over binary symmetric channels were first discovered by studying the correction of erasures [12, 13].

Classical erasure decoders – A linear code with length n is defined to be the kernel $C = \ker H$ of an $r \times n$ binary matrix H called the *parity-check matrix*. Our goal is to protect a *codeword* $x \in C$ against erasures. We assume that each bit is erased independently with probability p and erased bits are flipped independently with probability 1/2. The set of erased positions is known and is given by an *erasure vector* $\varepsilon \in \mathbb{Z}_2^n$ such that bit b_i is erased iff $\varepsilon_i = 1$. The initial codeword x is mapped onto a vector $y = x + e \in \mathbb{Z}_2^n$ where e is the indicator vector of the flipped bits of x. In particular the support of e satisfies $\mathrm{supp}(e) \subseteq \mathrm{supp}(\varepsilon)$. To detect e, we compute the *syndrome* $s = Hy = He \in \mathbb{Z}_2^r$. A non-trivial syndrome indicates the presence of bit-flips.

The goal of the decoder is to provide an estimation $\hat{e}$ of e given s and ε and it succeeds if $\hat{e} = e$. This can be done by solving the linear system $H\hat{e} = s$ with the condition $\mathrm{supp}(\hat{e}) \subseteq \mathrm{supp}(\varepsilon)$ thanks to Gaussian elimination. This *Gaussian decoder* runs in $O(n^3)$ bit operations which may be too slow in practice for large n.

Algorithm 1: Classical peeling decoder

input : An erasure vector $\varepsilon \in \mathbb{Z}_2^N$ and a syndrome $s \in \mathbb{Z}_2^r$.
output: Either **failure** or $\hat{e} \in \mathbb{Z}_2^n$ such that $H\hat{e} = s$ and $\mathrm{supp}(\hat{e}) \subseteq \mathrm{supp}(\varepsilon)$.

```
Set ê = 0.
while there exists a dangling check do
    Select a dangling check c_i.
    Let b_j be the dangling bit incident to c_i.
    if s_i = 1 then
        Flip bit j of ê.
        Flip s_k for all checks c_k incident with b_j.
    Set ε_j = 0.
if ε ≠ 0 return Failure, else return ê.
```

The classical peeling decoder [14], described in Algorithm 1, provides a fast alternative to the Gaussian decoder. It does not perform as well in general, but it can be implemented in linear time and displays good performance for LDPC codes. To describe this decoder, it is convenient to introduce the *Tanner graph*, denoted $T(H)$, of the linear code $C = \ker H$. It is the bipartite graph with one vertex $c_1, \ldots, c_r$ for each row of H and one vertex $b_1, \ldots, b_n$ for each column of H such that c_i and b_j are connected iff $H_{i,j} = 1$. We refer to c_i as a *check node* and b_j as a *bit node*. The codewords of C are the bit strings such that the sum of the neighboring bits of a check node is 0 mod 2. Given an erasure vector ε, a check node is said to be a *dangling check* if it is incident to a single erased bit. We refer to this erased bit as a *dangling bit*. The basic idea of the peeling decoder is to use dangling checks to recover the values of dangling bits and to repeat until the erasure is fully corrected.

The notion of stopping set was introduced in [15] to bound the failure probability of the decoder for classical

LDPC codes. A *stopping set* for the Tanner graph $T(H)$ is defined to be a subset of bits that contains no dangling bit. If the erasure covers a non-empty stopping set, then Algorithm 1 returns **Failure**.

The peeling decoder was adapted to surface code [16] and color codes [17]. In the rest of this paper, we design a fast erasure decoder inspired by the peeling decoder that applies to a broad class of quantum LDPC codes. Our design process relies on the analysis of stopping sets. At each design iteration, we propose a new version of the decoder, identify its most common stopping sets and modify the decoder to make it capable of correcting these dominant stopping sets.

Classical peeling decoder for quantum CSS codes – A CSS code [18, 19] with length N is defined by commuting N-qubit Pauli operators $S_{X,1}, \ldots, S_{X,R_X} \in \{I, X\}^{\otimes N}$ and $S_{Z,1}, \ldots, S_{Z,R_Z} \in \{I, Z\}^{\otimes N}$ called the *stabilizer generators*. We refer to the group they generate as the *stabilizer group* and its elements are called *stabilizers*.

We can correct X and Z errors independently with the same strategy. Therefore we focus on the correction of X errors, based on the measurement of the Z-type stabilizer generators. This produces a *syndrome* $\sigma(E) \in \mathbb{Z}_2^{R_Z}$, whose i^{th} component is 1 iff the error E anti-commutes with $S_{Z,i}$. An error with trivial syndrome is called a *logical error* and a *non-trivial logical error* if it is not a stabilizer, up to a phase.

We assume that qubits are erased independently with probability p and that an erased qubit suffers from a uniform error I or X [20]. This results in an X-type error E such that $\text{supp}(E) \subseteq \text{supp}(\varepsilon)$. The decoder returns an estimate $\hat{E}$ of E given the erasure vector ε and the syndrome s of E. It succeeds iff $\hat{E}E$ is a stabilizer (up to a phase). The *logical error rate* of the scheme, denoted $P_{\log}(p)$, is the probability that $\hat{E}E$ is a non-trivial logical error.

By mapping Pauli operators onto binary strings, one can cast the CSS erasure decoding problem as the decoding problem of a classical code with parity check matrix $\mathbf{H}_Z$ whose rows correspond to the Z-type stabilizer generators. As a result, one can directly apply the classical Gaussian decoder and the classical peeling decoder to CSS codes. From Lemma 1 of [16], the Gaussian decoder is an optimal decoder, *i.e.* a Maximum Likelihood (ML) decoder, but its complexity scaling like $O(N^3)$ makes it too slow for large codes. The peeling decoder is faster. However, the following lemma proves that, unlike its classical counterpart, it does not perform well for quantum LDPC codes.

Lemma 1 (Stabilizer stopping sets)**.** The support of an X-type stabilizer is a stopping set for the Tanner graph $T(\mathbf{H}_Z)$.

Proof. This is because an X-type stabilizer commutes with Z-type generators, and therefore its binary representation is a codeword for the classical linear code $\ker \mathbf{H}_Z$. □

As a consequence, the classical peeling decoder has no threshold for any family of quantum LDPC codes defined by bounded weight stabilizers. Indeed, if each member of the family has at least one X-type stabilizer with weight w, then the logical error rate satisfies $P_{\log}(p) \geq p^w$, which is a constant bounded away from zero when $N \to \infty$.This is in sharp contrast with the classical case for which the probability to encounter a stopping set provably vanishes for carefully designed families of LDPC codes [21].

Pruned peeling decoder – Since the peeling decoder gets stuck into stopping sets induced by the X-type generators, the idea is to look for such a generator S supported entirely within the erasure and to remove an arbitrary qubit of the support of S from the erasure. We can remove this qubit from the erasure because either the error E or its equivalent error ES (also supported inside ε) acts trivially on this qubit.

Algorithm 2: Pruned peeling decoder

input : An erasure vector $\varepsilon \in \mathbb{Z}_2^N$, a syndrome $s \in \mathbb{Z}_2^{R_Z}$, and an integer M.
output: Either **Failure** or an X-type error $\hat{E} \in \{I, X\}^N$ such that $\sigma(\hat{E}) = s$ and $\text{supp}(\hat{E}) \subseteq \text{supp}(\varepsilon)$.

Set $\hat{E} = I$.
while *there exists a dangling generator* **do**
  Select a dangling generator $S_{Z,i}$.
  Let j be the dangling qubit incident to $S_{Z,i}$.
  if $s_i = 1$ **then**
    Replace $\hat{E}$ by $\hat{E}X_j$ and s by $s + \sigma(X_j)$.
  Set $\varepsilon_j = 0$.
  if *There is no dangling generator and there exists a product S of up to M stabilizer generators $S_{X,1}, \ldots, S_{X,R_X}$ such that* $\text{supp}(S) \subseteq \text{supp}(\varepsilon)$ **then**
    Select a qubit $j \in \text{supp}(S)$ and set $\varepsilon_j = 0$.
if $\varepsilon \neq 0$ **return Failure**, **else return** $\hat{E}$.

This leads to the pruned peeling decoder described in Algorithm 2. To make it easier to follow, we use the terms *dangling generator* and *dangling qubit* in place of dangling check and dangling bit. A dangling generator is a Z generator in the context of correcting X errors. In order to keep the complexity of the peeling decoder linear, we look for an X-type stabilizer which is a product of up to up M stabilizer generators where M is a small constant. For low erasure rate, we expect the erased stabilizers to have small weight and therefore a small value of M should be sufficient.

Fig. 1 shows the performance of HGP codes equipped with the pruned peeling decoder with $M = 0, 1, 2$. The pruning strategy only slightly improves over the classical peeling decoder and increasing M beyond $M = 1$ does not significantly affect the performance. To understand why the ML decoder severely outperforms the pruned

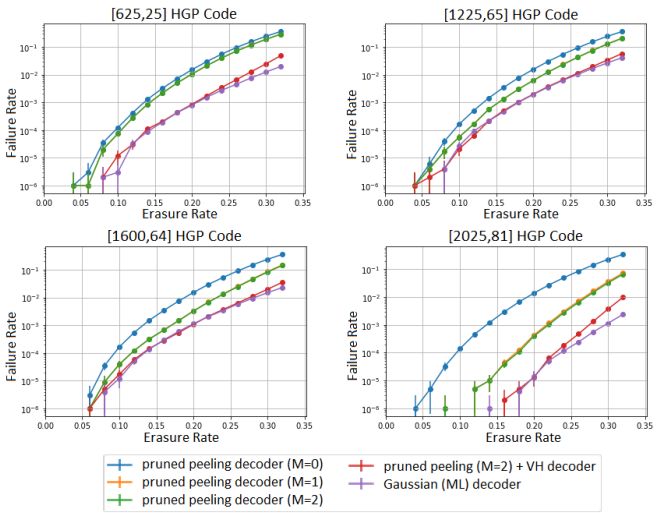


Figure 1. Performance of the pruned peeling and VH decoders using four HGP codes and compared with the ML decoder (10^6 simulations per data point). Plots show the failure rates of the decoders for recovering an X-type Pauli error supported on the erasure vector, up to multiplication by a stabilizer.

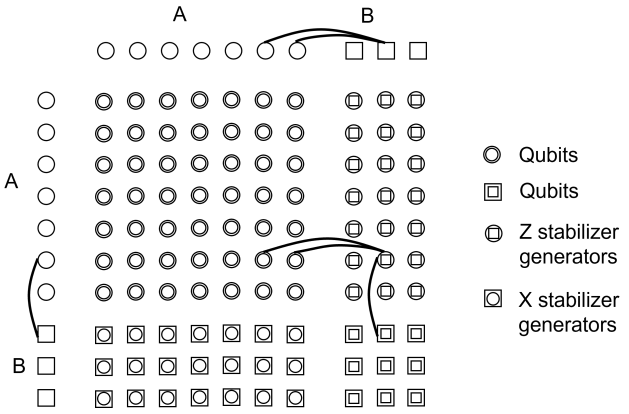


Figure 2. The HGP code derived from a linear code with 7 bits and 3 checks. The support of the Z stabilizer generator with index $(b, a') \in B \times A$ is given by the neighbors of (b, a') in the Cartesian product of the graph $T(H)$ with itself. In the product notation, we follow the $x \times y$ convention, where the first coordinate denotes the horizontal code and the second coordinate denotes the vertical code.

peeling decoder, we analyze its most common stopping sets with HGP codes.

Stopping sets of the pruned peeling decoder – Let us recall the hypergraph product construction from [5]. The HGP code associated with the Tanner graph $T(H) = (A \cup B, E_H)$ of a classical code is a CSS code, denoted HGP(H), defined from the cartesian product of $T(H)$ with itself (see Fig. 2). Qubits are labelled by the pairs $(a, a') \in A \times A$ and $(b, b') \in B \times B$. For each $(a, b') \in A \times B$, we define a stabilizer generator acting as X on the qubits (b, b') such that $\{a, b\} \in E_H$ and the qubits (a, a') such that $\{a', b'\} \in E_H$. For each $(b, a') \in B \times A$, we define a stabilizer generator acting as Z on the qubits (a, a') such that $\{a, b\} \in E_H$ and the qubits (b, b') such that $\{a', b'\} \in E_H$. If the input graph $T(H)$ is sparse, then HGP(H) is LDPC.

The input Tanner graph is generated using the standard progressive edge growth algorithm which is commonly used to produce good classical or quantum LDPC codes [22]. We use the implementation [23, 24] of the progressive edge growth algorithm.

By studying the failure configurations of the pruned peeling decoder, we observe that the gap between the pruned peeling decoder and the ML decoder is due to the following stopping sets of HGP codes.

Lemma 2 (Horizontal and vertical stopping sets)**.** If S_B is a stopping set for a Tanner graph $T(H)$, then for all $b \in B$ the set $\{b\} \times S_B$ is a stopping set for the Tanner graph $T(\mathbf{H}_Z)$ of the HGP code HGP(H). If S_A is a stopping set for a Tanner graph $T(H^T)$, then for all $a' \in A$ the set $S_A \times \{a'\}$ is a stopping set for the Tanner graph $T(\mathbf{H}_Z)$ of the HGP code HGP(H).

Proof. Consider a stopping set S_B for $T(H)$. Any Z-type stabilizer generator acting on $\{b\} \times S_B$ must be indexed by (b, a') for some a'. Moreover, the restriction of these stabilizers to $\{b\} \times S_B$ are checks for the linear code $\ker H$. Therefore is $\{b\} \times S_B$ is a stopping set for $T(\mathbf{H}_Z)$. The second case is similar. □

We refer to the stopping sets $\{b\} \times S_B$ as *vertical stopping sets* and $S_A \times \{a'\}$ are *horizontal stopping sets*. Numerically, we observe that these stopping sets are responsible for vast majority of the failures of the pruned peeling decoder. This is because the quantum Tanner graph $T(\mathbf{H}_Z)$ contains on the order of $\sqrt{N}$ copies of the type $\{b\} \times S_B$ for each stopping sets S_B of $T(H)$ and $\sqrt{N}$ copies of each stopping set of $T(H^T)$. Our idea is to use the Gaussian decoders of the classical codes $\ker H$ and $\ker H^T$ to correct these stopping sets.

VH decoder – The Vertical-Horizontal (VH) decoder is based on the decomposition of the erasure into vertical subsets of the form $\{b\} \times \varepsilon_b$ with $b \in B$ and $\varepsilon_b \subseteq B$, and horizontal subsets of the form $\varepsilon_{a'} \times \{a'\}$ with $a' \in A$ and $\varepsilon_{a'} \subseteq A$, that will be decoded using the Gaussian decoder.

Let T_v (resp. T_h) be the subgraph of $T(\mathbf{H}_Z)$ induced by the vertices of $B \times (A \cup B)$ (resp. $(A \cup B) \times A$). The graph T_v is made with the vertical edges of $T(\mathbf{H}_Z)$ and T_h is made with its horizontal edges. Given an erasure vector ε, denote by $V(\varepsilon)$ the set of vertices of $T(\mathbf{H}_Z)$ that are either erased qubits or check nodes incident to an erased qubit. A *vertical cluster* (resp. *horizontal cluster*) is a subset of $V(\varepsilon)$ that is a connected component for the graph T_v (resp. T_h).

The *VH graph* of ε is defined to be the graph whose vertices are the clusters and two clusters are connected iff their intersection is non-empty.

The following proposition provides some insights on the structure of the VH graph.

Proposition 1. The VH graph is a bipartite graph where each edge connects a vertical cluster with an horizontal cluster. There is a one-to-one correspondence between the check nodes of $T(\mathbf{H}_Z)$ that belong to one vertical cluster and one horizontal cluster and the edges of the VH graph.

Proof. Because the graph T_v contains only vertical edges, any vertical cluster must be a subset of $\{b_1\} \times (A \cup B)$ for some $b_1 \in B$. Similarly, any horizontal cluster is a subset of $(A \cup B) \times \{a'_1\}$ for some $a'_1 \in A$. As a result, two clusters with the same orientation (horizontal or vertical) cannot intersect and the only possible intersection between a cluster included in $\{b_1\} \times (A \cup B)$ and a cluster included in $(A \cup B) \times \{a'_1\}$ is the check node (b_1, a'_1). The bijection between check nodes and edges of the VH graph follows. □

A check node of $T(\mathbf{H}_Z)$ that belongs to a single cluster is called an *internal check*, otherwise it is called a *connecting check*. From Proposition 1, a connecting check must belong to one horizontal and one vertical cluster.

Given a cluster κ, let $E(\kappa)$ be the set of errors supported on the qubits of κ whose syndrome is trivial over the internal checks of κ. Let $S(\kappa)$ be the set of syndromes of errors $E \in E(\kappa)$ restricted to the connecting checks of κ. A cluster is said to be *isolated* if is has no connecting check. Then, it can be corrected independently of the other clusters. A *dangling cluster* is defined to be a cluster with a single connecting check.

A cluster κ can have two types of connecting check. If $S(\kappa)$ contains a weight-one vector supported on an connecting check c, we say that c is a *free check*. Otherwise, it is a *frozen check*. If a check is free, the value of the syndrome on this check can be adjusted at the end of the procedure to match s using an error included in the cluster κ.

To compute a correction $\hat{E}$ for a syndrome $s \in \mathbb{Z}_2^{R_Z}$, we proceed as follows. Denote by s_κ the restriction of s to a cluster κ. We initialize $\hat{E} = I$ and we consider three cases.

Case 1: Isolated cluster. If κ is a isolated cluster, we use Gaussian elimination to find an error $\hat{E}_\kappa$ supported on the qubits of κ whose syndrome matches s on the internal checks of κ. Then, we add $\hat{E}_\kappa$ to $\hat{E}$, we add $\sigma(\hat{E}_\kappa)$ to s and we remove κ from the erasure ε. This cluster can be corrected independently of the other cluster because it is not connected to any other cluster.

Case 2: Frozen dangling cluster. If κ is a dangling cluster and its only connecting check is frozen, we proceed exactly as in the case of an isolated cluster. This is possible because any correction has the same contribution to the syndrome on the connecting check.

Case 3: Free dangling cluster. The correction of a dangling cluster κ that contains a free check is delayed until the end of the procedure. We remove κ from the erasure and we remove its free check from the Tanner graph $T(\mathbf{H}_Z)$. Then, we look for a correction $\hat{E}'$ in the remaining erasure. We add $\hat{E}'$ to $\hat{E}$ and $\sigma(\hat{E}')$ to s. Once the remaining erasure is corrected and the syndrome is updated, we find a correction $\hat{E}_\kappa$ inside κ that satisfies the remaining syndrome s_κ in κ. We proceed in that order because the value of the syndrome on a free check can be adjusted at the end of the procedure to match s using an error included in the cluster κ (by definition of free checks).

Altogether, we obtain the VH decoder (Algorithm 3). Our implementation is available here [25]. It works by correcting all isolated and dangling clusters until the erasure is fully corrected. Otherwise, it returns **Failure**.

Algorithm 3: VH decoder

input : An erasure vector $\varepsilon \in \mathbb{Z}_2^N$, a syndrome $s \in \mathbb{Z}_2^{R_Z}$.
output: Either **Failure** or an X-type error $\hat{E} \in \{I, X\}^N$ such that $\sigma(\hat{E}) = s$ and $\mathrm{supp}(\hat{E}) \subseteq \mathrm{supp}(\varepsilon)$.

Set $\hat{E} = I$.
Construct an empty stack $L = []$.
while *there exists an isolated or a dangling cluster* κ **do**
  if κ *is isolated or frozen* **then**
    Compute an error $\hat{E}_\kappa$ supported on κ whose syndrome matches s on the internal checks of κ in $T(\mathbf{H}_Z)$.
    Replace $\hat{E}$ by $\hat{E}\hat{E}_\kappa$ and s by $s + \sigma(\hat{E}_\kappa)$.
    For all qubits j in κ, set $\varepsilon_j = 0$.
  else
    Then κ is free.
    Remove the free connecting check c of κ from the Tanner graph $T(\mathbf{H}_Z)$.
    Add the pair (κ, c) to the stack L.
    For all qubits j in κ, set $\varepsilon_j = 0$.
while *the stack* L *is non-empty* **do**
  Pop a cluster (κ, c) from the stack L.
  Add the check node c to the Tanner graph $T(\mathbf{H}_Z)$.
  Compute an error $\hat{E}_\kappa$ supported on κ whose syndrome matches s on all the checks of κ in $T(\mathbf{H}_Z)$, including the free check c.
  Replace $\hat{E}$ by $\hat{E}\hat{E}_\kappa$ and s by $s + \sigma(\hat{E}_\kappa)$.
if $\varepsilon \neq 0$ **return Failure**, **else return** $\hat{E}$.

For a $r \times n$ matrix H, the complexity of the VH decoder is dominated by the cost of the Gaussian decoder which grows as $O(n^3)$ per cluster and $O(n^4)$ including all the clusters (assuming $r = O(n)$). Therefore the VH decoder can be implemented in $O(N^2)$ bit operations where

$N = \Theta(n^2)$ is the length of the quantum HGP code. Using a probabilistic implementation of the Gaussian decoder [26–29], we can implement the Gaussian decoder in $O(n^2)$ operations, reducing the complexity of the VH decoder to $O(N^{1.5})$.

Algorithm 3 fails if the VH-graph of the erasure contains a cycle. However, one can modify the algorithm to eliminate some cycles by removing free checks of all clusters and not only dangling clusters. This may improve further the performance of the VH-decoder.

In comparison with our numerical results from Fig. 1, we see that the combination of pruned peeling and VH decoders performs almost as well as the ML decoder at low erasure erasure rates. This is to say that cycles of clusters, which are stopping sets for the VH decoder, are relatively infrequent in the low erasure rate regime. This behavior matches our intuition since errors for LDPC codes tend to be composed of disjoint small weight clusters [30].

Conclusion – We proposed a practical high-performance decoder for the correction of erasure with HGP codes. Our numerical simulations show that the combination of the pruned peeling decoder with the VH decoder achieves a close-to-optimal performance in complexity $O(N^2)$. This decoder can be used as a subroutine of the Union-Find decoder for LDPC codes [31] to speed up this algorithm.

In future work, it would be interesting to adapt our decoder to other quantum LDPC codes [32–35]. We are also wondering if one can reduce the complexity further to obtain a linear time ML decoder for the correction of erasure.

Finally, it would be interesting to investigate the resource overhead of quantum computing architectures capable of detecting erasures based on neutral atoms [11], trapped ions [36] or superconducting qubits [37].

This research was supported by the MSR-Inria Joint Centre. AL acknowledges support from the Plan France 2030 through the project ANR-22-PETQ-0006.

[1] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, Journal of Mathematical Physics **43**, 4452 (2002).
[2] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Physical Review A **86**, 032324 (2012).
[3] R. Gallager, IRE Transactions on Information Theory **8**, 21 (1962).
[4] D. J. MacKay, G. Mitchison, and P. L. McFadden, IEEE Transactions on Information Theory **50**, 2315 (2004).
[5] J.-P. Tillich and G. Zémor, IEEE Transactions on Information Theory **60**, 1193 (2013).
[6] D. Gottesman, Quantum Information & Computation **14**, 1338 (2014).
[7] O. Fawzi, A. Grospellier, and A. Leverrier, in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2018) pp. 743–754.
[8] M. A. Tremblay, N. Delfosse, and M. E. Beverland, arXiv preprint arXiv:2109.14609 (2021).
[9] E. Knill, R. Laflamme, and G. J. Milburn, nature **409**, 46 (2001).
[10] S. Bartolucci, P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, *et al.*, arXiv preprint arXiv:2101.09310 (2021).
[11] Y. Wu, S. Kolkowitz, S. Puri, and J. D. Thompson, arXiv preprint arXiv:2201.03540 (2022).
[12] S. Kudekar, T. Richardson, and R. L. Urbanke, IEEE Transactions on Information Theory **59**, 7761 (2013).
[13] T. Richardson and R. Urbanke, *Modern coding theory* (Cambridge university press, 2008).
[14] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, IEEE Transactions on Information Theory **47**, 569 (2001).
[15] V. V. Zyablov and M. S. Pinsker, Problemy Peredachi Informatsii **10**, 15 (1974).
[16] N. Delfosse and G. Zémor, Physical Review Research **2**, 033042 (2020).
[17] S. Lee, M. Mhalla, and V. Savin, in *2020 IEEE International Symposium on Information Theory (ISIT)* (IEEE, 2020) pp. 1886–1890.
[18] A. Steane, Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **452**, 2551 (1996).
[19] A. R. Calderbank and P. W. Shor, Physical Review A **54**, 1098 (1996).
[20] M. Grassl, T. Beth, and T. Pellizzari, Physical Review A **56**, 33 (1997).
[21] T. J. Richardson and R. L. Urbanke, IEEE Transactions on Information Theory **47**, 638 (2001).
[22] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, in *GLOBECOM'01. IEEE Global Telecommunications Conference (Cat. No.01CH37270)*, Vol. 2 (2001) pp. 995–1001 vol.2.
[23] X.-Y. Hu, E. Eleftheriou, and D. Arnold, IEEE Transactions on Information Theory **51**, 386 (2005).
[24] T. S. Manu, Progressive edge growth algorithm for generating LDPC matrices (2014).
[25] N. Connolly, Pruned peeling and vh decoder (2022).
[26] D. Wiedemann, IEEE Transactions on Information Theory **32**, 54 (1986).
[27] E. Kaltofen and B. David Saunders, in *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes* (Springer, 1991) pp. 29–38.
[28] B. A. LaMacchia and A. M. Odlyzko, in *Conference on the Theory and Application of Cryptography* (Springer, 1990) pp. 109–133.
[29] E. Kaltofen, Mathematics of Computation **64**, 777 (1995).
[30] A. A. Kovalev and L. P. Pryadko, Physical Review A **87**, 020304 (2013).
[31] N. Delfosse, V. Londe, and M. E. Beverland, IEEE Transactions on Information Theory (2022).
[32] N. P. Breuckmann and J. N. Eberhardt, IEEE Transactions on Information Theory **67**, 6653 (2021).
[33] P. Panteleev and G. Kalachev, in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing* (2022) pp. 375–388.
[34] A. Leverrier and G. Zémor, arXiv preprint arXiv:2202.13641 (2022).
[35] I. Dinur, M.-H. Hsieh, T.-C. Lin, and T. Vidick, arXiv preprint arXiv:2206.07750 (2022).

[36] M. Kang, W. C. Campbell, and K. R. Brown, arXiv preprint arXiv:2210.15024 (2022).

[37] A. Kubica, A. Haim, Y. Vaknin, F. Brandão, and A. Retzker, arXiv preprint arXiv:2208.05461 (2022).

Multiplexed Quantum Communication with Surface and Hypergraph Product Codes

Shin Nishio[1,2,3], Nicholas Connolly[2], Nicolò Lo Piparo[2], William John Munro[2,3], Thomas Rowan Scruby[2], and Kae Nemoto[2,3]

[1]SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan
[2]Okinawa Institute of Science and Technology Graduate University, Onna-son, Kunigami-gun, Okinawa, 904-0495, Japan
[3]National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan

Connecting multiple processors via quantum interconnect technologies could help to overcome issues of scalability in single-processor quantum computers. Transmission via these interconnects can be performed more efficiently using quantum multiplexing, where information is encoded in high-dimensional photonic degrees of freedom. We explore the effects of multiplexing on logical error rates in surface codes and hypergraph product codes. We show that, although multiplexing makes loss errors more damaging, assigning qubits to photons in an intelligent manner can minimize these effects, and the ability to encode higher-distance codes in a smaller number of photons can result in overall lower logical error rates. This multiplexing technique can also be adapted to quantum communication and multimode quantum memory with high-dimensional qudit systems.

1 Introduction

Quantum computers are expected to solve problems that are intractable using classical computation [1, 2], but these powerful quantum algorithms require high qubit counts and deep circuits to solve problems of interesting size [3, 4]. While the qubit counts of quantum processors have been increasing rapidly in recent years, various physical constraints impose limits on the possible size of a single quantum processor [5, 6]. *Quantum interconnects* provide a resolution to this problem by allowing for the networking and cooperative operation of multiple quantum processors [7], as well as the use of separate quantum memories [8], quantum repeaters [9–12] & networks [13–15] in analogy with classical computing architectures. Optical systems are considered leading candidates for practical implementations of quantum interconnects [16] and also as quantum memories [17] due to long coherence times [18].

Due to the high noise levels inherent in quantum systems, large-scale quantum algorithms cannot be executed reliably without the use of quantum error correcting codes (QECCs) [19,20], which enable fault-tolerant quantum computation (FTQC) [21,22]. Similarly, optical interconnects [7,16] can suffer from high photon loss rates and so QECCs should be used to protect information transmitted through these channels. In principle, it may be preferable to use different codes for these different settings [23], but in practice, the transfer of information between these different codes may be challenging enough that it is easier to use only a single code. For instance, fault-tolerant logic with surface codes [24] has been very well studied [25, 26], while quantum Reed-Solomon codes [27] provide efficient and loss-tolerant protection for transmission through optical channels, but it is not clear how to interface or switch between these two families codes. Therefore, for performing distributed computation with interconnects, using surface codes (or their generalizations) for both computation and transmission [28] is a natural alternative to using multiple codes. This is much less efficient in the sense of error-correction capability for the

Shin Nishio: parton@nii.ac.jp
Nicholas Connolly: nicholas.connolly@oist.jp
Thomas Rowan Scruby: thomas.scruby@oist.jp
Kae Nemoto: kae.nemoto@oist.jp

communication part, but these overheads can be reduced using *quantum multiplexing* [29].

Quantum multiplexing is a technique for encoding high-dimensional quantum information onto a single photon by exploiting multiple different photonic degrees of freedom (DoF) or a single multi-component degree of freedom. Such encodings can be performed using only linear optical elements and can significantly reduce the resources associated with quantum communication [30–32]. In this work, we examine the potential of quantum multiplexing for enabling efficient transmission of surface and hypergraph product (HGP) codes through optical channels. Densely encoding many qubits of these codes into small numbers of photons has the potential to make loss errors much more damaging, but we present various techniques (e.g. optimized strategies for qubit-to-photon assignment) that can mostly or completely eliminate these downsides.

The rest of this paper is organized as follows. In Sec. 2 we review the relevant background for quantum multiplexing and communication over lossy optical channels. Then in Sec. 3 we propose three approaches to error-corrected quantum communication using multiplexing that provide different ways of reducing the impact of loss errors. This is followed up in Sec. 4 and Sec. 5 with an examination of some of these approaches in more detail for surface codes and HGP codes respectively. Finally, we discuss our findings and conclude this work in Sec. 6.

2 Background

In this section, we briefly overview quantum multiplexing and erasure correction and show how these elements appear in practical quantum communication protocols.

2.1 Quantum Multiplexing

This subsection outlines the concept of quantum multiplexing and illustrates its possible implementation with an example.

In photon-based quantum information processing, various degrees of freedom (DOF) can be utilized to encode qubits. Polarizations [33], time-bins [34–36], paths (dual rail) [37], orbital angular momentum [38], and frequency-bin [39, 40] are typical examples of DOF in a single photon which are commonly used in experiment. Multi-level time-bins make it especially easy to encode high-dimensional quantum information in a single photon. For instance, Fig. 1 shows a method for encoding higher dimensional information (2^2-dimension) using polarization and time-bin DOF. This circuit takes a photon whose polarization is encoded with quantum information as input. This input photon has one qubit of information. After passing through this circuit, the photon has both polarization and time-bin degrees of freedom. The polarization encodes a two-dimensional Hilbert space, and the time-bin encodes a four-dimensional one. Therefore, the Hilbert space of the final encoded state has dimension 4 encoding, thus, 2 qubits of information. This encoding can easily generalized to higher dimensional multiplexed photons as shown in Appendix A. Significantly, encoding high-level time-bin states only requires linear optical elements and classical optical switches.

Quantum multiplexing [29] is a method to encode higher dimensional quantum information in a single photon using these multiple degrees of freedom. In this work, we consider encoding 2^m-dimensional quantum information using m components of a DOF per photon where m is an integer ($m = 1$ corresponds to no multiplexing).

It is worth noticing that while quantum multiplexing allows for efficient communication, it also changes the error model. In fact, in a lossy communication channel, the loss of a photon causes the simultaneous loss of multiple qubits encoded in that photon. This can be very detrimental to the performance of this system. However, in the next section, we will devise several strategies for qubit assignment to mitigate the effects of the loss of qubits.

2.2 Erasure Channel and Correction

Let us now describe the erasure channel and decoding, which will play an important role in the quantum communication protocol.

In photonic systems, the erasure error is a localized loss error of a photon due to imperfections in the photon source, the physical channel used for its transmission, and detectors. This is the dominant source of errors in optical systems [41, 42]. Moreover, theoretical [43–46] and experimental [47–51] works have been proposed on methods to map errors from different sources

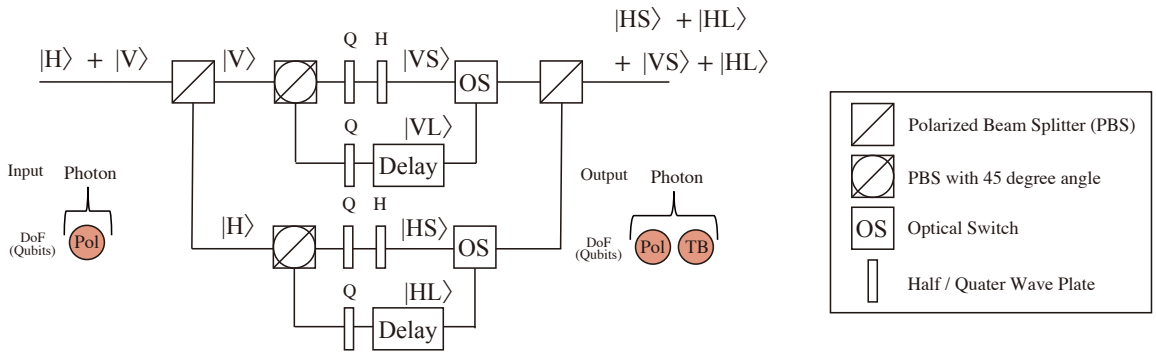


Figure 1: An example of an optical circuit encoding 2^2-dimensional quantum information into a single photon.

to erasure errors in multiple physical systems recently. Therefore, correction of erasure errors is of engineering importance because it can be applied in a variety of systems where erasure errors are not the main source of error.

The erasure channel is given by

$$\rho \to (1-\varepsilon)\rho + \varepsilon \left|e\right\rangle \left\langle e\right| \tag{1}$$

where $|e\rangle$ indicates the erased state, and ε is the probability of erasure. Due to the fact that the erased state is not in the original Hilbert space, it is possible to detect such errors without further damaging the encoded quantum information.

Several methods have been proposed to detect and correct erasure errors with QECCs [52]. It is possible to correct erasure by deforming the original logical operator [53, 54], as well as by converting erasure errors into random Pauli errors by replacing the lost qubits with mixed states:

$$\frac{\mathbb{I}}{2} = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z). \tag{2}$$

After replacing the qubits, one can perform stabilizer measurements as normally occurs in surface codes. Then, the erasure is converted into random Pauli errors with the exact probabilities (1/4) for $\{I, X, Y, Z\}$. This random Pauli can also be regarded as independent X and Z errors with a probability of 1/2. This allows for the decoding of an erasure error. The (surface code) peeling decoder [55], which is a linear-complexity erasure decoder using this procedure, has been proposed as a maximum-likelihood decoder for erasure errors in the surface code. We briefly overview the peeling decoder and its surface code generalization in Appendix C.

2.3 Applying quantum multiplexing to error-corrected erasure channel

We describe the steps to perform error-corrected quantum communication over a multiplexed erasure channel as an example with surface codes illustrated in Fig. 2. As the first step, the sender prepares an encoded quantum state. Then, in the second step, the sender assigns and converts each physical data qubit to a photon. In the conventional case, different qubits are assigned to different photons, whereas when quantum multiplexing is in use, different qubits can be assigned to the same photon. In the instance of Fig. 2, qubits 0 and 6 are attached to photon 0, qubits 1 and 7 are attached to photon 1, etc. We will discuss the optimal assignment strategy later. For the third step, the codeword then goes through an optical channel, which has a loss error. During the transmission, some photons can be lost, causing the loss of all the qubits attached to them as well. For instance, when photon 1 is lost, qubits 1 and 7 will also be lost, as shown in Fig. 2. In the fourth step, the receiver reconstructs (imperfect) codewords with remaining qubits. As the final step, the receiver converts the qubit loss to random unitary as explained in Sec. 2.2. Then, the decoding algorithm estimates the errors, and the receiver performs correction. In the second part of the paper, these steps were simulated to obtain the performance of communication.

3 Multiplexed quantum communication with error-correcting codes

We propose three different scenarios in which multiplexing is used to enhance the efficiency of quantum communication. In each case, m qubits

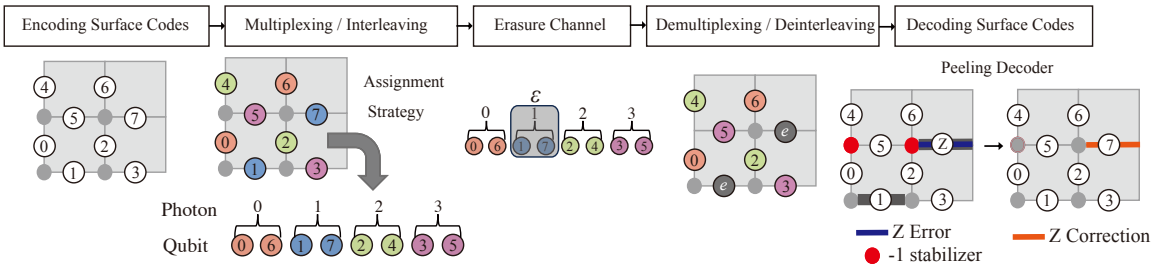


Figure 2: Flow of quantum communication with surface code using multiplexed photons. In the first step, a quantum state is encoded into a surface code. Each circle with a number inside is the physical data qubit, and the grey circles without any number are auxiliary qubits used for stabilizer measurement. For the second step, in a quantum multiplexing scenario, one assigns each physical qubit of the codeword to single photons using an assignment strategy. For instance, in this figure, two components of the time-bin DOF in each photon are used so that each photon can encode two qubits. There is a degree of freedom in which qubit is assigned to which photon, so it is required to make a map function. We call this function the interleaving assignment strategy. Here, the colors of the qubits indicate which photon the qubit is encoded to, which is the result of the assignment strategy. Then, the encoded photons go over a lossy channel. Here, we assume that we know which photons have been lost during the transmission (erasure channel). If a photon has been lost, all the qubits in the photon have been lost. Finally, we demultiplex and decode it to a code word of the surface code using the peeling decoder [55] and a correction method for erasure error shown in Sec. 2.2.

are encoded into each photon, and we compare them to the case of transmitting a codeword of a given code C without multiplexing ($m = 1$).). The three scenarios are

(A). m codewords of C are transmitted using the same number of photons as the $m = 1$ case.

(B). An m-times larger code from the same family as C is transmitted using the same number of photons as the $m = 1$ case.

(C). A codeword of C is transmitted using m-times fewer photons than the $m = 1$ case.

Examples for the case of the surface code are shown in Table. 1, where the parameters of this code are given as $[\![2d^2, 2, d]\!]$, with d being the code distance. Let us now explore each scenario in turn.

(A) Sending m different codewords

In the first scenario, the multiplexed photons are used to encode m codewords from m independent copies of the same code. The logical throughput of the channel increases m fold over the no-multiplexing case. One can assign qubits to photons so that each photon contains one qubit from a codeword of the distinct codes. The qubits from different codewords are correlated, but there is no correlation among the qubits in a fixed code. This correlation does not affect the logical error rate of the individual codes.

(B) Sending $m$times bigger codewords

In the second scenario, a larger number of qubits are used to encode a single codeword from a code in the same family with an m-fold longer length. If this scenario is applied to the surface code, it achieves $\sqrt{m}$ times larger distance than the no-multiplexing case ($m = 1$).

Fig. 3 shows a Monte Carlo simulation of the logical Z error rate for this scenario for the surface code. To determine whether a logical Z error occurred, we checked whether the errors left after the decoding process were anti-commutative with a logical X operator of any logical qubit in the codeword. Each data point in the simulation is obtained from 10^5 shots, and the error bar is given by the Agresti–Coull interval [56]. This scenario introduces correlations in errors between the qubits in the code, which may degrade the performance. However, if m is sufficiently small relative to the code size, the benefit gained by increasing the code size is more significant. All the programs we used to simulate multiplexed quantum communication with surface codes are available here [57]. The logical error rate significantly decreases as the code size and m increase.

Note that the logical Z error rate converges to 0.75. This is because there are two logical qubits

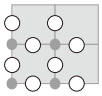
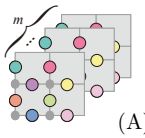
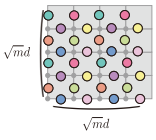
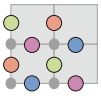
Scenarios	 without multiplexing	 (A)	 (B)	 (C)
Code parameters	$[\![2d^2, 2, d]\!]$	$[\![2d^2, 2, d]\!]$	$[\![2md^2, 2, \sqrt{md}]\!]$	$[\![2d^2, 2, d]\!]$
Number of Codes	1	m	1	1
Number of Data Qubits	$2d^2$	$2md^2$	$2md^2$	$2d^2$
Number of Photons	$2d^2$	$2d^2$	$2d^2$	$\lfloor 2d^2/m \rfloor$
Logical Error Rate	-	Same as without quantum multiplexing	Affected by correlation	Affected by correlation

Table 1: Comparison of the surface code communication without multiplexing and three scenarios with multiplexing. Parameters that are improved by multiplexing are in red fonts. The case without multiplexing requires one qubit per photon. (A) The first scenario is only applicable when sending multiple codewords. This enables one to send more codewords with the same number of photons, drastically improving the channel's throughput. (B) The second scenario sends the same number of codewords with the bigger code, improving the error tolerance. (C) The third scenario sends the same codeword with fewer photons, drastically improving the channel's throughput. The number of photons required in scenario (C) is $\lfloor 2d^2/m \rfloor$, where $\lfloor x \rfloor$ is the floor function of x.

in the codes, and the logical Z error for each qubit converges to 0.5; hence, the probability that both qubits are logical Z error-free is 0.25. In practice, this does not mean the encoded information is recovered, though.

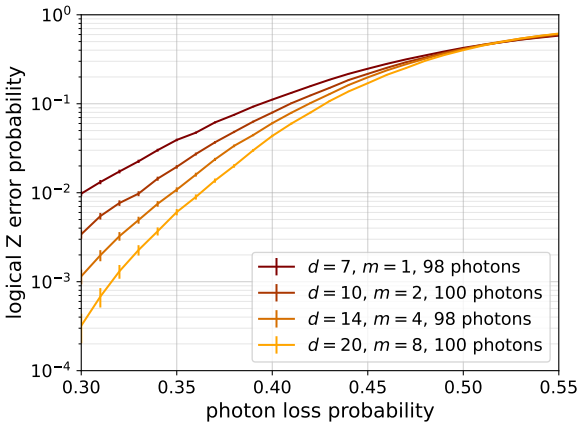


Figure 3: Performance of $[\![2d^2, 2, d]\!]$ toric codes in scenario (B) with about 100 photons. Each curve shows the case with different code sizes and the number of qubits encoded in each photon. The logical error rate can be reduced by increasing the number of qubits per photon m and the code distance d.

(C) Sending original codewords with fewer photons

In the third scenario, a smaller number of photons are used to encode a single codeword. The code parameters are the same as the case without multiplexing. It has no restriction on the number of codewords and can improve the efficiency of surface code communication in general. This method introduces a correlation to the errors. Fig. 4 shows this scenario's logical Z error rate versus the photon loss probability for different values of m. It shows that as m increases, the logical error rate decreases.

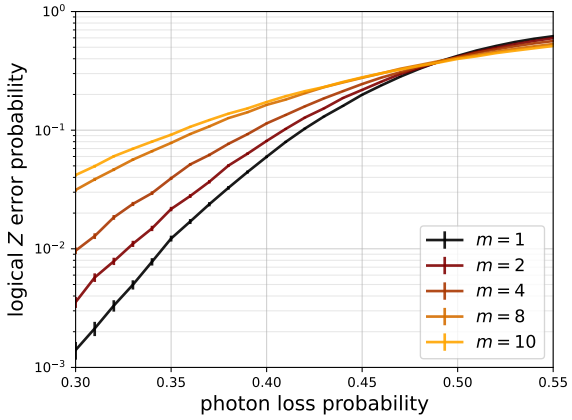


Figure 4: Scenario (C) multiplexing performance for $[\![200, 2, 10]\!]$ toric code with multiplexing using different values of m (the number of qubits per photon). The assignment of qubits to photons is uniformly random. Increasing m allows code words to be transmitted with fewer photons, but the logical error rate increases because multiple qubits in the same photon have strongly correlated errors.

While the number of photons is less compared to the no-multiplexing case, the effects of the correlated errors can be very detrimental to the performance of such a system. A more suitable assignment of the qubits to the multiplexed photos can ideally reduce those detrimental effects.

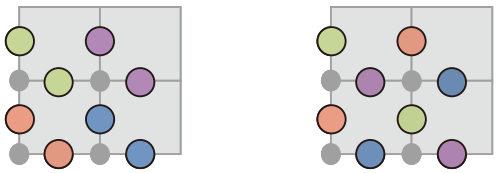
In the next subsection, we explore five different strategies of qubits assignment.

4 Quantum Communication with Multiplexed Surface Codes

4.1 Assignment Strategies for Surface Codes

In this section, we describe five strategies for assigning qubits that take advantage of multiplexing and evaluate their impact on performance. These strategies assume that each photon contains a fixed number of qubits m and can be applied in both scenarios **(B)** and **(C)**. We assume surface code communication scenario **(C)**, where we send the original code with $\lfloor 2d^2/m \rfloor$ photons.
Strategy i and ii: pair with minimum and maximum distance Strategies i and ii are applicable to the case with $m = 2$. Strategy i assigns the nearest neighbor pair of qubits, which form an L-shape in the 2D lattice of the toric code, to the same photon as an example shown in Fig. 5(a). This minimizes the Manhattan distance in the lattice between the qubits in the same photon.

Strategy ii assigns the qubit at coordinates (i, j) on the lattice and the qubit at coordinates $(i + d/2 - 1 \bmod d, j + d/2 - 1 \bmod d)$ to the same photon. An example is shown in Fig. 5. This is the arrangement that maximizes the Manhattan distance, in contrast to strategy i.



(a) (b)

Figure 5: Examples showing possible assignments of qubits to photons. Each numbered circle denotes a qubit, and the color indicates the photon to which the qubit is assigned. Strategy i, shown in (a), minimizes the distance between qubits in the same photon, while strategy ii in (b) maximizes this distance. Note that this code is defined on the torus represented as a lattice with periodic boundary conditions.

Strategy iii: random Strategy iii is a method in which qubits are uniform-randomly selected and assigned to photons.

Strategy iv: random + threshold Strategy iv was designed to increase the separation between qubits assigned to the same photon while exploiting randomness. The strategy works by randomly selecting qubits and accepting them as the set for a photon only if the distance is greater than a certain threshold. If no suitable set of qubits can be found the threshold value is reduced.

Strategy v: stabilizer Strategy v assigns the qubit support of stabilizer generators to the same photon. Realizations of this assignment strategy on a 4×4 surface code are shown in Fig. 6.

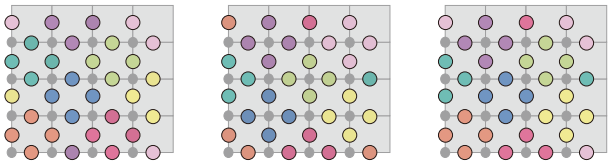


Figure 6: Examples of the stabilizer-based photon assignment strategy for a surface code on a 4×4 lattice. Edges representing qubits in the lattice are marked with colored nodes indicating photon assignment. In this lattice picture, the qubit support of Z-type stabilizer generators corresponds to squares, and of X-type stabilizer generators corresponds to crosses. Each photon in the stabilizer assignment strategy represents the qubit-support of one of these stabilizers.

We describe the details and the motivation of each strategy in Appendix. B

4.2 Performance of the assignment strategies

Here, we show the performances of these strategies observed in numerical simulations.

Fig. 7 (A) shows the performance of strategies i to iv, which are applicable to the case of $m = 2$. The performance of the distance-maximizing strategy (grey) outperforms the distance-minimizing strategy (brown). Logical errors in the toric codes correspond to errors covering a longitude or meridian curve on the torus (a vertical or horizontal closed loop in the periodic lattice). When decoding erasure errors, logical errors can only occur when the qubit-support of one of these vertical or horizontal loops is entirely erased. When adjacent qubits in the lattice are erased, as in the case with the distance-minimizing photon assignment strategy, clusters of errors are more likely to cover such loops in the torus. Hence, it is not surprising that the distance-maximizing strategy outperforms the distance-minimizing strategy in our

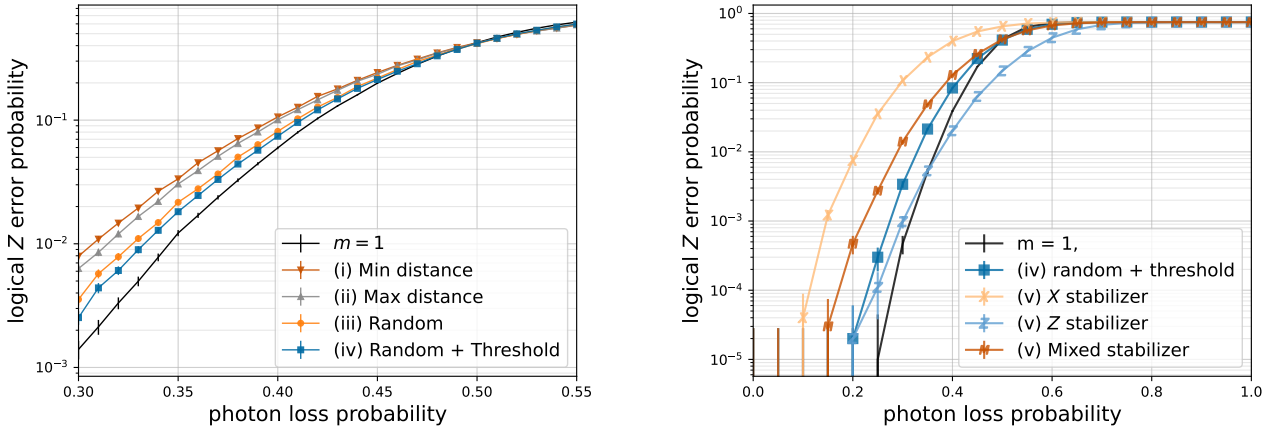


Figure 7: Comparison of multiplexing photon-assignment strategies for toric codes. Logical Z error rate versus photon loss probability. The black curve shows the case without multiplexing. (A) The code parameters are $[\![200, 2, 10]\!]$ and $m = 2$. The gray/brown curve shows the case for the assignment strategy for minimizing (strategy i) / maximizing (strategy ii) the distance between a pair of qubits in the same photon. The orange curve shows the case for uniformly random (strategy iii), and the blue line shows strategy iv, based on the algorithm 1. (B) The code parameters are $[\![288, 2, 12]\!]$ and $m = 4$. Z stabilizer-based assignment with light blue curve outperformed X stabilizer-based assignment with light orange curve for logical Z error. The mixed stabilizer-based assignment strategy performs between X and Z. Strategy iv (blue) outperforms other assignment strategies for low error rate areas.

numerical simulations. It also showed that the strategies with randomness (iii and iv) outperform deterministic ones (i and ii). In particular, strategy iv outperformed the other strategies, although there was an increase in logical Z-error probability compared to no multiplexing.

Next, we compare the logical Z error rates of strategies iii, iv, and v with $m = 4$ in Fig. 7 (B). Assignment strategies based on one type of stabilizer create a bias in observed logical error rates. Strategy v can be generalized to any stabilizer code, and the assignment strategy based only on the support of X or Z stabilizers will increase the error rate of one of X or Z and decrease the other. This result implies that the stabilizer-based assignment may be useful in quantum error correction codes with different X and Z distances.

Both Fig. 7 (A) and (B) showed that the strategy iv randomness + threshold outperformed the other strategies. Maximizing the distance between qubits while also introducing randomness gives the largest boost in performance against logical errors. Note that no assignment strategy does better than the case with $m = 1$ where no multiplexing is used.

We also analyzed the difference in the performance between cases with multiplexing ($m = 4$) and without it ($m = 1$), as shown in Fig. 8. When physical error rates are low, this difference decreases with increasing code distance, suggesting that the downsides of multiplexing are less significant in larger codes.

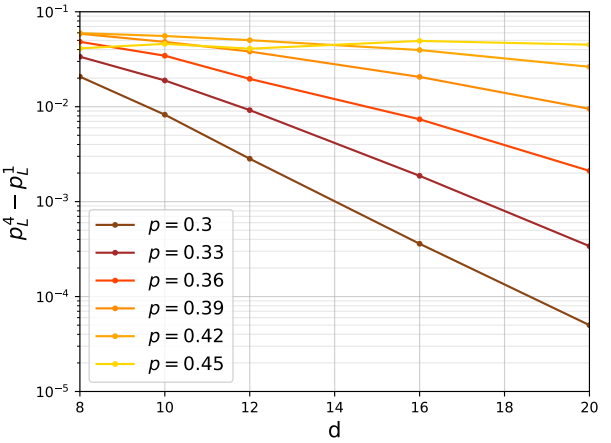


Figure 8: Difference of logical Z error rates for $m = 4$ (p_L^4) and $m = 1$ (p_L^1) for various photon loss probabilities (p). For low p ($0.3 \sim 0.42$), the gap decreases to 0 as d increases.

5 Quantum Communication with Multiplexed Hypergraph Product Codes

5.1 Hypergraph Product Code Structure

In addition to our exploration of the surface code, we also consider the use of multiplexing with hypergraph product (HGP) codes [58], of which surface codes are a special case. HGP codes are a special class of CSS code defined using any two classical linear codes. They are of particular interest because they can have an asymptotically finite rate as the code length increases (in contrast with the surface code, which has a rate approaching 0) and distance proportional to the minimum distance of the classical codes; in the best case, this is proportional to the square root of the quantum code length. They are also considered practical candidates for FTQC codes.

Given classical parity check matrices H_1 and H_2 with sizes $r_1 \times n_1$ and $r_2 \times n_2$, respectively, we may define the matrices H_X and H_Z of a CSS code via the formulas

$$H_X = (H_1 \otimes I_{n_2} | I_{r_1} \otimes H_2^T) \quad (3)$$
$$H_Z = (I_{n_1} \otimes H_2 | H_1^T \otimes I_{r_2}). \quad (4)$$

These matrices satisfy the condition $H_X H_Z^T = 0$ by construction and hence define a valid CSS code $\mathrm{HGP}(H_1, H_2)$. When H_1 and H_2 are low-density parity checks (LDPC), H_X and H_Z will also be LDPC. The sizes of H_X and H_Z are determined by the sizes of the input classical matrices according to the formulas

$$H_X = [r_1 n_2 \times (n_1 n_2 + r_1 r_2)] \quad (5)$$
$$H_Z = [r_2 n_1 \times (n_1 n_2 + r_1 r_2)]. \quad (6)$$

These both simplify to $rn \times (n^2 + r^2)$ in the special case where $r_1 = r_2 = r$ and $n_1 = n_2 = n$.

HGP codes have a geometrically rich Tanner graph structure which can be visualized as the cartesian product of the Tanner graphs for the two input classical codes as shown in Fig. 9. The subgraph corresponding to each row and column in this Tanner graph block structure can be understood as the classical Tanner graph for one of the classical codes used in the construction. As shown in the figure, qubits are represented by circular nodes, and stabilizer checks of both types are represented by square nodes. Additional details regarding this construction are discussed in Appendix D.1.

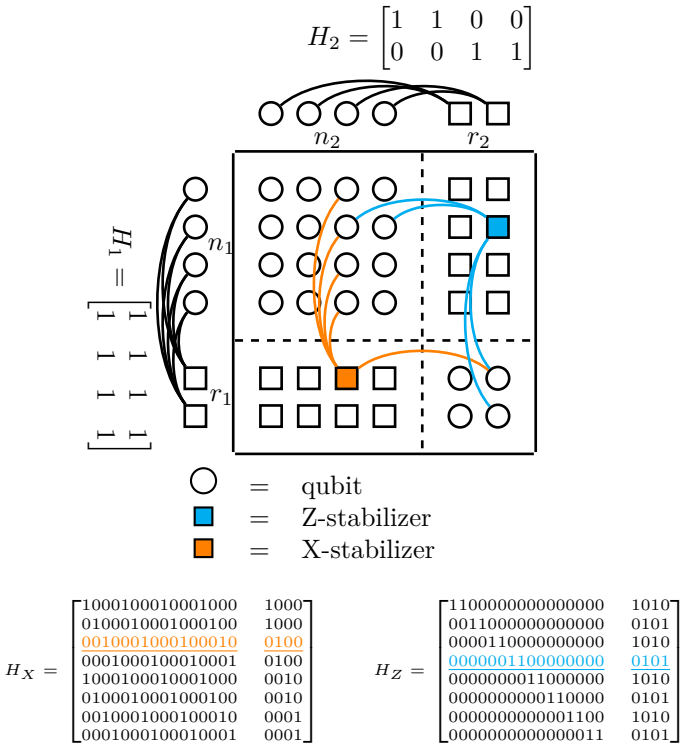


Figure 9: Example of the Tanner graph for a simple HGP code $\mathrm{HGP}(H_1, H_2)$ constructed from two classical codes with parity check matrices H_1 and H_2. This is the cartesian product of two classical Tanner graphs, and the subgraph corresponding to each row and column in the product is a copy of one of these classical Tanner graphs. This product structure can be partioned into four quadrants, each representing a different structural component of the HGP code. The nodes in the upper-left and lower-right blocks denote qubits. The nodes in the upper-right block denote Z-stabilizer generators; these correspond to the rows of H_Z. Similarly, the nodes in the lower-left block denote X-stabilizer generators; these correspond to the rows of H_X.

Surface codes may also be recovered as a special case of hypergraph product code. Using parity check matrices H_1 and H_2 for a classical repetition code, $\mathrm{HGP}(H_1, H_2)$ is exactly the toric code. Hence, adapting the multiplexing strategies discussed in Sec. 4 to this more general class of codes is a natural next question. However, the linear-time maximum-likelihood generalization of the peeling decoder [55] used in our previous simulations is only defined for the special case of the surface code. This decoder leverages the lattice structure of the surface code to ensure that the erasure subgraph can be completely peeled (Appendix C.3), but this technique does not apply to generic HGP codes. Instead, we introduce an-

other generalization of the peeling algorithm to extend our numerical analysis to HGP codes as well.

5.2 Pruned-Peeling + VH Decoder

The *pruned peeling + VH decoder* [59] is a generalization of the peeling algorithm (outlined in Appendix C) specifically designed for HGP codes. It has quadratic complexity and close to maximum-likelihood performance at low erasure rate, making it practically useful for our simulations. This decoder is a modified version of the standard classical peeling decoder based on analysis and correction of two common types of *stopping sets*, which are patterns of erased qubits that cannot be corrected by simple peeling.

A *stabilizer stopping set* occurs when the erasure pattern covers the qubit support of an X- or Z-type stabilizer. The *pruned peeling decoder* attempts to fix these by removing a qubit from the erasure, thus "breaking" the stabilizer support and possibly allowing the peeling algorithm to become unstuck. *Classical stopping sets* are patterns of erased qubits supported entirely on a single row or column in the HGP Tanner graph block structure of Fig. 9; any stopping set for a HGP code can be decomposed into a union of components of this form. The *VH decoder* algorithm attempts to order and efficiently solve each of these classical stopping sets in sequence. The combination of these decoding strategies is referred to as the *combined decoder* (peeling + pruned peeling + VH). A more detailed explanation is included in Appendix C.4.

The combined decoder is not a maximum likelihood decoder. In addition to logical errors, there still exist patterns of erased qubits where the decoder becomes stuck in a stopping set, leading to a decoder failure. We introduce the term *error recovery failure* to refer to both decoder failures and logical errors (discussed in Appendix D.2). Our numerical simulations for HGP codes are always with respect to the *error recovery failure rate*.

Fig. 10 shows the numerical performance of the combined decoder applied to the 10×10 surface code for comparison with the replotted data from Fig. 4, which shows the performance of the ML decoder applied to this same code. The performance degradation is explained by the presence of decoder failures that do not exist in the ML case. Even though it is not ML, the pruned peeling + VH decoder is still practically useful for our numerical simulations since decoder failures are infrequent at low erasure rates.

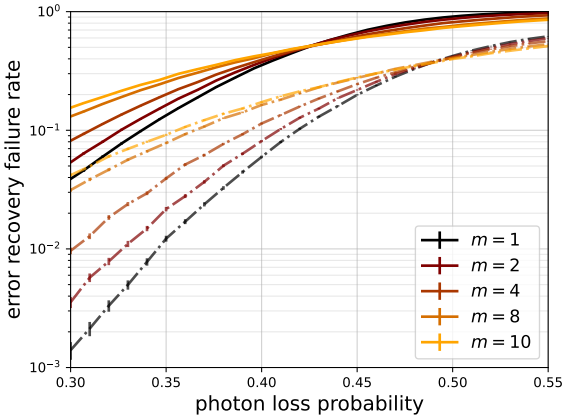


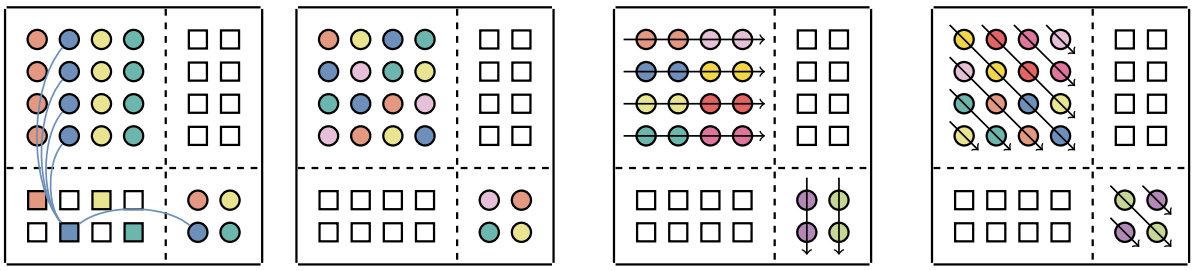
Figure 10: Performance of non-ML *combined decoder* (peeling + pruned peeling + VH) as shown in solid curves and the *surface code peeling decoder* as shown in dashed curves applied to the $[\![200, 2, 10]\!]$ toric code using the uniformly random assignment strategy with different numbers of qubits in a single photon, m.

5.3 Assignment Strategies for HGP Codes

As with the surface code, quantum multiplexing can also be utilized with HGP codes. In this section, we analyze the performance of HGP code communication in scenario **(C)**. The scenarios previously proposed in Sec. 4 are also valid for HGP codes, but unlike the special case of the surface code, the distance between any two qubits in a generic HGP code is not easily inferred from a grid. Hence, we do not consider the previously introduced strategies which use distance. We also introduce several new strategies for HGP codes based on stopping sets for the pruned peeling + VH decoder. These strategies are summarized in Table 2, and technical details are included in Appendix D.3.

Strategy i: random The simplest assignment strategy is based on assigning qubits to photons at random.

Strategy ii: stabilizer The stabilizer assignment strategy assigns qubits to photons so that photons correspond to the qubit-support of a stabilizer. This strategy is motivated by the fact that the pruned peeling decoder is designed to correct erased stabilizers.



Strategy ii. Stabilizer	Strategy iii. Sudoku	Strategy iv. Row-Column	Strategy v. Diagonal

Table 2: Examples of four different photon assignment strategies for the simple HGP code shown in Fig. 9. **(ii.)** Each photon in the *stabilizer strategy* is the qubit-support of an X or Z-type stabilizer generator, identified as a row of H_X or H_Z. The number of qubits per photon is a fraction or multiple of the weight of the corresponding row. **(iii.)** In the *sudoku strategy*, each qubit of a given photon is contained in a different row or column of the HGP Tanner graph. **(iv.)** Using the *row-column strategy*, each qubit of a given photon is contained in the same row or column of the HGP Tanner graph. **(v.)** Photons from the *diagonal strategy* contain qubits from the same diagonal slice of the HGP Tanner graph, allowing diagonal lines to wrap around. For strategies iii., iv., and v., the number of qubits per photon is a fraction or multiple of the shortest side length in the block structure.

Strategy iii: sudoku The sudoku strategy assigns qubits to photons at random subject to the condition that qubits within a given photon come from different rows and columns in the HGP Tanner graph structure. It is motivated by the goal of reducing classical stopping sets, a common source of peeling decoder failures for HGP codes. We name this the sudoku strategy due to its resemblance to the popular game.

Strategy iv: row-column In contrast to sudoku, the row-column strategy chooses qubits in a given photon from the same row or column of the HGP Tanner graph structure. It seeks to maximize the number of classical stopping sets and hence decoder failures. The row-column strategy can be interpreted as a worst-case scenario.

Strategy v: diagonal The diagonal assignment strategy is based on dividing the qubit blocks in the HGP Tanner graph into diagonal slices. Qubits from the same diagonal slice are assigned to the same photon. This is a modified version of the sudoku strategy which does not use randomness but still seeks to minimize classical stopping sets and hence decoder failures.

To compare the effectiveness of these strategies, we have simulated their performance for several codes at different multiplexing values as shown in Fig. 11 and Fig. 12. To understand these results, the case with no-multiplexing ($m = 1$) is used as the baseline. An assignment strategy is considered good if its failure rate is not significantly worse than the $m = 1$ case. Interestingly, our numerical simulations consistently show that

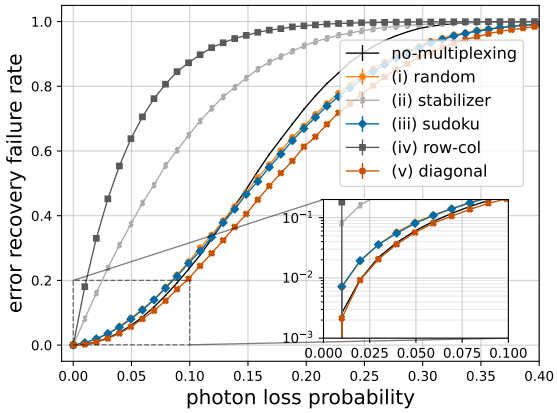
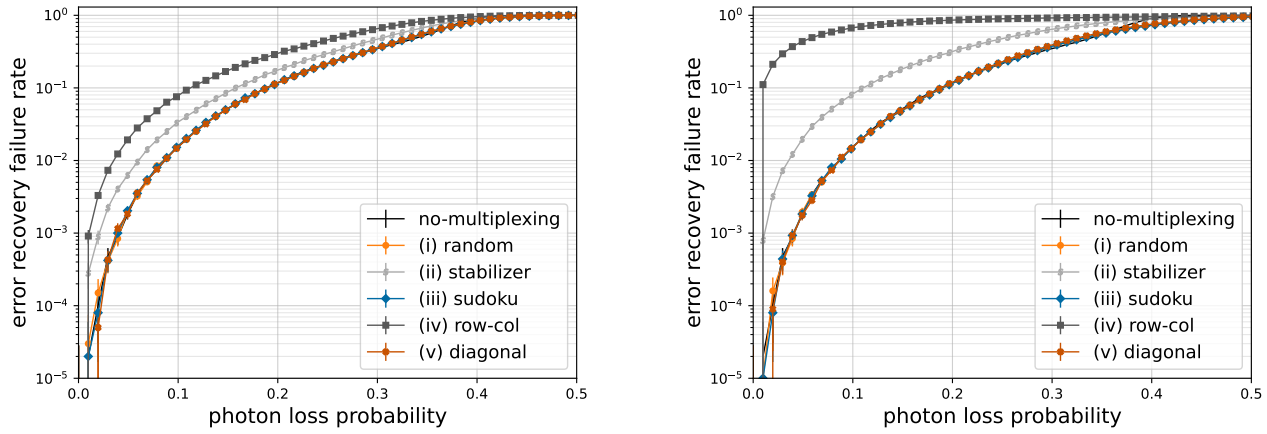


Figure 11: Multiplexing decoder performance for a $[\![320,82]\!]$ non-equal block (16×16 and 8×8) HGP code at fixed $m = 8$. In this example, strategy (v) diagonal outperforms all other strategies, including the no-multiplexing case.

the performances of some strategies (random, sudoku, and diagonal) are almost equivalent to or even exceed the $m = 1$ case, even at high multiplexing values. However, the row-col and stabilizer strategies are never seen to be effective in our results.

Fig. 11 shows an example of a code where the diagonal strategy consistently outperforms all other strategies, even the no-multiplexing case, and even at low erasure rates. This result is significant because even though multiplexing reduces the number of required physical resources, it is possible to improve the decoding performance while doing so. In fact, an analysis of these



(A) $m = 4$ (B) $m = 16$

Figure 12: Comparisons of multiplexing decoder performance for a ⟦512,8⟧ equal-block (16×16) HGP code obtained from the symmetric construction with $r = n = 16$ using various assignment strategies for $m = 4$ and $m = 16$. In both cases, the random, sudoku, and diagonal strategies are seen to be effectively equivalent to the no-multiplexing case, even at low erasure rates.

results reveals that the diagonal strategy yields fewer logical errors than the no-multiplexing case at the same physical erasure rate. This appears to be a feature of the structure of the logical operators in the randomly generated code used in this simulation, even though the strategy was not designed with this in mind. This also explains the gap between the sudoku and diagonal strategies, both of which have similar amounts of decoder failures but differ with respect to logical errors. These results show that strategies designed to avoid decoder failures can have comparable (or even favorable) performance relative to the no-multiplexing case.

Although not identical, we observe similar performance for a larger HGP code, as shown in Fig. 12. The random, sudoku, and diagonal strategies have nearly identical performance to the no-multiplexing case regardless of the chosen multiplexing number. (Simulations include $m \in \{2, 4, 8, 16\}$, although only plots for $m = 4$ and $m = 16$ are shown.) Furthermore, these results hold consistently at a low erasure rate, which is the regime of practical interest. This is significant because it implies there is no loss in performance when multiplexing, even though fewer physical resources are required, provided the assignment strategy is adapted to the decoder. If an ML decoder were used (e.g., Gaussian elimination rather than peeling + pruned peeling + VH), a gap is expected between the multiplexing and no-multiplexing cases. However, given that the combined decoder is a faster, more efficient alternative to a true ML decoder for HGP codes, these results are very promising.

All the programs we used to simulate multiplexed quantum communication with HGP codes are available here [60].

6 Discussion and Conclusion

We proposed three error-corrected quantum information processing scenarios for quantum memory storage and communication with quantum multiplexing over an erasure channel. We have shown that quantum multiplexing can improve throughput or resilience to errors, easing the bottleneck in quantum systems. This work can be adapted to error-corrected quantum communication [28] with quantum interconnects, quantum repeaters, and multimode quantum memory [61].

For multiplexed quantum communication, if multiple qubits in a single code word are encoded into the same photon, a correlation of errors in those qubits will be introduced. The simulation results show that it leads to an increase in the logical error rate. We showed that this performance gap can be significantly mitigated by introducing a code-aware (or decoder-aware) strategy to assign qubits to photons, which exploits code structure. In particular, for the surface codes, randomness and also distance maximization are

important factors for achieving this. For HGP codes with the VH decoder, minimizing decoder failures was found to be the most important factor.

These techniques can also be exploited to benefit other families of codes and decoders. Furthermore, it is possible to deal with the gap by increasing the code size. We have also shown that it is possible to introduce biased error by using a stabilizer-based assignment strategy. In the special case of the diagonal strategy for the HGP code of Fig. 11, we see that the photon-correlated errors offer an improvement over the no-multiplexing case. In this example, the improvement can be explained by the fact that the diagonal strategy reduces logical errors in addition to decoder failures. Furthermore, this shows the existence of strategies that improve over no-multiplexing despite the fact that fewer resources are used.

Even though a linear-time ML decoder has not yet been discovered for generic HGP codes as it has been for surface codes, the use of HGP codes with quantum multiplexing should not be overlooked. Unlike surface codes, which have fixed dimension 2, HGP codes can be chosen so that code dimension k increases linearly with code length n. This can be significant for applications using increasingly long codes since the code rate need not approach 0 in the HGP case. Furthermore, while an ML decoder is ideal, non-ML decoders are often good enough for error correction in the regime of practical interest. The speed-up gained by using a more efficient decoder can offset new errors that might arise when using a slower decoder. Our numerical results for HGP codes show that decoder-aware strategies enable us to gain all of the benefits of quantum multiplexing without sacrificing any additional performance. This, combined with the throughput advantage HGP codes have over the surface code, is a very promising practical result.

Although we propose several promising candidates, the optimal assignment strategy for both surface codes and HGP codes is still unknown. Furthermore, in actual communication with quantum multiplexing, various errors may occur when converting qubits in the quantum processor to photons, measuring stabilizers, and substituting erased qubits with mixed states. How to deal with these errors is a practically important next question.

Multiplexing could also be used for qubit $\rightarrow$ qudit encodings in non-photonic systems where loss errors are not the dominant source of noise. In these cases error locations may not be known and so knowledge of the assignment strategy could be used to inform decoding.

Acknowledgements

SN acknowledges Dan Browne, Antonio deMarti iOlius, and Hon Wai Lau for valuable discussions throughout this project. This work was supported by JSPS KAKENHI Grant Number JP21H04880, JP22J20882, the MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0118069605, the JST Moonshot R&D Grant Number JPMJMS2061 and JPMJMS226C, and a travel budget from the National Institute of Informatics.

References

[1] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE, 1994.

[2] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[3] Thomas Häner, Martin Roetteler, and Krysta M Svore. Factoring using 2n+ 2 qubits with toffoli based modular multiplication. *arXiv preprint arXiv:1611.07995*, 2016.

[4] Nobuyuki Yoshioka, Tsuyoshi Okubo, Yasunari Suzuki, Yuki Koizumi, and Wataru Mizukami. Hunting for quantum-classical crossover in condensed matter problems. *npj Quantum Information*, 10(1):45, 2024.

[5] Sebastian Krinner, Simon Storz, Philipp Kurpiers, Paul Magnard, Johannes Heinsoo, Raphael Keller, Janis Luetolf, Christopher Eichler, and Andreas Wallraff. Engineering cryogenic setups for 100-qubit scale superconducting circuit systems. *EPJ Quantum Technology*, 6(1):2, 2019.

[6] Shuhei Tamate, Yutaka Tabuchi, and Yasunobu Nakamura. Toward realization of scalable packaging and wiring for large-scale superconducting quantum computers. *IEICE Transactions on Electronics*, 105(6):290–295, 2022.

[7] David Awschalom, Karl K Berggren, Hannes Bernien, Sunil Bhave, Lincoln D Carr, Paul Davids, Sophia E Economou, Dirk Englund, Andrei Faraon, Martin Fejer, et al. Development of quantum interconnects (quics) for next-generation information technologies. *PRX Quantum*, 2(1):017002, 2021.

[8] Christopher Monroe, Robert Raussendorf, Alex Ruthven, Kenneth R Brown, Peter Maunz, L-M Duan, and Jungsang Kim. Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects. *Physical Review A*, 89(2):022317, 2014.

[9] Koji Azuma, Sophia E Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. *Reviews of Modern Physics*, 95(4):045006, 2023.

[10] WJ Munro, R Van Meter, Sebastien GR Louis, and Kae Nemoto. High-bandwidth hybrid quantum repeater. *Physical review letters*, 101(4):040502, 2008.

[11] Liang Jiang, Jacob M Taylor, Kae Nemoto, William J Munro, Rodney Van Meter, and Mikhail D Lukin. Quantum repeater with encoding. *Physical Review A*, 79(3):032325, 2009.

[12] William J Munro, Ashley M Stephens, Simon J Devitt, Keith A Harrison, and Kae Nemoto. Quantum communication without the necessity of quantum memories. *Nature Photonics*, 6(11):777–781, 2012.

[13] Rodney Van Meter. *Quantum networking*. John Wiley & Sons, 2014.

[14] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang. Optimal architectures for long distance quantum communication. *Scientific reports*, 6(1):20463, 2016.

[15] William J Munro, Nicolo'Lo Piparo, Josephine Dias, Michael Hanks, and Kae Nemoto. Designing tomorrow's quantum internet. *AVS Quantum Science*, 4(2), 2022.

[16] Jianwei Wang, Damien Bonneau, Matteo Villa, Joshua W Silverstone, Raffaele Santagati, Shigehito Miki, Taro Yamashita, Mikio Fujiwara, Masahide Sasaki, Hirotaka Terai, et al. Chip-to-chip quantum photonic interconnect by path-polarization interconversion. *Optica*, 3(4):407–413, 2016.

[17] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature photonics*, 3(12):706–714, 2009.

[18] Y-W Cho, GT Campbell, JL Everett, J Bernu, DB Higginbottom, MT Cao, J Geng, NP Robins, PK Lam, and BC Buchler. Highly efficient optical quantum memory with long coherence time in cold atoms. *Optica*, 3(1):100–107, 2016.

[19] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[20] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[21] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. In *NASA International Conference on Quantum Computing and Quantum Communications*, pages 302–313. Springer, 1998.

[22] A Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of physics*, 303(1):2–30, 2003.

[23] Shota Nagayama, Byung-Soo Choi, Simon Devitt, Shigeya Suzuki, and Rodney Van Meter. Interoperability in encoded quantum repeater networks. *Physical Review A*, 93(4):042338, 2016.

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

[25] Austin G Fowler, Matteo Mariantoni, John M Martinis, and Andrew N Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3):032324, 2012.

[26] Clare Horsman, Austin G Fowler, Simon Devitt, and Rodney Van Meter. Surface code quantum computing by lattice surgery. *New Journal of Physics*, 14(12):123011, 2012.

[27] Markus Grassl, Willi Geiselmann, and Thomas Beth. Quantum reed—solomon codes. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 13th International Symposium, AAECC-13 Honolulu, Hawaii, USA, November 15–19, 1999 Proceedings 13*, pages 231–244. Springer, 1999.

[28] Austin G Fowler, David S Wang, Charles D Hill, Thaddeus D Ladd, Rodney Van Meter, and Lloyd CL Hollenberg. Surface code quantum communication. *Physical review letters*, 104(18):180503, 2010.

[29] Nicolo Lo Piparo, William J Munro, and Kae Nemoto. Quantum multiplexing. *Physical Review A*, 99(2):022337, 2019.

[30] Shin Nishio, Nicolò Lo Piparo, Michael Hanks, William John Munro, and Kae Nemoto. Resource reduction in multiplexed high-dimensional quantum reed-solomon codes. *Physical Review A*, 107(3):032620, 2023.

[31] Nicolo Lo Piparo, Michael Hanks, Claude Gravel, Kae Nemoto, and William J Munro. Resource reduction for distributed quantum information processing using quantum multiplexed photons. *Physical Review Letters*, 124(21):210503, 2020.

[32] Nicolo Lo Piparo, Michael Hanks, Kae Nemoto, and William J Munro. Aggregating quantum networks. *Physical Review A*, 102(5):052613, 2020.

[33] Alfred B U'Ren, Konrad Banaszek, and Ian A Walmsley. Photon engineering for quantum information processing. *arXiv preprint quant-ph/0305192*, 2003.

[34] Jürgen Brendel, Nicolas Gisin, Wolfgang Tittel, and Hugo Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594, 1999.

[35] Ivan Marcikic, Hugues de Riedmatten, Wolfgang Tittel, Valerio Scarani, Hugo Zbinden, and Nicolas Gisin. Femtosecond time-bin entangled qubits for quantum communication. *arXiv preprint quant-ph/0205144*, 2002.

[36] Robert Thomas Thew, Sébastien Tanzilli, Wolfgang Tittel, Hugo Zbinden, and Nicolas Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Physical Review A*, 66(6):062304, 2002.

[37] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[38] Alison M Yao and Miles J Padgett. Orbital angular momentum: origins, behavior and applications. *Advances in optics and photonics*, 3(2):161–204, 2011.

[39] YH Shih and AV Sergienko. Observation of quantum beating in a simple beam-splitting experiment: Two-particle entanglement in spin and space-time. *Physical Review A*, 50(3):2564, 1994.

[40] S Ramelow, L Ratschbacher, A Fedrizzi, NK Langford, and A Zeilinger. Discrete tunable color entanglement. *Physical review letters*, 103(25):253601, 2009.

[41] Sergei Slussarenko and Geoff J Pryde. Photonic quantum information processing: A concise review. *Applied Physics Reviews*, 6(4), 2019.

[42] Atharv Joshi, Kyungjoo Noh, and Yvonne Y Gao. Quantum information processing with bosonic qubits in circuit qed. *Quantum Science and Technology*, 6(3):033001, 2021.

[43] Yue Wu, Shimon Kolkowitz, Shruti Puri, and Jeff D Thompson. Erasure conversion for fault-tolerant quantum computing in alkaline earth rydberg atom arrays. *Nature communications*, 13(1):4657, 2022.

[44] Aleksander Kubica, Arbel Haim, Yotam Vaknin, Harry Levine, Fernando Brandão, and Alex Retzker. Erasure qubits: Overcoming the t 1 limit in superconducting circuits. *Physical Review X*, 13(4):041022, 2023.

[45] Mingyu Kang, Wesley C Campbell, and Kenneth R Brown. Quantum error correction with metastable states of trapped ions using erasure conversion. *PRX Quantum*, 4(2):020358, 2023.

[46] Takahiro Tsunoda, James D Teoh, William D Kalfus, Stijn J de Graaf, Benjamin J Chapman, Jacob C Curtis, Neel Thakur, Steven M Girvin, and Robert J Schoelkopf. Error-detectable bosonic entangling gates with a noisy ancilla. *PRX Quantum*, 4(2):020354, 2023.

[47] Chao-Yang Lu, Wei-Bo Gao, Jin Zhang, Xiao-Qi Zhou, Tao Yang, and Jian-Wei Pan. Experimental quantum coding against qubit loss error. *Proceedings of the National Academy of Sciences*, 105(32):11050–11054, 2008.

[48] Shuo Ma, Genyue Liu, Pai Peng, Bichen Zhang, Sven Jandura, Jahan Claes, Alex P Burgers, Guido Pupillo, Shruti Puri, and Jeff D Thompson. High-fidelity gates and mid-circuit erasure conversion in an atomic qubit. *Nature*, 622(7982):279–284, 2023.

[49] Pascal Scholl, Adam L Shaw, Richard Bing-Shiun Tsai, Ran Finkelstein, Joonhee Choi, and Manuel Endres. Erasure conversion in a high-fidelity rydberg quantum simulator. *arXiv preprint arXiv:2305.03406*, 2023.

[50] Harry Levine, Arbel Haim, Jimmy SC Hung, Nasser Alidoust, Mahmoud Kalaee, Laura DeLorenzo, E Alex Wollack, Patricio Arrangoiz Arriola, Amirhossein Khalajhedayati, Yotam Vaknin, et al. Demonstrating a long-coherence dual-rail erasure qubit using tunable transmons. *arXiv preprint arXiv:2307.08737*, 2023.

[51] Kevin S Chou, Tali Shemma, Heather McCarrick, Tzu-Chiao Chien, James D Teoh, Patrick Winkel, Amos Anderson, Jonathan Chen, Jacob Curtis, Stijn J de Graaf, et al. Demonstrating a superconducting dual-rail cavity qubit with erasure-detected logical measurements. *arXiv preprint arXiv:2307.03169*, 2023.

[52] G Alber, Th Beth, Ch Charnes, A Delgado, M Grassl, and M Mussinger. Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes. *Physical Review Letters*, 86(19):4402, 2001.

[53] Thomas M Stace, Sean D Barrett, and Andrew C Doherty. Thresholds for topological codes in the presence of loss. *Physical review letters*, 102(20):200501, 2009.

[54] Sean D Barrett and Thomas M Stace. Fault tolerant quantum computation with very high threshold for loss errors. *Physical review letters*, 105(20):200502, 2010.

[55] Nicolas Delfosse and Gilles Zémor. Linear-time maximum likelihood decoding of surface codes over the quantum erasure channel. *Physical Review Research*, 2(3):033042, 2020.

[56] Alan Agresti and Brent A Coull. Approximate is better than "exact" for interval estimation of binomial proportions. *The American Statistician*, 52(2):119–126, 1998.

[57] Shin Nishio. C++ implementation of multiplexed toric codes simulator, May 2024. https://github.com/parton-quark/Multiplexed_Toric.

[58] Jean-Pierre Tillich and Gilles Zémor. Quantum ldpc codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2013.

[59] Nicholas Connolly, Vivien Londe, Anthony Leverrier, and Nicolas Delfosse. Fast erasure decoder for a class of quantum ldpc codes. *arXiv preprint arXiv:2208.01002*, 2022.

[60] Nicholas Connolly and Shin Nishio. Python implementation of multiplexed HGP codes simulator, May 2024. https://github.com/parton-quark/Multiplexed_HGP.

[61] Mikael Afzelius, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Multimode quantum memory based on atomic frequency combs. *Physical Review A*, 79(5):052329, 2009.

[62] Stephen B Wicker and Vijay K Bhargava. *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.

[63] Masahiro Hara, Motoaki Watabe, Tadao Nojiri, Takayuki Nagaya, and Yuji Uchiyama. Two-dimensional code, Japan Patent, 07-254037,A(1995). Toyota Central Research & Development Lab Inc.

[64] JG Proakis and M Salehi. Digital communications, vol. 1221, 1987.

[65] Shiro Kawabata. Quantum interleaver: quantum error correction for burst error.

Journal of the Physical Society of Japan, 69(11):3540–3543, 2000.

[66] Michael G Luby, Michael Mitzenmacher, Mohammad Amin Shokrollahi, and Daniel A Spielman. Efficient erasure correcting codes. *IEEE Transactions on Information Theory*, 47(2):569–584, 2001.

A Encoding 2^k dimensional quantum information in a photon

Here we show the circuit for encoding 2^k dimensional quantum information into time-bin in one photon in Fig. 13 where level i block is defined in Fig. 14. In the first half of the circuit, level i block is used to introduce a new component of the time-bin by applying a delay. Then, in the middle of the circuit, each state corresponds to a different mode. In the second half of the circuit, multiplexed photons are output to one mode by applying the optical switches, forming a complete binary tree. This encoding circuit can prepare a photon with 2^k dimensional time-bin and 2 dimensional polarization in linear time for k.

B Assignment strategies for surface codes

In this appendix, we describe the details and discussions on each assignment strategy.

strategy i and ii: pair with minimum and maximum distance The Manhattan distance between qubits within the same photon is crucial when considering the impact of correlated errors. These strategies are deterministic and can be realized with simple calculations.

strategy iii: random Errors with strong correlation are similar to burst errors in classical communication in the sense that the errors have spatial locality. This locality of errors can be addressed by classical error-correcting codes using two methods. The first method treats multiple bits as a single symbol (an element of a finite field), such as BCH codes and Reed-Solomon codes [62]. Thanks to the high ability to correct burst errors, Reed-Solomon codes are used in many classical systems, including QR codes [63], CDs, and satellite communications. Another method is the interleaving [64] technique. Interleaving eliminates locality by permuting the rows and columns of the code's generator matrix. There is also a method to apply interleaving to QECCs [65]. Inspired by interleaving, we have constructed two strategies for quantum multiplexing with randomness.

strategy iv: random + threshold The fourth strategy is a modified version of the third strategy. The pseudo-code is shown below in Algorithm 1. The flow of the algorithm is as follows: A "threshold" T is set as $2/d-1$, which is the maximal distance between two qubits in the $[\![2d^2, 2, d]\!]$ toric codes. This value will be used to check that the set of qubits in the same photon has enough distance between each other. Then, it randomly assigns qubits for each photon while respecting the distance threshold. It randomly selects the first qubit of the photon, then it randomly selects a qubit again and takes it as a candidate to assign it to this photon. When the distance between the candidate qubit and the qubit(s) already in the photon is greater than the threshold, the qubit is accepted, and when it is less, it is rejected. This procedure is repeated until the photon has been fulfilled. If no qubit satisfies the threshold, the threshold value is lowered by one. This is to ensure that the algorithm will always finish running. By repeating this process, we can assign all the qubits to photons. This strategy is designed to have randomness and to increase the distance between qubits in the same photon.

This algorithm requires calculating the distance between two qubits, which is easy for the surface codes because the taxicab metric defines the distance (Manhattan distance). Note that this and other assignment strategies can still be applied even if the number m of qubits per photon is not a divisor of the total number of qubits. In this case, we allow for a final "remainder" photon containing fewer than m qubits.

Strategy v: Stabilzier Error correction on the surface code is always considered up to multiplication by a stabilizer. This suggests that it may be useful to define photons using the qubit-support of a stabilizer check. Since the stabilizer generators for the surface code correspond to squares and crosses in the lattice, they have weight 4. On a $d \times d$ lattice, if d is divisible by 4, it will always be possible to partition the lattice into squares and crosses. In this perspective, the L-shapes used in the minimum-distance strategy can be thought of as "half-stabilizers" in the lat-

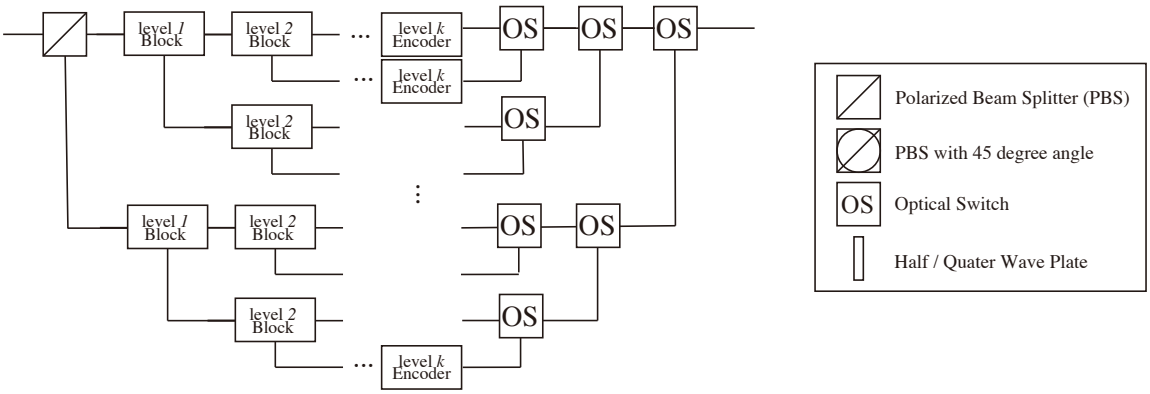


Figure 13: Optical circuit for preparing a photon with 2^k dimensional time-bin information.

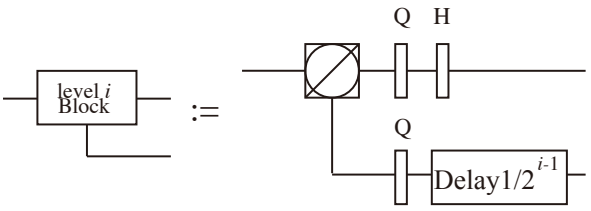


Figure 14: Level i block used in Fig. 13. It split single mode into two modes with new component of time-bin DOF introduced to the state.

tice. Since the usual strategy for converting an erasure problem into an error correction problem involves assigning erased qubits Pauli errors randomly, this stabilizer assignment strategy uses a mix of Z and X-type stabilizer generators from both squares and crosses. In this case, qubits are equally partitioned into the two types of stabilizers by tiling the lattice with alternating diagonal lines of squares and crosses.

C Peeling Decoder

The *peeling decoder* refers to a linear-complexity erasure decoding algorithm originally designed for classical codes [66]. This algorithm corrects an erasure error by examining the subgraph of the Tanner graph corresponding to erased bits, whereby degree-1 check nodes in this subgraph give perfect information about adjacent bit nodes. Although not a maximum-likelihood decoder, the peeling decoder works well for codes with sparse Tanner graphs, such as LDPC codes. Because this algorithm only uses the Tanner graph, it can be directly applied to CSS codes as well. In this section, we briefly summarize the peeling decoder algorithm and several of its variations, beginning with a review of the classical erasure setting.

C.1 Peeling Algorithm for Classical Codes

For a classical code, an erasure error on a codeword can be modeled as the loss of a known subset of bits. By assigning these erased bits the values 0 or 1 at random and then making a syndrome measurement, the erasure correction problem can be converted into an error correction problem. Unlike standard error correction, we make the additional assumption that non-erased bits do not have errors. Hence, it is sufficient to consider error correction using the subcode corresponding only to erased bits. In terms of the Tanner graph, this is equivalent to considering the subgraph induced by the erasure (consisting of the subset of erased bit-nodes and any adjacent check-nodes). The peeling algorithm is defined in terms of this erasure-induced subgraph.

A check is said to be *dangling* if it has degree 1 in the subgraph (i.e. a dangling check is adjacent to exactly one erased bit). Recall that each check-node corresponds to a position in the syndrome vector for the randomly selected erasure-supported error. The value of the syndrome bit corresponding to a dangling check gives perfect information about the error on the adjacent erased bit. Based on this, the error on this bit can be corrected and then removed from the original set of erased bits, thus shrinking the erasure-induced subgraph and possibly introducing new dangling checks. The peeling decoder functions by performing a sequence of partial corrections, one erased bit at a time, hence "peel-

Algorithm 1: Strategy iv. random + threshold

Input: $P = \{p_i\}$ (the set of photons) where initially $p_i = \{\emptyset\}$ (the set of qubits to be encoded in the i^{th} photon), $Q = \{q_j\}$ (the list of all physical qubits in the code), and the number m of qubits in a single photon.

Output: $P = \{p_i\}$ (set of set of qubits in i^{th} photon).

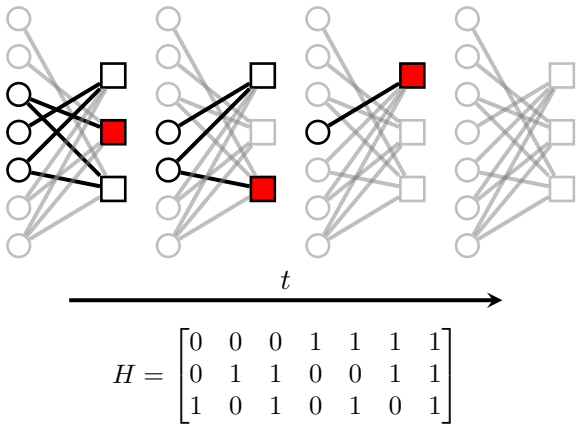
Initialize the threshold with $T := \frac{d}{2} - 1$;
for *photon* $p_i \in P$ **do**
  Pick a qubit $q_j \in Q$ randomly.;
  Move q_j from Q to p_i;
  while $|p_i| < m$ **do**
    while $|p_i| < m$ *and* $Q \neq \emptyset$ **do**
      Pick a candidate qubit $q_k \in Q$ randomly;
      if q_k *has minimum distance greater than* T *from all the qubits in* p_i **then**
        Move q_k from Q to p_i;
      else
        Move q_k from Q to a waiting list Q';
    Move all qubits in Q' to Q;
    Update $T := T - 1$;
Return P;

ing" the subgraph until no dangling checks remain. This process is shown visually in Fig. 15 and briefly summarized in Algorithm 2.

The decoding is successful if all erased bits have been corrected. A decoding failure occurs when all dangling checks have been peeled, but the remaining erasure is nonempty (i.e. all remaining checks in the subgraph have degree 2 or higher). Such a configuration is referred to as a *stopping set*. If an erasure pattern contains a stopping set, then the peeling algorithm will fail to find a correction. In particular, because the algorithm may not even return to the codespace, this shows that peeling is not a maximum-likelihood decoder.

C.2 Peeling Algorithm for CSS Codes

Erasure correction for a quantum code is modeled similarly to the classical case, with an erasure error on a codeword corresponding to the loss of a known subset of qubits. As in the classical case, erasure correction can be converted into error correction, with the modified rule that erased qubits are assigned Pauli errors in $\{I, X, Z, Y\}$ at random in the quantum case. For a CSS code, errors can be corrected by applying the peeling algorithm two times, once using the classical Tanner graph for H_Z and once again for H_X. Since X- and Z-type Pauli errors are corrected independently, the same initial erasure pattern is used both times.



$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Figure 15: Example of the peeling algorithm applied to an erasure-induced subgraph of the Tanner graph of the classical code $C = \mathrm{Ker}(H)$, where circle-nodes denote bits and square-nodes denote checks. Gray edges and nodes are not included in the erasure. Red squares indicate a dangling check (degree 1 check-node in the subgraph). At each time step, a dangling check and adjacent erased bit are removed from the erasure, until the erasure is empty.

C.3 Peeling Algorithm for Surface Codes

The *surface code peeling decoder* refers to a generalization of this algorithm adapted to surface codes [55], which uses additional information about stabilizers in the code. Before applying the standard peeling algorithm, the modified algorithm first computes a certain acyclic subgraph of the usual erasure-induced subgraph. By leveraging stabilizer equivalences, it is sufficient to apply the peeling algorithm only to this acyclic subgraph to correct the entire erasure error; the random values assigned to erased qubits not included in this subgraph are assumed to be correct. The advantage here is that an acyclic graph does not contain stopping sets; the peeling algorithm will always successfully terminate with a predicted erasure correction when applied to the

Algorithm 2: Peeling Algorithm

Input: A code $\mathrm{Ker}(H)$ with Tanner graph G, a set of erased bits E, and a syndrome vector s.

Output: A predicted error $\hat{e} \subseteq E$ such that $H\hat{e} = s$, or **Failure**.

```
Initialize ê = ∅;
while E ≠ ∅ do
    Compute erasure subgraph G_E ⊆ G;
    if ∃ dangling check s_i ∈ G_E then
        if s_i is unsatisfied then
            Error on adjacent bit b_j ∈ E;
            Flip bit b_j, update syndrome s;
            Update ê := ê ∪ {b_j};
        else
            No error on adjacent bit b_j;
        Update E := E \ {b_j};
    else
        Return Failure;
Return ê;
```

acyclic subgraph in question. Hence, unlike the standard peeling decoder, the surface code peeling decoder is maximum-likelihood.

It remains to comment on how we compute this acyclic subgraph of the erasure-induced subgraph of the Tanner graph for the surface code. To explain this, we consider the usual depiction of a distance d surface code on a $d \times d$ lattice, whereby qubits are identified with edges in the lattice and X- and Z-type stabilizer checks are identified with vertices and plaquettes, respectively. That is say, the H_X-computed syndrome for Z-type Pauli errors on qubits is visualized by the subset of vertices corresponding to unsatisfied X-checks. A similar visualization for X-type Pauli errors is possible using the dual graph of this lattice picture. In the context of an erasure error, a subset of erased qubits is visualized by a corresponding set of erased edges in the surface code lattice. This erasure can also be thought of as the subgraph of the lattice consisting of erased qubit-edges and any vertices adjacent to these edges (not to be confused with the related erasure-induced subgraph of the Tanner graph).

After assigning erased qubits Pauli errors at random, as usual, we consider the correction of Z- and X-type errors independently. In the Z-error case, the syndrome corresponding to the unsatisfied X-checks is a subset of the vertices in the erasure-induced subgraph of the lattice. The algorithm proceeds by computing a spanning tree of the erasure-induced subgraph of the lattice (or a spanning forest in the case of a disjoint subgraph). This spanning tree in the lattice also corresponds to a subgraph in the Tanner graph of H_X; each leaf in the spanning tree corresponds to a dangling check in the subgraph. In this way, we obtain the acyclic subgraph of the erasure-induced subgraph of the Tanner graph mentioned earlier. Any two spanning trees are equivalent up to multiplication by stabilizers, as are the predicted errors obtained via the peeling algorithm. The X-errors are corrected in exactly the same way, except using the dual lattice.

This modified peeling algorithm is a linear-complexity, maximum-likelihood decoder for the surface code. We use this algorithm in our numerical simulations for the surface code. Our implementation of the surface code peeling decoder is available in [57]. This process is briefly summarized in Fig. 16 and 17.

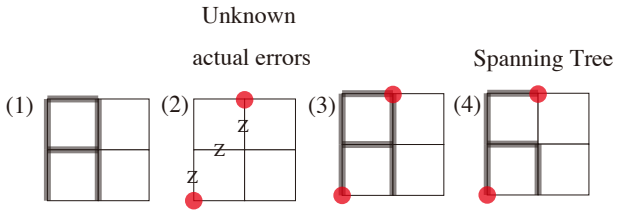


Figure 16: Illustration of the error correction process for an example of erasure errors with the surface code lattice. (1) Erased qubits are shown in bold grey lines. (2) Erasure errors are converted to random Pauli errors by replacing erased qubits with mixed states. The syndrome (indicated by the red vertices) is then computed by applying stabilizer measurement as explained in Sec. 2.2. (3) Information seen by the decoding algorithm: erasure pattern and syndrome. (4) A spanning tree for the erasure pattern in the lattice is computed; this is identified with a corresponding acyclic subgraph of the Tanner graph. The *surface code peeling decoder* then corrects the qubits one by one using this subgraph.

C.4 Peeling Algorithm for HGP Codes

The *pruned peeling + VH decoder* [59] is yet another generalization of the peeling decoder adapted to the special case of HGP codes. As mentioned in Appendix C.2, because these are a type of CSS code, the standard peeling algorithm can be directly applied to HGP codes. However, this algorithm performs very poorly in practice,

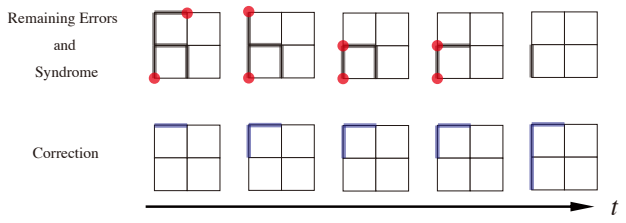


Figure 17: Peeling process to decode the erasure error pattern given in Fig. 16. Grey edges indicate the spanning tree in the surface code lattice and red vertices indicate the syndrome. The peeling algorithm is applied to the corresponding subgraph of the Tanner graph. Blue edges indicate corrections applied to qubits. Each time step denotes one iteration of the peeling algorithm, whereby the erasure is reduced by one qubit.

even for LDPC codes. This poor performance can be explained by the presence of stopping sets unique to HGP codes which have no analogue in the classical case. These stopping sets can be grouped into two types: *stabilizer* and *classical*, both of which cause the decoder to fail. The pruned peeling + VH decoder is designed to address these stopping sets.

Stabilizer stopping sets occur when the erasure contains the qubit-support of an X- or Z-type stabilizer. Recall that, for a CSS code, X- and Z-stabilizers overlap on an even number of qubits. Hence, restricting to the Tanner graph of H_Z, the check-nodes in the subgraph corresponding to the qubit-support of an X-stabilizer all have even degrees. In particular, there exist no dangling checks (which have degree 1) and hence this is a peeling decoder-stopping set. A similar relationship holds for Z-stabilizers in the Tanner graph of H_X.

Such a stopping set can be modified by fixing a value at random for one qubit of the stabilizer and removing this qubit from the erasure. This reduces the degree of a single check-node in the erasure subgraph by 1, possibly introducing a dangling check and allowing the standard peeling algorithm to become unstuck. Removing a qubit from the erasure is equivalent to declaring the random mixed state on this qubit to be correct. This technique is valid for CSS codes because there exists a solution on the remaining erased qubits in the stabilizer-support such that the combined contribution to the error is at most a stabilizer. This procedure, known as *pruned peeling*, is applicable to any CSS code, not just HGP codes.

Classical stopping sets are another common type of peeling decoder stopping set which are only defined for HGP codes. These refer to patterns of erased qubits supported entirely on a single row or column in the HGP Tanner graph block structure of Fig. 9. In the simplest case, a peeling decoder stopping set for one of the classical codes used in the HGP construction lifts to a classical stopping set for the HGP code. Furthermore, any HGP peeling decoder stopping set can be decomposed into a union of vertical and horizontal sets on the columns and rows of the Tanner graph; although we refer to these components as *classical stopping sets*, a single component in isolation need not be a stopping set for the corresponding classical code.

The *VH decoder* algorithm functions by ordering and efficiently solving each of these classical stopping sets in sequence, when possible, using the Gaussian decoder. The basic premise relies on the fact that, for a HGP code of length N, the component classical codes have length on the order of $\sqrt{N}$. Hence, even though Gaussian elimination (which has cubic complexity in the code length) is usually too slow for practical use, the complexity is reduced when restricted to a single classical stopping set. However, classical stopping sets often overlap (i.e. share a check-node in the Tanner graph), in which case the two stopping sets cannot be resolved independently without introducing some additional restrictions. By checking these conditions, the VH decoder attempts to find solutions for classical stopping sets which are compatible in these overlapping cases. If such a solution is found for each classical stopping set, these combine to give a solution for the HGP code. However, there exist erasure configurations where the VH decoder becomes stuck as well. In general, these will occur when there exist cycles of classical stopping sets in the erasure-induced subgraph.

The *pruned peeling + VH decoder* refers to the combination of these three strategies (standard peeling, correction of stabilizer stopping sets, and correction of classical stopping sets). For simplicity, we also use the term *combined decoder* to refer to peeling + pruned peeling + VH. A stopping set for the combined decoder meets three conditions: there exist no remaining dangling checks; the remaining erasure does not cover the qubit-support of a stabilizer; remaining classical stop-

ping sets form a cycle. Although these happen infrequently at a low erasure rate, an erasure pattern of this form will result in a decoder failure. These are distinct from logical errors, which can only be identified in numerical simulations where the decoding algorithm successfully terminates. The maximum-likelihood decoder always terminates, and thus, logical errors are the only source of failures. Although we make a distinction between these two possibilities, we will use the term *error recovery failure* to refer to either a decoder failure or a non-decoder failure logical error. A more detailed discussion of these differences is included in Appendix D.2.

The computational complexity of the combined decoder is dominated by the step applying cubic-complexity Gaussian elimination to classical stopping sets (peeling and pruned peeling both have linear complexity). The number of classical stopping sets is on the order of the number of rows and columns in the Tanner graph ($\sqrt{N}$ for an HGP code of length N). Furthermore, since classical stopping sets have a size of approximately $\sqrt{N}$, the effect of Gaussian elimination on a single classical stopping set contributes $O(N^{1.5})$ to the complexity. This becomes $O(N^2)$ across all classical stopping sets, establishing this algorithm as a quadratic complexity decoder for HGP codes.

D Additional Details for HGP Codes

D.1 Symmetric Constructions

Recall equations 3 and 4 used to define the parity check matrices for HGP codes. The the sizes of the matrices H_X and H_Z obtained in this way are determined by the sizes of the input classical matrices H_1 and H_2. Hence, the number of qubits and stabilizer checks are controlled by the size of the input classical matrices; equations 5 and 6 give the exact dimensions for H_X and H_Z obtained from matrices $H_1 = [r_1 \times n_1]$ and $H_2 = [r_2 \times n_2]$. Referring to the Tanner graph of Fig. 9, the $n_1 \times n_2$ and $r_1 \times r_2$ blocks denote the qubit nodes and the $r_1 \times n_2$ and $n_1 \times r_2$ blocks denote the X- and Z-type stabilizer generators, respectively.

Choosing classical matrices of the same size ensures an equal number of stabilizer checks in the HGP code, but a biased code can also be constructed by using matrices of different sizes. Furthermore, using $H_2 = H_1^T$ yields a symmetric construction for H_X and H_Z and guarantees that the two blocks of qubits in this product graph picture are squares of equal size. In our numerical simulations, we consider two types of HGP code construction: an *equal block* case coming from the symmetric construction with $H_2 = H_1^T$, whereby $r_2 = n_1$ and $n_2 = r_1$; and a *non-equal block* case using different matrices H_1 and H_2 of the same size, so $r_1 = r_2 = r$ and $n_1 = n_2 = n = 2r$ (we make a choice to use matrices with half as many rows as columns).

D.2 Types of Error Recovery Failures for the Pruned Peeling + VH Decoder

In Sec. 5.2, we observed that the combined decoder (peeling + pruned peeling + VH) is not maximum-likelihood since decoder failures are possible in addtion to logical errors. Failure rate in the literature usually refers to the logical error rate, which is the only source of errors for a maximum-likelihood decoder. Logical errors for the erasure channel can only occur when the erasure covers a logical code word. However, there may exist erasure patterns covering a logical error which result in a decoder failure, and hence are not properly identified as logical errors. This distinction is stated visually by the Venn diagram of Fig. 18. The failure rate computed in our numerical simulations for the *combined decoder* is the cummulative effect of these two possibilities, what we refer to as *error recovery failure rate* on the vertical axis in the plots of our numerical simulations for HGP codes. Note that failures at low erasure rates are almost exclusively due to logical errors, and so this distinction can be regarded as negligible in the practical regime.

Note that peeling + pruned peeling is theoretically a maximum likelihood decoder in the special case of the surface code. This is equivalent to the spanning-tree-based ML decoder for the surface code [55]. However, our implementation of pruned peeling is not perfect since it cannot identify the support of an arbitrary erased stabilizer. For the *combined decoder*, the simplest classical stopping sets correspond to a fully erased row or column in the HGP Tanner graph. These are exactly the stopping sets of a repetition code, coinciding with logical errors for the surface code. In general, there do not exist erasure patterns giving a VH decoder failure for the surface code which do not also cover a logical error.

Figure 10 shows the performance of the *combined decoder* applied to the 10×10 surface code. Comparing this to Fig. 4, which uses the ML decoder for the same surface code, we see a noticeable degradation in performance. This gap is explained by the existence of decoder failures in the combined case which do not exist for the ML decoder. Furthermore, the failure rate of the combined decoder converges to 1 as the erasure rate goes to 1, in contrast with the convergence to 0.75 for the ML decoder. This is because the erasure pattern is always a VH decoder stopping set when all qubits are erased, guaranteeing a decoder failure. Since there are no stopping sets in the ML case, however, a 100% erasure rate is equivalent to generating a uniformly random physical Pauli error on the code. We see a convergence to 0.75 logical error rate because this error is identity 25% of the time.

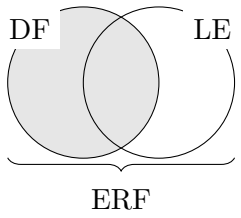


Figure 18: Venn diagram distinguishing between the types of failures possible using the pruned peeling + VH decoder. A *decoding failure* (DF) occurs when the decoder becomes stuck in a stopping set it cannot correct. A *logical error* (LE) occurs when the decoder successfully terminates with a predicted error, but the actual and predicted errors combine to give a logical code word. An *error recovery failure* (ERF) refers to the union of these two possibilities.

D.3 Technical Details for Assignment Strategies used with Multiplexed HGP Codes

Strategy ii. stabilizer The stabilizer strategy was initially introduced in Sec. 4 for the surface code, but it can be applied to CSS codes more generally. The erased qubit-support of a stabilizer will be a peeling decoder stopping set, but these are precisely the stopping sets that the pruned peeling algorithm attempts to correct. Hence, this strategy is motivated by the idea that losing a photon corresponding to a single stabilizer individually induces a correctable erasure pattern.

In the stabilizer strategy for HGP codes, we partition the qubits into sets corresponding to the qubit-support for disjoint stabilizers. Qubits are assigned to stabilizers based on these sets. The number of qubits per stabilizer is fixed for an LDPC code and matches the row weight of H_X or H_Z. Depending on the multiplexing number, the photons can also represent partial stabilizers or multiple stabilizers.

In the special case of the surface code with a $d \times d$ lattice, where d is divisible by 4, it is always possible to partition the qubits into a combination of disjoint X- and Z-type stabilizer generators as seen in Fig. 6, each of which is supported on 4 qubits. For a more general HGP code, we may attempt a similar assignment strategy by identifying the qubit-support of the stabilizer generators from the rows of H_X and H_Z. However, we cannot guarantee that a partition of qubits into disjoint stabilizers is possible without placing constraints on the number of qubits and the row and column weights in the parity check matrices. Instead, we adopt an imperfect but simpler strategy for generic HGP codes, which does not require any additional assumptions about the code except that H_X and H_Z are LDPC. This strategy can be used with stabilizers coming only from H_X, only from H_Z, or a combination of both, provided that these matrices have the same row weight. Note that restricting to a single type of stabilizer creates a bias in the error correction, as was commented in the surface code case.

The first step of this strategy is to search for a partition of the qubits into disjoint stabilizers. To do this, we begin by choosing a row at random from H_X or H_Z; the nonzero entries in this row represent the qubit-support of a single stabilizer. We then eliminate any overlapping stabilizers by deleting the rows from the matrices that share columns with nonzero entries with the previously selected row. Then we repeat this strategy until either all qubits have been divided into disjoint stabilizers or we exhaust the remaining rows that do not overlap with our previous selections. The result is that as many qubits as possible have been divided into non-overlapping sets corresponding to the qubit-support of disjoint stabilizers, possibly with some remaining ungrouped qubits.

Finally, the qubits are assigned to photons based on the disjoint sets identified in the previous step. Ordering the qubits by their stabilizer assignments, we then redistribute these into

photons. The remaining ungrouped qubits are assigned after exhausting the chosen stabilizers. When the multiplexing number matches the stabilizer weight (that is, the row weight of H_X or H_Z), each photon ideally matches a stabilizer, possibly with some remainder photons at the end for the ungrouped qubits. When the multiplexing number matches a fraction or multiple of the stabilizer weight, then the photons represent a partial stabilizer or multiple stabilizers, respectively. Allowing for the leftover qubits at the end ensures that this strategy can be applied with various multiplexing numbers, even when a perfect partition of qubits into stabilizers is not found. Because stabilizers are selected at random, this assignment strategy can be understood as a combination of the random and stabilizer strategies introduced before.

Strategy iii. sudoku The VH decoder is designed to address classical stopping sets for the peeling decoder, but there exist combinations of classical stopping sets that cannot be solved using this technique and result in a decoder failure. However, we may reduce the likelihood of a decoder failure by reducing the number of classical stopping sets in general. Classical stopping sets are supported on a single row or column of the HGP code Tanner graph. Thus, we propose an assignment strategy based on choosing qubits in the same photon from different rows and columns. The method for doing this is outlined in Algorithm 3.

This strategy assumes that the number of qubits per photon does not exceed the minimum length of a row or column in the Tanner graph, although this condition may be relaxed by instead allowing for a minimal number of qubits from the same row or column to be added to the same photon. Qubits are assigned to photons at random, checking that each newly added qubit is not supported on the same row or column as any qubit already assigned to a given photon. In the case of a fixed number of photons where no valid qubit assignments remain, we drop the condition and default to random assignment.

Strategy iv: row-col Although not a practical assignment strategy, the case where only qubits from the same row or column of the HGP code Tanner graph are assigned to the same photon is of theoretical interest. This strategy attempts to maximize the number of classical stopping sets resulting from photon loss and thus increase the likelihood of a VH decoder failure. Verifying that this assignment strategy performs very poorly in numerical simulations serves as a proof of concept for the VH decoder and also justifies the preferred strategies using qubits from different rows and columns.

Algorithm 3: Strategy iii. sudoku

Input: $P = \{p_i\}$ (the set of photons, where p_i is the set of qubits in photon i), $Q = \{q_j = (r_j, c_j, b_j)\}$ (a list of 3-tuples with the row, column, and block of each physical qubit in the HGP code), and the number m of qubits per photon.

Output: $P = \{p_i\}$ (photon assignments).

for *photon* $p_i \in P$ **do**
  Pick a qubit $q_j \in Q$ randomly;
  Move q_j from Q to p_i;
  while $|p_i| < m$ *and* $Q \neq \emptyset$ **do**
    Pick a candidate qubit $q_k \in Q$;
    if q_k *is in a different row and column (or block) from each previously selected* $q_j \in p_i$ *(*$(r_k \neq r_j$ *and* $c_k \neq c_j)$ *or* $b_k \neq b_j)$ **then**
      Move q_k from Q to p_i;
    else
      Move q_k from Q to a temporary waiting list Q';
  Move all qubits in Q' back to Q;
  while $|p_i| < m$ **do**
    Pick a qubit $q_k \in Q$ randomly;
    Move q_k from Q to p_i;
Return P;

Fig. 19 shows the performance of this strategy for a ⟦512,8⟧ HGP code at several multiplexing numbers. Although surprisingly the $m = 2$ case seems to outperform the no-multiplexing case, the failure rate otherwise increases as m increases. Failures of the VH decoder are the result of certain configurations of classical stopping sets, and hence increasing the latter also increases the former. In particular, this explains the dramatic jump between the $m = 8$ and $m = 16$ cases. Since the blocks in this code's Tanner graph are 16×16, each photon in the $m = 16$ case corresponds to an entire row or column. Loss of any photon yields a classical stopping set, and hence VH decoder fail-

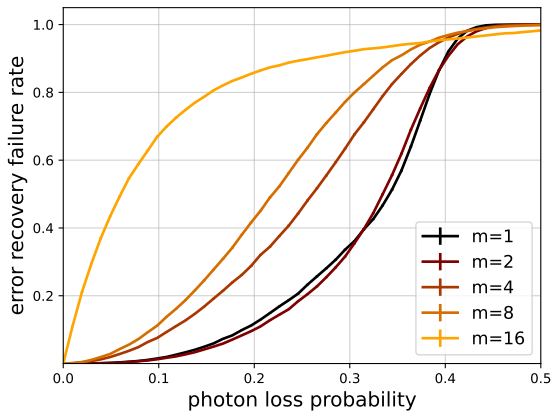


Figure 19: The performance for multiplexed communication with a ⟦512,8⟧ equal-block (16×16) HGP code obtained from the symmetric construction using $r = n = 16$ with assignment strategy (iv) row-column. Increasing the number of qubits per photon using this strategy rapidly increases the failure rate. At $m = 16$, each photon corresponds to an entire row or column in the HGP Tanner graph, whereby losing even one photon guarantees a classical stopping set.

ures are common. This also confirms the significance of designing assignment strategies to avoid classical stopping sets in our simulations of HGP codes. In general, we expect the performance of the row-column strategy to drop significantly as m becomes equal to or larger than the side length of the block in the HGP Tanner graph.

Strategy v. diagonal Whereas the sudoku strategy assigns qubits at random subject to the condition of being in a different row or column, qubits in the HGP code Tanner graph may also be grouped diagonally within each block. In this way, it is possible to satisfy the sudoku condition without relying on randomness. A $d \times d$ grid can be divided into d non-overlapping diagonal slices, where we allow slices to wrap around. Since no two qubits in the same diagonal slice are contained in the same row or column of the grid, this technique also guarantees that we avoid classical stopping sets within a single photon. Photon assignment is thus based on grouping together the qubits in the same diagonal slice. Each of the two qubit-squares in the HGP code Tanner graph is considered separately, but if we require that the ratio of the squares' side lengths is a whole number, then the qubits can be cleanly partitioned into photons of size matching the side length of the smaller square. HGP codes with rectangular Tanner graph block sizes can also use the diagonal strategy, provided that the length of the diagonal slice does not exceed the length of the shortest side. If longer slices are permitted in the rectangular case, then instead a minimal number of qubits in the same row or column are allowed.

The implementation of this strategy as described in Algorithm 4 is simple, provided one precomputes a *diagonal ordering* on the qubits in the HGP Tanner graph. Referring to the block structure of Fig. 9, the qubits in a given block are indexed along the non-overlapping diagonal slices. These slices are allowed to wrap around the sides of the square, which guarantees that no two qubits in the same slice are contained in the same row or column. The qubits in the second block are indexed sequentially after the first block. In our numerical implementation, a separate function to compute this ordering on the qubits in an HGP code is used along with the assignment function.

Algorithm 4: Strategy v. diagonal

Input: $P = \{p_i\}$ (the set of photons where p_i is the set of qubits in photon i), $Q = \{q_j\}$ (a list of physical qubits ordered along the diagonal), and the number m of qubits per photon.

Output: $P = \{p_i\}$ (photon assignments).

```
for photon p_i ∈ P do
    for qubits with indices
      j ∈ {im, ··· , (i + 1)m} do
        Move q_j from Q to p_i
return P;
```

Quantifying Operational Costs of Quantum Internet Applications Through Blind Variational Quantum Computing

Masaki Nagai[1] * Hideaki Kawaguchi[2] † Takahiko Satoh[1] ‡

[1] *Faculty of Science and Technology, Keio University*
[2] *Graduate School of Science and Technology, Keio University*

Abstract. We organize the requirements for Quantum Internet applications and quantitatively analyze the operational costs of blind variational quantum computing. Initially, we examine the protocol for concealing parameters and outputs in the Variational Quantum Eigensolver (VQE). We develop a toy model to identify the main bottlenecks and subsequently quantify the operational costs of the blind variational quantum computing algorithm. By comparing these quantified costs, we evaluate different models of blind quantum computation. These analyses allow us to quantitatively assess the operational costs and bottlenecks of blind variational quantum computing algorithms.

Keywords: Quantum Internet Application, Blind Quantum Computation, Variational Quantum Eigensolver

1 Introduction

Quantum computers, based on quantum mechanics, are expected to exceed classical computational capabilities. Concurrently, the Quantum Internet, a new-era network that distributes quantum entanglement, is attracting significant attention. The Quantum Internet enables unprecedented applications such as distributed quantum computing and blind quantum computing. Research spans experiments to architecture, with significant testbeds in China, the Netherlands [3, 6], and Japan surpassing laboratory environments.

However, the technical difficulties of quantum hardware, along with the burdens of infrastructure development and maintenance, impose stringent constraints on the Quantum Internet, raising concerns about the high operational costs associated with Quantum Internet applications. Estimating these costs is necessary to promote the development of feasible applications in the future. Therefore, this study designs the blind quantum computing application, one of the Quantum Internet applications, and quantifies its time costs.

In this study, we first designed applications incorporating feasibility modifications with the parameter-blind variational quantum computing algorithm[7], which will likely be implemented early in developing Noisy Intermediate Scale Quantum Internet algorithms. Second, we implemented the Variational Quantum Eigensolver (VQE) [5] as a toy model to calculate the ground state energy of a hydrogen molecule in its minimal basis set and analyzed performance metrics from the implemented toy model for Quantum Internet applications. Third, we established quantitative cost metrics for Quantum Internet applications and compared several blind quantum computing algorithms based on the identified metrics.

From these approaches, it has become clear that methods to reduce costs by limiting functionality are crucial in the development of Quantum Internet applications.

*masaki0818nagai@keio.jp
†hikawaguchi@keio.jp
‡satoh@ics.keio.ac.jp

2 Blind VQC for Quantum Internet

Quantum Internet applications are those in which clients who lack sufficient quantum computing resources connect via the Quantum Internet to servers that possess extensive quantum computing resources, thereby performing the exchange and processing of information. Quantum Internet applications can execute classical tasks, such as classical communication and computation, and quantum tasks, such as communication using quantum entanglement and quantum computing. Blind quantum computation denotes a protocol for secure quantum cloud computing and is one of the most promising applications of the quantum internet. We anticipate that parameter-blind VQC, due to its low implementation costs, will be operational in the initial stages of Quantum Internet deployment, and we have implemented it as a toy model for Quantum Internet applications.

2.1 Implementation

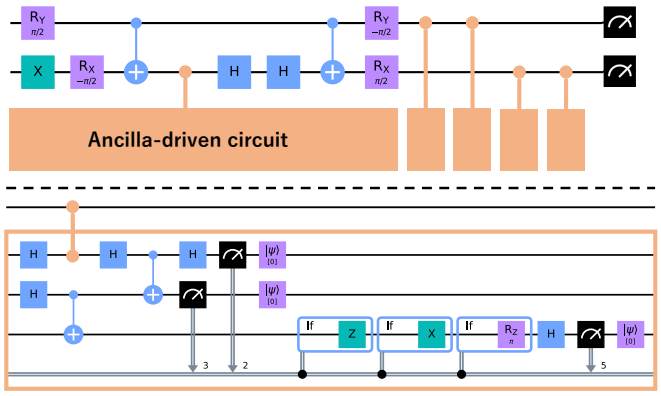


Figure 1: (Upper part) Our customized parameter-blind VQE circuit. Notably, the feed-forward operations affect only the client's bits. (Lower part) Gate configuration of the ancilla-driven circuit. The initial R_z gate remotely acts on the first qubit through ancilla-driven computation. The initial $|\psi\rangle$ gate represents initialization.

To adapt the original parameter-blind VQE for use with the Quantum Internet, we modified the protocol to utilize quantum teleportation for the qubits measured by the client. We performed an additional four ancilla-driven quantum computations to correct the quantum state altered by the byproducts of quantum teleportation. We show the protocol diagram in Fig. 2.

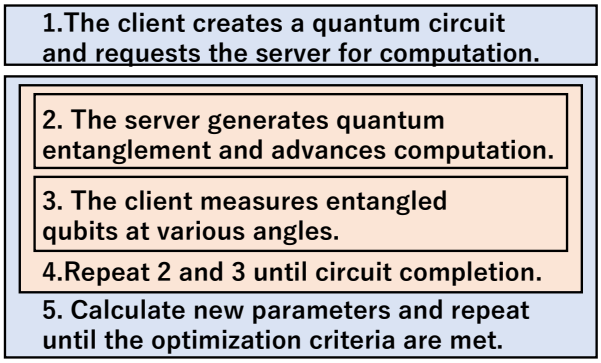


Figure 2: Steps 1 and 5 involve classical tasks, while steps 2, 3, and 4 pertain to quantum tasks.

2.2 Identifying Cost Indicators

In this protocol, the bottlenecks include the typical ones associated with VQE (such as the calculation of new parameters and the extensive repetitions) and the correction of byproducts from the client's measurement angles, the client's measurement time, and the server's scheduling. The protocol analysis revealed that three key indicators influence the application: 1. The server's capabilities, including gate time and the number of qubits. 2. The bandwidth of the Quantum Internet for distributing high-fidelity entanglement. 3. The delays caused by the necessary classical communication.

3 Cost Metrics Analysis

This section analyzes the cost metrics for the major bottlenecks identified in the previous section.

3.1 Quantum Internet Bandwidth

The formula can quantitatively analyze the Q-bandwidth cost of Quantum Internet:

$$\text{Q-Bandwidth Cost} = \frac{\#\text{ Entangled Pairs}}{\text{Bandwidth}}. \quad (1)$$

Here,Total Required Entangled Pairs represents the aggregate number of entangled pairs needed for specific Quantum Internet applications, and Bandwidth is the number of entangled pairs per unit time.

3.2 Quantum Server Performance

$$\text{Q-Server Cost} = \frac{\text{Circuit Size}}{\text{Computational Speed}}. \quad (2)$$

In applications, the total execution time requested by the server varies significantly depending on the choice of physical systems and hardware configurations. Therefore, it is impossible to quantify this uniformly, and one should select a cost function suitable for each situation. Here, the Circuit Size depends on the selected cost functions, such as T count or circuit depth. Similarly, Computational Speed refers to the circuit execution speed, which varies according to the server's performance and the chosen cost functions.

3.3 Classical Communication

The formula can quantitatively analyze the Classical Communication cost for Application:

$$\text{C-Comm. Cost} = \#\text{ C-Comm.} \times \frac{\text{Delay}}{\text{C-Comm.}} \quad (3)$$

This formula helps determine the impact of classical communication delays on the overall performance of Quantum Internet systems.

3.4 Comprehensive Metrics Overview

Although these three cost metrics generally do not depend on each other, their ability to be processed independently and in parallel can vary depending on the application's content and circumstances. To maximize application performance, minimizing and optimizing these metrics' bottlenecks is crucial.

4 Algorithmic Performance Comparison

4.1 Evaluation of Blind Quantum Computation Protocols

Based on the defined cost functions, we estimate the costs for various blind quantum computations. We assume the Q-Server's capability is that of an ion trap computer, specifically the Ionq Aria [2]. We also assume that the Quantum Internet can supply quantum entanglement with sufficiently high fidelity and set the simulation parameters in Table 1.

Table 1: Quantum Internet and Q-Server performance.

Parameter	Value
`Bandwidth`	200 Hz
`Channel length`	1000 km
`Light speed in fiber`	$\approx 200,000$ km/s
`1-Qubit Gate duration`	135 μs
`2-Qubit Gate duration`	600 μs
`Measurement duration`	200 μs
`Initialisation duration`	1 μs

This paper defines the Q-Server cost for the gate model as the product of the not depth and the two-qubit gate time. Numerous methods exist for converting from the gate model to MBQC. In this paper, we approximate it by the product of the number of qubits and the depth. Since universal rotation requires three qubits, we define the Q-Server cost in the MBQC model as the product of the number of qubits, depth, three, and measurement time. We present the results as shown in Table 2.

Table 2: Comparison of Quantum and Classical costs in blind quantum computing protocols.

Blind-Protocols	Q-Bandwidth Cost	Q-Server Cost	C-Communication Cost
`Parameter-blind` [7]	**25**	6.6	**25**
`BFK protocol` [1]	175	7	350
`MF protocol` [4]	175	**0**	175

In the BFK[1] protocol, the amount of classical communication doubles relative to the amount of quantum entanglement as the server transmits the next measurement angle to the client based on previous measurement results. The MF protocol[4] employs a straightforward approach using quantum teleportation. The Parameter-blind protocol blinds only parameters and outputs, whereas the other two protocols conceal everything, including inputs, outputs, and the contents of the algorithms. In the BFK protocol, clients must randomly generate qubits with specific rotations, while the MF and Parameter-blind protocols necessitate measurement devices. The Parameter-blind protocol significantly reduces costs by limiting blinding to only the parameters of the ansatz.Thus, reducing the cost of protocols and enhancing the potential for practical quantum computing by focusing on specific functionalities is crucial.

4.2 Distribution of Bottlenecks

This section clarifies the distribution of bottlenecks in variational blind quantum computation. Initially, we briefly define the problem size. Assuming Ansatz is the k-UpCCGSD, the depth scales are $\mathcal{O}(kN)$ relative to the number of qubits N, and the number of parameters scales are $\mathcal{O}(kN^2/4)$. Based on this model, we analyze the distribution of bottlenecks. Assume the bandwidth is 3500 Hz over 50 km, and four entanglements are consumed through purification to compensate for the fidelity degradation caused by a single entanglement swapping. Thus, three bottlenecks emerge due to various variable settings. Protocols that utilize classical communication equivalent to quantum entanglement struggle with long-distance communication. Each protocol exhibits different sensitivities to these costs, necessitating tailored strategies depending on the specific protocol and application scenario.

5 Conclusion

We designed a parameter-blind variational quantum eigensolver (VQE) application and quantified costs for Quantum Internet applications. Using a VQE circuit for a hydrogen molecule, we found that the main bottlenecks are Quantum Internet bandwidth, server computation, and classical communication delay. We established cost metrics for each bottleneck and evaluated several blind quantum computation protocols. The results showed that the parameter-blind protocol is low-cost, with classical communication being the primary bottleneck for long-distance computations. Developing protocols that reduce costs by limiting functionalities is crucial for Quantum Internet applications. This work provides a foundation for advancing practical Quantum Internet technologies and indicates future development directions.

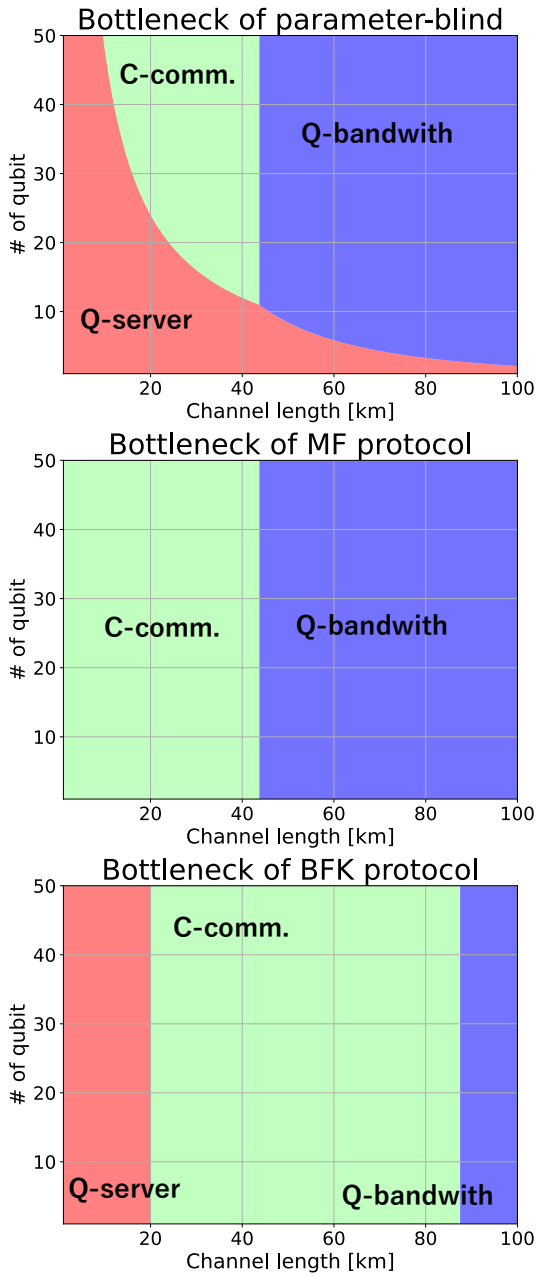


Figure 3: The distribution of bottlenecks for each protocol. The horizontal axis indicates the distance between the client and server, and the vertical axis represents the problem size, as defined by the number of qubits in the Ansatz.

Acknowledgment

MN, HK, and TS are supported by JST Moonshot R&D Grant Number JPMJMS226C. TS is also supported by JST COI-NEXT Grant Number JPMJPF2221 and MEXT KAKENHI Grant Number 22K1978.

References

[1] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th annual IEEE symposium on foundations of computer science*, pages 517–526. IEEE, 2009.

[2] Colin D Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M Sage. Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, 6(2), 2019.

[3] Jian-Long Liu, Xi-Yu Luo, Yong Yu, Chao-Yang Wang, Bin Wang, Yi Hu, Jun Li, Ming-Yang Zheng, Bo Yao, Zi Yan, et al. A multinode quantum network over a metropolitan area. *arXiv preprint arXiv:2309.00221*, 2023.

[4] Tomoyuki Morimae and Keisuke Fujii. Blind quantum computation protocol in which alice only makes measurements. *Physical Review A*, 87(5):050301, 2013.

[5] P J J O'Malley, R Babbush, I D Kivlichan, J Romero, J R McClean, R Barends, J Kelly, P Roushan, A Tranter, N Ding, B Campbell, Y Chen, Z Chen, B Chiaro, A Dunsworth, A G Fowler, E Jeffrey, E Lucero, A Megrant, J Y Mutus, M Neeley, C Neill, C Quintana, D Sank, A Vainsencher, J Wenner, T C White, P V Coveney, P J Love, H Neven, A Aspuru-Guzik, and J M Martinis. Scalable quantum simulation of molecular energies. *Phys. Rev. X*, 6(3):031007, July 2016.

[6] Matteo Pompili, Sophie LN Hermans, Simon Baier, Hans KC Beukers, Peter C Humphreys, Raymond N Schouten, Raymond FL Vermeulen, Marijn J Tiggelman, Laura dos Santos Martins, Bas Dirkse, et al. Realization of a multinode quantum network of remote solid-state qubits. *Science*, 372(6539):259–264, 2021.

[7] Yuta Shingu, Yuki Takeuchi, Suguru Endo, Shiro Kawabata, Shohei Watabe, Tetsuro Nikuni, Hideaki Hakoshima, and Yuichiro Matsuzaki. Variational secure cloud quantum computing. *Physical Review A*, 105(2):022603, 2022.

Quantifying non-Gaussianity of a quantum state by the negative entropy of quadrature distributions

Jiyong Park[1] * Jaehak Lee[2] Kyunghyun Baek[2] Hyunchul Nha[3]

[1] *School of Basic Sciences, Hanbat National University, Daejeon, 34158, Korea*
[2] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 02455, Korea*
[3] *Department of Physics, Texas A&M University at Qatar, Education City, P.O. Box 23874, Doha, Qatar*

Abstract. We propose a non-Gaussianity measure of a multimode quantum state based on the negentropy of quadrature distributions. Our measure satisfies desirable properties as a non-Gaussianity measure, i.e., faithfulness, invariance under Gaussian unitary operations, and monotonicity under Gaussian channels. Furthermore, we find a quantitative relation between our measure and the previously proposed non-Gaussianity measures defined via quantum relative entropy and the quantum Hilbert-Schmidt distance. This allows us to estimate the non-Gaussianity measures readily by homodyne detection, which would otherwise require a full quantum-state tomography.

Keywords: non-Gaussianity, negentropy, homodyne detection

1 Introduction

In continuous variable (CV) quantum information, non-Gaussian resources are essential as several CV quantum information tasks are not achievable by Gaussian resources only. Addressing the role of non-Gaussianity in CV quantum information rigorously, it is desirable to quantify the non-Gaussianity of quantum resources. In this regard, there have been several proposals to characterize the non-Gaussianity of quantum states, e.g., employing quantum Hilbert-Schmidt distance [1], quantum relative entropy [2], and Wigner-Yanase skew information [3]. While the previously proposed measures have provided a valuable basis for analyzing non-Gaussian resources, it is difficult to determine the values of those measures without the complete information on the state under examination. With this in mind, for non-Gaussianity measure via quantum relative entropy, an observable lower bound was provided using the statistics from a photon-number-resolving detector [4]. However, it works when there is a priori information, i.e., the covariance matrix of a quantum state. Thus, it is natural to ask whether we can estimate the non-Gaussianity of a quantum state by a readily accessible measurement setup, e.g., homodyne detection. In addition, it is worth investigating whether we can define a desirable non-Gaussianity measure for general multi-mode quantum states utilizing the non-Gaussianity manifested by a quadrature distribution. Here we propose a non-Gaussianity measure of a quantum state in terms of the maximum negentropy of quadrature distributions [5]. Our measure fulfills several desirable properties. It is non-negative, faithful, invariant under Gaussian unitary operations, non-increasing under Gaussian channels. Furthermore, we show that our measure provides lower bounds for non-Gaussianty measures based on quantum relative entropy and quantum Hilbert-Schmidt distance. These quantitative connections make our approach valuable to address a general quantum non-Gaussian state by a highly efficient homodyne detection.

*jiyong.park@hanbat.ac.kr

2 Non-Gaussianity measure by classical relative entropy

In classical information theory, a representative measure for the non-Gaussianity of a probability distribution is negentropy [6]. It quantifies the relative entropy between a given probability distribution X and its reference Gaussian distribution $X_{\rm G}$ having the same mean and variance as X,

$$J(X) \equiv D_{\rm KL}(X||X_{\rm G}), \tag{1}$$

where $D_{\rm KL}(X||Y) = \int d\mu X(\mu)[\ln X(\mu) - \ln Y(\mu)]$ is the Kullback-Leibler divergence [7], also known as classical relative entropy, between two probability distributions X and Y. It is known that Eq. (1) can be rewritten simply as

$$J(X) = H(X_{\rm G}) - H(X), \tag{2}$$

where $H(X) = -\int d\mu X(\mu) \ln X(\mu)$ is the differential entropy of a probability distribution X [8].

2.1 Our measure

We here define a non-Gaussianity measure of an N-mode quantum state ρ by means of negentropy as

$$\mathcal{N}_{\rm KL}(\rho) = \max_{\Theta,\Phi} J_\rho(Q_{\Theta,\Phi}), \tag{3}$$

where $Q_{\Theta,\Phi}$ denotes a probability distribution for an N-mode quadrature operator $\hat{Q}_{\Theta,\Phi}$ given by

$$\hat{Q}_{\Theta,\Phi} = \sum_{j=1}^{N} c_j \hat{q}_{j,\phi_j}. \tag{4}$$

Here $\hat{q}_{j,\phi_j} = \frac{1}{\sqrt{2}}(\hat{a}_j e^{i\phi_j} + \hat{a}_j^\dagger e^{-i\phi_j})$ is a quadrature amplitude for the jth mode, $\Phi = (\phi_1, \phi_2, ..., \phi_N)^T$ the set of quadrature phases ϕ_j, and $\Theta = (\theta_1, \theta_2, ..., \theta_{N-1})^T$ the set

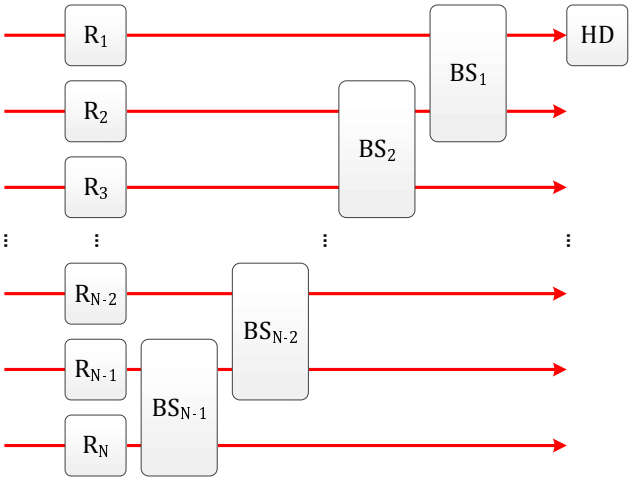


Figure 1: Linear optical network for measuring the probability distribution $Q_{\Theta,\Phi}$. R_j and BS_k represent the phase rotation on the jth mode and the beam-splitting operation between the kth and $(k+1)$th modes, respectively. Applying these Gaussian unitary operations and performing homodyne detection (HD) on the first mode, we obtain the probability distribution $Q_{\Theta,\Phi}$ for the input state.

of angular coordinates that determines the superposition coefficient c_j in Eq. (4) as

$$c_j = \begin{cases} \cos\theta_1 & \text{for } j=1, \\ \cos\theta_j \prod_{k=1}^{j-1} \sin\theta_k & \text{for } 1<j<N, \\ \prod_{k=1}^{N-1} \sin\theta_k & \text{for } j=N. \end{cases} \tag{5}$$

Before introducing the properties of our measure, we briefly explain how the probability distribution $Q_{\Theta,\Phi}$ can be experimentally accessible. Using a Heisenberg picture, we see that the N-mode quadrature $\hat{Q}_{\Theta,\Phi}$ in Eq. (4) can be addressed via a linear optical network composed of beam splitters and phase shifters as

$$\hat{Q}_{\Theta,\Phi} = \hat{L}^\dagger \hat{q}_{1,0} \hat{L}, \tag{6}$$

where the Gaussian unitary operation $\hat{L}$ for the linear optical network is given by

$$\hat{L} = \hat{B}_{1,2}(\theta_1)\cdots\hat{B}_{N-1,N}(\theta_{N-1})\hat{R}_1(\phi_1)\cdots\hat{R}_N(\phi_N), \tag{7}$$

with $\hat{R}_j(\phi) = \exp(i\phi\hat{a}_j^\dagger\hat{a}_j)$ and $\hat{B}_{j,k}(\theta) = \exp(\theta\hat{a}_j^\dagger\hat{a}_k - \theta\hat{a}_k^\dagger\hat{a}_j)$ representing the phase rotation on the jth mode and the beam-splitting operation between the jth and kth modes with the transmittance $T = \cos^2\theta$, respectively (see Fig. 1). Using $\hat{R}_j^\dagger(\phi)\hat{q}_{j,0}\hat{R}_j(\phi) = \hat{q}_{j,\phi}$ and $\hat{B}_{jk}^\dagger(\theta)q_{j,0}\hat{B}_{jk}(\theta) = \cos\theta\hat{q}_{j,0} + \sin\theta\hat{q}_{k,0}$ [9, 10], Eq. (6) gives the result in Eq. (4). The relation in Eq. (6) implies that we obtain the probability distribution $Q_{\Theta,\Phi}$ by a single-mode homodyne detection using a linear optical network. Note that one can fully reconstruct the N-mode quantum state ρ by examining the whole set of $Q_{\Theta,\Phi}$ [11].

2.2 Properties

Our measure has the following properties:

1. The measure is non-negative. $\mathcal{N}_{\mathrm{KL}}(\rho) \geq 0$.
2. The measure is faithful. That is, $\mathcal{N}_{\mathrm{KL}}(\rho)$ is zero if and only if the state ρ is Gaussian.
3. The measure is invariant under Gaussian unitary operations, i.e., $\mathcal{N}_{\mathrm{KL}}(\hat{U}_{\mathrm{G}}\rho\hat{U}_{\mathrm{G}}^\dagger) = \mathcal{N}_{\mathrm{KL}}(\rho)$, where $\hat{U}_{\mathrm{G}}$ is a Gaussian unitary operation.
4. The measure is nonincreasing under partial trace. $\mathcal{N}_{\mathrm{KL}}(\rho_{AB}) \geq \mathcal{N}_{\mathrm{KL}}(\rho_A)$.
5. The measure is invariant under the addition of Gaussian ancilla, i.e., $\mathcal{N}_{\mathrm{KL}}(\rho\otimes\sigma) = \mathcal{N}_{\mathrm{KL}}(\rho)$ with a Gaussian state σ.
6. The measure is nonincreasing under a Gaussian channel $\mathcal{T}_{\mathrm{G}}$, i.e., $\mathcal{N}_{\mathrm{KL}}(\mathcal{T}_{\mathrm{G}}[\rho]) \leq \mathcal{N}_{\mathrm{KL}}(\rho)$.

3 Estimating non-Gaussianity measure defined by quantum relative entropy

In [2], a non-Gaussianity measure of a quantum state was proposed by employing quantum relative entropy as

$$\mathcal{N}_{\mathrm{QR}}(\rho) \equiv S(\rho||\rho_{\mathrm{G}}), \tag{8}$$

where $S(\rho||\rho_G) = \mathrm{tr}[\rho(\ln\rho - \ln\rho_G)]$ is the quantum relative entropy between ρ and its reference Gaussian state ρ_{G} with the same first- and second-order quadrature moments as the state ρ. Note that we have used the subscript QR to imply that the measure is based on quantum relative entropy. Similar to the negentropy, i.e., $J(X) \equiv D_{\mathrm{KL}}(X||X_{\mathrm{G}}) = H(X_{\mathrm{G}}) - H(X)$, the measure based on the quantum relative entropy can also be given by the difference between the von Neumann entropies of ρ and ρ_G,

$$\mathcal{N}_{\mathrm{QR}}(\rho) = S_1(\rho_{\mathrm{G}}) - S_1(\rho), \tag{9}$$

where $S_1(\tau) = -\mathrm{tr}[\tau\ln\tau]$ is the von Neumann entropy of a quantum state τ.

Our measure $\mathcal{N}_{\mathrm{KL}}(\rho)$ provides a lower bound for $\mathcal{N}_{\mathrm{QR}}(\rho)$ as

$$\mathcal{N}_{\mathrm{QR}}(\rho) \geq \mathcal{N}_{\mathrm{KL}}(\rho). \tag{10}$$

3.1 Application in entanglement detection

It is worth noting that the inequality (10) can be used to derive a new uncertainty relation whose bound is determined by the non-Gaussianity and the entropy of the state (cf. [12]). For a Gaussian state, we have the identity $S_1(\rho_{\mathrm{G}}) = h(\sqrt{\det\Gamma})$, where $h(x) = (x+\frac{1}{2})\ln(x+\frac{1}{2}) - (x-\frac{1}{2})\ln(x-\frac{1}{2})$. That is, the von Neumann entropy of a Gaussian state is completely determined by the covariance matrix. The inequality (10), which can be written as $S_1(\rho_{\mathrm{G}}) \geq S_1(\rho) + \mathcal{N}_{\mathrm{KL}}(\rho)$, then leads to $h(\sqrt{\det\Gamma(\rho)}) \geq \mathcal{N}_{\mathrm{KL}}(\rho) + S_1(\rho)$. Therefore, we obtain

$$\sqrt{\det\Gamma(\rho)} \geq h^{-1}(\mathcal{N}_{\mathrm{KL}}(\rho) + S_1(\rho)), \tag{11}$$

where $h^{-1}(y)$ is the inverse of the monotonically increasing function $h(x)$. This uncertainty relation can be considered as a generalization of the Robertson-Schrödinger (RS) uncertainty relation $\sqrt{\det\Gamma} \geq \frac{1}{2}$, because the relation (11) gives a stronger bound, particularly for non-Gaussian or mixed states, i.e., when $\mathcal{N}_{\mathrm{KL}}(\rho) > 0$ or $S_1(\rho) > 0$, respectively.

Non-Gaussianity- and entropy-bounded uncertainty relations such as Eq. (11) are potentially applicable to improve Simon-Duan entanglement criterion [13, 14], which is a necessary and sufficient criterion for Gaussian states only. For example, if the inequality Eq. (11) is violated under partial transposition, it is a direct signature of quantum entanglement. The inequality, Eq. (11), thus leads to improved entanglement criteria, particularly for non-Gaussian entangled states, like those in [12].

4 Estimation of non-Gaussianity measure by Hilbert-Schmidt distance

In [1], a non-Gaussianity measure of a quantum state was proposed by using Hilbert-Schmidt distance as

$$\mathcal{N}_{\rm HS}(\rho) = \frac{D_{\rm HS}(\rho, \rho_{\rm G})}{2{\rm tr}\rho^2}, \tag{12}$$

where $D_{\rm HS}(\rho, \rho_{\rm G}) = {\rm tr}(\rho - \rho_{\rm G})^2$ is the Hilbert-Schmidt distance between ρ and $\rho_{\rm G}$.

Our measure $\mathcal{N}_{\rm KL}(\rho)$ provides a lower bound for $\mathcal{N}_{\rm HS}(\rho)$ as

$$\mathcal{N}_{\rm HS}(\rho) \geq \frac{1}{2}\{1 - \mathcal{F}_N(\rho)\}^2, \tag{13}$$

with

$$\mathcal{F}_N(\rho) = \min\left[1, \exp\left\{-\frac{\mathcal{N}_{\rm KL}(\rho)}{2} + \frac{N}{2}\ln\frac{e}{2}\right\}\right]. \tag{14}$$

5 Discussion

We have proposed the maximum negentropy of quadrature distributions as a non-Gaussianity measure of a general N-mode quantum state. Our measure fulfills desirable properties, i.e., it is faithful, invariant under a Gaussian unitary operation, and nonincreasing under a trace-preserving Gaussian channel. Furthermore, we have shown that our measure provides lower bounds for other non-Gaussianity measures based on quantum relative entropy and Hilbert-Schmidt distance, respectively. As our measure is experimentally accessible by a highly efficient homodyne detection, the connection between our measure and others makes it possible to address the issue of non-Gaussianity in an experimentally friendly form. Therefore we hope our approach could be broadly adopted in assessing the role of non-Gaussianity in continuous-variable quantum information protocols.

References

[1] M. G. Genoni, M. G. A. Paris, and K. Banaszek, Phys. Rev. A **76**, 042327 (2007).

[2] M. G. Genoni, M. G. A. Paris, and K. Banaszek, Phys. Rev. A **78**, 060303(R) (2008).

[3] S. Fu, S. Luo, and Y. Zhang, Phys. Rev. A **101**, 012125 (2020).

[4] M. G. Genoni and M. G. A. Paris, Phys. Rev. A **82**, 052341 (2010).

[5] J. Park, J. Lee, K. Baek, and H. Nha, Phys. Rev. A **104**, 032415 (2021).

[6] E. Schrödinger, *What Is Life? The Physical Aspect of the Living Cell* (Cambridge University Press, Cambridge, 1944).

[7] T. van Erven and P. Harremoës, IEEE Trans. Inf. Theor. **60**, 3797 (2014).

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley-Interscience, New York, 2006).

[9] S. Olivares, Eur. Phys. J. Spec. Top. **203**, 3 (2012).

[10] S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics* (Clarendon Press, Oxford, 1997).

[11] G. M. D'Ariano, M. F. Sacchi, and P. Kumar, Phys. Rev. A **61**, 013806 (1999).

[12] K. Baek and H. Nha, Phys. Rev. A **98**, 042314 (2018).

[13] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).

[14] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).

Limitations of Classically-Simulable Measurements for Quantum State Discrimination

Chengkai Zhu[1] Zhiping Liu[1 2] Chenghong Zhu[1] Xin Wang[1]

[1] *The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511453, China*
[2]*Nanjing University, Nanjing 210093, China*

Abstract. In the realm of fault-tolerant quantum computing, stabilizer operations play a pivotal role, characterized by their remarkable efficiency in classical simulation. In this work, we investigate the limitations of classically-simulable measurements in distinguishing quantum states. We demonstrate that any pure magic state and its orthogonal complement of odd prime dimensions cannot be unambiguously distinguished by stabilizer operations, regardless of how many copies of the states are supplied. We reveal intrinsic similarities and distinctions between the quantum resource theories of magic states and entanglement in quantum state discrimination. The results emphasize the inherent limitations of classically-simulable measurements and contribute to a deeper understanding of the quantum-classical boundary.

Keywords: Quantum state discrimination, quantum resource theory, classically-simulable measurement, magic state.

Background. The computational power of quantum computers for solving computationally challenging problems [1–5] can only be unlocked with a scalable quantum computing solution. Fault-tolerant quantum computation (FTQC) provides a scheme to overcome obstacles of physical implementation such as decoherence and inaccuracies [6–8]. A cornerstone of the FTQC resides in stabilizer circuits which can be efficiently classically simulated [9], and therefore do not confer any quantum computational advantage. However, the so-called *magic state* can promote the stabilizer circuits to universal quantum computation via state injection [10–12]. In this context, the magic states and non-stabilizer operations characterize the computational power of universal quantum computation.

While extensive research has explored the stabilizerness of quantum states and gates within circuits [13, 14], a crucial yet underexplored facet is the stabilizerness of quantum measurements [15] – a critical process for reliably decoding classical information encoded in quantum states. In general, it is not applicable for one to access the physical properties of a locally interacting quantum many-body system by classical simulation. However, when information is encoded in a stabilizer state, the decoding process via stabilizer measurements remains efficiently classically simulable [16]. This prompts a fundamental question: can stabilizer measurements perfectly decode all tasks, or are there inherent limitations? Investigating the distinction in decoding capabilities between stabilizer measurements, which are classically efficiently simulable, and other measurements becomes paramount for understanding the intricate relationship between classical information encoded in quantum states and the measurement process.

In fact, the ability to retrieve classical information from quantum systems varies significantly with different measurements. One celebrated example is the quantum nonlocality without entanglement [17]. This primitive gap between distinct classes of measurements makes quantum state discrimination (QSD) a crucial aspect of fundamental physics [18, 19]. It also has fruitful applications in quantum cryptography [20–22], quantum dimension witness [23, 24] and quantum data hiding [25–27]. Inspired by the intrinsic behavior of different measurements in entanglement theory [28–35], a natural question arises: is there a sharp gap between the classically-simulable measurements and those that could potentially promote universal quantum computation? If such a gap exists, it will imply considerable advantages that the resource of magic states can provide to the measurement in quantum information processing.

Overview of results: In this work, we give an affirmative answer to this question. Our results imply considerable advantages that the quantum resource of magic states can provide to measurements in quantum information processing. In particular, we establish the following results:

1. **Limitations of Classically Simulable**

Measurements: We demonstrate that any pure magic state and its orthogonal complement cannot be unambiguously distinguished via PWF POVMs (positive operator-valued measures with positive discrete Wigner functions), which are classically-simulable and strictly include stabilizer measurements, no matter how many copies of the states are supplied.

2. **Minimum error discrimination by PWF POVMs:** We study the minimum error QSD via PWF POVMs. There is an exponential decay in the asymptotic minimal error probability for distinguishing the Strange state and its orthogonal complement via PWF POVMs.

3. **Comparison between QRT of magic states and entanglement in QSD:** We establish a comparison between the quantum resource theory of magic states and the entanglement theory within the task of quantum state discrimination, including their similarities and distinctions.

Limitations of Classically Simulable Measurements: Our first contribution is to reveal the asymptotic limits of PWF POVMs for discriminating a pair of quantum states. In odd prime dimensions, quantum circuits with initial states and all subsequent quantum operations having PWFs, which strictly include stabilizer (STAB) operations, admit efficient classical simulations [16, 36]. On the contrary, negativity in Wigner functions is usually regarded as an indication of 'nonclassicality' [37, 38] and identified as a computational resource. Let $\mathbf{E} = \{E_j\}_{j=0}^{n-1}$ be a n-valued POVM acting on $\mathcal{H}_d$ with $\sum_{j=0}^{n-1} E_j = I_d$. $\mathbf{E}$ is said to be a PWF POVM if each E_j has positive discrete Wigner functions. Thus, PWF POVMs are recognized as classically-simulable measurements [39]. They strictly include all STAB POVMs as STAB POVMs $\subsetneq$ PWF POVMs $\subsetneq$ All POVMs [12].

It is well-known that the asymptotic regime of QSD can unravel the underlying mechanism of entanglement [31, 34, 40], and a particularly simple yet insightful scenario for QSD is to discriminate a pure state and its orthogonal complement. Notably, in the regime of many copies, greater flexibility and options exist for the potential POVMs. However, our main result is to show a wide range of quantum states that cannot be unambiguously distinguished via PWF POVMs, including STAB POVMs, no matter how many copies are supplied.

Theorem 1 *Let $\rho_0 \in \mathcal{D}(\mathcal{H}_d)$ be a pure magic state and $\rho_1 = (I_d - \rho_0)/(d-1)$ be its orthogonal complement, where I_d is the identity. Then for any integer $n \in \mathbb{Z}^+$, $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$ cannot be unambiguously distinguished by PWF POVMs.*

From the angle of quantum resource theories (QRTs) [41], this theorem unravels the difficulty of distinguishing a pure resourceful state and its orthogonal complement via free operations in the QRT of magic states. Technically, we develop the notion of *PWF unextendible* subspace for the proof of Theorem 1 and prove the theorem based on Lemma 2. We call a subspace $\mathcal{S} \subseteq \mathcal{H}_d$ *PWF unextendible* if there is no PWF state ρ whose support is a subspace of $\mathcal{S}^\perp$, and *PWF extendible* otherwise. A subspace $\mathcal{S} \subseteq \mathcal{H}_d$ is called *strongly PWF unextendible* if for any positive integer n, $\mathcal{S}^{\otimes n}$ is PWF unextendible. The unextendibility of subspaces indicates the distinguishability of quantum states and the following lemma implies the asymptotic distinguishability of quantum states by PWF POVMs.

Lemma 2 *For a PWF unextendible subspace $\mathcal{S} \subseteq \mathcal{H}_d$, if there is a PWF state $\rho \in \mathcal{D}(\mathcal{S})$ such that $\mathrm{supp}(\rho) = \mathcal{S}$, then $\mathcal{S}$ is strongly PWF unextendible.*

Minimum error discrimination by PWF POVMs: Our second contribution is to study the minimum error QSD which unveils the capabilities inherent in PWF POVMs. For states ρ_0 and ρ_1 with prior probability p and $1-p$, respectively, we denote $P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0, \rho_1, p)$ as the optimal error probability of distinguishing them by PWF POVMs. Mathematically, this optimal error probability can be expressed via semidefinite programming (SDP) [42]. For ρ_0 to be the Strange state and ρ_1 to be its orthogonal complement, we demonstrate the following asymptotic error behavior.

Proposition 3 *Let ρ_0 be the Strange state $|\mathbb{S}\rangle\langle\mathbb{S}|$ and $\rho_1 = (I - |\mathbb{S}\rangle\langle\mathbb{S}|)/2$ be its orthogonal complement. For $n \in \mathbb{Z}^+$, we have*

$$P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}, \frac{1}{2}) = \frac{1}{2^{n+1}}. \tag{1}$$

The optimal PWF POVM is $\{E, I - E\}$, where $E = (|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)^{\otimes n}$ and $|\mathbb{K}\rangle = (|1\rangle + |2\rangle)/\sqrt{2}$.

It can be seen that the optimal error probability will exponentially decay with respect to the number of copies supplied. Nevertheless, it is important to note that the error persists for all finite values of n, aligning with the indistinguishability established in Theorem 1. The celebrated

quantum Chernoff theorem [43–45] establishes that $\xi_C(\rho_0,\rho_1) := \lim_{n\to\infty} -\frac{1}{n}\log P_e(\rho_0^{\otimes n},\rho_1^{\otimes n},p) = -\min_{0\le s\le 1}\log \mathrm{Tr}[\rho_0^{1-s}\rho_1^s]$, where $P_e(\rho_0^{\otimes n},\rho_1^{\otimes n},p)$ is the average error of distinguishing ρ_0 and ρ_1 via global measurements, $\xi_C(\rho_0,\rho_1)$ is the so-called Chernoff exponent. The Chernoff exponent concerning a specific class of measurements, e.g., $\{\mathrm{LOCC},\mathrm{PPT},\mathrm{SEP}\}$, is defined in [40]. The authors proved that the Chernoff bounds in these cases are indeed faithful by showing an exponential decay of $P_e^X(\rho_0,\rho_1,p)$ where $X\in\{\mathrm{LOCC},\mathrm{PPT},\mathrm{SEP}\}$. Similarly, Proposition 3 may give an insight that the Chernoff bound concerning PWF measurements is also faithful.

It further has applications in quantum data hiding [25, 46, 47] considering a scenario in which information is encoded in a way that Pauli measurements have less capability of decoding it than arbitrary measurements. Then only the party with the ability to generate magic can reliably retrieve the message. Here, we define $\|\cdot\|_{\mathrm{PWF}}$ and $R(\mathrm{PWF})$ as the *distinguishability norm* and the *data-hiding ratio* [47] associated with PWF POVMs, respectively. Proposition 3 directly gives a lower bound on the *data-hiding ratio* against PWF POVMs as follows.

$$R(\mathrm{PWF}) = \max \frac{\|p\rho-(1-p)\sigma\|_{\mathrm{All}}}{\|p\rho-(1-p)\sigma\|_{\mathrm{PWF}}} \ge \frac{1}{1-2^{-n}}.$$

Comparison between QRT of magic states and entanglement in QSD: Our third contribution is to establish a comparison between the QRT of magic states and the entanglement theory within QSD, including their similarities and distinctions as summarized in Table 1.

For similarities, we note the asymptotic limit of PWF POVMs is an analog to the phenomenon in entanglement theory that any pure entangled state and its orthogonal complement cannot be unambiguously distinguished via PPT POVMs with an arbitrary number of copies provided [40, 48, 49]. However, they can always be perfectly distinguished if global measurements are allowed. For distinctions, recall that the unextendible product basis (UPB) in entanglement theory indicates the indistinguishability of orthogonal product states using LOCC operations [35]. We show that in the QRT of magic states, there is no similar phenomenon as the UPB in entanglement theory. That is there is no incomplete orthogonal stabilizer basis whose complementary subspace contains no stabilizer state.

Theorem 4 *For a subspace $\mathcal{S}\in\mathcal{H}_d$, if $\mathcal{S}$ has a set of basis $\{|\psi_i\rangle\}_{i=1}^n$ where every $|\psi_i\rangle$ is a stabilizer state, then $\mathcal{S}$ is PWF extendible.*

	QRT of magic states	QRT of entanglement
Asymptotic limits of free POVMs	✔	✔
Existence of UPB phenomenon	✗	✔
Perfect discrimination with the aid of one copy of maximal resource	✗	✔

Table 1: Comparison between the QRT of magic states and entanglement.

A direct consequence of this theorem is that any set of orthogonal pure stabilizer states $\{|\psi\rangle_i\}_{i=1}^n$ can be unambiguously distinguished via PWF POVMs as we can choose $E_i = |\psi_i\rangle\langle\psi_i|$ for $i=1,2,\cdots,n$ and $E_{n+1} = I - \sum_{i=1}^n |\psi_i\rangle\langle\psi_i|$. Therefore, we demonstrate the absence of an analogous UPB phenomenon in the QRT of magic states.

Besides, the distinction emerges when considering the minimum resource required to achieve optimal discrimination via free operations. It was shown that one copy of the Bell state is always sufficient for perfectly distinguishing any pure state ρ_0 and its orthogonal complement ρ_1 via PPT POVMs [48], i.e., distinguishing $\rho_0\otimes\Phi_2^+$ and $\rho_1\otimes\Phi_2^+$. However, things are different in the QRT of magic states where we show that the Strange state and its orthogonal complement cannot be perfectly distinguished by PWF POVMs with the assistance of one or two copies of any qutrit magic state.

Proposition 5 *Let ρ_0 be the Strange state $|\mathbb{S}\rangle\langle\mathbb{S}|$ and $\rho_1 = (I-|\mathbb{S}\rangle\langle\mathbb{S}|)/2$ be its orthogonal complement. $\rho_0\otimes\tau^{\otimes k}$ and $\rho_1\otimes\tau^{\otimes k}$ cannot be perfectly distinguished for any qutrit magic state τ and $k=1$ or 2.*

Concluding remarks: We have explored the limitations of PWF POVMs which can be efficiently classically simulated and strictly include all stabilizer measurements. Our results show that the QRT of magic states and entanglement exhibit significant similarities and distinctions in quantum state discrimination. These results have implications in various fields, including connections between the QRT of magic states and quantum data hiding [27, 46, 47, 50], limits of stabilizer measurements or classically-simulable ones in quantum channel discrimination [51–53] and other operational tasks [54–56].

References

[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, oct 1997. URL https://doi.org/10.1137%2Fs0097539795293172.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996.

[3] Andrew M. Childs and Wim van Dam. Quantum algorithms for algebraic problems. *Rev. Mod. Phys.*, 82:1–52, Jan 2010. URL https://link.aps.org/doi/10.1103/RevModPhys.82.1.

[4] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996. URL https://www.science.org/doi/10.1126/science.273.5278.1073.

[5] 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, sep 2018. URL https://doi.org/10.1073%2Fpnas.1801723115.

[6] Peter W. Shor. Fault-tolerant quantum computation, 1997.

[7] Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, sep 2017. doi: 10.1038/nature23460. URL https://doi.org/10.1038%2Fnature23460.

[8] Emanuel Knill. Quantum computing with realistically noisy devices. *Nature*, 434(7029):39–44, 2005. URL https://www.nature.com/articles/nature03350.

[9] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997. URL https://arxiv.org/abs/quant-ph/9705052.

[10] Xinlan Zhou, Debbie W. Leung, and Isaac L. Chuang. Methodology for quantum logic gate construction. *Physical Review A*, 62(5), oct 2000. doi: 10.1103/physreva.62.052316. URL https://doi.org/10.1103%2Fphysreva.62.052316.

[11] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, nov 1999. doi: 10.1038/46503. URL https://doi.org/10.1038%2F46503.

[12] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A*, 71(2), feb 2005. doi: 10.1103/physreva.71.022316. URL https://doi.org/10.1103%2Fphysreva.71.022316.

[13] Earl T. Campbell, Hussain Anwar, and Dan E. Browne. Magic-state distillation in all prime dimensions using quantum reed-muller codes. *Physical Review X*, 2(4), dec 2012. URL https://doi.org/10.1103%2Fphysrevx.2.041021.

[14] Mithuna Yoganathan, Richard Jozsa, and Sergii Strelchuk. Quantum advantage of unitary clifford circuits with magic state inputs. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 475(2225):20180427, may 2019. URL https://doi.org/10.1098%2Frspa.2018.0427.

[15] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[16] A. Mari and J. Eisert. Positive wigner functions render classical simulation of quantum computation efficient. *Physical Review Letters*, 109(23):1–7, 2012. ISSN 00319007. doi: 10.1103/PhysRevLett.109.230503. URL http://dx.doi.org/10.1103/PhysRevLett.109.230503.

[17] Charles H Bennett, David P DiVincenzo, Christopher A Fuchs, Tal Mor, Eric Rains, Peter W Shor, John A Smolin, and William K Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070–1091, feb 1999. ISSN 1050-2947. doi: 10.1103/PhysRevA.59.1070. URL https://link.aps.org/doi/10.1103/PhysRevA.59.1070.

[18] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, 2015. URL http://dx.doi.org/10.1088/1751-8113/48/8/083001.

[19] Willian H. G. Correa, Ludovico Lami, and Carlos Palazuelos. Maximal gap between local and

global distinguishability of bipartite quantum states. *IEEE Transactions on Information Theory*, 68(11):7306–7314, nov 2022. URL https://doi.org/10.1109%2Ftit.2022.3186428.

[20] Nicolas Gisin, Gré goire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, mar 2002. URL https://doi.org/10.1103%2Frevmodphys.74.145.

[21] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83(3):648–651, jul 1999. URL https://doi.org/10.1103%2Fphysrevlett.83.648.

[22] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102(18), may 2009. URL https://doi.org/10.1103%2Fphysrevlett.102.180504.

[23] Nicolas Brunner, Miguel Navascué s, and Tamás Vértesi. Dimension witnesses and quantum state discrimination. *Physical Review Letters*, 110(15), apr 2013. URL https://doi.org/10.1103%2Fphysrevlett.110.150501.

[24] Martin Hendrych, Rodrigo Gallego, Michal Mičuda, Nicolas Brunner, Antonio Acín, and Juan P. Torres. Experimental estimation of the dimension of classical and quantum systems. *Nature Physics*, 8(8):588–591, jun 2012. doi: 10.1038/nphys2334. URL https://doi.org/10.1038%2Fnphys2334.

[25] Barbara M. Terhal, David P. DiVincenzo, and Debbie W. Leung. Hiding bits in bell states. *Phys. Rev. Lett.*, 86:5807–5810, Jun 2001. doi: 10.1103/PhysRevLett.86.5807. URL https://link.aps.org/doi/10.1103/PhysRevLett.86.5807.

[26] T. Eggeling and R. F. Werner. Hiding classical data in multipartite quantum states. *Phys. Rev. Lett.*, 89:097905, Aug 2002. doi: 10.1103/PhysRevLett.89.097905. URL https://link.aps.org/doi/10.1103/PhysRevLett.89.097905.

[27] William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, 2009. ISSN 00103616. doi: 10.1007/s00220-009-0890-5.

[28] Debbie Leung, Andreas Winter, and Nengkun Yu. LOCC protocols with bounded width per round optimize convex functions. *Reviews in Mathematical Physics*, 33(05):2150013, jan 2021. doi: 10.1142/s0129055x21500136. URL https://doi.org/10.1142%2Fs0129055x21500136.

[29] Somshubhro Bandyopadhyay, Alessandro Cosentino, Nathaniel Johnston, Vincent Russo, John Watrous, and Nengkun Yu. Limitations on separable measurements by convex optimization. *IEEE Transactions on Information Theory*, 61(6):3593–3604, 2015. doi: 10.1109/TIT.2015.2417755. URL https://web.stanford.edu/~boyd/cvxbook/.

[30] Andrew M Childs, Debbie Leung, Laura Mančinska, and Maris Ozols. A framework for bounding nonlocality of state discrimination. *Communications in Mathematical Physics*, 323(3):1121–1153, 2013. doi: 10.1007/s00220-013-1784-0.

[31] Somshubhro Bandyopadhyay. More nonlocality with less purity. *Physical Review Letters*, 106 (21):1–4, 2011. ISSN 00319007. doi: 10.1103/PhysRevLett.106.210402. URL http://dx.doi.org/10.1103/PhysRevLett.106.210402.

[32] J. Calsamiglia, J. I. De Vicente, R. Muñoz-Tapia, and E. Bagan. Local discrimination of mixed states. *Physical Review Letters*, 105 (8):1–4, 2010. ISSN 00319007. doi: 10.1103/PhysRevLett.105.080504.

[33] Saronath Halder, Manik Banik, Sristy Agrawal, and Somshubhro Bandyopadhyay. Strong Quantum Nonlocality without Entanglement. *Physical Review Letters*, 122(4):40403, 2019. ISSN 10797114. URL https://doi.org/10.1103/PhysRevLett.122.040403.

[34] Jonathan Walgate, Anthony J Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85(23): 4972, 2000. URL http://dx.doi.org/10.1103/PhysRevLett.85.4972.

[35] Charles H. Bennett, David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin,

and Barbara M. Terhal. Unextendible Product Bases and Bound Entanglement. *Physical Review Letters*, 82(26):5385–5388, jun 1999. ISSN 0031-9007. doi: 10.1103/PhysRevLett.82.5385. URL https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.82.5385https://link.aps.org/doi/10.1103/PhysRevLett.82.5385.

[36] Victor Veitch, Christopher Ferrie, David Gross, and Joseph Emerson. Negative quasi-probability as a resource for quantum computation. *New Journal of Physics*, 14:1–15, 2012. ISSN 13672630. doi: 10.1088/1367-2630/14/11/113011.

[37] Ernesto F. Galvã o. Discrete wigner functions and quantum computational speedup. *Physical Review A*, 71(4), apr 2005. URL https://doi.org/10.1103%2Fphysreva.71.042302.

[38] Cecilia Cormick, Ernesto F. Galvã o, Daniel Gottesman, Juan Pablo Paz, and Arthur O. Pittenger. Classicality in discrete wigner functions. *Physical Review A*, 73(1), jan 2006. URL https://doi.org/10.1103%2Fphysreva.73.012301.

[39] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the 'magic' for quantum computation. *Nature*, 510(7505):351–355, jun 2014. URL https://doi.org/10.1038%2Fnature13460.

[40] Hao-Chung Cheng, Andreas Winter, and Nengkun Yu. Discrimination of quantum states under locality constraints in the many-copy setting. *Communications in Mathematical Physics*, pages 1–33, 2023. URL http://dx.doi.org/10.1007/s00220-023-04836-0.

[41] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2), apr 2019. URL https://doi.org/10.1103%2Frevmodphys.91.025001.

[42] Stephen P Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004. URL https://web.stanford.edu/~boyd/cvxbook/.

[43] K. M. R. Audenaert, J. Calsamiglia, R. Muñ oz-Tapia, E. Bagan, Ll. Masanes, A. Acin, and F. Verstraete. Discriminating states: The quantum chernoff bound. *Physical Review Letters*, 98(16), apr 2007. URL https://doi.org/10.1103%2Fphysrevlett.98.160501.

[44] K. M. R. Audenaert, M. Nussbaum, A. Szkoła, and F. Verstraete. Asymptotic error rates in quantum hypothesis testing. *Communications in Mathematical Physics*, 279(1):251–283, feb 2008. URL https://doi.org/10.1007%2Fs00220-008-0417-5.

[45] 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. URL https://link.springer.com/article/10.1007/BF02100287.

[46] D.P. DiVincenzo, D.W. Leung, and B.M. Terhal. Quantum data hiding. *IEEE Transactions on Information Theory*, 48(3):580–598, mar 2002. doi: 10.1109/18.985948. URL https://doi.org/10.1109%2F18.985948.

[47] Ludovico Lami, Carlos Palazuelos, and Andreas Winter. Ultimate data hiding in quantum mechanics and beyond. *Communications in Mathematical Physics*, 361(2):661–708, jun 2018. URL https://doi.org/10.1007%2Fs00220-018-3154-4.

[48] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Distinguishability of quantum states by positive operator-valued measures with positive partial transpose. *IEEE Transactions on Information Theory*, 60(4):2069–2079, 2014. ISSN 00189448. doi: 10.1109/TIT.2014.2307575. URL http://dx.doi.org/10.1109/TIT.2014.2307575.

[49] Yinan Li, Xin Wang, and Runyao Duan. Indistinguishability of bipartite states by positive-partial-transpose operations in the many-copy scenario. *Physical Review A*, 95(5):052346, 2017. URL http://dx.doi.org/10.1103/PhysRevA.95.052346.

[50] Ryuji Takagi and Bartosz Regula. General resource theories in quantum mechanics and beyond: Operational characterization via discrimination tasks. *Physical Review X*, 9(3), sep 2019. doi: 10.1103/physrevx.9.031053. URL https://doi.org/10.1103%2Fphysrevx.9.031053.

[51] Stefano Pirandola, Riccardo Laurenza, Cosmo Lupo, and Jason L. Pereira. Fundamental limits to quantum channel discrimination. *npj Quantum Information*, 5(1), jun 2019. URL https://doi.org/10.1038%2Fs41534-019-0162-y.

[52] Xin Wang and Mark M. Wilde. Resource theory of asymmetric distinguishability for quantum channels. *Physical Review Research*, 1(3), dec 2019. URL https://doi.org/10.1103%2Fphysrevresearch.1.033169.

[53] Ryuji Takagi, Bartosz Regula, Kaifeng Bu, Zi-Wen Liu, and Gerardo Adesso. Operational advantage of quantum resources in subchannel discrimination. *Physical Review Letters*, 122 (14), apr 2019. URL https://doi.org/10.1103%2Fphysrevlett.122.140402.

[54] Roope Uola, Tom Bullock, Tristan Kraft, Juha-Pekka Pellonpää, and Nicolas Brunner. All quantum resources provide an advantage in exclusion tasks. *Physical Review Letters*, 125(11), sep 2020. URL https://doi.org/10.1103%2Fphysrevlett.125.110402.

[55] André s F. Ducuara and Paul Skrzypczyk. Operational interpretation of weight-based resource quantifiers in convex quantum resource theories. *Physical Review Letters*, 125(11), sep 2020. URL https://doi.org/10.1103%2Fphysrevlett.125.110401.

[56] Patryk Lipka-Bartosik, André s F. Ducuara, Tom Purves, and Paul Skrzypczyk. Operational significance of the quantum resource theory of buscemi nonlocality. *PRX Quantum*, 2(2), apr 2021. URL https://doi.org/10.1103%2Fprxquantum.2.020301.

Limitations of Classically-Simulable Measurements for Quantum State Discrimination

Chengkai Zhu,[1,*] Zhiping Liu,[1,2,*] Chenghong Zhu,[1] and Xin Wang[1,†]

[1]*Thrust of Artificial Intelligence, Information Hub, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511453, China*

[2]*National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*

(Dated: May 19, 2024)

In the realm of fault-tolerant quantum computing, stabilizer operations play a pivotal role, characterized by their remarkable efficiency in classical simulation. This efficiency sets them apart from non-stabilizer operations within the quantum computational theory. In this paper, we investigate the limitations of classically-simulable measurements in distinguishing quantum states. We demonstrate that any pure magic state and its orthogonal complement of odd prime dimensions cannot be unambiguously distinguished by stabilizer operations, regardless of how many copies of the states are supplied. We also reveal intrinsic similarities and distinctions between the quantum resource theories of magic states and entanglement in quantum state discrimination. The results emphasize the inherent limitations of classically-simulable measurements and contribute to a deeper understanding of the quantum-classical boundary.

Introduction.— The computational power of quantum computers, including a substantial speed-up over their classical counterparts in solving certain number-theoretic problems [1–3] and simulating quantum systems [4, 5], can only be unlocked with a scalable quantum computing solution. Fault-tolerant quantum computation (FTQC) provides a scheme to overcome obstacles of physical implementation such as decoherence and inaccuracies [6–8].

A cornerstone of the FTQC resides in stabilizer circuits, comprised exclusively of the Clifford gates. It is well-known that the stabilizer circuits can be efficiently classically simulated [9], and therefore do not confer any quantum computational advantage. However, *magic states* are quantum states that cannot be prepared using the stabilizer formalism [10], and can promote the stabilizer circuits to universal quantum computation via state injection [11–13]. In this context, the magic states and non-stabilizer operations characterize the computational power of universal quantum computation.

While extensive research has explored the stabilizerness of quantum states and gates within circuits [14, 15], a crucial yet underexplored facet is the stabilizerness of quantum measurements [16] – a critical process for reliably decoding classical information encoded in quantum states. In general, it is not applicable for one to access the physical properties of a locally interacting quantum many-body system by classical simulation. However, when information is encoded in a stabilizer state, the decoding process via stabilizer measurements remains efficiently classically simulable [17]. This prompts a fundamental question: can stabilizer measurements perfectly decode all tasks, or are there inherent limitations? Investigating the distinction in decoding capabilities between stabilizer measurements, which are classically efficiently simulable, and other measurements becomes paramount for understanding the intricate relationship between classical information encoded in quantum states and the measurement process.

The ability to retrieve classical information from quantum systems varies significantly with different measurements. One celebrated example is the quantum nonlocality without entanglement [18]. In essence, global measurements can always perfectly distinguish mutually orthogonal quantum states, while there is a set of product states that cannot be distinguished via local quantum operations and classical communications (LOCC). This distinction between global and local measurements has garnered substantial attention, proving to be intricately linked with quantum entanglement theory and the concept of nonlocality [19–26]. This primitive gap between distinct classes of measurements makes quantum state discrimination (QSD) a crucial aspect of fundamental physics [27, 28], where it can be used to test the principles and nature of quantum mechanics. Moreover, QSD has led to fruitful applications in quantum cryptography [29–31], quantum dimension witness [32, 33] and quantum data hiding [34–36].

Inspired by the intrinsic behavior of different measurements in entanglement theory, we raise a natural and important question for understanding the limit and power of the classically-simulable measurements. In particular, is there a sharp gap between the classically-simulable measurements and those that could potentially promote universal quantum computation? If such a gap exists, it will imply considerable advantages that the resource of magic states can provide to the measurement in quantum information processing.

In this Letter, we give an affirmative answer to this question. We show that any pure magic state and its orthogonal complement cannot be unambiguously distinguished via Positive Operator-Valued Measures (POVMs) having positive discrete Wigner functions, which are classically-simulable and strictly include stabilizer measurements [17, 37], no matter how many copies of the states are supplied. We also demonstrate an exponential decay on the asymptotic minimal error probability for distinguishing the Strange state and its orthogonal complement via POVMs having positive discrete Wigner functions, where the Strange state is a representative qutrit magic state defined as $|\mathbb{S}\rangle := (|1\rangle - |2\rangle)/\sqrt{2}$ [10].

In addition, we show that every set of orthogonal pure stabilizer states can be unambiguously distinguished via POVMs

having positive discrete Wigner functions, indicating there is no similar phenomenon as the unextendible product basis (UPB) in entanglement theory. Moreover, we demonstrate that even with the assistance of one or two copies of any qutrit magic state, the Strange state and its orthogonal complement remain indistinguishable via POVMs having positive discrete Wigner functions. It is different from entanglement theory where a single copy of the Bell state is always sufficient to perfectly distinguish a pure entangled state and its orthogonal complement using PPT POVMs [38].

Preliminaries.— To characterize the stabilizerness of quantum states and operations, we first recall the definition of the discrete Wigner function [39–41]. Throughout the paper, we study the Hilbert space $\mathcal{H}_d$ with an odd dimension d, and if the dimension is not prime, it should be understood as a tensor product of Hilbert spaces each having an odd prime dimension. 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 $\mathcal{H}_d$. It is worth noting that qudit-based quantum computing is gaining increasing significance, as numerous problems in the field are awaiting further exploration [42].

Given a standard computational basis $\{|j\rangle\}_{j=0,\cdots,d-1}$, the unitary boost and shift operators $X, Z \in \mathcal{L}(\mathcal{H}_d)$ are defined by $X|j\rangle = |j \oplus 1\rangle, Z|j\rangle = w^j|j\rangle$, where $w = e^{2\pi i/d}$ and $\oplus$ is the addition in $\mathbb{Z}_d$. The *discrete phase space* of a single d-level system is $\mathbb{Z}_d \times \mathbb{Z}_d$. At each point $\mathbf{u} = (a_1, a_2) \in \mathbb{Z}_d \times \mathbb{Z}_d$, the discrete Wigner function of a state ρ is defined as $W_\rho(\mathbf{u}) := \frac{1}{d}\operatorname{Tr}[A_\mathbf{u}\rho]$ where $A_\mathbf{u}$ is the phase-space point operator given by $A_\mathbf{0} := \frac{1}{d}\sum_\mathbf{u} T_\mathbf{u}, A_\mathbf{u} := T_\mathbf{u} A_\mathbf{0} T_\mathbf{u}^\dagger$ and $T_\mathbf{u} = \tau^{-a_1 a_2} Z^{a_1} X^{a_2}, \tau = e^{(d+1)\pi i/d}$. We say a state ρ has positive discrete Wigner functions (PWFs) if $W_\rho(\mathbf{u}) \geq 0, \forall \mathbf{u} \in \mathbb{Z}_d \times \mathbb{Z}_d$ and briefly call it PWF state. Let $\mathbf{E} = \{E_j\}_{j=0}^{n-1}$ be an n-valued POVM acting on $\mathcal{H}_d$ with $\sum_{j=0}^{n-1} E_j = \mathbb{1}$. The discrete Wigner function of each effect E_j is given by $W(E_j|\mathbf{u}) = \operatorname{Tr}[E_j A_\mathbf{u}]$. $\mathbf{E}$ is said to be a PWF POVM if each E_j has PWFs. More details can be found in appendix.

In odd prime dimensions, quantum circuits with initial states and all subsequent quantum operations having PWFs, which strictly include stabilizer (STAB) operations, admit efficient classical simulations [17, 37], extending the Gottesman-Knill theorem. On the contrary, negativity in Wigner functions is usually regarded as an indication of 'non-classicality' [43, 44] and identified as a computational resource. Thus, PWF POVMs are recognized as classically-simulable measurements [45]. The exclusive applicability of these results to odd prime dimensions may stem from the unique property that only quantum systems of such dimensions exhibit covariance of the Wigner function w.r.t. Clifford operations [46]. It's worth noting that there exist mixed magic states with PWFs, rendering them useless for magic state distillation [13]. These states are termed *bound universal states* [47], analogous to states with a positive partial transpose (PPT) in entanglement distillation [48]. Therefore, PWF POVMs strictly include all STAB POVMs as

$$\text{STAB POVMs} \subsetneq \text{PWF POVMs} \subsetneq \text{All POVMs}.$$

Asymptotic limits of PWF POVMs for a pure state and its orthogonal complement.— Our primary aim is to elucidate the constraints inherent in measurements that can be efficiently classically simulated. QSD describes a general process of extracting classical information from quantum systems via measurements. To distinguish two states, one usually performs a two-outcome POVM on the received state and then determines which state it is according to the measurement outcome.

It is well-known that the asymptotic regime of QSD can unravel the underlying mechanism of entanglement [22, 25, 49]. The limit of local measurements exhibits a fundamental distinction between pure and mixed states [22]. Moreover, the asymptotic error probability in QSD is interlinked with the quantum relative entropy, Petz's Rényi divergence [50], and the sandwiched Rényi divergence [51, 52]. Notably, in the regime of many copies, greater flexibility and options exist for the potential POVMs. However, we shall show a wide range of quantum states that cannot be unambiguously distinguished via PWF POVMs, including STAB POVMs, no matter how many copies are supplied.

Theorem 1 *Let $\rho_0 \in \mathcal{D}(\mathcal{H}_d)$ be a pure magic state and $\rho_1 = (\mathbb{1} - \rho_0)/(d-1)$ be its orthogonal complement, where $\mathbb{1}$ is the identity matrix. Then for any integer $n \in \mathbb{Z}^+$, $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$ cannot be unambiguously distinguished by PWF POVMs.*

Theorem 1 reveals a significant disparity in the ability of PWF POVMs and other measurements in QSD. It indicates that the classical information you are allowed to extract from the encoded states is limited when the measurements allowed are restricted to those classically-simulable ones. The limitation of the classically-simulable measurements cannot be overcome even by increasing the number of copies of the states.

From the angle of quantum resource theories (QRTs) [53], this theorem unravels the challenge of distinguishing a pure resourceful state and its orthogonal complement via free operations in the QRT of magic states. This parallels a phenomenon in entanglement theory where any pure entangled state and its orthogonal complement cannot be unambiguously distinguished via PPT POVMs with an arbitrary number of copies provided [38, 49, 54]. However, perfect distinguishability is achievable through global measurements. Notably, Takagi and Regula introduced a quantifier of resourcefulness for measurements [55], demonstrating that resourceful measurements can outperform free measurements in certain QSD tasks [56]. Here, our result further specifies the constraints of free measurements within the QRT of magic states, revealing that free operations cannot distinguish a pure resourceful state and its orthogonal complement, even in the many-copy regime.

The proof of Theorem 1 relies on Lemma 2 which identifies the feature of *PWF unextendible* subspaces, and a fact that the orthogonal complement of any pure magic state is PWF since $-1/d \leq W_\rho(\mathbf{u}) \leq 1/d, \forall \rho \in \mathcal{D}(\mathcal{H}_d), \forall \mathbf{u}$ [46]. We call a subspace $\mathcal{S} \subseteq \mathcal{H}_d$ *PWF unextendible* if there is no

PWF state ρ whose support is a subspace of $\mathcal{S}^\perp$, and *PWF extendible* otherwise. A subspace $\mathcal{S} \subseteq \mathcal{H}_d$ is called *strongly PWF unextendible* if for any positive integer n, $\mathcal{S}^{\otimes n}$ is PWF unextendible. As a simple example, if we let $\mathcal{S}^\perp$ be a one-dimensional subspace spanned by the strange state $|\mathbb{S}\rangle$, then $\mathcal{S}$ is (strongly) PWF unextendible. In fact, the unextendibility of subspaces indicates the distinguishability of quantum states. It is well-known that a UPB for a multipartite quantum system indicates indistinguishability under LOCC operations [26].

Lemma 2 *For a PWF unextendible subspace $\mathcal{S} \subseteq \mathcal{H}_d$, if there is a PWF state $\rho \in \mathcal{D}(\mathcal{S})$ such that $\mathrm{supp}(\rho) = \mathcal{S}$, then $\mathcal{S}$ is strongly PWF unextendible.*

We note that Lemma 2 implies that for a set of orthogonal quantum states $\{\rho_1, ..., \rho_n\}$, if there is a ρ_i whose support is strongly PWF unextendible, then $\{\rho_1, ..., \rho_n\}$ cannot be unambiguously distinguished by PWF POVMs no matter how many copies are used. This leads to and generalizes the result of Theorem 1. We sketch the proof of Lemma 2 as follows.

First, we demonstrate that $\mathcal{S}^{\otimes 2}$ is PWF unextendible through a proof by contradiction. Suppose $\rho_s \in \mathcal{D}(\mathcal{S})$ is a PWF state such that $\mathrm{supp}(\rho_s) = \mathcal{S}$. If there is a PWF state σ supporting on $(\mathcal{S}^{\otimes 2})^\perp$, then we have $\mathrm{Tr}[\sigma(\rho_s \otimes \rho_s)] = 0$ which leads to $\mathrm{Tr}[\rho_s \,\mathrm{Tr}_2[\sigma(\mathbb{1} \otimes \rho_s)]] = 0$. It is easy to check that $\sigma' = \mathrm{Tr}_2[\sigma(\mathbb{1} \otimes \rho_s)]$ is a positive semi-definite operator with PWFs if it is non-zero. If it is zero, we can check that $\mathrm{Tr}_1 \sigma$ is a positive semi-definite operator with PWFs. In either case, we will get a PWF state supported on $\mathcal{S}^\perp$, a contradiction to the PWF unextendibility of $\mathcal{S}$. Hence, we conclude that $\mathcal{S}^{\otimes 2}$ is PWF unextendible. Using a similar technique, we can conclusively demonstrate that $\mathcal{S}^{\otimes n}$ is PWF unextendible for any positive integer n. The details can be found in appendix.

Asymptotic limits of PWF POVMs for mixed states.— Followed by Lemma 2, we note that Theorem 1 displays a special case of a strongly PWF unextendible subspace. The orthogonal complement of a pure magic state turns out to be a PWF state which lies in a $d-1$ dimensional PWF unextendible subspace. This prompts an intriguing inquiry into the minimal dimension of such subspace. Notably, we will show there is a much smaller strongly PWF unextendible subspace, indicating the presence of mixed magic states that cannot be unambiguously distinguished from their orthogonal complements via PWF POVMs in the many-copy scenario.

Proposition 3 *There exists a strongly PWF unextendible subspace $\mathcal{S} \subseteq \mathcal{H}_d$ of dimension $(d+1)/2$.*

This proposition implies there is a $(d-1)/2$-dimensional subspace in which all states are magic states. The detailed proof is in appendix and we give a simple example as follows.

Example 1 Consider a qudit system with $d = 5$. We have the following basis that spans $\mathcal{H}_5$.

$$\begin{aligned} |v_0\rangle &= |0\rangle, \\ |v_1\rangle &= (|1\rangle + |2\rangle + |3\rangle + |4\rangle)/2, \\ |v_2\rangle &= (-|1\rangle + |2\rangle + |3\rangle - |4\rangle)/2, \\ |v_3\rangle &= (|1\rangle - |2\rangle + |3\rangle - |4\rangle)/2, \\ |v_4\rangle &= (|1\rangle + |2\rangle - |3\rangle - |4\rangle)/2. \end{aligned} \tag{1}$$

Let $\rho_0 = (|v_0\rangle\langle v_0| + |v_1\rangle\langle v_1| + |v_2\rangle\langle v_2|)/3$, $\rho_1 = (|v_3\rangle\langle v_3| + |v_4\rangle\langle v_4|)/2$, and $\mathcal{S}_0 = \mathrm{supp}(\rho_0), \mathcal{S}_1 = \mathrm{supp}(\rho_1)$. Followed by the idea in the proof of Proposition 3, one can check that there is no PWF state in $\mathcal{S}_1$, and ρ_0 is a PWF state. Thus, $\mathcal{S}_0$ is a strongly PWF unextendible subspace. ρ_0 and ρ_1 cannot be unambiguously distinguished by PWF POVMs, no matter how many copies of them are supplied.

More generally, we establish an easy-to-compute criterion for identifying the circumstances under which two quantum states cannot be unambiguously distinguished by PWF POVMs in the many-copy scenario.

Theorem 4 *Given $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H}_d)$, if any of them has strictly positive discrete Wigner functions, i.e., $W_{\rho_i}(\mathbf{u}) > 0, \forall \mathbf{u}$, then for any integer $n \in \mathbb{Z}^+$, $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$ cannot be unambiguously distinguished by PWF POVMs.*

Theorem 4 is of broad applicability for both pure and mixed states. The indistinguishability can be checked through a simple computation of the discrete Wigner functions, streamlining the conventional method by analyzing exponentially large Hilbert space.

Minimum error discrimination by PWF POVMs.— After characterizing the limits of PWF POVMs, we further study the minimum error QSD to unveil the capabilities inherent in PWF POVMs. For states ρ_0 and ρ_1 with prior probability p and $1-p$, respectively, we denote $P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0, \rho_1, p)$ as the optimal error probability of distinguishing them by PWF POVMs. Mathematically, this optimal error probability can be expressed via semidefinite programming (SDP) [57] as follows.

$$P_{\mathrm{e}}^{\mathrm{PWF}} = \min_{E_0, E_1} \; (1-p)\,\mathrm{Tr}(E_0\rho_1) + p\,\mathrm{Tr}(E_1\rho_0), \tag{2a}$$

$$\text{s.t.} \;\; E_0 \geq 0, E_1 \geq 0, E_0 + E_1 = \mathbb{1}, \tag{2b}$$

$$W(E_0|\mathbf{u}) \geq 0, W(E_1|\mathbf{u}) \geq 0, \forall \mathbf{u}, \tag{2c}$$

where Eq. (2c) ensures $\{E_0, E_1\}$ is a PWF POVM. We provide the dual SDP in appendix. For ρ_0 to be the Strange state and ρ_1 to be its orthogonal complement, we demonstrate the following asymptotic error behavior.

Proposition 5 *Let ρ_0 be the Strange state $|\mathbb{S}\rangle\langle\mathbb{S}|$ and $\rho_1 = (\mathbb{1} - |\mathbb{S}\rangle\langle\mathbb{S}|)/2$ be its orthogonal complement. For $n \in \mathbb{Z}^+$, we have*

$$P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}, \frac{1}{2}) = \frac{1}{2^{n+1}}. \tag{3}$$

The optimal PWF POVM is $\{E, \mathbb{1} - E\}$, where $E = (|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)^{\otimes n}$ and $|\mathbb{K}\rangle = (|1\rangle + |2\rangle)/\sqrt{2}$.

We remark what we obtain here is the optimal error probability using PWF POVMs to distinguish n copies of the Strange state and its orthogonal complement. We first find the protocol above for the desired error probability and then utilize the dual SDP of (2) to establish the optimality of this protocol. The detailed proof is provided in appendix. It can be seen that the optimal error probability will exponentially decay with respect to the number of copies supplied. Nevertheless, it is important to note that the error persists for all finite values of n, aligning with the indistinguishability established in Theorem 1.

We further discuss the relationship between Proposition 5 and the Chernoff exponent in hypothesis testing. The celebrated quantum Chernoff theorem [50, 58, 59] establishes that $\xi_C(\rho_0,\rho_1) := \lim_{n\to\infty} -\frac{1}{n}\log P_e(\rho_0^{\otimes n},\rho_1^{\otimes n},p) = -\min_{0\le s\le 1}\log \mathrm{Tr}[\rho_0^{1-s}\rho_1^s]$, where $P_e(\rho_0^{\otimes n},\rho_1^{\otimes n},p)$ is the average error of distinguishing ρ_0 and ρ_1 via global measurements, $\xi_C(\rho_0,\rho_1)$ is the so-called Chernoff exponent. The Chernoff exponent concerning a specific class of measurements, e.g., $\{\mathrm{LOCC},\mathrm{PPT},\mathrm{SEP}\}$, is defined in [49]. The authors proved that the Chernoff bounds in these cases are indeed faithful by showing an exponential decay of $P_e^X(\rho_0,\rho_1,p)$ where $X\in\{\mathrm{LOCC},\mathrm{PPT},\mathrm{SEP}\}$. Similarly, Proposition 5 may give an insight that the Chernoff bound concerning PWF measurements is also faithful.

Proposition 5 also implies applications in quantum data hiding [34, 60, 61]. Despite the original data-hiding setting where pairs of states of a bipartite system are perfectly distinguishable via general entangled measurements yet almost indistinguishable under LOCC, it is conceivable to extend data-hiding techniques to broader contexts dictated by specific physical circumstances [55]. As discussed in [55], one may consider the scenario that information is encoded in a way that Pauli measurements have less capability of decoding it than arbitrary measurements. Then only the party with the ability to generate magic can reliably retrieve the message. Here, we define $\|\cdot\|_{\mathrm{PWF}}$ and $R(\mathrm{PWF})$ as the *distinguishability norm* and the *data-hiding ratio* [61] associated with PWF POVMs, respectively. Proposition 5 directly gives a lower bound on the *data-hiding ratio* against PWF POVMs as follows.

$$R(\mathrm{PWF}) = \max \frac{\|p\rho-(1-p)\sigma\|_{\mathrm{All}}}{\|p\rho-(1-p)\sigma\|_{\mathrm{PWF}}} \ge \frac{1}{1-2^{-n}}. \quad (4)$$

We also observe that a potential correlation between $R(\mathrm{PWF})$ and the generalized robustness of measurement [55] merits further investigation, with preliminary evidence provided in appendix.

Distinctions between QRT of magic states and entanglement in QSD tasks.— The asymptotic limits of PWF POVMs share similarities with LOCC operations, both of which are considered free within their respective resource theories. Whereas, there are fundamental distinctions between the QRT of magic states and entanglement, considering the QSD tasks. In Table I, we display a comparison between the QRT of magic states and entanglement in QSD, including their similarities and the following distinctions.

	QRT of magic states	QRT of entanglement
Asymptotic limits of free POVMs	✔	✔
Existence of UPB phenomenon	✗	✔
Perfect discrimination with the aid of one copy of maximal resource	✗	✔

TABLE I. **Comparison between the QRT of magic states and entanglement.** The second row represents if any resourceful pure state and its orthogonal complement are indistinguishable by free measurements in the many-copy scenario. The third row represents whether there is a UPB phenomenon. The last row represents whether the assistance of one copy of the maximally resourceful state is sufficient for perfect discrimination.

Recall that in entanglement theory, the UPB is an incomplete orthogonal product basis whose complementary subspace contains no product state [26]. It shows examples of orthogonal product states that cannot be perfectly distinguished by LOCC operations. Correspondingly, we may imagine whether there is a similar 'UPB' phenomenon in the QRT of magic states. That is if there is an incomplete orthogonal stabilizer basis whose complementary subspace contains no stabilizer state. We show that this is not the case as follows.

Theorem 6 *For a subspace $\mathcal{S}\in\mathcal{H}_d$, if $\mathcal{S}$ has a set of basis $\{|\psi_i\rangle\}_{i=0}^{n-1}$ where every $|\psi_i\rangle$ is a stabilizer state, then $\mathcal{S}$ is PWF extendible.*

A direct consequence of this theorem is that any set of orthogonal pure stabilizer states $\{|\psi\rangle_i\}_{i=0}^{n-1}$ can be unambiguously distinguished via PWF POVMs as we can choose $E_i = |\psi_i\rangle\langle\psi_i|$ for $i=0,2,\cdots,n-1$ and $E_n = \mathbb{1}-\sum_{i=0}^{n-1}|\psi_i\rangle\langle\psi_i|$. Therefore, we confirm the absence of an analogous UPB phenomenon in the QRT of magic states.

Besides, it was shown that one copy of the Bell state is always sufficient for perfectly distinguishing any pure state ρ_0 and its orthogonal complement ρ_1 via PPT POVMs [38], i.e., distinguishing $\rho_0\otimes\Phi_2^+$ and $\rho_1\otimes\Phi_2^+$. However, things are different in the QRT of magic states where we find the Strange state and its orthogonal complement cannot be perfectly distinguished by PWF POVMs with the assistance of one or two copies of any qutrit magic state.

Proposition 7 *Let ρ_0 be the Strange state $|\mathbb{S}\rangle\langle\mathbb{S}|$ and $\rho_1 = (\mathbb{1}-|\mathbb{S}\rangle\langle\mathbb{S}|)/2$ be its orthogonal complement. $\rho_0\otimes\tau^{\otimes k}$ and $\rho_1\otimes\tau^{\otimes k}$ cannot be perfectly distinguished by PWF POVMs for any qutrit magic state τ and $k=1$ or 2.*

The main idea is to analyze the minimal *mana* [62] $\tau^{\otimes k}$ must have to perfectly distinguish $\rho_0\otimes\tau^{\otimes k}$ and $\rho_1\otimes\tau^{\otimes k}$ by PWF POVMs. A similar result can be obtained for the Norell state $|\mathbb{N}\rangle := (-|0\rangle+2|1\rangle-|2\rangle)/\sqrt{6}$ [10]. Hence, we have witnessed the distinctions of the QRT of magic states and entanglement in regard to the resource cost for perfect discrimination.

Concluding remarks.— We have explored the limitations of PWF POVMs which can be efficiently classically simulated and strictly include all stabilizer measurements. Our results show that the QRT of magic states and entanglement exhibit significant similarities and distinctions in quantum state discrimination.

These results have implications in various fields, including connections between the QRT of magic states and quantum data hiding [36, 55, 60, 61]. It remains interesting to further study the limits of stabilizer measurements or classically-simulable ones in quantum channel discrimination [63–65] and other operational tasks [66–68]. Note that as it is still open whether all operations with negative discrete Wigner functions are useful for magic state distillation [10], a comprehensive characterization of the quantum-classical boundary of measurements is still needed. Additionally, it is interesting to study the limitations of stabilizer measurements in a multi-qubit system [69–72], and recent advances in generalized phase-space simulation methods for qubits [73, 74] offer potential avenues to explore this, which we will leave to future work.

Acknowledgments.– We would like to thank the anonymous referees for their helpful comments. This work was supported by the Start-up Fund (No. G0101000151) from The Hong Kong University of Science and Technology (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.

* Chengkai Zhu and Zhiping Liu contributed equally to this work.
† felixxinwang@hkust-gz.edu.cn

[1] P. W. Shor, SIAM Journal on Computing **26**, 1484 (1997).
[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," (1996), arXiv:quant-ph/9605043 [quant-ph].
[3] A. M. Childs and W. van Dam, Rev. Mod. Phys. **82**, 1 (2010).
[4] S. Lloyd, Science **273**, 1073 (1996).
[5] A. M. Childs, D. Maslov, Y. Nam, N. J. Ross, and Y. Su, Proceedings of the National Academy of Sciences **115**, 9456 (2018).
[6] P. W. Shor, "Fault-tolerant quantum computation," (1997), arXiv:quant-ph/9605011 [quant-ph].
[7] E. T. Campbell, B. M. Terhal, and C. Vuillot, Nature **549**, 172 (2017).
[8] E. Knill, Nature **434**, 39 (2005).
[9] D. Gottesman, *Stabilizer codes and quantum error correction* (California Institute of Technology, 1997).
[10] V. Veitch, S. A. Hamed Mousavian, D. Gottesman, and J. Emerson, New Journal of Physics **16**, 1 (2014).
[11] X. Zhou, D. W. Leung, and I. L. Chuang, Physical Review A **62** (2000), 10.1103/physreva.62.052316.
[12] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).
[13] S. Bravyi and A. Kitaev, Physical Review A **71** (2005), 10.1103/physreva.71.022316.
[14] E. T. Campbell, H. Anwar, and D. E. Browne, Physical Review X **2** (2012).
[15] M. Yoganathan, R. Jozsa, and S. Strelchuk, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **475**, 20180427 (2019).
[16] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge university press, 2010).
[17] A. Mari and J. Eisert, Physical Review Letters **109**, 1 (2012).
[18] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Physical Review A **59**, 1070 (1999).
[19] D. Leung, A. Winter, and N. Yu, Reviews in Mathematical Physics **33**, 2150013 (2021).
[20] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, IEEE Transactions on Information Theory **61**, 3593 (2015).
[21] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, Communications in Mathematical Physics **323**, 1121 (2013).
[22] S. Bandyopadhyay, Physical Review Letters **106**, 1 (2011).
[23] J. Calsamiglia, J. I. De Vicente, R. Muñoz-Tapia, and E. Bagan, Physical Review Letters **105**, 1 (2010).
[24] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, Physical Review Letters **122**, 40403 (2019).
[25] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Physical Review Letters **85**, 4972 (2000).
[26] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Physical Review Letters **82**, 5385 (1999).
[27] J. Bae and L.-C. Kwek, Journal of Physics A: Mathematical and Theoretical **48**, 083001 (2015).
[28] W. H. G. Correa, L. Lami, and C. Palazuelos, IEEE Transactions on Information Theory **68**, 7306 (2022).
[29] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **74**, 145 (2002).
[30] R. Cleve, D. Gottesman, and H.-K. Lo, Physical Review Letters **83**, 648 (1999).
[31] A. Leverrier and P. Grangier, Physical Review Letters **102** (2009).
[32] N. Brunner, M. Navascué s, and T. Vértesi, Physical Review Letters **110** (2013).
[33] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Nature Physics **8**, 588 (2012).
[34] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).
[35] T. Eggeling and R. F. Werner, Phys. Rev. Lett. **89**, 097905 (2002).
[36] W. Matthews, S. Wehner, and A. Winter, Communications in Mathematical Physics **291**, 813 (2009).
[37] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New Journal of Physics **14**, 1 (2012).
[38] N. Yu, R. Duan, and M. Ying, IEEE Transactions on Information Theory **60**, 2069 (2014).
[39] W. K. Wootters, Annals of Physics **176**, 1 (1987).
[40] D. Gross, Journal of Mathematical Physics **47** (2006).
[41] D.Gross, Applied Physics B **86**, 367 (2006).
[42] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, Frontiers in Physics **8** (2020).
[43] E. F. Galvã o, Physical Review A **71** (2005).
[44] C. Cormick, E. F. Galvã o, D. Gottesman, J. P. Paz, and A. O. Pittenger, Physical Review A **73** (2006).
[45] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature **510**, 351 (2014).
[46] H. Zhu, Phys. Rev. Lett. **116**, 040501 (2016).
[47] E. T. Campbell and D. E. Browne, Physical Review Letters **104** (2010).
[48] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev.

Lett. **80**, 5239 (1998).
[49] H.-C. Cheng, A. Winter, and N. Yu, Communications in Mathematical Physics , 1 (2023).
[50] K. M. R. Audenaert, M. Nussbaum, A. Szkoła, and F. Verstraete, Communications in Mathematical Physics **279**, 251 (2008).
[51] T. Ogawa and H. Nagaoka, in *Asymptotic Theory of Quantum Statistical Inference* (WORLD SCIENTIFIC, 2005) pp. 28–42.
[52] M. Mosonyi and T. Ogawa, Communications in Mathematical Physics **334**, 1617 (2014).
[53] E. Chitambar and G. Gour, Reviews of Modern Physics **91** (2019).
[54] Y. Li, X. Wang, and R. Duan, Physical Review A **95**, 052346 (2017).
[55] R. Takagi and B. Regula, Physical Review X **9** (2019), 10.1103/physrevx.9.031053.
[56] M. Oszmaniec and T. Biswas, Quantum **3**, 133 (2019).
[57] S. P. Boyd and L. Vandenberghe, *Convex optimization* (Cambridge university press, 2004).
[58] K. M. R. Audenaert, J. Calsamiglia, R. Muñ oz-Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete, Physical Review Letters **98** (2007).
[59] F. Hiai and D. Petz, Communications in mathematical physics **143**, 99 (1991).
[60] D. DiVincenzo, D. Leung, and B. Terhal, IEEE Transactions on Information Theory **48**, 580 (2002).
[61] L. Lami, C. Palazuelos, and A. Winter, Communications in Mathematical Physics **361**, 661 (2018).
[62] X. Wang, M. M. Wilde, and Y. Su, Physical Review Letters **124**, 090505 (2018).
[63] S. Pirandola, R. Laurenza, C. Lupo, and J. L. Pereira, npj Quantum Information **5** (2019).
[64] X. Wang and M. M. Wilde, Physical Review Research **1** (2019).
[65] R. Takagi, B. Regula, K. Bu, Z.-W. Liu, and G. Adesso, Physical Review Letters **122** (2019).
[66] R. Uola, T. Bullock, T. Kraft, J.-P. Pellonpää, and N. Brunner, Physical Review Letters **125** (2020).
[67] A. F. Ducuara and P. Skrzypczyk, Physical Review Letters **125** (2020).
[68] P. Lipka-Bartosik, A. F. Ducuara, T. Purves, and P. Skrzypczyk, PRX Quantum **2** (2021).
[69] M. Howard and E. Campbell, Physical Review Letters **118** (2017).
[70] S. Bravyi, G. Smith, and J. A. Smolin, Physical Review X **6**, 1 (2016).
[71] J. R. Seddon and E. T. Campbell, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **475**, 20190251 (2019).
[72] O. Hahn, A. Ferraro, L. Hultquist, G. Ferrini, and L. Garcí a-Álvarez, Physical Review Letters **128** (2022).
[73] M. Zurel, C. Okay, and R. Raussendorf, Physical Review Letters **125** (2020), 10.1103/physrevlett.125.260404.
[74] R. Raussendorf, J. Bermejo-Vega, E. Tyhurst, C. Okay, and M. Zurel, Physical Review A **101** (2020), 10.1103/physreva.101.012350.
[75] X. Wang, M. M. Wilde, and Y. Su, New Journal of Physics **21**, 103002 (2019).
[76] D. Gross, Journal of mathematical physics **47** (2006).
[77] H. Pashayan, J. J. Wallman, and S. D. Bartlett, Physical Review Letters **115** (2015).
[78] P.-E. Emeriau, M. Howard, and S. Mansfield, PRX Quantum **3**, 020307 (2022).
[79] T. M. Inc., "Matlab version: 9.13.0 (r2022b)," (2022).
[80] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," `http://cvxr.com/cvx` (2014).
[81] N. Johnston, "QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9," `https://qetlab.com` (2016).

Supplemental Material for:

Limitations of Classically-Simulable Measurements for Quantum State Discrimination

In this Supplemental Material, we provide detailed proofs of the theorems and propositions in the manuscript "Limitations of Classically-Simulable Measurements for Quantum State Discrimination". In Appendix , we cover the basics of the discrete Wigner function. In Appendix , we first present the detailed proofs for Lemma 2 and Proposition 3, which characterize the asymptotic limits of PWF POVMs for distinguishing a pure magic state and its orthogonal complement and a mixed magic state and its orthogonal complement, respectively. Then, we provide the proof of Theorem 4 which serves as an easy-to-compute criterion for when PWF POVMs cannot unambiguously distinguish two quantum states in the many-copy scenario. Appendix introduces the primal and dual SDP for calculating the optimal error probability of distinguishing two quantum states via PWF POVMs. We further provide detailed proof of Proposition 5. Then in Appendix , we furnish detailed proofs for Theorem 6 and Proposition 7, both of which characterize the distinctions between the QRT of magic states and entanglement in QSD tasks.

THE DISCRETE WIGNER FUNCTION

We denote $\mathcal{H}_d$ as a Hilbert space of dimension d, and $\{|j\rangle\}_{j=0,\cdots,d-1}$ as the standard computational basis. Let $\mathcal{L}(\mathcal{H}_d)$ be the space of operators mapping $\mathcal{H}_d$ to itself. For odd prime dimension d, the unitary boost and shift operators $X, Z \in \mathcal{L}(\mathcal{H}_d)$ are defined as [75]:

$$X|j\rangle = |j \oplus 1\rangle, \quad Z|j\rangle = w^j|j\rangle, \tag{S1}$$

where $w = e^{2\pi i/d}$ and $\oplus$ denotes addition modulo d. The *discrete phase space* of a single d-level system is $\mathbb{Z}_d \times \mathbb{Z}_d$, which can be associated with a $d \times d$ cubic lattice. For a given point in the discrete phase space $\mathbf{u} = (a_1, a_2) \in \mathbb{Z}_d \times \mathbb{Z}_d$, the Heisenberg-Weyl operators are given by

$$T_{\mathbf{u}} = \tau^{-a_1 a_2} Z^{a_1} X^{a_2}, \tag{S2}$$

where $\tau = e^{(d+1)\pi i/d}$. These operators form a group, the Heisenberg-Weyl group, and are the main ingredient for representing quantum systems in finite phase space. The case of non-prime dimension can be understood to be a tensor product of $T_{\mathbf{u}}$ with odd prime dimension. For each point $\mathbf{u} \in \mathbb{Z}_d \times \mathbb{Z}_d$ in the discrete phase space, there is a phase-space point operator $A_{\mathbf{u}}$ defined as

$$A_{\mathbf{0}} := \frac{1}{d} \sum_{\mathbf{w}} T_{\mathbf{w}}, \quad A_{\mathbf{u}} := T_{\mathbf{u}} A_{\mathbf{0}} T_{\mathbf{u}}^{\dagger}. \tag{S3}$$

The discrete Wigner function of a state ρ at the point $\mathbf{u}$ is then defined as

$$W_\rho(\mathbf{u}) := \frac{1}{d} \operatorname{Tr}\left[A_{\mathbf{u}} \rho\right]. \tag{S4}$$

More generally, we can replace ρ with H for the discrete Wigner function of a Hermitian operator H. For the case of H being an effect E of some Positive Operator-Valued Measure (POVM), its discrete Wigner function is given by

$$W(E|\mathbf{u}) := \operatorname{Tr}[E A_{\mathbf{u}}]. \tag{S5}$$

There are several useful properties of the set $\{A_{\mathbf{u}}\}_{\mathbf{u}}$ as follows:

1. $A_{\mathbf{u}}$ is Hermitian;
2. $\sum_{\mathbf{u}} A_{\mathbf{u}}/d = \mathbb{1}$;
3. $\operatorname{Tr}[A_{\mathbf{u}} A_{\mathbf{u}'}] = d\delta(\mathbf{u}, \mathbf{u}')$;
4. $\operatorname{Tr}[A_{\mathbf{u}}] = 1$;
5. $H = \sum_{\mathbf{u}} W_H(\mathbf{u}) A_{\mathbf{u}}$;
6. $\{A_{\mathbf{u}}\}_{\mathbf{u}} = \{A_{\mathbf{u}}{}^T\}_{\mathbf{u}}$.

We say a Hermitian operator H has positive discrete Wigner functions (PWFs) if $W_H(\mathbf{u}) \geq 0, \forall \mathbf{u} \in \mathbb{Z}_d \times \mathbb{Z}_d$. According to the discrete Hudsons theorem [76], a pure state ρ is a stabilizer state, if and only if it has PWFs. Similarly, an n-valued POVM $\mathbf{E} = \{E_j\}_{j=0}^{n-1}$ is said to be a PWF POVM if each E_j has PWFs. The discrete Wigner function of each measurement outcome of a POVM $\{E_j\}_{j=0}^{n-1}$ has a conditional quasi-probability interpretation over the phase space

$$\sum_j W(E_j|\mathbf{u}) = 1, \tag{S6}$$

where $E_j \geq \mathbf{0}$ and $\sum_j E_j = \mathbb{1}$. In the case of E_j having PWFs, $W(E_j|\mathbf{u})$ can be interpreted as the probability of obtaining outcome j given that the system is at the phase space point $\mathbf{u}$. This property is crucial for efficiently simulating quantum computation classically. The total probability of obtaining outcome j from a measurement on state ρ is then given by

$$P(j|\rho) = \sum_{\mathbf{u}} W_\rho(\mathbf{u}) W(E_j|\mathbf{u}), \tag{S7}$$

where $P(j|\rho)$ can be effectively estimated [17, 77] when both ρ and E_j have PWFs, implying that both $W_\rho(\mathbf{u})$ and $W(E_j|\mathbf{u})$ possess classical probability interpretations. Therefore, negative quasi-probability is a vital resource for quantum speedup in stabilizer computation and has deep connections with contextuality in stabilizer measurements [37, 45]. In this sense, PWF POVMs are regarded as classically-simulable measurements [45], which strictly include all stabilizer measurements.

Lemma S1 *For any phase-space point operator $A_\mathbf{u} \in \mathcal{L}(\mathcal{H}_d)$, $\mathbf{u} \in \mathbb{Z}_d \times \mathbb{Z}_d$, $A_\mathbf{u}$ is a unitary operator with eigenvalues of $+1$ or -1, where eigenvalue +1 has a degeneracy of $\frac{d+1}{2}$ and eigenvalue -1 has a degeneracy of $\frac{d-1}{2}$.*

Proof Suppose $A_\mathbf{0}$ has a spectral decomposition

$$A_\mathbf{0} = \sum_i a_i |a_i\rangle\langle a_i|. \tag{S8}$$

Since $A_\mathbf{u} = T_\mathbf{u} A_\mathbf{0} T_\mathbf{u}^\dagger$, we have $A_\mathbf{u} = \sum_i a_i T_\mathbf{u} |a_i\rangle\langle a_i| T_\mathbf{u}^\dagger$ which means all possible $A_\mathbf{u}$ have same eigenvalues $\{a_i\}$ with corresponding eigenvectors $\{T_\mathbf{u}|a_i\rangle\}$. Note that $A_\mathbf{0} = \sum_{k\in\mathbb{Z}_d} |k\rangle\langle -k|$ [78], we conclude that the matrix representation of $A_\mathbf{0}$ is $A_\mathbf{0} = \begin{bmatrix} 1 & 0 \\ 0 & {\sigma_x}^{\otimes \lfloor \frac{d}{2} \rfloor} \end{bmatrix}$, where $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Now we consider the eigenvalues of $A_\mathbf{0}$. Notice that

$$\det(|aI_d - A_\mathbf{0}|) = \det\left(\left|aI_d - \begin{bmatrix} 1 & 0 \\ 0 & {\sigma_x}^{\otimes \lfloor \frac{d}{2} \rfloor} \end{bmatrix}\right|\right) = (1-a)\det\left|aI_{d-1} - {\sigma_x}^{\otimes \lfloor \frac{d}{2} \rfloor}\right| = (1-a)(1-a^2)^{\lfloor \frac{d}{2} \rfloor} = 0, \tag{S9}$$

where a denotes the eigenvalue of $A_\mathbf{0}$. Thus, eigenvalues of $A_\mathbf{u}$ are $+1$ or -1, and eigenvalue $+1$ has a degeneracy of $\frac{d+1}{2}$ and eigenvalue -1 has a degeneracy of $\frac{d-1}{2}$ due to $\mathrm{Tr}(A_\mathbf{u}) = 1$. We can further conclude that $A_\mathbf{u}$ is unitary according to the possible eigenvalues of $A_\mathbf{u}$. ■

ASYMPTOTIC LIMITS OF PWF POVMS

Lemma 2 *For a PWF unextendible subspace $\mathcal{S} \subseteq \mathcal{H}_d$, if there is a PWF state $\rho \in \mathcal{D}(\mathcal{S})$ such that $\mathrm{supp}(\rho) = \mathcal{S}$, then $\mathcal{S}$ is strongly PWF unextendible.*

Proof First, we will demonstrate that $\mathcal{S}^{\otimes 2}$ is PWF unextendible through a proof by contradiction. Suppose $\rho_s \in \mathcal{S}$ is a PWF state such that $\mathrm{supp}(\rho_s) = \mathrm{supp}(\mathcal{S})$. If there is a PWF state σ supporting on $(\mathcal{S}^{\otimes 2})^\perp$, then we have $\mathrm{Tr}[\sigma(\rho_s \otimes \rho_s)] = 0$ which leads to

$$\mathrm{Tr}\left[\rho_s \,\mathrm{Tr}_2[\sigma(\mathbb{1} \otimes \rho_s)]\right] = 0. \tag{S10}$$

Now we construct an operator $\sigma' \in \mathcal{L}(\mathcal{H}_d)$ by

$$\sigma' = \mathrm{Tr}_2[\sigma(\mathbb{1} \otimes \rho_s)]. \tag{S11}$$

It is easy to check that σ' is hermitian, $\sigma' \geq \mathbf{0}$ and $\mathrm{Tr}(\sigma'\rho_s) = 0$.

If $\sigma' = \mathbf{0}$, we know that $\mathrm{Tr}\,\sigma' = 0$ which indicates that $\mathrm{Tr}[\sigma(\mathbb{1} \otimes \rho_s)] = \mathrm{Tr}[\rho_s\,\mathrm{Tr}_1\,\sigma] = 0$. We note that $\mathrm{Tr}_1\,\sigma \neq \mathbf{0}$ otherwise $\sigma = \mathbf{0}$. Also, $\mathrm{Tr}_1\,\sigma$ is PWF because partial trace preserves the positivity of the discrete Wigner functions which can be observed by expressing the state as $\sigma = \sum_{\mathbf{u}} W_\sigma(\mathbf{u}) A_{\mathbf{u}}$. Thus, we will get a PWF state supporting on $\mathcal{S}^\perp$ after normalizing $\mathrm{Tr}_1\,\sigma$, a contradiction to the PWF unextendibility of $\mathcal{S}$.

If $\sigma' \neq \mathbf{0}$, we can calculate the Wigner functions of σ' and demonstrate their non-negativity as follows.

$$W_{\sigma'}(\mathbf{u}_1) = \frac{1}{d}\,\mathrm{Tr}(\sigma' A_{\mathbf{u}_1}) = \frac{1}{d^2}\sum_{\mathbf{u}_2} \mathrm{Tr}[\sigma(A_{\mathbf{u}_1} \otimes A_{\mathbf{u}_2})]\,\mathrm{Tr}(\rho_s A_{\mathbf{u}_2}). \tag{S12}$$

Since σ and ρ_s are PWF, i.e., $\mathrm{Tr}[\sigma(A_{\mathbf{u}_1} \otimes A_{\mathbf{u}_2})] \geq 0, \mathrm{Tr}(\rho_s A_{\mathbf{u}_2}) \geq 0, \forall \mathbf{u}_1, \mathbf{u}_2$, we have $W_{\sigma'}(\mathbf{u}_1) \geq 0$. Thus σ' is PWF. Consequently, we have obtained a PWF state supporting on $\mathcal{S}^\perp$ after normalizing σ', a contradiction to the PWF unextendibility of $\mathcal{S}$.

Hence, we conclude that $\mathcal{S}^{\otimes 2}$ is PWF unextendible. Using a similar technique, we can prove that $\mathcal{S}^{\otimes 3}$ is PWF unextendible by making a contradiction to the PWF unextendibility of $\mathcal{S}^{\otimes 2}$. In turn, we can conclusively demonstrate that $\mathcal{S}^{\otimes k}$ is PWF unextendible for any positive integer k, which completes the proof. ■

Proposition 3 *There exists a strongly PWF unextendible subspace $\mathcal{S} \subseteq \mathcal{H}_d$ of dimension $(d+1)/2$.*

Proof First, we construct a $(d-1)/2$ dimensional subspace $\mathcal{S}_m \subseteq \mathcal{H}_d$ that supports only magic states. Then we will show that $\mathcal{S}_m^\perp \subseteq \mathcal{H}_d$ is a strongly PWF unextendible subspace of dimension $(d+1)/2$. We consider the eigenspace of the phase-space point operator $A_{\mathbf{0}}$. Denote the set of all eigenvectors of $A_{\mathbf{0}}$ corresponding to eigenvalue of -1 as $S^- \coloneqq \{|a_i^-\rangle\}_{i=1}^{\frac{d-1}{2}}$. We will show these states in S^- span a subspace $\mathcal{S}_m \in \mathcal{H}_d$ that contains no PWF states.

Obviously, any $|a_i^-\rangle \in S^-$ is a magic state due to $\mathrm{Tr}(|a_i^-\rangle\langle a_i^-|A_{\mathbf{0}}) = -1$. Suppose $|\psi\rangle$ is an arbitrary pure state in S^-. It can be written as $|\psi\rangle = \sum_i \alpha_i |a_i^-\rangle$. The Wigner function of $|\psi\rangle$ at the phase-space point $\mathbf{0}$ is

$$W_\psi(\mathbf{0}) = \frac{1}{d}\langle\psi|A_{\mathbf{0}}|\psi\rangle = \frac{1}{d}\sum_{i,j}\alpha_i^*\alpha_j\langle a_i^-|A_{\mathbf{0}}|a_j^-\rangle = -\frac{1}{d}\sum_{i,j}\alpha_i^*\alpha_j\langle a_i^-|a_j^-\rangle = -\frac{1}{d}\sum_i \alpha_i\alpha_i^* = -\frac{1}{d}, \tag{S13}$$

which tells $|\psi\rangle$ is a magic state. For any mixed state $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ on $\mathcal{S}_m$, we have

$$W_\rho(\mathbf{0}) = \sum_i p_i W_{\psi_i}(\mathbf{0}) = -\frac{1}{d}\sum_i p_i = -\frac{1}{d}. \tag{S14}$$

Thus, we construct a $(d-1)/2$ dimensional subspace $\mathcal{S}_m$ that contains no PWF states. Obviously, $\mathcal{S}_m^\perp$ is a PWF unextendible subspace of dimension $(d+1)/2$. $\mathcal{S}_m^\perp$ is spanned by the set of all eigenvectors of $A_{\mathbf{0}}$ corresponding to eigenvalue of $+1$, denoted as $S^+ \coloneqq \{|a_i^+\rangle\}_{i=1}^{\frac{d+1}{2}}$. We show that $\rho_n = \frac{2}{d+1}\sum_j |a_j^+\rangle\langle a_j^+|$ is a PWF state on $\mathcal{S}_m^\perp$ as follows:

$$\begin{aligned}
W_{\rho_n}(\mathbf{u}) &= \frac{1}{d}\,\mathrm{Tr}(A_{\mathbf{u}}\rho_n) && \text{(S15a)}\\
&= \frac{2}{(d+1)d}\,\mathrm{Tr}(A_{\mathbf{u}}\sum_j |a_j^+\rangle\langle a_j^+|) && \text{(S15b)}\\
&= \frac{2}{(d+1)d}\,\mathrm{Tr}[A_{\mathbf{u}}(I + A_{\mathbf{0}})/2] && \text{(S15c)}\\
&= \frac{1+\delta_{\mathbf{u},\mathbf{0}}}{(d+1)} > 0. && \text{(S15d)}
\end{aligned}$$

From Eq. (S15b) to Eq. (S15c), we use the properties that $A_{\mathbf{0}} = \sum_j |a_j^+\rangle\langle a_j^+| - \sum_i |a_i^-\rangle\langle a_i^-|$ with spectral decomposition, and $I_d = \sum_j |a_j^+\rangle\langle a_j^+| + \sum_i |a_i^-\rangle\langle a_i^-|$. Note that $\mathrm{supp}(\rho_n) = \mathcal{S}_m^\perp$, combined with Lemma 2, we can conclude that $\mathcal{S}_m^\perp \subseteq \mathcal{H}_d$ is a strongly PWF unextendible subspace of dimension $(d+1)/2$. ■

Theorem 4 *Given $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H}_d)$, if any of them has strictly positive discrete Wigner functions, i.e., $W_{\rho_i}(\mathbf{u}) > 0, \forall \mathbf{u}$, then for any integer $n \in \mathbb{Z}^+$, $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$ cannot be unambiguously distinguished by PWF POVMs.*

Proof Suppose the state ρ_0 and ρ_1 can be unambiguously distinguished by a PWF POVM $\{E_0, E_1\}$. By definition, we have

$$\mathrm{Tr}(E_0\rho_1) = 0 \text{ and } \mathrm{Tr}(E_1\rho_0) = 0. \tag{S16}$$

Then we are going to establish the theorem using a proof by contradiction. Without loss of generality, we suppose ρ_1 has strictly positive Wigner functions. Notice that

$$\mathrm{Tr}(E_0\rho_1) = \sum_{\mathbf{u}} W(E_0|\mathbf{u})W_{\rho_1}(\mathbf{u}) = 0. \tag{S17}$$

By the strictly positivity of the Wigner functions of ρ_1, i.e., $W_{\rho_1}(\mathbf{u}) > 0, \forall \mathbf{u}$, we have that Eq. (S17) holds if and only if $W(E_0|\mathbf{u}) = 0, \forall \mathbf{u}$. Combining the fact that $\sum_{\mathbf{u}} W(E_0|\mathbf{u}) = d\,\mathrm{Tr}(E_0)$, we have $\mathrm{Tr}(E_0) = 0$. It follows that all eigenvalues of E_0 are equal to zero since $E_0 \geq 0$. Then we have $E_0 = \mathbf{0}$ which gives $\mathrm{Tr}(E_1\rho_0) = \mathrm{Tr}(\mathbb{1}\rho_0) = 1$, a contradiction.

Hence, there is no effect E_0 having PWFs such that $\mathrm{Tr}(E_0\rho_0) > 0$ and $\mathrm{Tr}(E_0\rho_1) = 0$ if ρ_1 has strictly positive Wigner functions. Similarly, we can show there is no effect E_1 having PWFs such that $\mathrm{Tr}(E_1\rho_0) = 0$ and $\mathrm{Tr}(E_1\rho_1) > 0$ if ρ_0 has strictly positive Wigner functions. Using the fact that

$$W_{\rho^{\otimes 2}}(\mathbf{u}_i \oplus \mathbf{u}_j) = W_\rho(\mathbf{u}_i)W_\rho(\mathbf{u}_j), \quad \forall \mathbf{u}_i, \mathbf{u}_j \in \mathbb{Z}_d \times \mathbb{Z}_d, \tag{S18}$$

we complete the proof. ■

MINIMUM ERROR DISCRIMINATION BY PWF POVMS

Note that given a two-valued PWF POVM $\{E, \mathbb{1} - E\}$, the discrete Wigner function of an effect E is $W(E|\mathbf{u}) = \mathrm{Tr}(EA_{\mathbf{u}})$. The SDP of discriminating an equiprobable pair of states $\{\rho_0, \rho_1\}$ via PWF POVMs can be written as

$$\begin{aligned} P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0, \rho_1, \frac{1}{2}) = \min_{E}\ & \frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}[E(\rho_1 - \rho_0)], \\ \text{s.t.}\ & 0 \leq E \leq \mathbb{1}, \\ & 0 \leq \mathrm{Tr}[EA_{\mathbf{u}}] \leq 1, \forall\, \mathbf{u}, \end{aligned} \tag{S19}$$

where $E \leq \mathbb{1}$ implies $\mathbb{1} - E$ is positive semidefinite. For different linear inequality constraints, we introduce corresponding dual variables $V, U, a_{\mathbf{u}}, b_{\mathbf{u}} \geq 0$. Then the Lagrange function of the primal problem can be written as

$$\begin{aligned} L(E, V, U, a_{\mathbf{u}}, b_{\mathbf{u}}) &= \frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}[E(\rho_1 - \rho_0)] + \mathrm{Tr}[V(E - \mathbb{1})] - \mathrm{Tr}(UE) \\ &\quad - \sum_{\mathbf{u}} a_{\mathbf{u}}\,\mathrm{Tr}(EA_{\mathbf{u}}) + \sum_{\mathbf{u}} b_{\mathbf{u}}[\mathrm{Tr}(EA_{\mathbf{u}}) - 1] \\ &= \frac{1}{2} + \mathrm{Tr}\left[E\Big(V - U + \frac{1}{2}(\rho_1 - \rho_0) - \sum_{\mathbf{u}} a_{\mathbf{u}}A_{\mathbf{u}} + \sum_{\mathbf{u}} b_{\mathbf{u}}A_{\mathbf{u}}\Big)\right] - \mathrm{Tr}(V) - \sum_{\mathbf{u}} b_{\mathbf{u}} \end{aligned} \tag{S20}$$

The corresponding Lagrange dual function is

$$g(V, U, a_{\mathbf{u}}, b_{\mathbf{u}}) = \inf_{E} L(E, V, U, a_{\mathbf{u}}, b_{\mathbf{u}}). \tag{S21}$$

We can see that $V - U + \frac{1}{2}(\rho_1 - \rho_0) - \sum_{\mathbf{u}} a_{\mathbf{u}}A_{\mathbf{u}} + \sum_{\mathbf{u}} b_{\mathbf{u}}A_{\mathbf{u}} \geq 0$, otherwise $g(V, U, a_{\mathbf{u}}, b_{\mathbf{u}})$ is unbounded. Thus the dual SDP is

$$\begin{aligned} \max_{V,U,a_{\mathbf{u}},b_{\mathbf{u}}}\ & \frac{1}{2} - \mathrm{Tr}(V) - \sum_{\mathbf{u}} b_{\mathbf{u}}, \\ \text{s.t.}\ & U \geq 0, V \geq 0, \\ & V - U + \frac{1}{2}(\rho_1 - \rho_0) \geq \sum_{\mathbf{u}} (a_{\mathbf{u}} - b_{\mathbf{u}})A_{\mathbf{u}}, \\ & a_{\mathbf{u}} \geq 0, b_{\mathbf{u}} \geq 0, \quad \forall\, \mathbf{u}. \end{aligned} \tag{S22}$$

Proposition 5 *Let ρ_0 be the Strange state $|\mathbb{S}\rangle\langle\mathbb{S}|$ and $\rho_1 = (\mathbb{1} - |\mathbb{S}\rangle\langle\mathbb{S}|)/2$ be its orthogonal complement. For $n \in \mathbb{Z}^+$, we have*

$$P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}, \frac{1}{2}) = \frac{1}{2^{n+1}}. \tag{S23}$$

The optimal PWF POVM is $\{E, \mathbb{1} - E\}$, where $E = (|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)^{\otimes n}$ and $|\mathbb{K}\rangle = (|1\rangle + |2\rangle)/\sqrt{2}$.

Proof First, we are going to prove $P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}, \frac{1}{2}) \leq \frac{1}{2^{n+1}}$ using SDP (S19). We will show that $E = (|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)^{\otimes n}$ is a feasible solution with a discrimination error $\frac{1}{2^{n+1}}$. In specific, it is easy to check $0 \leq E \leq \mathbb{1}$. Furthermore, we can check that $|0\rangle, |\mathbb{K}\rangle$ and $|\mathbb{S}\rangle$ are eigenvectors of $A_{\mathbf{0}}$ with eigenvalue $+1, +1$ and -1, respectively. It follows

$$\mathrm{Tr}[A_{\mathbf{u}}(|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)] = \mathrm{Tr}[A_{\mathbf{u}}(\mathbb{1} - |0\rangle\langle 0|)] = 1 - \mathrm{Tr}(A_{\mathbf{u}}|0\rangle\langle 0|) \geq 0, \tag{S24}$$

where the inequality is due to the fact that $A_{\mathbf{u}}$ has eigenvalues no larger than 1. Also, we have $\mathrm{Tr}[A_{\mathbf{u}}(|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)] = 1 - \mathrm{Tr}(A_{\mathbf{u}}|0\rangle\langle 0|) \leq 1$ as $|0\rangle\langle 0|$ is a stabilizer state with $\mathrm{Tr}(A_{\mathbf{u}}|0\rangle\langle 0|) \geq 0$. Thus, for the n-copy case, we have

$$0 \leq \prod_{i=1}^{n} \Big(\langle\mathbb{K}|A_{\mathbf{u}_i}|\mathbb{K}\rangle + \langle\mathbb{S}|A_{\mathbf{u}_i}|\mathbb{S}\rangle \Big) \leq 1, \tag{S25}$$

which makes E satisfies $0 \leq \mathrm{Tr}[EA_{\mathbf{u}}] \leq 1$. Hence, E is a feasible solution to the primal SDP (S19). Note that

$$\mathrm{Tr}[(|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)\rho_0] = \langle\mathbb{K}|\mathbb{S}\rangle\langle\mathbb{S}|\mathbb{K}\rangle + \langle\mathbb{S}|\mathbb{S}\rangle\langle\mathbb{S}|\mathbb{S}\rangle = 1, \tag{S26a}$$

$$\mathrm{Tr}[(|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)\rho_1] = \frac{1}{2}\langle\mathbb{K}|(\mathbb{1} - |\mathbb{S}\rangle\langle\mathbb{S}|)|\mathbb{K}\rangle + \frac{1}{2}\langle\mathbb{S}|(\mathbb{1} - |\mathbb{S}\rangle\langle\mathbb{S}|)|\mathbb{S}\rangle = \frac{1}{2}. \tag{S26b}$$

The corresponding discrimination error is

$$P_{pr}^{*} = \frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}\left[(|\mathbb{K}\rangle\langle\mathbb{K}| + |\mathbb{S}\rangle\langle\mathbb{S}|)^{\otimes n}(\rho_1^{\otimes n} - \rho_0^{\otimes n})\right] \tag{S27a}$$

$$= \frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}\left[(|\mathbb{K}\rangle\langle\mathbb{K}|\rho_1 + |\mathbb{S}\rangle\langle\mathbb{S}|\rho_1)^{\otimes n} - (|\mathbb{K}\rangle\langle\mathbb{K}|\rho_0 + |\mathbb{S}\rangle\langle\mathbb{S}|\rho_0)^{\otimes n}\right] \tag{S27b}$$

$$= \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2^n} - 1\right] = \frac{1}{2^{n+1}}. \tag{S27c}$$

Second, we use the dual SDP (S22) to show $P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}, \frac{1}{2}) \geq \frac{1}{2^{n+1}}$. We will construct a valid $a_{\mathbf{u}}$ combined with $\{V = (2^n - 1)\rho_0/2^{n+1}, U = 0, b_{\mathbf{u}} = 0\}$ as a feasible solution to the dual problem. We note that $\rho_0 = (\mathbb{1} - A_{\mathbf{0}})/2$ and $\rho_1 = (\mathbb{1} + A_{\mathbf{0}})/4$ and introduce the following notation. Let $\mathbf{k} = (k_1, k_2, ..., k_n) \in \{0,1\}^n$ be a n-bit binary string and $|\mathbf{k}|$ be the Hamming weight of it. We then denote $A_{\mathbf{k}} = A_{k_1} \otimes A_{k_2} \otimes ... \otimes A_{k_n}$ where $A_{k_i} = A_{\mathbf{0}}$ if $k_i = 1$ and $A_{k_i} = \mathbb{1}$ if $k_i = 0$. Then we have

$$V - U + \frac{1}{2}(\rho_1^{\otimes n} - \rho_0^{\otimes n}) = \frac{2^n - 1}{2^{n+1}}\left(\frac{\mathbb{1} - A_{\mathbf{0}}}{2}\right)^{\otimes n} + \frac{1}{2}\left[\left(\frac{\mathbb{1} + A_{\mathbf{0}}}{4}\right)^{\otimes n} - \left(\frac{\mathbb{1} - A_{\mathbf{0}}}{2}\right)^{\otimes n}\right] \tag{S28a}$$

$$= \frac{1}{2^{2n+1}}(\mathbb{1} + A_{\mathbf{0}})^{\otimes n} - \frac{1}{2^{2n+1}}(\mathbb{1} - A_{\mathbf{0}})^{\otimes n} \tag{S28b}$$

$$= \frac{1}{2^{2n+1}} \sum_{\mathbf{k}\in\{0,1\}^n} \Big(1 - (-1)^{|\mathbf{k}|}\Big) A_{\mathbf{k}} \tag{S28c}$$

$$= \frac{1}{2^{2n+1}} \sum_{\mathbf{k}\in\{0,1\}^n} \Big(\frac{1 - (-1)^{|\mathbf{k}|}}{3^{n-|\mathbf{k}|}} \sum_{\mathbf{u_k}} A_{\mathbf{u_k}}\Big), \tag{S28d}$$

where $A_{\mathbf{u_k}} = A_{\mathbf{u}_1} \otimes A_{\mathbf{u}_2} \otimes \cdots \otimes A_{\mathbf{u}_n}$ with $\mathbf{u}_j = \mathbf{0}$ if $k_j = 1$ for $j = 1, 2..., n$. To derive Eq. (S28d) from Eq. (S28c), we express each $A_{k_i} = \mathbb{1}$ with $k_i = 0$ in $A_{\mathbf{k}}$ as $\mathbb{1} = \frac{1}{3}\sum_{\mathbf{u}} A_{\mathbf{u}}$, where each $A_{\mathbf{k}}$ contains $(n - |\mathbf{k}|)$ occurrences of $\mathbb{1}$. Thus, we can find a set of $\hat{a}_{\mathbf{u}}$ such that

$$V - U + \frac{1}{2}(\rho_1^{\otimes n} - \rho_0^{\otimes n}) = \sum_{\mathbf{u}} \hat{a}_{\mathbf{u}} A_{\mathbf{u}}, \tag{S29}$$

by the following argument. For each $A_{\mathbf{u}'}$ in the n-copy system, we may find it as the sum of some terms in Eq. (S28d) with all coefficient positive since $\frac{1-(-1)^{|\mathbf{k}|}}{3^{n-|\mathbf{k}|}} \geq 0$. We can then let $\hat{a}_{\mathbf{u}}$ be the sum of those coefficients, which makes $\{V = (2^n - 1)\rho_0/2^{n+1}, \hat{a}_{\mathbf{u}}, U = 0, b_{\mathbf{u}} = 0\}$ a feasible solution of the dual SDP. Thus we have

$$P_{du}^{*} = \frac{1}{2} - \mathrm{Tr}(V) = \frac{1}{2^{n+1}}. \tag{S30}$$

Combining it with the primal part and utilizing Slater's condition for strong duality [57], we have that $P_{\mathrm{e}}^{\mathrm{PWF}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}, \frac{1}{2}) = \frac{1}{2^{n+1}}$. ■

Notice that for a given measurement $\mathbf{M} := \{M_j\}_j$, we define the PWF robustness of measurement as

$$\mathbf{R}_{\mathcal{E}_{\text{PWF}}}(\mathbf{M}) = \min\left\{r \in \mathbb{R}_+ \middle| M_j + rN_j \in \mathcal{E}_{\text{PWF}}\, \forall j, \{N_j\}_j \in \mathcal{M}\right\}, \tag{S31}$$

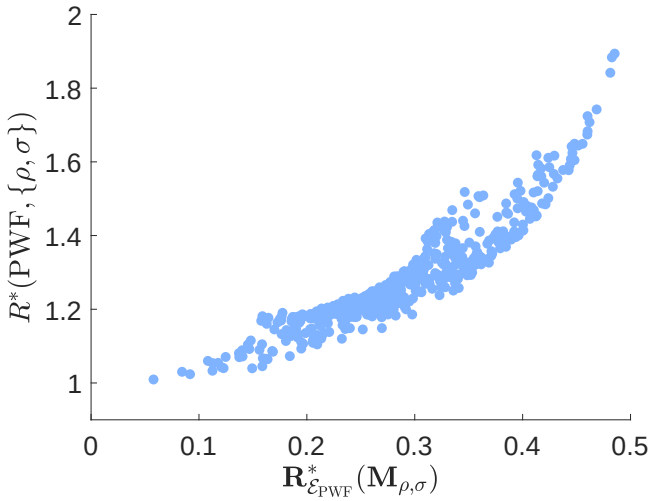
where we denote by $\mathcal{M}$ the set of all possible POVMs, and denote by $\mathcal{E}_{\text{PWF}}$ the set of all PWF effects. An effect E belongs to $\mathcal{E}_{\text{PWF}}$ if it has PWFs. The *data-hiding ratio* [61] associated with PWF POVMs is defined in our manuscript as

$$R(\text{PWF}) = \max \frac{\|p\rho - (1-p)\sigma\|_{\text{All}}}{\|p\rho - (1-p)\sigma\|_{\text{PWF}}}, \tag{S32}$$

where the maximization ranges over all pairs of states ρ, σ and a priori probabilities p (here we also define $\|\cdot\|_{\text{PWF}}$ as the *distinguishability norm* associated with PWF POVMs). In an intuitive sense, we could imagine that a higher data-hiding ratio in Eq. (S32) will be obtained if the optimal POVMs for $\|\cdot\|_{\text{All}}$ exhibit 'less PWF'. This would suggest a more pronounced disparity allowing the agent to access the optimal discrimination strategy without a 'magic factory' in the given physical setting. Therefore, given an equiprobable pair of states $\{\rho, \sigma\}$, we define $\mathbf{R}^*_{\mathcal{E}_{\text{PWF}}}(\mathbf{M}_{\rho,\sigma})$ as the minimum PWF robustness of measurement that an optimal POVM must have to discriminate $\{\rho, \sigma\}$. It can be computed via the following SDP

$$\begin{aligned}
\mathbf{R}^*_{\mathcal{E}_{\text{PWF}}}(\mathbf{M}_{\rho,\sigma}) = \min\ & r && \text{(S33a)}\\
\text{s.t. } & E_0, E_1, N_0, N_1 \geq 0, && \text{(S33b)}\\
& E_0 + E_1 = \mathbb{1}, N_0 + N_1 = r \cdot \mathbb{1}, && \text{(S33c)}\\
& \text{Tr}\left[(\rho - \sigma)E_0\right] = \frac{1}{2}\|\rho - \sigma\|_1, && \text{(S33d)}\\
& W(E_0 + N_0|\mathbf{u}) \geq 0, W(E_1 + N_1|\mathbf{u}) \geq 0, \forall \mathbf{u}, && \text{(S33e)}
\end{aligned}$$

where the constraint in Eq. (S33d) ensures that optimal discrimination is achieved, and the constraints in Eq. (S33e) ensure that $E_j + rN_j \in$ PWF. We generate 500 equiprobable pair of states $\{\rho_j, \sigma_j\}_{j=1}^{500}$ where ρ_j is a random pure qutrit state according to the Haar measure and σ_j is its orthogonal complement. Then we compute the ratio $R^*(\text{PWF}, \{\rho, \sigma\}) = \|\frac{1}{2}\rho_j - \frac{1}{2}\sigma_j\|_{\text{All}} / \|\frac{1}{2}\rho - \frac{1}{2}\sigma\|_{\text{PWF}}$ and $\mathbf{R}^*_{\mathcal{E}_{\text{PWF}}}(\mathbf{M}_{\rho_j,\sigma_j})$. The numerical calculations are implemented in MATLAB [79] with the interpreters CVX [80] and QETLAB [81]. The results are depicted as follows.



We observe that there is a possible correlation between the PWF robustness of measurement and the data-hiding ratio associated with a state pair: as the optimal POVM for a state pair exhibits a higher PWF robustness, the corresponding data-hiding ratio also increases. However, their specific relationship remains unclear so far. This experiment also indicates that the data-hiding ratio associated with the Strange state and its orthogonal complement is already relatively high, which equals 2 when $n = 1$ as stated in Eq. (4) in our manuscript. A deeper relationship between the data-hiding ratio and the PWF robustness of measurement in the case of PWF POVMs merits further investigation.

DISTINCTIONS BETWEEN THE QRT OF MAGIC STATES AND ENTANGLEMENT

Theorem 6 *For a subspace $\mathcal{S} \in \mathcal{H}_d$, if $\mathcal{S}$ has a set of basis $\{|\psi_i\rangle\}_{i=1}^n$ where every $|\psi_i\rangle$ is a stabilizer state, then $\mathcal{S}$ is PWF extendible.*

Proof Since $\{|\psi_i\rangle\}_{i=1}^n$ is a basis for $\mathcal{S}$, we have $|\psi_i\rangle$ and $|\psi_j\rangle$ are orthogonal which yields

$$\langle\psi_i|\psi_j\rangle = \sum_{\mathbf{u}} W_{\psi_i}(\mathbf{u}) W_{\psi_j}(\mathbf{u}) = 0. \tag{S34}$$

for any $i \neq j$. Note that every pure stabilizer state has Wigner functions 0 or $1/d$ [76]. Then we know that for a fixed point $\mathbf{u}'$, there is at most one state $|\psi_{j'}\rangle$ that has $W_{\psi_{j'}}(\mathbf{u}') = 1/d$. For any other states $|\psi_i\rangle, i \neq j'$, we have $W_{\psi_i}(\mathbf{u}') = 0$ otherwise $\langle\psi_{j'}|\psi_i\rangle \geq 1/d^2 > 0$, a contradiction to Eq. (S34). Thus, we have $\sum_{i=1}^n W_{\psi_i}(\mathbf{u}) = 0$ or $\sum_{i=1}^n W_{\psi_i}(\mathbf{u}) = 1/d$. Then we denote $P_{\mathcal{S}} = \sum_{i=1}^n |\psi_i\rangle\langle\psi_i|$ as the projection of $\mathcal{S}$ and consider its orthogonal complement $P_{\mathcal{S}}^{\perp} = \mathbb{1} - P_{\mathcal{S}}$. Considering $P_{\mathcal{S}}^{\perp}$ as an effect of the POVM $\{P_{\mathcal{S}}^{\perp}, P_{\mathcal{S}}\}$, we have

$$W(P_{\mathcal{S}}^{\perp}|\mathbf{u}) = 1 - d\sum_{i=1}^{n} W_{\psi_i}(\mathbf{u}) = 1 \text{ or } 0, \tag{S35}$$

which shows that $P_{\mathcal{S}}^{\perp}$ has PWFs. After normalization, we can obtain a PWF state supported on $\mathcal{S}^{\perp}$, which indicates that $\mathcal{S}$ is PWF extendible. ■

Proposition 7 *Let ρ_0 be the Strange state $|\mathbb{S}\rangle\langle\mathbb{S}|$ and $\rho_1 = (\mathbb{1} - |\mathbb{S}\rangle\langle\mathbb{S}|)/2$ be its orthogonal complement. $\rho_0 \otimes \tau^{\otimes k}$ and $\rho_1 \otimes \tau^{\otimes k}$ cannot be perfectly distinguished for any qutrit magic state τ and $k = 1$ or 2.*

Proof First, suppose there is a PWF POVM $\{E, \mathbb{1} - E\}$ that can perfectly distinguish $\rho_0 \otimes \tau^{\otimes k}$ and $\rho_1 \otimes \tau^{\otimes k}$. Then we have

$$\mathrm{Tr}[(\rho_0 \otimes \tau^{\otimes k})E] = 1, \mathrm{Tr}[(\rho_1 \otimes \tau^{\otimes k})E] = 0. \tag{S36}$$

We can write $\mathrm{Tr}[(\rho_0 \otimes \tau^{\otimes k})E] = \mathrm{Tr}[\rho_0 \mathrm{Tr}_2[(\mathbb{1} \otimes \tau^{\otimes k})E]] = 1$. Notice the fact that when ρ_0 is a pure state, $\mathrm{Tr}(\rho_0 X) = 1, \mathrm{Tr}(\rho_1 X) = 0$ if and only if $X = \rho_0$. Then for any $\mathbf{u}_1$, we have

$$\mathrm{Tr}(\rho_0 A_{\mathbf{u_1}}) = \frac{1}{d^k} \sum_{\mathbf{u_2},\cdots,\mathbf{u_{k+1}}} \mathrm{Tr}(E A_{\mathbf{u_1},\cdots,\mathbf{u_{k+1}}}) \mathrm{Tr}(\tau A_{\mathbf{u_2}}) \cdots \mathrm{Tr}(\tau A_{\mathbf{u_{k+1}}}). \tag{S37}$$

Suppose the value of maxneg(ρ_0) is obtained at phase point $\mathbf{u_1} = (a, b)$ for ρ_0, where maxneg$(\rho) := -\min_{\mathbf{u}} W_\rho(\mathbf{u})$ denotes the maximal negativity of ρ. We consider the right hand of Eq. (S37) by choosing $\mathbf{u_1} = (a, b)$:

$$\begin{aligned}
-d \cdot \mathrm{maxneg}(\rho_0) =& \frac{1}{d^k} \sum_{\mathbf{u_2},\cdots,\mathbf{u_{k+1}}} \mathrm{Tr}(E A_{(a,b),\cdots,\mathbf{u_{k+1}}}) \mathrm{Tr}(\tau A_{\mathbf{u_2}}) \cdots \mathrm{Tr}(\tau A_{\mathbf{u_{k+1}}}) && \text{(S38)}\\
\geq& \max(\mathrm{Tr}(E A_{(a,b),\cdots,\mathbf{u_{k+1}}})) \frac{1}{d^k} \sum_{\mathbf{u_2},\cdots,\mathbf{u_{k+1}}}^{<0} \mathrm{Tr}(\tau A_{\mathbf{u_2}}) \cdots \mathrm{Tr}(\tau A_{\mathbf{u_{k+1}}}) && \text{(S39)}\\
&+ \min(\mathrm{Tr}(E A_{(a,b),\cdots,\mathbf{u_{k+1}}})) \frac{1}{d^k} \sum_{\mathbf{u_2},\cdots,\mathbf{u_{k+1}}}^{\geq 0} \mathrm{Tr}(\tau A_{\mathbf{u_2}}) \cdots \mathrm{Tr}(\tau A_{\mathbf{u_{k+1}}}) && \text{(S40)}\\
\geq& \frac{1}{d^k} \sum_{\mathbf{u_2},\cdots,\mathbf{u_{k+1}}}^{<0} \mathrm{Tr}(\tau A_{\mathbf{u_2}}) \cdots \mathrm{Tr}(\tau A_{\mathbf{u_{k+1}}}) && \text{(S41)}\\
=& -\mathrm{sn}(\tau^{\otimes k}), && \text{(S42)}
\end{aligned}$$

where the inequality in Eq. (S41) is due to the fact that $0 \leq W(E|\mathbf{u}) \leq 1$ for the PWF POVM $\{E, \mathbb{1} - E\}$ and sn$(\rho) := \sum_{\mathbf{u}:W_\rho(\mathbf{u})<0} |W_\rho(\mathbf{u})|$ denotes the sum negativity of a magic state ρ. Thus, we have

$$d \cdot \mathrm{maxneg}(\rho_0) \leq \mathrm{sn}(\tau^{\otimes k}). \tag{S43}$$

Note that the Strange state $\rho_0 = |\mathbb{S}\rangle\langle\mathbb{S}|$ satisfies $d \cdot \text{maxneg}(\rho_0) = 1$, which implies $\text{sn}(\tau^{\otimes k}) \geq 1$. Since it has been shown that the maximal sum negativity of a qutrit state is $1/3$ [10], we conclude that

$$\text{sn}(\tau^{\otimes k}) = [(2\text{sn}(\tau) + 1)^k - 1]/2 \leq [(5/3)^k - 1]/2 < 1, \tag{S44}$$

for any qutrit magic state τ and $k = 1$ or 2, where we use the composition law of $\text{sn}(\cdot)$ derived by Ref. [10]. Eq. (S44) is in contradiction with the inequality $\text{sn}(\tau^{\otimes k}) \geq 1$. Thus, we complete the proof. ■

Similarly, we can conclude that for the case of Norell state $\rho_0 = |\mathbb{N}\rangle\langle\mathbb{N}|$, where $|\mathbb{N}\rangle = (-|0\rangle + 2|1\rangle - |2\rangle)/\sqrt{6}$ [10], $\rho_0 \otimes \tau$ and $\rho_1 \otimes \tau$ cannot be perfectly distinguished by PWF POVMs for any qutrit state τ.