1 A Reconciliation Protocol Based on Polar Codes for CVQKD1
Shengmei Zhao (Nanjing University of Posts and Telecommunications), Le Wang (Nanjing
University of Posts and Telecommunications), and Hanwu Chen (Southeast University)
2 ABC's of bosonic non-Gaussian channels: photon-added Gaussian channels
Krishna Kumar Sabapathy (Universitat Autònoma de Barcelona)
3 An explicit classical strategy for winning a CHSH _q game9
Martin Plesch (Masaryk University / Slovak Academy of Sciences) and Matej Pivoluska
(Masaryk University / Slovak Academy of Sciences)
4 Cache-Aware Quantum Circuit Simulation on a GPGPU11
Masaki Nakanishi (Yamagata University), Naohiro Morioka (Yamagata University), and
Kenta Shoji (Yamagata University)
5 Clauser-Horne Bell test with imperfect random inputs13
Xiao Yuan (Tsinghua University, Beijing), Qi Zhao (Tsinghua University, Beijing), and
Xiongfeng Ma (Tsinghua University, Beijing)
6 Creating cat states in one-dimensional quantum walks using delocalized initial states15
Wei-Wei Zhang (Beijing University of Posts and Telecommunications / University of
Calgary), Sandeep K. Goya (Beijing University of Posts and Telecommunications /
University of Calgary), Fei Gao (Beijing University of Posts and Telecommunications),
Barry C. Sanders (University of Calgary / University of Science and Technology of China/
Canadian Institute for Advanced Research), and Christoph Simon (University of Calgary)
7 Entropic uncertainty relations for successive generalized measurements
Kyunghyun Baek (Sogang University), Gwangil Bae (Sogang University), and Wonmin Son
(Sogang University / University of Oxford)
8 Fault-tolerant quantum computation using a maximum-likelihood decoder with the GKP code
states
Kosuke Fukui (Hokkaido University), Akihisa Tomita (Hokkaido University), and Atsushi
Okamoto (Hokkaido University)
9 Generation and Characterization of Quantum Cluster States using Surface Acoustic Waves
MG Majumdar and CHW Barnes
10 Generation and evaluation of entanglement using multiple single photon sources and linear
optics
Jun-Yi Wu (Hiroshima University) and Holger F. Hofmann (Hiroshima University)
11 Geometrical distance on quantum channels
Haidong Yuan (The Chinese University of Hong Kong) and Chi-Hang Fred Fung (Huawei
Technologies Canada)
12 Group covariance of q-ary PSK coherent-state signals coded by codes over extension field
\mathbb{F}_q

Minami Tanaka (Aichi Prefectural University), Asuka Ohashi (Ritsumeikan University), and Tsuyoshi Sasaki Usuda (Aichi Prefectural University)

- 13 Intensity fluctuation suppression in a decoy-state quantum key distribution transmitter......41 Kensuke Nakata (Hokkaido University), Akihisa Tomita (Hokkaido University), Yu Kadosawa (Hokkaido University), Kazuhisa Ogawa (Hokkaido University), and Atsushi Okamoto (Hokkaido University)
- 14 Measurement based quantum computation and Quantum Error correction codes......43 Abhishek Sharma (SRM University), Divyanshi Bhatnagar (SRM University), and Atipriya Bajaj (SRM University)
- 15 *Multipartite key distribution in networks*48 Stefan Bäuml (NTT) and Koji Azuma (NTT)

- 21 Quantum information approach to Bose-Einstein condensation of composite bosons.......63 Su-Yong Lee (Korea Institute for Advanced Study / National University of Singapore) Jayne Thompson (National University of Singapore), Sadegh Raeisi (National University of Singapore/ Friedrich-Alexander-Universität Erlangen-Nürnberg), Pawel Kurzyński (National University of Singapore / Adam Mickiewicz University), Dagomir Kaszlikowski (National University of Singapore), and Jaewan Kim (Korea Institute for Advanced Study)

Le Wang (Nanjing University of Posts and Telecommunications) and Shengmei Zhao (Nanjing University of Posts and Telecommunications)

A Reconciliation Protocol Based on Polar Codes for CVQKD

Shengmei Zhao¹ *

Le Wang¹

Hanwu $Chen^2$

¹ Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications(NUPT), Nanjing 210003, China

² School of Computer Science and Engineering, Southeast University, Nanjing, 210096, China

Abstract. This paper proposes a multidimensional reconciliation protocol for continuous variable quantum key distribution based on Polar codes. This protocol consists of two components, one is the multidimensional algorithm, and the other is Polar coding. In the first component, the continuous sifted key at Alice is first normalized then transformed to a binary data by a sphere and rotation transform operation. Then the continuous sifted key at Bob is also operated by normalization and the same rotation above. A virtual binary additive white Gaussian-like channel between Alice and Bob is established. In the second component, a specific decoding scheme with side information for Polar codes is presented, where the frozen bits locations are used as the reconciliation information. Simulation results show that the bit error rate performance and the efficiency of the proposed protocol are improved.

Keywords: Multidimensional Reconciliation, Continuous Variable Quantum Key Distribution, Polar Code

1 Introduction

Quantum key distribution (QKD) allows two remote parties (Alice and Bob) to share a secret key, even in the presence of an eavesdropper (Eve) with unlimited computational power [1]. Continuous-variable quantum key distribution (CVQKD) [2] attracts a lot of attention recently for its high rate of key generation and no limitations of single photon source and single photon detectors. But the quantum channel for the CVQKD system is not perfect one, the errors in the secret key is unavoidable. Moreover, the CVQKD quantum transmission process can only provide continuously distributed raw keys [3], they have been converted to binary ones. Thus, a reconciliation protocol [4] is crucial to extract the errorless secret keys in a CVQKD system. Furthermore, a high efficient reconciliation protocol would provide a promising way to achieve the long distance CVQKD protocol at low signal-to-noise ratio (SNR). In this paper, we propose a multidimensional reconciliation protocol for CVQKD using Polar codes. The proposed protocol includes multidimensional reconciliation component and polar coding component. In the multidimensional reconciliation component, the continuous Gaussian variables are normalized and transferred to binary without quantization. In the polar coding component, a novel construction is designed. The numerical simulation shows that the bit error rate performance and the efficiency of the proposed protocol are higher than that protocol in [5] with the same condition.

2 Multidimensional Reconciliation Protocol of CVQKD using Polar Codes

Figure 1 shows the schematic diagram of the proposed protocol. There are two components in the proposed protocol. One is multidimensional reconciliation component (named MR), the other is error correction component using polar coding.



Figure 1: The schematic diagram of Multidimensional Reconciliation protocol using Polar code.

In a CVQKD system, the continuous variable carriers for the key is usually modulated with Gaussian distribution. The raw keys X and Y for Alice and Bob are continuous Gaussian distribution random variables, and it is always assumed that Y = X + N, where N is an Additive White Gaussian Noise.

In the multidimensional reconciliation component, Alice and Bob first separately normalize their own raw keys, which are generated from the quantum process. Both Alice and Bob first divide their key variables which generated from the quantum process into a set of shorter ones, Xand Y, in the size of the dimension d, where Y = X + Z, $X \sim N(0, \Sigma^2)$ and $Z \sim N(0, \sigma^2)$. Then Alice and Bob normalize their key variables X and Y to get x and yseparately. Alice generates a random binary string u as her final key for x and obtains the transformation matrix $\mathbf{M}(x, u)$ with the constraints $\mathbf{M}(x, u)x = u$. She sends the transformation matrix $\mathbf{M}(x, u)$ to Bob. Bob makes the same transformation on his own key information y to get v, where $v = \mathbf{M}(x, u)y$. Subsequently, a virtual bi-

^{*}zhaosm@njupt.edu.cn

nary additive white Gaussian-like channel between Bob and Alice is established. Therefore, Alice and Bob hold a pair of key (u and v) without quantization, where u is a binary string, and v is a Gaussian distribution. It should be noted that that v is also the error version of u, that is v = u + e, the final noise e is just a rotated version of the noise N Bob has, in particular, both noises are Gaussian with the same variance. This is true because the Gaussian distribution of the noise is invariant under orthogonal transformations. In Polar coding component, the frozen bits information are used as the side information to correct errors e. Alice constructs a Polar code with the code rate R and code length N, and shares the frozen bits information to Alice. With the frozen bits information, Bob decodes v with BP decoding algorithm. Finally, they get a pair of common binary key.

3 Discussion and Conclusion

In this section, numerical simulation results are presented to discuss the proposed reconciliation protocol. The simulations are done with CPU of Intel Core i5-3230M. For simulation, the dimension d is set to 4. The variance of signal is set to 1. Belief propagation decoding algorithm is adopted for Polar codes. The maximum value for the frame number is set to be 500.

The efficiency is an important parameter for reconciliation protocol, which is defined as,

$$\beta = \frac{D_{eccOutput}}{D_{eccInput}} (1 - FER), \tag{1}$$

where $D_{eccOutput}$ denotes the error-correction output rate, $D_{eccInput}$ denotes for the data output rate of the system used as an input for the error-correction, and FER is frame error rate. The bigger β is, the higher efficiency the protocol has.



Figure 2: The bit error rate (BER) performance of the proposed reconciliation protocol, together with the BER performance of the protocol in [5].

Fig.2 shows the bit error rate (BER) performance of the proposed reconciliation protocol, together with the BER performance of the protocol in [5]. For the comparison, the code length for Polar code is 1024, the code length for low density parity check (LDPC) code in [5] is set to 2000. The code rate is set to 0.375. The results

Table 1: Efficiency of the proposed reconciliation protocol, in comparison with the efficiency with the protocol in [5].

SNR	Proposed protocol	Protocol in $[5]$
0.8	63.75	49.54
0.9	66.90	57.60
1.0	73.16	62.22
1.1	78.16	64.00

show that the BER performance of the proposed protocol is better than that using the protocol in [5]. When SNR=1, the BER for the proposed protocol is 10^{-3} , while it is 5×10^{-1} for the protocol in [5]. It is indicated that the proposed reconciliation protocol is better for CVQKD systems.

Table 1 further presents the efficiency of the proposed reconciliation protocol, in comparison with the efficiency with the protocol in [5]. The results show that the efficiency of the proposed protocol is higher than that using protocol in [5]. Although the proposed reconciliation protocol with code length of 1024 and code rate of 0.375 doesnt get the required efficiency, the length of practical key in CVQKD is much longer than 1024. It is believable that the efficiency of the proposed protocol can be up to 90% because the performance of Polar code is increasingly improved with a longer code length at low SNRs.

In this paper, we have presented a protocol of multidimensional reconciliation using Polar codes for CVQKD system. It has been shown that the protocol can correct the error without the need to discrete the continuous variable, it can be implemented only by constructing a special kind of side information. It is more adaptable for a long distance CVQKD system.

References

- P. Jouguet. High performance error correction for quantum key distribution using polar codes. *Quan*tum Inf. Comput., 14, 329-338, 2014.
- [2] A. Leverrier, P. Grangier. Unconditional security proof of long -distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, 102, 180504, 2009.
- [3] P. Jouguet. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A*, 84, 062317, 2011.
- [4] F. Grosshans, V. A. Gilles, W. Jerome, et al. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421, 238-241, 2003.
- [5] A. Leverrier, R. Alleaume, J. Boutros, et. al. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 77, 042325, 2008.

ABC's of bosonic non-Gaussian channels: photon-added Gaussian channels

Krishna Kumar Sabapathy^{1,*}

¹Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain.

We present a framework for systematically studying linear bosonic non-Gaussian channels. A strong motivation being that it is compulsory to go beyond the Gaussian regime for numerous tasks in continuous-variable quantum information protocols. Our emphasis is on a class of channels that we call photon-added Gaussian channels and these are experimentally viable with current quantum-optical technologies. These channels are obtained by extending Gaussian channels with photon addition applied to the ancilla ports (in its respective Stinespring unitary representation) giving rise to a one-parameter family of non-Gaussian channels indexed by photon number $n \ge 1$ with n = 0 corresponding to the underlying Gaussian channel. We then derive the corresponding operator-sum representation which becomes indispensable since the phase-space framework has limited usefulness in the present context. We observe that these channels are Fock-preserving, i.e., coherence non-generating on incoherent states in the Fock basis. Furthermore, noisy Gaussian channels can be expressed as a convex mixture of these non-Gaussian channels analogous to the Fock basis representation of a thermal state. We then report examples of activation of nonclassicality, using this method of photon-addition, at outputs of channels that would otherwise output only classical states, and present a classicality no-go theorem. We also derive many structure theorems for these channels. Finally, we observe that there exists an environment-assisted error-correction scheme for transmitting classical information through these channels.

Keywords: non-Gaussianity, non-Gaussian channels, photon-addition, Gaussian channels, Stinespring dilation, continuous-variable systems

Non-Gaussian states and operations have recently received much attention with respect to theoretical and experimental schemes in continuous-variable quantum information theory. Commonly used non-Gaussian operations include photon addition [1, 2], photon subtraction [3–5], photon counting [6], cubic phase gates[7], and Kerr nonlinearities [8]. Experimentally realizable non-Gaussian states include Fock states [9–11], noon states [12], cat states [13, 14], and photon-added coherent states [15, 16], among other examples [17–19].

There are various motivations and uses for going beyond the Gaussian regime for implementing quantum information protocols. These include no-go theorems against Gaussian-

^{*}Electronic address: krishnakumar.sabapathy@gmail.com



FIG. 1: Showing a schematic diagram for the construction of a class of non-Gaussian channels by using two constituent elements of photon-addition and bosonic Gaussian channels.

only toolbox like distillation of entanglement from Gaussian states [20–22], use as quantum repeaters [23], and for other quantum information protocols like cloning [24], error-correction [25], bit-commitment [26], and computing with cluster states [27], to list a few examples. Also non-Gaussian resources have proven advantageous in many scenarios like parameter estimation [28], generation of entangled states [29–32], teleportation [33–35], and universal quantum computation [36–38].

In this article we generate non-Gaussian operations using two main ingredients, the commonly used photon-addition and the ubiquitous class of bosonic Gaussian channels[39]. We call the resulting non-Gaussian operations as photon-added Gaussian channels and this is schematically represented in Fig. 1. Here the photon-addition will be applied to the environment state in the Stinespring dilation of the underlying Gaussian channel. As a consequence we generate non-Gaussian operations on the initial system when the environment system is ignored.

The method can also be thought of as being one example of the many protocols and implementations which concern manipulating the environment state in the Stinespring representation of a channel that have been considered in literature. Some illustrative examples include implementation of general gates [40], using mixed environment states for channel simulation [41], manipulating the environment to generate additional capacities either as a helper or adversary [42–44], and using feedback from the environment to correct for transmission of information through the channel [45–47].

I. SUMMARY OF MAIN RESULTS

Our main contribution is to formulate and present a systematic framework to study non-Gaussian channels. We focus on a special class of channels we call as photon-added Gaussian channels. These channels are realized by extending quantum-limited Gaussian channels with photon-addition applied to the environment state in the Stinespring dilation of these channels. The resulting channels are linear and non-Gaussian in nature. We consider the case of photon-added attenuator, amplifier, and phase conjugator as our main examples.

We then obtain the operator-sum representation[39] of the photon-added channels and study various implications. We find that for each of the three families of channels there exists an operator-sum representation in which the Kraus operators are real. Furthermore, the positive quadratic operators associated with the Kraus operators can all be taken to be simultaneously diagonal in the Fock basis. This allows for environment-assisted classical information transmission through these channels.

We derive a series of structure theorems for these channels. The photon-added amplifier, attenuator, and phase-conjugation channels take incoherent states in the Fock basis to incoherent states showing that they belong to the class of the so-called maximally incoherent operations from a resource-theoretic point of view for coherence in the Fock basis. We also see that the photon-added channels are complementary to the photon-added amplifier channels leading to a trivial implication on the minimum output entropy for these channels.

We show that the output nonclassicality of the phase conjugation channel can be activated by a non-trivial photon-addition leading to a classicality no-go theorem concerning the nonclassicality-breaking nature of the channel [48–50]. We also provide a decomposition of noisy Gaussian channels in terms of their respective photon-added quantum-limited channels analogous to the Fock basis representation of a thermal state.

The present study is one approach contributing to the systematic study of non-Gaussian operations that have not only proved advantageous for many quantum information protocols but are also necessary due to many Gaussian no-go theorems as mentioned earlier. The non-Gaussian channels that we introduce are arguably the simplest class of channels that go beyond the Gaussian scenario.

Furthermore, our method allows for tuning between the Gaussian and non-Gaussian regime in the space of channels through photon-addition where n plays the role of the tuning parameter, with n = 0 corresponding to a Gaussian channel and n > 0 corresponding to a non-Gaussian channel. Also the photon-added channels considered in the article [51] are experimentally realizable. We believe that there are many applications of the present work in light of the increasing use of non-Gaussian resources in continuous-variable quantum computing, cryptography, and communications tasks.

For technical details please refer arXiv:1604.07859 [quant-ph] [51].

- [1] V. Parigi, A. Zavatta, M. S. Kim, and M. Bellini, Probing quantum commutation rules by addition and subtraction of single photons to/from a light field, Science **317**, 1890 (2007).
- [2] J. Fiurášek, Engineering quantum operations on traveling light beams by multiple photon addition and subtraction, Phys. Rev. A 80, 052822 (2009).
- [3] A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles, Entanglement evaluation of non-Gaussian states generated by photon subtraction from squeezed states, Phys. Rev. A 73, 042310 (2006).
- [4] N. Namekata, Y. Takahashi, G. Fujii, D. Fukuda, S. Kurimura and S. Inoue, Non-Gaussian operation based on photon subtraction using a photon-number-resolving detector at a telecommunications wavelength, Nat. Photonics 4, 655 (2010).
- [5] K. Wakui, H. Takahashi, A. Furusawa, and M. Sasaki, Photon subtracted squeezed states generated with periodically poled *KTiOPO*₄, Opt. Exp. **15**, 3568 (2007).
- [6] C. Guerlin et. al., Progressive field-state collapse and quantum non-demolition photon counting, Nature 448, 889 (2007).
- [7] K. Miyata et. al., Implementation of a quantum cubic gate by an adaptive non-Gaussian measurement, Phys. Rev. A 93, 022301 (2016).
- [8] T. Tyc and N. Korolkova, Highly non-Gaussian states created via cross-Kerr nonlinearity, New J. Phys. 10, 023041 (2008).
- [9] M. Hofheinz et. al., Generation of Fock states in a superconducting quantum circuit, Nature 454, 310 (2008).
- [10] C. Sayrin et. al., Real-time quantum feedback prepares and stabilizes photon number states, Nature 477, 73 (2011).
- [11] K. R. Motes et. al., Efficient recycling strategies for preparing large Fock states from singlephoton sources — Applications to quantum metrology, arXiv:1603.00533[quant-ph].
- [12] I. Afek, O. Ambar, and Y. Silberberg, High-NOON states by mixing quantum and classical light, Science 328, 879 (2010).
- [13] M. Sasaki and M. Suzuki, Multimode theory of measurement-induced non-Gaussian operation on wideband squeezed light: Analytical formula, Phys. Rev. A 73, 043807 (2006).
- [14] A, Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier, Generation of optical 'Schrödinger cats' from photon number states, Nature **448**, 784 (2007).
- [15] G. S. Agarwal and K. Tara, Nonclassical properties of states generated by the excitations on a coherent state, Phys. Rev. A 43, 492 (1991).
- [16] A. Zavatta, S. Viciani, and M. Bellini, Quantum-to-Classical Transition with Single-Photon-Added Coherent States of Light, Science 306, 660 (2004).
- [17] J. Wenger, R. Tualle-Brouri, and P. Grangier, Non-Gaussian Statistics from Individual Pulses of Squeezed Light, Phys. Rev. Lett. 92, 153601 (2004).
- [18] J. S. Neergaard-Nielsen, B. M. Nielsen, C. Hettich, K. Mølmer, and E. S. Polzik, Generation of a Superposition of Odd Photon Number States for Quantum Information Networks, Phys. Rev. Lett. 97, 083604 (2006).
- [19] J. Stanojevic et. al., Generating non-Gaussian states using collisions between Rydberg polaritons, Phys. Rev. A 86, 021403(R) (2012).

4

5

- [20] J. Eisert, S. Scheel, and M. B. Plenio, Distilling Gaussian states with Gaussian operations is impossible, Phys. Rev. Lett. 89, 137903 (2002).
- [21] J. Fiurášek, Gaussian transformations and distillation of entangled Gaussian states, Phys. Rev. Lett. 89, 137904 (2002).
- [22] G. Giedke and J. I. Cirac, Characterization of Gaussian operations and distillation of Gaussian states, Phys. Rev. A 66, 032316 (2002).
- [23] R. Namiki, O. Gittsovich, S. Guha, and N. Lütkenhaus, Gaussian-only regenerative stations cannot act as quantum repeaters, Phys. Rev. A 90, 062316 (2014).
- [24] N. J. Cerf, O. Krüger, P. Navez, R. F. Werner, and M. M. Wolf, Non-Gaussian Cloning of Quantum Coherent States is Optimal, Phys. Rev. Lett. 95, 070501 (2005).
- [25] J. Niset, J. Fiurášek, and N. J. Cerf, No-Go Theorem for Gaussian Quantum Error Correction, Phys. Rev. Lett. 102, 120501 (2009).
- [26] L. Magnin, F. Magniez, A. Leverrier, and N. J. Cerf, Strong no-go theorem for Gaussian quantum bit commitment, Phys. Rev. A 81, 010302(R) (2010).
- [27] M. Ohliger, K. Kieling, and J. Eisert, Limitations of quantum computing with Gaussian cluster states, Phys. Rev. A 82, 042336 (2010).
- [28] G. Adesso, F. Dell'Anno, S. De Siena, F. Illuminati, and L. A. M. Souza, Optimal estimation of losses at the ultimate quantum limit with non-Gaussian states, Phys. Rev. A 79, 040305(R) (2009).
- [29] A. Ourjoumtsev, A. Dantan, R. Tualle-Brouri, and P. Grangier, Increasing Entanglement between Gaussian States by Coherent Photon Subtraction, Phys. Rev. Lett. 98, 030502 (2007).
- [30] H. Yakahashi, J. S. Neergaard-Nielsen, M. Takeuchi, M. Takeoka, K. Hayasaka, A. Furusawa, and M. Sasaki, Entanglement distillation from Gaussian input states, Nat. Photonics 4, 178 (2010).
- [31] K. K. Sabapathy, J. S. Ivan, and R. Simon, Robustness of Non-Gaussian Entanglement against Noisy Amplifier and Attenuator Environments, Phys. Rev. Lett. 107, 130501 (2011).
- [32] C. Navarrete-Benlloch, R. García-Patrón, J. H. Shapiro, and N. J. Cerf, Enhancing quantum entanglement by photon addition and subtraction, Phys. Rev. A 86, 012328 (2012).
- [33] S. Olivares, M. G. A. Paris, and R. Bonifacio, Teleportation improvement by inconclusive photon subtraction, Phys. Rev. A 67, 032314 (2003).
- [34] T. Opatrný, G. Kurizki, and D.-G. Welsch, Improvement on teleportation of continuous variables by photon subtraction via conditional measurement, Phys. Rev. A 61, 032302 (2000).
- [35] F. Dell'Anno, S. De Siena, L. Albano, and F. Illuminati, Continuous-variable quantum teleportation with non-Gaussian resources, Phys. Rev. A 76, 022301 (2007).
- [36] S. Lloyd and S. L. Braunstein, Quantum Computation over Continuous Variables, prl 82, 1784 (1999).
- [37] S. D. Bartlett and B. C. Sanders, Universal continuous-variable quantum computation: Requirement of optical nonlinearity for photon counting, Phys. Rev. A 65, 042304 (2002).
- [38] N. C. Menicucci *et al.*, Universal Quantum Computation with Continuous-Variable Cluster States, Phys. Rev. Lett. **97**, 110501 (2006).
- [39] J. S. Ivan, K. K. Sabapathy, and R. Simon, Operator-sum representation for bosonic Gaussian channels, Phys. Rev. A 84, 042311 (2011).
- [40] S. Ghose and B. C. Sanders, Non-Gaussian ancilla states for continuous variable quantum computation via Gaussian maps, J. Mod. Opt. 54, 855 (2007).
- [41] B. M. Terhal, I. L. Chuang, D. P. DiVincenzo, M. Grassl, and J. A. Smolin, Simulating quantum operations with mixed environments, Phys. Rev. A 60, 881 (1999).

- [43] S. Karumanchi, S. Mancini, A. Winter, and D. Yang, Classical capacities of quantum channels with environment assistance, arXiv:1602.02036 [quant-ph].
- [44] J. A. Smolin, F. Verstraete, A. Winter, Entanglement of assistance and multipartite state distillation, Phys. Rev. A 72, 052317, 2005.
- [45] M. Gregoratti and R. F. Werner, Quantum lost and found, J. Mod. Opt. 50, 915 (2003).
- [46] M. Gregoratti and R. F. Werner, On quantum error-correction by classical feedback in discrete time, J. Math. Phys. 45, 2600 (2004).
- [47] P. Hayden and C. King, Correcting quantum channels by measuring the environment, Quantum Inf. Comput. 5, 156 (2005).
- [48] J. S. Ivan, K. K. Sabapathy, R. Simon, Nonclassicality breaking is the same as entanglement breaking for bosonic Gaussian channels, Phys. Rev. A 88, 032302 (2013).
- [49] K. K. Sabapathy, Quantum-optical channels that output only classical states, Phys. Rev. A 92, 052301 (2015).
- [50] K. K. Sabapathy, Process output nonclassicality and nonclassicality depth of quantum-optical channels, Phys. Rev. A 93, 042103 (2016).
- [51] K. K. Sabapathy, On bosonic non-Gaussian processes: photon-added Gaussian channels, arXiv:1604.07859 [quant-ph].

An explicit classical strategy for winning a $CHSH_q$ game

Martin Plesch $^{*1 2}$

Matej Pivoluska^{†1 2}

¹Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic ²Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia

Abstract. A CHSH_q game is a generalization of the standard two player CHSH game, having q different input and output options. In contrast to the binary game, the best classical and quantum winning strategies are not known exactly. In our work [8] we provide a constructive classical strategy for winning a CHSH_q game, with q being a prime. Our construction achieves a winning probability better than $\frac{1}{22}q^{-\frac{2}{3}}$, which is in contrast with the previously known constructive strategies achieving only the winning probability of $O(q^{-1})$.

Keywords: Non-locality, CHSH game

1 Introduction

Non-locality is one of the defining features of quantum mechanics qualitatively differentiating it from classical physics [4]. Apart from its foundational importance, scientists have recently realized that quantum non-locality is also an extremely valuable resource enabling various tasks, such as quantum key distribution [1] or randomness expansion and amplification [9]. All these applications use a unifying feature of quantum mechanics namely its possibility to provide the experimentalist results that exhibit super-classical correlations. Measurements on distant parts of a quantum system can, if performed in a specific way, produce results that are not reproducible by any classical system, even with the help of pre-shared information. Since the seminal work of Bell [3], who first realized this fact, a long line of research was devoted both to experimental realization of different tests of quantumness and its theoretical implications.

Arguably the simplest and most studied generalization of the original Bell setting is the Clauser-Horne-Shimony-Holt (CHSH) setting [5], where two experimentalists choose one out of two possible binary measurements on their part of the system. The setting can be rephrased into a language of games, where two noncommunicating players, Alice and Bob, both receive a uniformly chosen single bit input x and y respectively and their goal is to produce single bit outputs a and b, such that $a + b \equiv xy \mod 2$ (see Fig. 1a).

It is well known that classical players can win this game with probability no more than 75%. Utilizing quantum mechanics, players can share a maximally entangled state of two qubits and perform a suitable measurement (dependent on the input) on their respective qubit. In such a way they can increase the probability of wining the game up to $\frac{2+\sqrt{2}}{4} \approx 85\%$.

A straightforward generalization is a CHSH_q game, where the dimensionality of both inputs and outputs is limited to a prime q (see Fig. 1b). In this case, the winning condition states $a + b \equiv xy \mod q$. However, in order for this game to be interesting, the probability of winning the game with a quantum strategy must be higher than the probability with purely classical systems. Therefore, bounds for these probabilities are of utmost importance for its possible use.

Contrary to the binary CHSH game, neither the exact value of the probability of winning the game with a quantum strategy $\omega^*(\text{CHSH}_q)$, nor a strategy obtaining the optimal value is known. The only existing result due to [2] introduces an upper bound for the quantum probability

$$\omega^*(\text{CHSH}_q) \le \frac{1}{q} + \frac{q-1}{q} \frac{1}{\sqrt{q}} = \frac{1}{\sqrt{q}} + \frac{1}{q} - \frac{1}{q\sqrt{q}}.$$

For classical strategies [2], there exists an upper bound in the form

$$\omega(\text{CHSH}_q) = O\left(q^{-\frac{1}{2}-\varepsilon}\right) \quad \text{for } q = p^{2k+1}$$

where p is a prime, $k \ge 1$ and $\varepsilon > 0$ is a constant. It is only valid for the case of an odd prime power, but still could serve for a proof of a classical – quantum gap if the quantum bound would be proven tight.

There also exists a set of lower bounds (also proven in [2]) in the form

$$\omega(\text{CHSH}_q) = \begin{cases} \Omega\left(q^{-\frac{1}{2}}\right) & \text{for } q = p^{2k} \\ \Omega\left(q^{-\frac{2}{3}}\right) & \text{for } q = p^{2k+1} \end{cases}$$

We see that for q being an even power prime the lower bound is higher than for odd powers and thus for all values of q there is a significant gap between the lower or upper (partly non-existent) bounds.

Even more importantly and perhaps surprisingly, these lower bounds are not connected with any concrete strategy. Quantum strategies existing so far are limited to different heuristics (*e.g.* trying to maximize the winning probability over all measurements of the maximally entangled bipartite state), random searches and numerics [6, 7]. Best known classical strategies so far obtained only $\omega(\text{CHSH}_q) = \Omega\left(\frac{1}{q}\right)$ [7], which corresponds to a trivial strategy (both Alice and Bob output 0 irrespective on

^{*}plesch@savba.sk

[†]mpivoluska@mail.muni.cz

a.)
$$\begin{array}{c|c} x \in \{0,1\} & y \in \{0,1\} \\ & \downarrow \\ & \downarrow \\ & A \\ & \downarrow \\ & a \in \{0,1\} \\ & a + b \stackrel{?}{\equiv} xy \mod 2 \end{array} \end{array} b.) \\ \begin{array}{c|c} x \in \mathbb{F}_q \\ & \downarrow \\ & A \\ & \downarrow \\ & a \in \mathbb{F}_q \\ & a + b \stackrel{?}{\equiv} xy \mod q \end{array} b.) \\ \begin{array}{c|c} x \in \mathbb{F}_q \\ & a \in \mathbb{F}_q \\ & a + b \stackrel{?}{\equiv} xy \mod q \end{array}$$
b.) \\ \begin{array}{c|c} x \in \mathbb{F}_q \\ & a \in \mathbb{F}_q \\ & a + b \stackrel{?}{\equiv} xy \mod q \end{array} b.)

Figure 1: a.) Two non-communicating players Alice (A) and Bob (B) get one bit inputs x and y each, chosen at random. Their goal is to produce two outputs a and b such that $a + b \equiv xy \mod 2$. b.) The same situation with inputs x and y chosen at random from a finite field \mathbb{F}_q with prime q. Goal of the players it to produce two outputs $a, b \in \mathbb{F}_q$ respectively, such that $a + b \equiv xy \mod q$.

their input and win if either x = 0 or y = 0, thus in 2q - 1 out of q^2 cases).

In our paper [8] we presented the first constructive classical strategy for the CHSH_q game with the probability of winning $\Omega\left(q^{-\frac{2}{3}}\right)$ for q being a prime. With this strategy we close the gap between constructive strategies and existence bounds. To be able to prove this result, we first related the problem of classical CHSH_q game strategies to a well-known problem of point-line incidences. Doing that we were able to construct an explicit strategy for winning a generalized CHSH_q game with a winning probability lower bounded by $\frac{p^{-2/3}}{22}$, what perfectly mimics the non-constructive existence bound known so far.

This result is useful for potential design of device independent algorithms based on higher alphabet CHSH games in different aspects. First, it closes the gap between existing explicit strategies and proven existence bounds, which helps the understanding of the nature of the problem. Second, and most importantly, the presented result provides the first non-trivial classical strategy for a CHSH game, where Alice and Bob need to act in a way that depends on their input and their output is a result of a non-trivial calculation.

There is also a set of open questions that remain. The obvious one is, how one could generalize the result presented in this paper for prime power fields. This is not easy, as the nature of the proof relays on the relation between addition and multiplication, which is unique for prime fields. Also the fact that known existence bounds crucially depend on whether they are deployed on even or odd power prime field suggests that any possible generalization will not be straightforward.

More ambitious goals include the aim of finding tight bounds on classical strategies. This might, in accordance with suitable heuristic results for quantum strategies, lead to the possibility of direct use of higher-order $CHSH_q$ games in experiments. The ultimate goal, naturally, remains to directly prove a gap between classical and quantum strategies.

References

- A. Acín, et. al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.
- [2] M. Bavarian and P. W. Shor. Information causality, szemerédi-trotter and algebraic variants of chsh. ITCS '15, pages 123–132, New York, NY, USA, 2015. ACM.
- [3] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.
- [4] N. Brunner, et. al. Bell nonlocality. Rev. Mod. Phys., 86:419–478, Apr 2014.
- [5] John F. Clauser, et. al. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.
- [6] Se-Wan Ji, et. al. Multisetting bell inequality for qudits. Phys. Rev. A, 78:052103, Nov 2008.
- [7] Y.-C. Liang, C.-W. Lim, and D.-L. Deng. Reexamination of a multisetting bell inequality for qudits. *Phys. Rev. A*, 80:052116, Nov 2009.
- [8] M. Pivoluska and M. Plesch. An explicit classical strategy for winning a $chsh_q$ game. New Journal of Physics, 18, 2016.
- [9] M. Pivoluska and M. Plesch. Device independent random number generation. Acta Physica Slovaca, 64(6):600 - 663, 2014.

Cache-Aware Quantum Circuit Simulation on a GPGPU

Masaki Nakanishi¹ *

Naohiro Morioka¹[†]

Kenta Shoji^{1 ‡}

¹ Department of Education, Art and Science, Yamagata University, Yamagata 990–8560, Japan

Abstract. Quantum computer simulators play an important role when we develop and evaluate quantum algorithms. Quantum computation can be regarded as parallel computation in some sense, and thus, it is suitable to implement a simulator on a device that can process many operations in parallel. In this research, we propose a GPGPU-based quantum computer simulator. The proposed simulator recursively decomposes the state space so that the sizes of the subspaces will fit the sizes of hierarchical caches. This makes cache hit rates higher. We also developed the method that can avoid bank conflicts. We implemented the proposed simulator on an NVIDIA GeForce GTX 970. Experimental results show that the proposed simulator has better performance.

Keywords: quantum circuit simulation, GPGPU, cache-aware simulation

1 Introduction

Development of quantum algorithms is a difficult task and sometimes needs analysis based on simulation as well as theoretical analysis. For this purpose, simulation of quantum computers is highly demanded. However, simulation of quantum computers is a time-consuming task, and thus, various kinds of simulation methods have been investigated intensively [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14].

Since quantum computation is parallel computation in some sense, which is called *quantum parallelism*, it is suitable to implement simulators on parallel computation devices such as GPGPUs, many-core CPUs, and ASICs. In this research, we focus on simulators on GPGPUs. In [5], a GPGPU-based simulator was proposed. The simulator is designed so that it can access data in a coalesced manner since coalesced memory access is crucial for high performance in GPGPU computing. The simulator generates coalesced access patterns by decomposing the state space into subspaces so that each subspace may have consecutive computational basis vectors as its basis.

In GPGPU computing, memory access often becomes a bottleneck, and so is the case of quantum circuit simulation. Thus, reducing memory access overhead is the main concern in this research field. One of the solutions for this problem is to make efficient use of L2-cache. A GPGPU has an L2-cache between shared memory and global memory, and by achieving high L2-cache hit rate we can improve the performance of the simulator. In GPGPU computing, shared memory is used as a usercontrollable cache. Shared memory is divided into memory banks. Data stored in different banks can be accessed in parallel. On the other hand, data stored in the same bank must be accessed sequentially, which is called a bank conflict. Thus, generating memory access patterns that avoids bank conflicts also improves the performance.

In this research, we extended the method in [5] and developed a GPGPU-based quantum circuit simulator that achieves high L2-cache hit rate. We also developed a method that can avoid bank conflicts in shared memory. We implemented our simulator on an NVIDIA GeForce GTX 970. Experimental results show that the proposed simulator has better performance.

2 GPGPU Programming Model

The programming model of the target GPGPU is so-called SIMT (Single Instruction, Multiple Thread) model. A bunch of threads (32 threads for our target architecture), called a *warp*, executes the same instruction on different data. Threads are grouped into *threadblocks*. Threads in a thread-block share on-chip shared memory. The shared memory can be used to communicate between threads in the same thread-block. On the other hand, communication across thread-blocks needs to transfer data to the off-chip global memory. The global memory has an L2-cache, and the L2-cache can be used to boost inter-block communication. The shared memory can be used as a user-controllable L1-cache. Thus, the shared memory together with the L2-cache forms a hierarchical cache architecture.

3 Cache-Aware Quantum Circuit Simulation

We use the linearity of matrix-vector multiplication to simulate quantum gates efficiently, which is commonly used in quantum circuit simulations[5, 7, 8, 12]. Let $Q = \{q_0, \ldots, q_{n-1}\}$ be a set of qubits, and also let $v = (\alpha_0, \ldots, \alpha_{2^{n-1}})^T$ be a state vector of the *n*-qubit system. For m < n, we divide Q into two disjoint subsets, $S_1 = \{q_{i_1}, \ldots, q_{i_m}\}, S_2 = \{q_{j_1}, \ldots, q_{j_{n-m}}\}$ where $i_1 < \cdots < i_m$ and $j_1 < \cdots < j_{n-m}$. We fix the values of the qubits in S_2 as $x_{j_1}, x_{j_2}, \ldots, x_{j_{n-m}}$ ($x_{j_k} \in \{0, 1\}$), respectively. Then, $v_{x_{j_1}x_{j_2}\cdots x_{j_{n-m}}}$ denotes the projection of v onto the subspace where the qubits in S_2 are fixed to $x_{j_1}x_{j_2}\cdots x_{j_{n-m}}$. Note that the following holds:

$$\sum_{\substack{x_{j_1}x_{j_2}\cdots x_{j_{n-m}}=00\cdots 0}}^{11\cdots 1} v_{x_{j_1}x_{j_2}\cdots x_{j_{n-m}}} = v, \text{ and}$$
$$v_x \cdot v_y = 0 \text{ for } x \neq y(x, y \in \{0, 1\}^{n-m}).$$

^{*}masaki@cs.e.yamagata-u.ac.jp

[†]n-morioka@cs.e.yamagata-u.ac.jp

[‡]k-shoji@cs.e.yamagata-u.ac.jp

We consider a sequence of quantum gates, (g_1, g_2, \ldots, g_k) . We restrict each of g_i 's to be a one-qubit gate or a controlled-unitary gate. We identify each of the quantum gates g_i with the corresponding transformation. Then by linearity, the following holds:

$$g_k \circ \cdots \circ g_2 \circ g_1(v) = \sum_i g_k \circ \cdots \circ g_2 \circ g_1(v_i)$$

where $g_j \circ g_i$ is a composite transformation of g_i and g_j . This means that we may apply quantum gates to each v_i independently, and then sum up the resulting vectors $v'_i = g_k \circ \cdots \circ g_2 \circ g_1(v_i) \ (0 \leq i < 2^{n-m})$ to obtain a complete result. Note that if the target bits of g_j 's $(1 \leq j \leq k)$ are placed on the qubits in S_1 , v'_i is in the same subspace as v_i .

In order to make L2-cache hit rate higher, we apply the above method recursively. That is, we decompose the state space into subspaces whose size fits in the L2cache. Then, we recursively decompose each of the subspaces into smaller subspaces whose size fits in the shared memory. Then, by simulating quantum gate operations within each subspace, we can achieve high memory access locality. The simulation can be done for each subspace one by one. However, in order to achieve high memory access locality for L2-cache, it is needed to appropriately schedule the order of the subspaces to be simulated. The proposed method does this without spoiling the parallel computation of a GPGPU.

4 Avoiding Bank Conflicts

When simulating a quantum gate sequence for a subspace, the amplitudes of the basis vectors that lies in the target subspace are in the shared memory. Let the number of memory banks be 2^k . Also, let the shared memory have amplitudes of the basis vectors $|00...0\rangle, ..., |11...1\rangle$ where the amplitude of $|x\rangle$ is stored at address x. When simulating a quantum gate whose target bit is on the *i*-th qubit, each thread fetches from the shared memory a pair of amplitudes whose corresponding computational basis state differs only on the *i*-th bit. When $i \leq k$, the *j*-th thread and the $(j + 2^{k-1})$ -th thread access to the same bank, which causes a bank conflict.

To avoid the bank conflict, we modified the access patterns so that the $(j + 2^{k-1})$ -th thread may access to the other amplitude of the pair first. By this, the *j*-th to the $(j+2^k-1)$ -th threads access to mutually distinct banks, and we can improve memory access performance.

5 Implementation and Experiments

We implemented our method on an NVIDIA GeForce GTX 970. The CUDA runtime version used for the implementation is 7.0. We used 25-qubit quantum circuits as benchmarks. The experimental results show that the proposed method can achieve from 4.3% to 10% improvement of the performance.

Acknowledgement. This work was partially supported by JSPS KAKENHI Grant Numbers 16K00007,

24500003 and 24106009, and also by the Asahi Glass Foundation.

References

- M. Aminian, M. Saeedi, M.S. Zamani, and M. Sedighi. FPGA-based circuit model emulation of quantum algorithms. In *IEEE Computer Society Annual Symposium* on VLSI, ISVLSI '08, pages 399–404, April 2008.
- [2] K. De Raedt, K. Michielsen, H De Raedt, B. Trieu, G. Arnold, M. Richter, Th Lippert, H. Watanabe, and N. Ito. Massively parallel quantum computer simulator. *Computer Physics Communications*, 176(2):121 – 136, 2007.
- [3] Michael P. Frank, Uwe H. Meyer-Baese, Irinel Chiorescu, Liviu Oniciuc, and Robert A. van Engelen. Spaceefficient simulation of quantum computers. In *Proceedings of the 47th Annual Southeast Regional Conference*, ACM-SE 47, pages 83:1–83:6, New York, NY, USA, 2009. ACM.
- [4] M. Fujishima. FPGA-based high-speed emulator of quantum computing. In Proceedings of IEEE International Conference on Field-Programmable Technology, FPT 2003, pages 21–26, Dec 2003.
- [5] Eladio Gutiérrez, Sergio Romero, María A. Trenas, and Emilio L. Zapata. Quantum computer simulation using the CUDA programming model. *Computer Physics Communications*, 181(2):283–300, 2010.
- [6] A.U. Khalid, Z. Zilic, and K. Radecka. FPGA emulation of quantum circuits. In Proceedings of IEEE International Conference on Computer Design: VLSI in Computers and Processors, ICCD 2004., pages 310–315, Oct 2004.
- [7] Masaki Nakanishi, Miki Matsuyama, and Yumi Yokoo. A fast quantum computer simulator based on register reordering. *IEICE Trans. Inf. & Syst.*, E99-D(2):332– 340, 2016.
- [8] Jumpei Niwa, Keiji Matsumoto, and Hiroshi Imai. General-purpose parallel simulator for quantum computing. In Proceedings of the Third International Conference on Unconventional Models of Computation, UMC '02, pages 230–251, 2002.
- [9] Kevin M. Obenland and Alvin M. Despain. A parallel quantum computer simulator. quant-ph/9804039, 1998.
- [10] S. O'uchi, M. Fujishima, and K. Hoh. An 8-qubit quantum-circuit processor. In *Proceedings of IEEE In*ternational Symposium on Circuits and Systems, ISCAS 2002., pages 209–212, 2002.
- [11] G. Patz. A parallel environment for simulating quantum computation. PhD thesis, MIT, 2003.
- [12] A. Shibata, T. Nakada, M. Nakanishi, S. Yamashita, and Y. Nakashima. A method of reducing communication costs for parallel simulations of quantum computation. *IEICE Transactions on Information and Systems* (Japanese Edition), 93(3):253–264, mar 2010.
- [13] Frank Tabakin and Bruno Juliá-Díaz. Qcmpi: A parallel environment for quantum computing. *Computer Physics Communications*, 180(6):948 – 964, 2009.
- [14] George F. Viamontes, Igor L. Markov, and John P. Hayes. Graph-based simulation of quantum computation in the density matrix representation. *Quantum Info. Comput.*, 5(2):113–130, March 2005.

Clauser-Horne Bell test with imperfect random inputs

Xiao Yuan¹

Qi Zhao¹

Xiongfeng Ma¹ *

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

Abstract. Bell test is one of the most important tools in quantum information science. In practice, loopholes existing in experimental demonstrations of Bell tests may affect the validity of the conclusions. In this work, we focus on the randomness (freewill) loophole and investigate the randomness requirement in a well-known Bell test, the Clauser-Horne test, under various conditions. Our result thus provides input randomness requirements on the Clauser-Horne test under varieties of practical scenarios. The employed analysis technique can also be generalized to other Bell inequalities.

Keywords: Bell test, Clauser-Horne test, randomness (freewill) loophole

1 Introduction

Since the inception of quantum mechanics, whether the law of nature is deterministic or truly random has been long debated.During this debate, Einstein, Podolsky, and Rosen (EPR) proposed a paradox [1] that eventually leaded to a counterintuitive phenomenon — quantum nonlocality. Later, Bell put the EPR paradox in an experimentally testable framework, known as Bell test [2]. In the bipartite scenario, a Bell test involves two remotely separated parties, Alice and Bob, who receive random inputs x and y and produce outputs a and b, respectively. Based on the probability distribution $\tilde{p}_{AB}(a, b|x, y)$ of the outputs conditioned on the inputs, Bell's inequality can be defined by a linear combination of $\tilde{p}_{AB}(a, b|x, y)$ according to

$$J = \sum_{a,b,x,y} \beta_{a,b}^{x,y} \tilde{p}_{AB}(a,b|x,y) \le J_C, \qquad (1)$$

where J_C is a bound for all local hidden variable models (LHVMs), meaning that, any LHVM cannot violate any Bell's inequality.

There are three main inherent loopholes. The first one is the locality loophole and the second one is the detection efficiency loophole. These two loopholes can be closed by separating the two parties sufficiently apart with regard to the synchronization precision of different measurements in the tests. Third, the randomness (freewill) loophole refers to the underlying assumption in Bell tests that different measurement settings can be chosen randomly (freely). Generally, a Bell test requires the input of each party to be fully random in order to avoid information leakage between different parties. If there is a local hidden variable that shares information about the random inputs, where in the worst scenario, the inputs are all predetermined such that each party knows exactly the input of the other party, it is possible to violate Bell inequalities just with LHVM strategies. Yet, it is still meaningful to discuss the randomness requirement of Bell tests in a practical scenario. This is especially meaningful when considering a loophole free Bell test [3, 4] and its applications to practical tasks in the presence of an eavesdropper.

2 Randomness Requirement

In this work, we consider Bell's inequalities with input settings not chosen fully randomly. That is, the inputs x and y depend on some local hidden variable, denoted as λ . The input randomness can be quantified by the dependence of the inputs conditioned on λ . Suppose the inputs x and y are chosen according to a priori probability $p(x, y|\lambda)$, the input randomness can be measured by its upper and lower bounds,

$$P = \max_{x,y,\lambda} p(x,y|\lambda),$$

$$Q = \min_{x,y,\lambda} p(x,y|\lambda).$$
(2)

When the input settings are determined by $p(x, y|\lambda)$, the observed probability $\tilde{p}_{AB}(a, b|x, y)$ of outputs conditioned on inputs is given by

$$\tilde{p}_{AB}(a,b|x,y) = \frac{\sum_{\lambda} \tilde{p}_{AB}(a,b|x,y,\lambda)p(x,y|\lambda)q(\lambda)}{p(x,y)}, \quad (3)$$

where $q(\lambda)$ is the priori probability of λ , $p(x, y) = \sum_{\lambda} p(x, y|\lambda)q(\lambda)$ is the averaged probability of choosing x and y, and $\tilde{p}_{AB}(a, b|x, y, \lambda)$ is the strategy of Alice and Bob conditioned on λ . Then, the Bell's inequality defined in Eq. (1) should be rephrased by

$$J = \sum_{x,y} \frac{1}{p(x,y)} \sum_{\lambda} \sum_{a,b} \beta_{a,b}^{x,y} \tilde{p}_{AB}(a,b|x,y,\lambda) p(x,y|\lambda) q(\lambda)$$

$$\leq J_C.$$
(4)

3 CH inequality

In this section, we will investigate the randomness requirement of the CH inequality under different conditions, including whether $\tilde{p}_{AB}(a, b|x, y)$ is signaling or NS, and whether the factorizable condition is satisfied or not.

3.1 CH inequality with LHVMs

The CH inequality is defined in the bipartite scenario, where the input settings x and y and the outputs a and b are all bits. Based on the probability distribution that

^{*}xma@tsinghua.edu.cn

obtains a specific measurement outcome, for instance 00, the CH inequality is defined according to

$$J_{\rm CH} = \tilde{p}_{AB}(0,0) + \tilde{p}_{AB}(0,1) + \tilde{p}_{AB}(1,0) - \tilde{p}_{AB}(1,1) - \tilde{p}_{A}(0) - \tilde{p}_{B}(0) \le 0,$$
(5)

where we omit the outputs a and b and define $\tilde{p}_A(x)$ $(\tilde{p}_B(y))$ to be the probability of detecting 0 with input setting x (y) by Alice (Bob), and $\tilde{p}_{AB}(x, y)$ the probability of coincidence detection 00 for both sides with input settings x and y for Alice and Bob, respectively.

In real experiments, the input probability can be arbitrary, where our result can still apply with certain modifications on normalization. With the normalization condition, the CH value with LHVMs strategies is given by

$$J_{\rm CH}^{\rm LHVM} = 4 \sum_{\lambda} q(\lambda) J_{\lambda} \tag{6}$$

with J_{λ} defined by

$$J_{\lambda} = \tilde{p}_{A}(0,\lambda)\tilde{p}_{B}(0,\lambda)p(0,0|\lambda) + \tilde{p}_{A}(0,\lambda)\tilde{p}_{B}(1,\lambda)p(0,1|\lambda) + \tilde{p}_{A}(1,\lambda)\tilde{p}_{B}(0,\lambda)p(1,0|\lambda) - \tilde{p}_{A}(1,\lambda)\tilde{p}_{B}(1,\lambda)p(1,1|\lambda) - \tilde{p}_{A}(0,\lambda)(p(0,0|\lambda) + p(0,1|\lambda))/2 - \tilde{p}_{B}(0,\lambda)(p(0,0|\lambda) + p(1,0|\lambda))/2.$$

$$(7)$$

With the randomness parameter defined in Eq. (2), our target is to maximize $J_{\rm CH}^{\rm LHVM}$ defined in Eq. (6).

3.2 General strategy (attack)

In this part, we consider a general strategy (attack) where no additional assumption is imposed. Note that the optimization of Eq. (6) requires to optimize over the strategy of Alice and Bob, $\tilde{p}_A(x,\lambda)$ and $\tilde{p}_B(y,\lambda)$, and also the strategy of deciding the inputs, $p(x,y|\lambda)$. Here, we first analyze how to optimize the strategy of Alice and Bob.

Because all probabilistic LHVM strategies can be realized with a convex combination of deterministic strategies, it is sufficient to just consider deterministic strategies, i.e., $\tilde{p}_A(x), \tilde{p}_B(y) \in \{0, 1\}$ for the optimization. Conditioned on different values of $\tilde{p}_A(x)$ and $\tilde{p}_B(y)$, we should choose the optimal strategy of $\tilde{p}_A(x)$ and $\tilde{p}_B(y)$ that maximize J_{λ} .

	7	ъ
$(p_A(0), p_A(1), p_B(0), p_B(1))$	J_{λ}	Π
(0,1,1,0)	(p(1,0) - p(0,0))/2	_ [1]
(0,1,1,1)	(p(1,0) - p(0,0))/2 - p(1,1)	ι
(1,0,0,1)	(p(0,1) - p(0,0))/2	
(1,0,1,1)	(p(0,1) - p(1,0))/2	
(1,1,0,1)	(p(0,1) - p(0,0))/2 - p(1,1)	[2]
(1,1,1,0)	(p(1,0) - p(0,1))/2	
(1,1,1,1)	(p(1,0) + p(0,1))/2 - p(1,1)	_[3]

Table 1: Possible strategies for letting J_{λ} be positive.

For simple notation, we denote p(i, j) by p_{2*i+j} hereafter, thus the possible deterministic strategies for J_{λ} are in the following set

$$\left\{\frac{p_2 - p_0}{2}, \frac{p_1 - p_0}{2}, \frac{p_1 - p_2}{2}, \frac{p_2 - p_1}{2}, \frac{p_2 + p_1}{2} - p_3\right\}.$$
(8)

Because there are only five possible strategies of Alice and Bob, we can also consider that there are only five different strategies of choosing the input settings. Therefore, we label λ_j to be the *j*th strategy of choosing the input settings and $J_{\rm CH}^{\rm LHVM}$ can be rewritten in the following way,

$$J_{\rm CH}^{\rm LHVM}/4 = q(\lambda_1)(p_2(\lambda_1) - p_0(\lambda_1))/2 + q(\lambda_2)(p_1(\lambda_2) - p_0(\lambda_2))/2 + q(\lambda_3)(p_1(\lambda_3) - p_2(\lambda_3))/2 + q(\lambda_4)(p_2(\lambda_4) - p_1(\lambda_4))/2 + q(\lambda_5)[(p_2(\lambda_5) + p_1(\lambda_5))/2 - p_3(\lambda_5)].$$
(9)

Then $J_{\rm CH}^{\rm LHVM}$ can be expressed by

$$J_{\rm CH}^{\rm LHVM} = 4 \sum_{ij} \beta_{ij} q(\lambda_j) p_i(\lambda_j), \qquad (10)$$

Based on the value of P and Q, we give the optimal CH value $J_{\rm CH}^{\rm LHVM}$ with LHVMs by

$$J_{\rm CH}^{\rm LHVM}(P,Q) = \begin{cases} \frac{5}{2}(4P-1) & 3P+Q \le 1, \\ 1-4Q & 2P+Q \ge \frac{3}{4}, \\ 4P-2Q-\frac{1}{2} & \text{else}, \end{cases}$$
(11)

Note that when P is greater than 3/8, the value of J_{CH}^{LHVM} is independent of P.

3.3 Results

Let us compare the results of the CH values $J_{\rm CH}^{\rm LHVM}$ under different conditions. For the maximal quantum violation $J_Q = (\sqrt{2} - 1)/2$, we calculate the critical values of Q and P such that $J_{\rm CH}^{\rm LHVM}(P,Q) = J_Q$. When Q is small, the optimal CH value $J_{\rm CH}^{\rm LHVM}(P,Q)$ depends only on P. In this case, the critical values of P for the signaling, signaling+fac, NS, and NS+fac are 0.207, 0.302, 0.285, 0.354, respectively. On the other hand, when Qis large, the optimal CH value $J_{\rm CH}^{\rm LHVM}(P,Q)$ depends only on Q instead. In this case, the critical values of Qfor the signaling and NS condition are 0.198 and 0.146, respectively.

References

- 1] Einstein, A. and Podolsky, B. and Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev.47.777
- [2] Bell, John Stuart. On the Einstein-Podolsky-Rosen Paradox. Physics 1, 195–200 (1964).
- [3] Larsson, J.-Å. Loopholes in Bell inequality tests of local realism. Journal of Physics A Mathematical General, 2014.
- [4] Kofler, J. and Giustina, M. Requirements for a loophole-free Bell test using imperfect setting generators. ArXiv e-prints.1411.4787.

Creating cat states in one-dimensional quantum walks using delocalized initial states

Wei-Wei Zhang,^{1,2,*} Sandeep K. Goyal,^{2,†} Fei Gao,^{1,‡} Barry C. Sanders,^{2,3,4,5,§} and Christoph Simon^{2,¶}

¹State Key Laboratory of Networking and Switching Technology,

Beijing University of Posts and Telecommunications, Beijing 100876, China

²Institute for Quantum Science and Technology, and Department of

Physics and Astronomy, University of Calgary, Canada, T2N 1N4

University of Science and Technology of China, Hefei, Anhui 230026, China

⁴Shanghai Branch, CAS Center for Excellence and Synergetic

Innovation Center in Quantum Information and Quantum Physics,

University of Science and Technology of China, Shanghai 201315, China

⁵Program in Quantum Information Science, Canadian Institute for Advanced Research, Toronto, Ontario M5G 128, Canada

Cat states are coherent quantum superpositions of macroscopically distinct states and are useful for understanding the boundary between the classical and the quantum world. Due to their macroscopic nature, cat states are difficult to prepare in physical systems. We propose a method to create cat states in one-dimensional quantum walks using delocalized initial states of the walker. Since the quantum walks can be performed on any quantum system, our proposal enables a platformindependent realization of the cat states. We further show that the linear dispersion relation of the effective quantum walk Hamiltonian, which governs the dynamics of the delocalized states, is responsible for the formation of the cat states. We analyze the robustness of these states against the environmental interactions and present methods to control and manipulate the cat states in the photonic implementation of quantum walks.

I. INTRODUCTION

Schrödinger cat states can be defined as quantum superpositions of macroscopically distinct states of a quantum system [1-4]. Due to their macroscopic nature, the cat states play an important role in fundamental tests of quantum theory and precision measurements [5–8]. Numerous attempts are being made to prepare the cat states in various physical systems [9–27].

The macroscopic superposition, which makes the cat states interesting also makes them hard to create in physical systems. This is because of the difficulty in controlling the evolution of macroscopic quantum systems while preserving the coherence in the state. Quantum walks inherently involve the coherent evolution of a macroscopic system.

In a quantum walk process, a quantum walker propagates on a lattice where the propagation is conditioned over its internal states (the coin states) [28, 29]. The quantum walker, unlike its classical counterpart, preserves the coherence during the propagation which results in a faster spread of the walker over the lattice as compared to the classical random walks. Quantum walks have been extensively studied to devise quantum algorithms [30–34] and to simulate various quantum phenomena [35–55].

Here we propose a method to prepare the cat states in a one-dimensional discrete time quantum walk (DTQW) using delocalized initial states of the walker. The quantum walks can be implemented on virtually any quantum system that meets the requirements (a lattice and a coin). Thus, our proposal provides a platform-independent method to create cat states, which enables us to test the fundamental theories on more accessible systems.

In Ref. [56], Cardano et al. implemented a onedimensional quantum walk on the orbital angular momentum (OAM) space of a single photon, following the proposal of Refs. [57, 58]. In this experiment, they demonstrated that the state of the walker, which is delocalized initially, evolves to form a bimodal distribution that resembles a cat state. Their experimental finding, which is consistent with their numerical calculations, motivates the research to find the cause of the formation of cat states and analysis of the stability of these states against the decoherence in quantum walks.

Here we start with a Gaussian (delocalized) initial state and prove that it evolves to form a cat state. We clarify the conditions for the formation of the cat states for the entire range of the parameter θ , which characterizes the bias in the coin flip in the quantum walk. The linearity of the dispersion relation of the low-momentum effective Hamiltonian, which governs the dynamics of the delocalized states, is shown to be the reason for the formation of the cat states in the one-dimensional quantum walks. Furthermore, experimentally viable methods are proposed to demonstrate the coherence in the presence of environmental interactions. Our analysis of the effects of decoherence on the quality of the cat states show that large separations in the cat states are possible even in the presence of noise. Finally, we provide a method to stabilize and manipulate the cat states over the OAM of light.

³Hefei National Laboratory for Physical Sciences at Microscale,

^{*} weiwei.zhang@ucalgary.ca

 $^{^\}dagger$ sandeep.goyal@ucalgary.ca

 $^{^\}ddagger$ gaofei_bupt@hotmail.com

[§] sandersb@ucalgary.ca

[¶] csimo@ucalgary.ca

The structure of the article is as follows: we provide the relevant background regarding the one-dimensional quantum walks in Sec. II. In Sec. III and IV we present our numerical and analytical findings. We discuss the effect of decoherence on the cat states in Sec. V. Method to control and manipulate the cat states are presented in Sec. VI. We conclude in Sec. VII.

II. BACKGROUND

In this section, we present the relevant background of the one-dimensional quantum walks. We describe the regular coined quantum walks on a one-dimensional lattice, its generalization and the Hamiltonian, which governs the dynamics of the quantum walks. We conclude the section with an optical implementation scheme where the walk is performed over the OAM of a light beam.

A. One-dimensional Discrete time quantum walks

In a one-dimensional DTQW the walker propagates on a one-dimensional lattice. The movements of the walker on the lattice are conditioned over the state of a twostate quantum coin. Each step in the walk consists of a coin-flip (C) followed by the conditional propagation (S). If $\{|\uparrow\rangle, |\downarrow\rangle\}$ represents a set of two orthogonal states of the coin then the coin-flip operator C reads [59]

$$C = \left(\cos\theta \left|\uparrow\right\rangle + \sin\theta \left|\downarrow\right\rangle\right) \left\langle\uparrow\right| + \left(\sin\theta \left|\uparrow\right\rangle - \cos\theta \left|\downarrow\right\rangle\right) \left\langle\downarrow\right|,$$
(1)

where the parameter $\theta \in [0, 2\pi)$. The conditional propagator S instructs the walker to move forward $(F = \sum_{x} |x+1\rangle \langle x|)$ or backward (F^{\dagger}) on the lattice conditioned over the states of the coin,

$$S = F \otimes |\uparrow\rangle \langle\uparrow| + F^{\dagger} \otimes |\downarrow\rangle \langle\downarrow|.$$
⁽²⁾

Here x is the index for the lattice sites. Thus, the quantum walk propagator Z reads

$$Z = S(1 \otimes C). \tag{3}$$

Repeated action of the propagator Z gives rise to the quantum walk dynamics.

One-dimensional DTQW has been generalized to simulate various dynamics. One of the most interesting generalizations is where a phase, which is linear in the position, is introduced after every step of the quantum walk [60, 61]. The operator $F_{\rm m}$ which gives the sitedependent phase reads

$$F_{\rm m} = \sum_{x} \exp(i\Phi x) \left| x \right\rangle \left\langle x \right|, \qquad (4)$$

where Φ is an independent parameter. The subscript m in the operator $F_{\rm m}$ is just a reminder that the operator $F_{\rm m}$ is a shift operator in the momentum space. The propagator for the generalized quantum walk reads

$$\bar{Z} = F_{\rm m} Z. \tag{5}$$

This generalized quantum walk demonstrates various interesting properties such as Bloch oscillations and quasi-periodic dynamics [61]. If the strength of the parameter Φ is set to be $\Phi = 2\pi/p$, where p is a positive integer, then the walker recovers its original state after 2p number of steps for odd p and after p number of steps for even p. This feature can be used to restrict the spread of the walker on the lattice.

B. Quantum walk Hamiltonian

The Hamiltonian H that governs the quantum walk dynamics can be calculated by substituting

$$Z = \exp(-iH\delta t),\tag{6}$$

where δt is the duration of a single step in the quantum walk. Here we have taken $\hbar \equiv 1$.

From the definition of the conditional propagator Sin (2) and the operator F, we can assert that the propagator Z and the Hamiltonian H are translation invariant. Thus, the Hamiltonian H can be block diagonalized in the momentum (or Fourier transform) basis $\{|k\rangle\}$

$$H = \bigoplus_{k \in [-\pi,\pi)} H(k).$$
(7)

Here we have considered a lattice of size N with periodic boundary condition, where N is taken to be much larger than the number of quantum walk steps. The variable k represents the (quasi-) momentum that can take discrete values between $-\pi$ and π in the integer multiples of $2\pi/N$.

The Hamiltonian H(k) in the momentum basis can be calculated by expanding the position eigenstates $\{|x\rangle\}$ in the momentum basis $\{|k\rangle\}$ as

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{k} \exp(ikx) |k\rangle.$$
(8)

By substituting Eq. (8) into the definition of the propagator Z and using Eq. (6) we arrive at

$$H(k) = \boldsymbol{h}(k) \cdot \boldsymbol{\sigma}.$$
 (9)

Here $\boldsymbol{\sigma}$ is the vector $(\sigma_x, \sigma_y, \sigma_z)$ of Pauli spin matrices and $\boldsymbol{h}(k) = (h_1(k), h_2(k), h_3(k))$ is a three dimensional real vector, which reads

$$h_1(k) = -R(k)\sin\theta\cos k, \qquad (10)$$

$$h_2(k) = R(k)\sin\theta\sin k, \qquad (11)$$

$$h_3(k) = -R(k)\cos\theta\cos k,\tag{12}$$

$$R(k) = \frac{\cos^{-1}(-\cos\theta\sin k)}{\sqrt{\sin^2\theta\sin^2k + \cos^2k}}.$$
 (13)

Interestingly, for small values of the parameter θ and small k, the Hamiltonian H(k) takes a special form that

resembles a two-component Dirac Hamiltonian (see Appendix A). In this limit the effective Hamiltonian, which we represent by $H_{\rm d}$, reads

$$H_{\rm d}(k) = -\left(k + \frac{\pi}{2}\right)\sigma_z - \theta \frac{\pi}{2}\sigma_x.$$
 (14)

In the Hamiltonian $H_{\rm d}(k)$ the parameter θ characterizes the mass of the particle.

C. Implementing quantum walks in optical system

In this section, we describe an implementation scheme to realize a one-dimensional quantum walk on the OAM of light. This scheme was proposed in [58] and experimentally demonstrated in [56]. The purpose of this section is to familiarize the readers with an implementation scheme for the cat states in the quantum walks. Using this implementation for the one-dimensional quantum walks we will propose a method to manipulate and control the cat states.

In this implementation scheme, the OAM of light serves as the lattice and the polarization is used as the coin. The conditional propagator S (2) is constructed by means of a q-plate which is a device that couples the OAM of light with its spin angular momentum (polarization) [62]. The action of a q-plate on the combined state of the OAM and the polarization is given by

$$|L,\ell\rangle \to |R,\ell-2q\rangle,$$
 (15)

$$|R,\ell\rangle \to |L,\ell+2q\rangle, \tag{16}$$

where $|L\rangle$ and $|R\rangle$ are the left- and right-handed circular polarization of light, and $|\ell\rangle$ is the OAM state that has angular momentum proportional to $\ell\hbar$. The half-integer parameter q characterizes the q-plate.

A half-wave plate with its fast axis parallel to the horizontal axis interchange the left- and right-handed circular polarization. Therefore, a q-plate with q = 1/2 followed by a half-wave plate give rise to the conditional propagator S (2).

The coin-flip operator C (1) can be implemented using the Simon-Mukunda polarization gadget [63]. This gadget is a combination of one half-wave plate and two quarter-wave plates, and can be used to realize an arbitrary SU(2) operation on the polarization of light. Hence, the quantum walk propagator Z can be simulated using a q-plate, a half-wave plate, and a Simon-Mukunda polarization gadget in series. Placing these three components in a loop can realize a one-dimensional quantum walk on the OAM of light.

III. CAT STATES IN QUANTUM WALKS

In this section, we demonstrate the formation of the cat states in the one-dimensional DTQW. We show that the walker in a delocalized (Gaussian) initial state evolves



FIG. 1. The evolution of the walker on a one-dimensional lattice for (a) localized and (b) delocalized initial states. Here, the parameter $\theta = \pi/4$, and the width of the Gaussian for the figure (b) is $\sigma \approx 10$.

to form a cat state. We present methods to analyze the cat nature of the evolved state of the walker.

Quantum walk evolution, typically, results in a bimodal distribution of the walker on the lattice. In Fig. 1, we plot the probability distribution of the walker at time t = 90, 120, 150 steps for a localized and a delocalized initial states. In Fig. 1a, the initial state of the walker is localized at the origin. The state of the walker evolves to a bimodal distribution with a residual probability between the two components of the distribution. The residual probability signifies the overlap between the two components of the distribution. Hence, the evolved state is not a cat state.

In Fig. 1b, we start with a delocalized initial state $|\Psi(0)\rangle_{de}$ of the walker

$$\left|\Psi(0)\right\rangle_{\rm de} = \frac{1}{\mathcal{N}} \sum_{n} \exp\left(-\frac{n^2}{4\sigma^2}\right) \left|n\right\rangle \otimes \left|\chi\right\rangle_c,\qquad(17)$$

which has a Gaussian probability distribution. We find that the delocalized state $|\Psi(0)\rangle_{de}$ evolves to a state $|\Psi(t)\rangle_{de}$ after time t that has the bimodal probability distribution with vanishing residual probability between the two components of the bimodal distribution. Here we have chosen the width σ of the Gaussian to be sufficiently large (about 10 lattice sites). $|\chi\rangle_c$ is a normalized initial state of the coin, and \mathcal{N} is the normalization constant. The two components of the bimodal distribution can represent macroscopically distinct states of the walker. Hence, the evolved state can be seen as a cat state. In the remainder of this section, we analyze the conditions required for the evolved state to be a cat state.

A. Small θ case

We start with a simple case when the parameter θ is small. In this limit, the quantum walk Hamiltonian can be approximated to a two-component Dirac Hamiltonian H_d (14). In this limit, the quantum walk can be used to simulate quantum relativistic effects such as Klein paradox and Zitterbewegung [38, 43]. Thus, this limit can be considered as the relativistic limit of the quantum walk.

The parameter θ in the Dirac Hamiltonian H_d characterizes the mass of the particle. For $\theta = 0$ the Hamiltonian H_d represents a massless particle. If the initial state of the walker in the momentum space is

$$|\Psi(0)\rangle = \sum_{k} |\psi_{k}\rangle \otimes (a|\uparrow\rangle + b|\downarrow\rangle), \qquad (18)$$

then the evolved state, for the case $\theta = 0$, reads

$$\begin{aligned} |\Psi(t)\rangle &= \exp(-iH_{\rm d}t) |\Psi(0)\rangle ,\\ &= \sum_{k} \left(iae^{ikt} |\psi_k\rangle \otimes |\uparrow\rangle - ibe^{-ikt} |\psi_k\rangle \otimes |\downarrow\rangle \right) . \end{aligned}$$
(19)

Here, the two orthogonal spin components of the particle propagate in the opposite directions independent of each other. Due to the linear dispersion relation in the Dirac Hamiltonian, the evolution does not result in the spreading of the wave function of the particle, which results in the formation of cat states.

The same feature, namely, the non-dispersive behaviour of the wave function, persists for non-zero values of θ as long as θ is small. Thus, cat states can be formed in the relativistic limit of the one-dimensional quantum walks.

B. Arbitrary θ case

In the limit when θ is large, the Dirac description of the quantum walk breaks down, therefore, one might not expect to observe the cat states. In Fig. 2, we plot the probability distribution of the walker over the lattice at different times. Here we have considered two different dynamics for the walker, one where we use the exact quantum walk evolution to propagate the walker on the lattice and other where we use Dirac Hamiltonian to propagate the walker. We have chosen $\theta = \pi/2.4$, i.e., a large value of θ . From this figure, we see that the Dirac Hamiltonian and the exact quantum walk dynamics result in strikingly different evolutions. The cat-state-like distribution persists for large θ in the exact quantum walk evolution where Dirac description predicts only dispersed wave function.

In the following, we show that the evolved states achieved for an arbitrary θ and the state $|\Psi(t)\rangle$ (19) achieved in the small θ limit are qualitatively the same. In order to see that, first, we notice that the state $|\Psi(t)\rangle$ in Eq. (19) is highly entangled and the wave-packets corresponding to the orthogonal states of the coin propagate in the opposite directions.



FIG. 2. The comparison between the exact quantum walk evolution (the dashed line) and the evolution using the Dirac Hamiltonian (the solid line) for large values of θ ($\theta = \pi/2.4 = 75^{\circ}$). This figure shows the spread in the width of the Gaussian in the case of the Dirac evolution but almost no spread in the exact quantum walks evolution.

In Fig. 3a we plot the entanglement in the state $|\Psi(t)\rangle_{\rm de}$ between the coin and the walker. The entanglement is calculated by first calculating the reduced density matrix of the coin (or the walker) and then calculating the von-Neumann entropy of the reduce density matrix [64]. In this figure, we can see that the entanglement approaches the maximum value after sufficiently long time. In Fig. 3b we plot the distribution for the states of the walker corresponding to the two orthogonal states of the coin, which are calculated by diagonalizing the reduced density matrix of the coin. Clearly the two wave-packets are moving in the opposite directions. The maximum entanglement along with the purity show that the state $|\Psi(t)\rangle_{\rm de}$ must have the form

$$\left|\Psi(t)\right\rangle_{\rm de} = \frac{1}{\sqrt{2}} \left(\left|X(t)\right\rangle \otimes \left|\phi(t)\right\rangle + \left|X_{\perp}(t)\right\rangle \otimes \left|\phi_{\perp}(t)\right\rangle\right),\tag{20}$$

where the states $|X(t)\rangle$ and $|X_{\perp}(t)\rangle$ represent the two non-overlapping wave-packets and $|\phi(t)\rangle$ and $|\phi_{\perp}(t)\rangle$ are the orthogonal states of the coin.

Another method to verify the coherence in the two wave-packets in the evolved state $|\Psi(t)\rangle_{\rm de}$ is by studying the probability distribution of the walker in the momentum space after projecting over an appropriate state of the coin. This can be done as follows: if the states $|X(t)\rangle$ and $|X_{\perp}(t)\rangle$ are coherent Gaussian states that have the form

$$|G(\pm n_t, \sigma)\rangle = \frac{1}{\mathcal{M}} \sum_{n} \exp\left(-\frac{(n \pm n_t)^2}{4\sigma^2}\right) |n\rangle, \quad (21)$$

with the mean at $\pm n_t$ and the width σ , then the Fourier transform of these states read

$$|G(\pm n_t, \sigma)\rangle \to \frac{1}{\mathcal{M}} \sum_k e^{\mp i n_t k} e^{-\sigma^2 k^2/2} |k\rangle.$$
 (22)



FIG. 3. In this figure we summarize the numerical evidence in favour of the cat states in one dimensional DTQW. Here we have chosen the parameter $\theta = \pi/4$ and the width of the Gaussian $\sigma \approx 10$, unless specified explicitly. In Fig. (a) we plot the entanglement between the coin and the lattice as a function of time for different values of θ . The entanglement is calculated by calculating the von-Neumann entropy of the reduced density matrix of the coin. In Fig. (b) we show the macroscopically distinct states of the walker propagating in the opposite directions. The two macroscopically distinct states correspond to the states $|X\rangle$ and $|X_{\perp}\rangle$ introduced in Eq. (20). Here the solid curves are the Gaussian moving towards the right and the dashed curves are the Gaussian moving towards the left. (c) The probability distribution in the momentum space after projecting the evolved state on a chosen coin state. Here we have chosen the coin states $|\chi\rangle_c = |\chi'\rangle_c = |u_-(0)\rangle + i |u_+(0)\rangle$, where $|u_{\pm}(0)\rangle$ are the eigenvectors of the quantum walk Hamiltonian corresponding to k = 0. The occurrence of the fringes in this distribution signifies the coherence between the two macroscopic states $|X\rangle$ and $|X_{\perp}\rangle$ of the walker.

Thus, the state $|\Psi(t)\rangle_{de}$ in the momentum basis reads

$$\left|\tilde{\Psi}_{t}\right\rangle = \frac{1}{\sqrt{2}\mathcal{M}}\sum_{k}e^{-\sigma^{2}k^{2}/2}\left|k\right\rangle\otimes\left(e^{-in_{t}k}\left|\phi\right\rangle + e^{in_{t}k}\left|\phi_{\perp}\right\rangle\right).$$
(23)

After projecting the state $|\tilde{\Psi}_t\rangle$ on the coin state $|\chi'\rangle_c$, the state of the walker reads

$$|\Psi\rangle = \frac{1}{\sqrt{2}\mathcal{M}} \sum_{k} e^{-\sigma^{2}k^{2}/2} \left(\alpha e^{-in_{t}k} + \beta e^{in_{t}k}\right) |k\rangle, \quad (24)$$

where

$$\alpha = {}_{c}\langle \chi' \,|\, \phi(t) \rangle, \quad \beta = {}_{c}\langle \chi' \,|\, \phi_{\perp}(t) \rangle. \tag{25}$$

Note that, $|\Psi\rangle$ in (24) represents a state of the walker which is a superposition of two Gaussians in the position space centred around $\pm n_t$. Thus, the state $|\Psi\rangle$ itself is a cat state as it contains a coherent superposition of two macroscopically distinct states.

For $\alpha = \beta$, the probability distribution corresponding to $|\Psi\rangle$ in the momentum space will be a product of a Gaussian and $\cos^2 n_t k$. For an appropriate choice of $|\chi'\rangle_c$ one can acquire $\alpha = \beta$. Thus, the presence of the fringes in the momentum space probability distribution signifies the coherence in the two Gaussian probability distributions in the evolved state of the quantum walk. In Fig. 3c we plot the probability distribution for the state $|\Psi\rangle$ in the momentum space. The clear presence of the fringes in the plot ensures that the two Gaussian probability distributions in the evolved state of the walker are coherent, thus, the evolved state is a cat state.

Until now we have considered only those cases when the initial state of the walker is centred around k = 0;



FIG. 4. The plot for the probability distribution of the evolved state for different values of the mean momentum k_0 . Here we have set $\theta = \pi/4$ and the width of the Gaussian $\sigma = 10$.

therefore, the average momentum of the walker is small. What happens when the initial state is a Gaussian but not centred at k = 0? In Fig. 4 we plot the probability distribution for different initial states. Here we consider the initial state of the walker to have a Gaussian probability distribution and the mean value of the momentum to be $0 \le k_0 \le \pi/2$. From Fig. 4 it can be seen that we get perfect cat states only when $k_0 \approx 0$.

In this section, we have shown that the delocalized initial states of a quantum walker evolve to form the cat states. This result is independent of the coin parameter θ . However, the formation of the cat states strongly depends on the mean value of the momentum in the initial state. So far our analysis was based only on numerical results. In the following section, we present the analytic description for the formation of the cat states in quantum walks for the entire range of θ including the large θ regime where Dirac Hamiltonian does not comply.

IV. ANALYTIC APPROACH TO THE CAT STATES IN QUANTUM WALKS

The numerical results, although compelling, do not give us the real physics behind the formation of the cat states in the quantum walks. In this section, we present the reasons behind the formation of the cat states in the quantum walk.

An important result in the previous section is that the cat states are formed due to the delocalized initial states that are centred around zero momentum. It suggests that the low-momentum behaviour of the quantum walks is responsible for the formation of the cat states. Furthermore, from the small θ limit of the quantum walk Hamiltonian, i.e., Dirac Hamiltonian, we can see that the linear dispersion relation and the momentum-independent eigenvectors of the Hamiltonian cause the formation of the cat states.

Interestingly, for small values of the momentum k the Hamiltonian H(k) in Eq. (9) also has linear dispersion even though the Hamiltonian H(k) itself is non-linear in k (see Appendix A for detailed calculations)

$$E_{\pm}(k) = \pm \left(k\cos\theta + \frac{\pi}{2}\right) + O(k^3). \tag{26}$$

In other words, the energy $E_{\pm}(k)$ does not have second order terms in k and for small values of k (say $k < \pi/20$) the k^3 terms can be neglected, hence, giving rise to linear dispersion relation.

Furthermore, the eigenvectors $|u_{\pm}(k)\rangle$ of the Hamiltonian H(k) depend weakly on the momentum k for small values of k (see Appendix A)

$$|\langle u_i(0) | u_j(k) \rangle|^2 = \delta_{ij} + O(k^2).$$
 (27)

Eq. (27) along with the linear dispersion relation is responsible for the formation of the cat states. This can be understood as follows: if we start with a delocalized state $\left|\tilde{\Psi}(0)\right\rangle_{\rm de}$ of the walker

$$\left|\tilde{\Psi}(0)\right\rangle_{\rm de} = \frac{1}{\mathcal{N}'} \sum_{k} \exp\left(-\frac{k^2}{4\delta^2}\right) \left|k\right\rangle \otimes \left|\chi\right\rangle_c,\qquad(28)$$

which has a Gaussian spread in the momentum space, centred around k = 0 and having the width $\delta < \pi/20$, and the coin state $|\chi\rangle_c$, then the evolved state at time t reads

$$\left|\tilde{\Psi}(t)\right\rangle = \frac{1}{\mathcal{N}'} \sum_{k} \exp\left(-\frac{k^2}{4\delta^2}\right) \left|k\right\rangle \otimes \left(e^{-iE_{-}(k)t}a_{-}(k)\left|u_{-}(k)\right\rangle + e^{-iE_{+}(k)t}a_{+}(k)\left|u_{+}(k)\right\rangle\right),\tag{29}$$

where $a_{\pm}(k) = \langle u_{\pm}(k) | \chi \rangle_c$. Now projecting the state $\left| \tilde{\Psi}(t) \right\rangle$ on the coin state $|\chi\rangle_c$ results in state of the walker

$$\begin{split} |\Psi\rangle_{\rm mom} &= \frac{1}{\mathcal{N}'} \sum_{k} \exp\left(-\frac{k^2}{4\delta^2}\right) \left(e^{-iE_{-}(k)t} |a_{-}(k)|^2 + e^{-iE_{+}(k)t} |a_{+}(k)|^2\right) |k\rangle \,. \end{split}$$
(30)

The state $|\Psi\rangle_{\text{mom}}$ in (30) is same as the state $|\Psi\rangle$ in (24) with $\alpha = |a_-|^2$, $\beta = |a_+|^2$ and $\delta = 1/\sigma$, and in the position space $|\Psi\rangle_{\text{mom}}$ represents a state which is in a superposition of two Gaussians centred around $\pm t \cos \theta$. Hence, $|\Psi\rangle_{\text{mom}}$ represents a cat state.

Alternatively, if $|a_{-}(k)|^{2} = |a_{+}(k)|^{2}$ and independent of k then the probability distribution corresponding to the state $|\Psi\rangle_{\text{mom}}$ in the momentum space is a product of a Gaussian and $\cos^{2} E_{-}(k)t$. This means the probability distribution corresponding to the state $|\Psi\rangle_{\text{mom}}$ has fringes exactly like the one in Fig. 3c. In that case the state $|\tilde{\Psi}(t)\rangle_{\text{de}}$ represents a cat state.

For appropriate choices for the state $|\chi\rangle_c$ we can get $|a_-(k)|^2 \approx |a_+(k)|^2$ which, for small values of k, is k-independent. Using Eq. (27) we can construct one such class of state which reads

$$\left|\chi\right\rangle_{c} = \frac{1}{\sqrt{2}} \left(\left|u_{-}(0)\right\rangle + e^{i\varphi} \left|u_{+}(0)\right\rangle\right),\tag{31}$$

where φ is a free parameter. This class satisfies the relation

$$|a_{-}(k)|^{2} \approx |a_{+}(k)|^{2} \approx \frac{1}{2}.$$
 (32)

This completes our proof that the Hamiltonian H(k), and hence the one-dimensional DTQW, gives rise to the cat states.

Let us emphasize that the linear dispersion (26) does not mean that the Hamiltonian is linear. In fact in our case, if we truncate the Hamiltonian H(k) to the first order in k, then we will not get the linear dispersion relation for large values of the parameter θ . The $O(k^2)$ terms in the Hamiltonian H(k) make the dispersion relation linear.

To summarize, we have shown that the formation of the cat states is due to the linear dispersion relation and the weak dependence of the eigenvectors of the quantum walk Hamiltonian on the momentum k. In the following section, we analyze the effect of decoherence on the cat states in quantum walks.

V. EFFECT OF DEPHASING ON THE CAT STATES

The discussion of the cat states is incomplete without considering the effects of the environmental interactions with the quantum system. Cat states are highly susceptible to their surroundings. Therefore, establishing the feasibility of forming a cat states in a quantum system interacting with a bath is important. In this section, we study the effect of pure dephasing type bath interactions on the quality of the cat states. We consider three different scenarios, (i) the bath is acting only on the walker, (ii) the bath is acting only on the coin, and (iii) the bath is acting on both, the walker and the coin.

The action of a pure dephasing type bath on a given density matrix ρ can be defined by the relation [65–67]

$$\rho \to \tilde{\rho} = e^{-\eta t} \rho + (1 - e^{-\eta t}) \operatorname{diag}(\rho) = \hat{V}(\rho).$$
(33)

Here η characterizes the strength of the bath, $\eta = 0$ implies no interaction with the bath. The function diag (ρ) keeps the diagonal elements of the matrix ρ and discard all the off-diagonal elements. Formally, the action of the pure dephasing bath can be represented by the superoperator \hat{V} .

We incorporate the effect of the dephasing in our evolution by applying the superoperator \hat{V} after every step of the quantum walk on either the walker or the coin or on both. In Fig. 5, we plot the spread of the walker over the lattice in the presence of dephasing. Interestingly, we still get the bimodal distribution with an additional residual probability between the two peaks.

Although the evolved state in the presence of dephasing has a similar bimodal distribution as in the case of pure states (without dephasing), the coherence in the two cases can be very different. To quantify the coherence in the evolved state of the walker we can calculate the revival fidelity of the evolved state upon reversing the dynamics using a physical operation [18, 68]. If the state of the walker remains pure in the evolution then the walker can regain its original state by reversing the dynamics. However, if the walker loses the purity in the evolution then the revival is not perfect.

To quantify the coherence, first, we need to devise an operation that can reverse the dynamics of the quantum walk. In our numerical calculations, we find that the Pauli spin operator σ_y acting on the coin state of the walker can be used to reverse the direction of propagation of the walker if the initial state of the walker is delocalized.

Using the σ_y operator we can calculate the revival fidelity as follows: we first evolve the initial delocalized state of the walker for time T in the presence of the bath. At this point, we reverse the dynamics by applying the σ_y operator on the coin. We again evolve the state for time T in the presence of the bath followed by σ_y operation. Now we can calculate the fidelity between the evolved state $\rho(2T)$ and the initial state $|\Psi(0)\rangle_{de}$ as

$$r = {}_{\mathrm{de}} \langle \Psi(0) \,|\, (\mathbb{1} \otimes \sigma_y) \rho(2T) (\mathbb{1} \otimes \sigma_y) \,|\, \Psi(0) \rangle_{\mathrm{de}}.$$
(34)

High values of the revival fidelity r signifies high amount of coherence in the state.

In Fig. 6 we plot the revival fidelity in the quantum walk evolution for various values of θ in the absence of the dephasing. Here we apply the σ_y operation after



FIG. 5. Spread of the walker on the lattice in the presence of dephasing after 250 steps.



FIG. 6. Plot for the revival fidelity between the evolved state and the initial state for different values of θ in the absence of the dephasing. For first n = 97 steps the walk is uninterrupted at which point we apply the σ_y operation. The application of σ_y causes the walker to retrace its footsteps resulting in a rise in the fidelity reaching the maximum at n = 194 steps. Here we have plotted the values of the fidelity only for the even number of steps as the fidelity for the odd number of steps is zero.

n number of steps. Till then the fidelity between the evolved state and the initial state decreases monotonically. After we apply the dynamic-reversing operation, the fidelity start increasing which acquire the maximum value 1 at 2n steps. From this plot it is clear that the system regains its initial state with high fidelity, thus, confirming the high coherence in the state.

In Fig. 7 we plot the revival fidelity as a function of the bath strength η . Here we have chosen T = 250 steps, thus, the total evolution is for 2T = 500 steps. This figure shows that we can achieve a very high revival fidelity for small η ($\eta \approx 0.001$). If we choose T to be smaller then the revival fidelity can be high even for stronger bath interactions. This suggests that the cat states with significant separation between the two components in the bimodal distribution should be possible in the physical implementations of quantum walks.



FIG. 7. Revival fidelity of the quantum walk under the action of different baths

VI. CONTROLLING THE CAT STATES IN OAM IMPLEMENTATION OF QUANTUM WALKS

In this section, we consider the optical implementation of the one-dimensional quantum walk which we introduced in Sec. II C. In this implementation, the quantum walk is performed over the OAM space of light. Here we propose a method to manipulate and control the separation between the two distinct components in the cat state.

The first requirement to realize a cat state in a onedimensional quantum walk is the delocalized (Gaussian) initial state. The Gaussian initial state in the OAM implementation of the quantum walk can be constructed, simply, by using a spatial light modulators [56]. Thus, by using a spatial light modulator and using the scheme presented in Ref. [56, 58] we can form the cat states in the optical quantum walks.

After realizing the cat state, the next step is to control the separation between the macroscopic states of the walker. In Sec. II A we have seen that the application of the momentum shift operator $F_{\rm m}$ in a one-dimensional DTQW causes a periodic revival of the initial state of the walker. The walker regains its initial state after 2pnumber of steps where the number $p = 2\pi/\Phi$ is related to the parameter of the operator $F_{\rm m}$.

We use the same $F_{\rm m}$ to stabilize the cat state in the quantum walks. In order to stabilize the cat state at time t, first, we evolve the initial Gaussian state of the walker for time t using the quantum walk propagator Z (3). The evolved state $|\Psi(t)\rangle$ reads

$$|\Psi(t)\rangle \approx \frac{1}{\sqrt{2}} \left(|G(-n_t, \sigma)\rangle \otimes |u_-\rangle + |G(n_t, \sigma)\rangle \otimes |u_+\rangle \right).$$
(35)

At time t we introduce the momentum shift operator $F_{\rm m}$ in the quantum walk with a certain value of p. Due to the momentum shift operator the state of the walker start oscillating, recovering the state $|\Psi(t)\rangle$ periodically after the time period 2p. Hence, we can preserve the cat state



FIG. 8. Here we plot the revival fidelity of the cat state after the experiencing electric field for $n \times 2p$. Here the width of the delocalized initial state is $\sigma = 9$ and the time of evolution is t = 100 steps.

 $|\Psi(t)\rangle$ for a long time. The only obstacle in preserving the cat states in the decoherence.

Now if we want to increase the separation between the two Gaussian wave-packets of the cat state $|\Psi(t)\rangle$, then we remove the operator $F_{\rm m}$ after a time period which is a multiple of 2p. On the other hand, if we want to decrease the separation between the two Gaussian wave-packets we remove $F_{\rm m}$ after 2np followed immediately by one-time application of σ_y operation. Hence, by introducing the $F_{\rm m}$ and the reversal operation σ_y we can control and manipulate the cat states in the quantum walks.

In Fig. 8 we show the numerically calculated revival fidelity of the cat states. Here we have evolved the delocalized initial state for 100 steps. Then we apply $F_{\rm m}$ for $n \times 2p$ number of steps. We remove the operator $F_{\rm m}$ and apply the quantum walk reversal operation σ_y and evolve the system for 100 steps and calculate the fidelity with the initial state. Here n is an integer between 1 and 100. We can see that for sufficiently large values of p the revival fidelity converges to the value 1.

The action of the operator $F_{\rm m}$ can be implemented in the OAM quantum walk by means of a Dove prism [69]. The action of the dove prism on the OAM states of light can be written as

$$|\ell\rangle \to \exp(i2\varphi\ell) |-\ell\rangle,$$
 (36)

where φ is the angle of rotation of the dove prism along the propagation axis of the light beam. Thus, two dove prisms in a sequence with angles $\varphi/4$ and $-\varphi/4$ can implement the action of the operator $F_{\rm m}$ (4) with $\Phi = \varphi$.

The final component required to achieve the complete control over the cat states in one-dimensional quantum walks is the reversal operation σ_y . In the current scheme, this operation can be achieved by simply using a halfwave plate that has the fast axis parallel to the horizontal axis.

To summarize, we have discussed an optical scheme to manipulate and control the cat state in OAM quantum walks using linear optical devices half-wave plates and dove prisms.

VII. CONCLUSION

In conclusion, we have proposed a method to prepare the cat states in the quantum walk setup using delocalized initial states. Our method is system-independent and works for the entire range of the parameter θ . We have also studied the effects of environmental interactions on the cat states and demonstrated that the large separation in the cat states is possible even in the presence of noise. Finally, we presented a method to control and manipulate the cat states in the optical systems.

The formation of the cat states in one-dimensional DTQW yields an interesting class of low-momentum Hamiltonians that, despite being non-linear in the momentum, possess linear dispersion relation. Both quantum walks and the cat states have been used to describe the coherent energy transfer in the photosynthesis process [35, 36, 40–42, 70]. The current proposal of preparing cat states using quantum walks threads the two concepts

together, which might also contribute to a better understanding of the underlying physics of photosynthesis.

ACKNOWLEDGMENTS

SKG and CS acknowledge the support from NSERC. BCS thanks NSERC, Alberta Innovates, and China's 1000 Talent Plan for financial support. WZ appreciates the financial support from the BUPT Excellent Ph.D. Students Foundation (Grant No. CX201325), the China Scholarship Council (Grant No. 201406470022), and NSERC. FG acknowledges the financial support from NSFC (Grants No. 61272057 and No. 61572081).

Appendix A: Hamiltonian for the one-dimensional discrete time quantum walk

The low-momentum expansion of the Hamiltonian H(k) in (9) can be calculated by using the Taylor series expansion of the Hamiltonian H(k) and discarding the $O(k^3)$ and higher order terms. The truncated 2nd-order Hamiltonians read

$$H^{(2)} = \begin{pmatrix} -\cos\theta \left(k\cos\theta + \frac{\pi}{2} - \frac{1}{4}\pi k^2\sin^2\theta\right) & \begin{pmatrix} -\sin\theta \left(k\cos\theta + \frac{\pi}{2} - \frac{1}{4}\pi k^2\sin^2\theta\right) \\ -ik\sin\theta \left(k\cos\theta + \frac{\pi}{2}\right) & \begin{pmatrix} -\sin\theta \left(k\cos\theta + \frac{\pi}{2} - \frac{1}{4}\pi k^2\sin^2\theta\right) \\ +ik\sin\theta \left(k\cos\theta + \frac{\pi}{2}\right) & \end{pmatrix} & \cos\theta \left(k\cos\theta + \frac{\pi}{2} - \frac{1}{4}\pi k^2\sin^2\theta\right) \end{pmatrix}.$$
 (A1)

The eigenvalues $E_{\pm}(k)$ of the Hamiltonian (A1) read

$$E_{\pm}(k) = \pm \left(k\cos\theta + \frac{\pi}{2}\right) + O(k^3), \qquad (A2)$$

and the corresponding eigenvectors read

$$|u_{-}(k)\rangle = \frac{1}{N_{1}} \begin{pmatrix} \left(-\frac{1}{2}k^{2}\cos\theta + k^{2} - 2ik - 2\right)\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix},$$
(A3)

$$|u_{+}(k)\rangle = \frac{1}{N_{2}} \left(\begin{pmatrix} -\frac{1}{2}k^{2}\cos\theta - k^{2} + 2ik + 2 \end{pmatrix} \sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{pmatrix}.$$
(A4)

Here, N_1 and N_2 are normalization factors which read

$$N_{1} = \sqrt{\sin^{2} \frac{\theta}{2}} + \left| -\frac{k^{2}}{2} \cos \theta + k^{2} - 2ik - 2 \right|^{2} \cos^{2} \frac{\theta}{2},$$
(A5)
$$N_{2} = \sqrt{\cos^{2} \frac{\theta}{2}} + \left| \frac{k^{2}}{2} \cos \theta + k^{2} - 2ik - 2 \right|^{2} \sin^{2} \frac{\theta}{2}.$$
(A6)

With these eigenvectors and eigenvalues we can rewrite the Hamiltonian $H^{(2)}(k)$ as

$$H^{(2)}(k) = E_{+}(k) |u_{+}(k)\rangle \langle u_{+}(k)| + E_{-} |u_{-}(k)\rangle \langle u_{-}(k)|.$$
(A7)

For the small values of the parameter θ and small k, the Hamiltonian H(k) reduces to a simpler form H_d that reads [37, 48]

$$H_{\rm d}(k) = -\left(k + \frac{\pi}{2}\right)\sigma_z - \theta \frac{\pi}{2}\sigma_x.$$
 (A8)

The Hamiltonian H_d is linear in k; hence, it corresponds to a two-component Dirac Hamiltonian. From Eq. (A8) it is clear that the parameter θ characterizes the mass and the velocity of the walker. For small values of θ the walker behaves like a quantum relativistic particle with energy

$$E_d(k) = \pm \sqrt{\left(k + \frac{\pi}{2}\right)^2 + \frac{\pi^2}{4}\theta^2} = \pm \left(k + \frac{\pi}{2}\right) + O(\theta^2).$$
(A9)

The Hamiltonian H_d is valid only for the small values of the parameter θ . For large values of θ (but still small k) the effective quantum walk Hamiltonian takes a slightly more complicated form which is the truncated 1st-order

Hamiltonian $H^{(1)}$ for quantum walks

$$H^{(1)} = \begin{pmatrix} -\cos\theta \left(k\cos\theta + \frac{\pi}{2}\right) & -\sin\theta \left(k\cos\theta + \frac{\pi}{2}\right) - ik\frac{\pi}{2}\sin\theta \\ -\sin\theta \left(k\cos\theta + \frac{\pi}{2}\right) + ik\frac{\pi}{2}\sin\theta & \cos\theta \left(k\cos\theta + \frac{\pi}{2}\right) \end{pmatrix},\tag{A10}$$

The eigenvalues for this Hamiltonian are

$$E_{\pm}^{(1)} = \pm \sqrt{\left(k\cos\theta + \frac{\pi}{2}\right)^2 + \left(k\frac{\pi}{2}\sin\theta\right)^2},\qquad(A11)$$

- [1] E. Schrödinger, Naturwissenschaften **23**, 807 (1935).
- [2] G. J. Milburn, Phys. Rev. A **33**, 674 (1986).
- [3] B. Yurke and D. Stoler, Phys. Rev. Lett. 57, 13 (1986).
- [4] V. Bužek and P. L. Knight, Prog. Opt. 34, 1 (1995).
- [5] B. C. Sanders, Phys. Rev. A 45, 6811 (1992).
- [6] W. J. Munro, K. Nemoto, G. J. Milburn, and S. L. Braunstein, Phys. Rev. A 66, 023819 (2002).
- [7] J. Wenger, M. Hafezi, F. Grosshans, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A 67, 012105 (2003).
- [8] M. Stobińska, H. Jeong, and T. C. Ralph, Phys. Rev. A 75, 052105 (2007).
- [9] C. Monroe, D. M. Meekhof, B. E. King, and D. J. Wineland, Science **272**, 1131 (1996).
- [10] M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J. M. Raimond, and S. Haroche, Phys. Rev. Lett. 77, 4887 (1996).
- [11] J. J. Slosser and G. J. Milburn, Phys. Rev. Lett. 75, 418 (1995).
- [12] H. Jeong, M. S. Kim, T. C. Ralph, and B. S. Ham, Phys. Rev. A 70, 061801 (2004).
- [13] Y. P. Huang and M. G. Moore, Phys. Rev. A 73, 023606 (2006).
- [14] D. D. Bhaktavatsala Rao, N. Bar-Gill, and G. Kurizki, Phys. Rev. Lett. **106**, 010404 (2011).
- [15] G. Csire and B. Apagyi, Phys. Rev. A 85, 033613 (2012).
- [16] C.-W. Lee, J. Lee, H. Nha, and H. Jeong, Phys. Rev. A 85, 063815 (2012).
- [17] B. Wu and J. Zhang, Sci. China Phys. Mech. Astron. 56, 1810 (2013).
- [18] H. W. Lau, Z. Dutton, T. Wang, and C. Simon, Phys. Rev. Lett. **113**, 090401 (2014).
- [19] U. R. Fischer and M.-K. Kang, Phys. Rev. Lett. 115, 260404 (2015).
- [20] T. Wang, H. W. Lau, H. Kaviani, R. Ghobadi, and C. Simon, Phys. Rev. A 92, 012316 (2015).
- [21] J. R. Friedman, V. Patel, W. Chen, S. K. Tolpygo, and J. E. Lukens, Nature **406**, 43 (2000).
- [22] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri1, R. Reichle1, and D. J. Wineland, Nature 438, 639 (2005).
- [23] A. Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier, Nature 448, 784 (2007).
- [24] A. I. Lvovsky, R. Ghobadi, A. Chandra, A. S. Prasad, and C. Simon, Nat. Phys. 9, 541 (2013).

which are, in general, not linear in k. However, one can recover the linear dispersion relation (A9) from (A11) by restricting the parameter θ to small values or introducing $O(k^2)$ terms in the Hamiltonian.

- [25] N. Bruno, A. Martin, P. Sekatski, N. Sangouard, R. T. Thew, and N. Gisin, Nat. Phys. 9, 545 (2013).
- [26] B. Vlastakis, G. Kirchmair, Z. Leghtas, S. E. Nigg, L. Frunzio, S. M. Girvin, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, Science **342**, 607 (2013).
- [27] C. Wang, Y. Y. Gao, P. Reinhold, R. W. Heeres, N. Ofek, K. Chou, C. Axline, M. Reagor, J. Blumoff, K. M. Sliwa, and et al., Science **352**, 1087 (2016).
- [28] S. E. Venegas-Andraca, Quantum Inf. Process. 11, 1015 (2012).
- [29] J. Kempe, Contemp. Phys. 44, 307 (2003).
- [30] A. Ambainis, Int. J. Quantum Inf. **01**, 507518 (2003).
- [31] N. Shenvi, J. Kempe, and K. B. Whaley, Phys. Rev. A 67, 052307 (2003).
- [32] A. M. Childs and J. Goldstone, Phys. Rev. A 70, 022314 (2004).
- [33] A. M. Childs, Phys. Rev. Lett. **102**, 180501 (2009).
- [34] N. B. Lovett, S. Cooper, M. Everitt, M. Trevers, and V. Kendon, Phys. Rev. A 81, 042330 (2010).
- [35] J. Klafter and R. Silbey, Phys. Lett. **125**, 339 (1980).
- [36] I. Barvík and V. Szöcs, Phys. Lett. A **125**, 339 (1987).
- [37] F. W. Strauch, Phys. Rev. A **73**, 054302 (2006).
- [38] F. W. Strauch, J. Math. Phys. 48, 082102 (2007).
- [39] A. J. Bracken, D. Ellinas, and I. Smyrnakis, Phys. Rev. A 75, 022322 (2007).
- [40] G. S. Engel, T. R. Calhoun, E. L. Read, T.-K. Ahn, T. Mančal, Y.-C. Cheng, R. E. Blankenship, and G. R. Fleming, Nature 446, 782 (2007).
- [41] H. Lee, Y.-C. Cheng, and G. R. Fleming, Science 316, 1462 (2007).
- [42] M. Mohseni, P. Rebentrost, S. Lloyd, and A. Aspuru-Guzik, J. Chem. Phys. **129**, 174106 (2008).
- [43] P. Kurzyński, Phys. Lett. A **372**, 6125 (2008).
- [44] A. M. Childs, Commun. Math. Phys. **294**, 581 (2009).
- [45] T. Kitagawa, M. S. Rudner, E. Berg, and E. Demler, Phys. Rev. A 82, 033429 (2010).
- [46] A. Schreiber, K. N. Cassemiro, V. Potoček, A. Gábris, P. J. Mosley, E. Andersson, I. Jex, and C. Silberhorn, Phys. Rev. Lett. **104**, 050502 (2010).
- [47] A. Schreiber, A. Gábris, P. P. Rohde, K. Laiho, M. Štefaňak, V. Potoček, C. Hamilton, I. Jex, and C. Silberhorn, Science **336**, 55 (2012).
- [48] C. M. Chandrashekar, S. Banerjee, and R. Srikanth, Phys. Rev. A 81, 062340 (2010).
- [49] D. W. Berry and A. M. Childs, Q. Info. Comp. 12, 29 (2012).

- [50] T. Kitagawa, Quantum Inf. Process. 11, 1107 (2012).
- [51] T. Kitagawa, M. A. Broome, A. Fedrizzi, M. S. Rudner, E. Berg, I. Kassal, A. Aspuru-Guzik, E. Demler, and A. G. White, Nat. Commun. 3, 882 (2012).
- [52] J. K. Asbóth, Phys. Rev. B 86, 195414 (2012).
- [53] S. Moulieras, M. Lewenstein, and G. Puentes, J. Phys.
 B: At. Mol. Opt. Phys. 46, 104005 (2013).
- [54] H. Obuse, J. K. Asbóth, Y. Nishimura, and N. Kawakami, Phys. Rev. B 92, 045424 (2015).
- [55] J. M. Edge and J. K. Asbóth, Phys. Rev. B 91, 104202 (2015).
- [56] F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, and L. Marrucci, Sci. Adv. 1, 1500087 (2015).
- [57] P. Zhang, B.-H. Liu, R.-F. Liu, H.-R. Li, F.-L. Li, and G.-C. Guo, Phys. Rev. A 81, 052322 (2010).
- [58] S. K. Goyal, F. S. Roux, A. Forbes, and T. Konrad, Phys. Rev. Lett. **110**, 263602 (2013).
- [59] S. K. Goyal, T. Konrad, and L. Diósi, Phys. Lett. A 379, 100 (2015).
- [60] M. Genske, W. Alt, A. Steffen, A. H. Werner, R. F. Werner, D. Meschede, and A. Alberti, Phys. Rev. Lett.

110, 190601 (2013).

- [61] C. Cedzich, T. Rybár, A. H. Werner, A. Alberti, M. Genske, and R. F. Werner, Phys. Rev. Lett. 111, 160601 (2013).
- [62] L. Marrucci, C. Manzo, and D. Paparo, Phys. Rev. Lett. 96, 163905 (2006).
- [63] R. Simon and N. Mukunda, Phys. Lett. A 138, 474 (1989).
- [64] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).
- [65] V. Kendon and B. Tregenna, Phys. Rev. A 67, 042315 (2003).
- [66] V. Kendon, Math. Struct. Comput. Sci. 17, 1169 (2007).
- [67] M. A. Broome, A. Fedrizzi, B. P. Lanyon, I. Kassal, A. Aspuru-Guzik, and A. G. White, Phys. Rev. Lett. 104, 153602 (2010).
- [68] D. A. R. Dalvit, J. Dziarmaga, and W. H. Zurek, Phys. Rev. A 62, 013607 (2000).
- [69] M. J. Padgett and J. P. Lesso, J. Mod. Opt. 46, 175 (1999).
- [70] P. Nalbach, D. Braun, and M. Thorwart, Phys. Rev. E 84, 041926 (2011).

Entropic uncertainty relations for successive generalized measurements

Kyunghyun Baek¹

Gwangil Bae¹

Wonmin Son^{1 2}

¹ Department of Physics, Sogang University, Mapo-gu, Shinsu-dong, Seoul 121-742, Korea
 ² Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, UK

Abstract. We derive entropic uncertainty relations for successive generalized measurements by using general descriptions of quantum measurement within two distinctive operational scenarios. In the first scenario, by merging two successive measurements into one we consider successive measurement scheme as a method to perform an overall composite measurement. In the second scenario, on the other hand, we consider it as a method to measure a pair of jointly measurable observables by marginalizing over the distribution obtained in this scheme. Entropic uncertainty relations derived in both scenarios are examined in specific examples of spin-1/2 systems.

Keywords: Entropic uncertainty relations, Successive measurements, Unsharpness, Disturbance

1 Introduction

Uncertainty principle has been considered as one of the most important concepts in quantum physics, since Heisenberg suggested a trade-off between imprecision of instrument measuring a particle's position and disturbance of its momentum. From the Heisenberg's viewpoint, the uncertainty principle is actively discussed recently with increasing abilities to control quantum systems, and successive measurement(SM) scheme plays key roles in clarifying meanings of imprecision and disturbance of measurements.

In this work, we investigate statistical properties of probability distributions obtained via SM scheme, and derive entropic uncertainty relations(URs) for successive generalized measurements, by generalizing the previous work [1] for the concept of positive-operator-valued measures(POVMs). We refer to [2] for detailed discussions and references of this manuscript.

1.1 Measure of unsharpness

To begin with, let us clarify notations and terminologies as follows. For a finite *d*-dimensional Hilbert space \mathcal{H}_d , we denote the vector space of all linear operators on \mathcal{H}_d by $\mathcal{L}(\mathcal{H}_d)$. Any observable *A* then is described by POVM $\{\hat{A}_i\}$ which is a set of positive operators $\hat{A}_i \in \mathcal{L}(\mathcal{H}_d)$ obeying $\sum_{i=1}^{n_A} \hat{A}_i = \hat{I}$ with the number of elements n_A . In a particular case that all POVM elements are given as projections, *A* is a projection-valued measure (PVM). In this case, A is called a *sharp observable*. On the other hand, if A is not a PVM, it is called an *unsharp observable*.

To characterize the unsharpness, we consider \hat{A}_i in the form of spectral decomposition $\hat{A}_i = \sum_{k=1}^d a_i^k |a_i^k\rangle \langle a_i^k|$, where $0 \leq a_i^k \leq 1$ is an eigenvalue corresponding to an eigenvector $|a_i^k\rangle$. Then the measure of unsharpness is defined as

$$D_{\rho}(A) = \sum_{i=1}^{n_A} \sum_{k=1}^d \langle a_i^k | \hat{\rho} | a_i^k \rangle h(a_i^k) \tag{1}$$

for $\hat{\rho}$ with $h(a_i^k) = -a_i^k \log a_i^k$, which is so-called *device* uncertainty (see [3] for details). This quantity has an important property that a nontrivial lower bound of entropy



Figure 1: Relations among measurement schemes. (a) SM of observables A and B, where the first measurement A gives rise to output state $\mathcal{I}_i^A(\rho)/p_A(i)$ conditioned on its outcome i; (b) Overall measurement of C, (c) Joint measurements of A and B'.

is given by itself such that

$$H_{\rho}(A) \ge D_{\rho}(A) \ge \min_{\rho} D_{\rho}(A) \ge -\log\max_{i} \|\hat{A}_{i}\| \quad (2)$$

due to the concavity of entropy. The minimal device uncertainty can be obtained by diagonalizing $\sum_{i=1}^{n_A} \sum_{k=1}^d h(a_i^k) |a_i^k\rangle \langle a_i^k|$ and taking the lowest eigenvalue, which is stronger than $-\log \max_i ||\hat{A}_i||$ proposed in [4].

1.2 General description of successive measurement

In the present work, by a successive measurement(SM), we mean a scheme where two measurements are performed one after the other successively as the second one is performed immediately on an output state conditionally transformed according to an outcome of the first one. To describe SM, we need the concept of an A-compatible instrument, which is a mapping $\mathcal{I}^A : i \to \mathcal{I}_i^A$ such that each \mathcal{I}_i^A is a completely positive linear map on $\mathcal{L}(\mathcal{H}_d)$ satisfying $\operatorname{tr}[\mathcal{I}_i^A(\hat{\rho})] = \operatorname{tr}[\hat{A}_i\hat{\rho}]$ for all states $\hat{\rho}$. Accordingly, the instrument illustrates that a measurement outcome *i* is obtained with the probability $p_i^A = \operatorname{tr}[\hat{A}_i\hat{\rho}]$ for a state $\hat{\rho}$, and a normalized output state $\mathcal{I}_i^A(\hat{\rho})/p_i^A$ is generated as depicted in Fig. 1-(a).

Now, let us consider the first scenario as depicted in Figure 1-(b) that can be seen as a method to obtain the



Figure 2: Graphs illustrate the lower bounds in Equation (5) for SM of Z and $X(\theta)$ with respect to angle θ and the unsharpness parameters s and t.

overall observable C described by POVM $\{\hat{C}_{ij}\}$ obeying

$$\operatorname{tr}[\hat{C}_{ij}\hat{\rho}] = \operatorname{tr}[\mathcal{I}_i^A(\hat{\rho})\hat{B}_j] = p_{AB}(i,j) \tag{3}$$

for all i, j and all states $\hat{\rho}$. In the Heisenberg picture, equivalently, it can be rewritten as $\hat{C}_{ij} = \mathcal{I}_i^{A*}(\hat{B}_j)$ where \mathcal{I}_i^{A*} denotes the adjoint map of \mathcal{I}_i^A . Namely, the SM of A, B are merged into C having $n_A n_B$ outcomes.

On the other hand, in the second scenario the scheme is considered as a strategy to perform a joint measurement of A and B' as depicted in Fig. 1-(c), where A and B'are described by

$$\hat{A}_{i} = \sum_{j=1}^{n_{B}} \hat{C}_{ij}$$
 and $\hat{B}'_{j} = \sum_{i=1}^{n_{A}} \hat{C}_{ij}$ (4)

for all i, j, respectively.

2 Overall observables obtained via SM

In the first scenario, we can consider performing SM of A and B as a method to implement the overall measurement of C. This fact implies $H_{\rho}(A, B) = H_{\rho}(C)$, since $p_{AB}(i, j) = p_C(i, j)$ for all i, j. Thus, our goal to analyze uncertainty existing in the first scenario can be achieved under consideration of the overall observable C. By using the fact that uncertainty of a measurement does not vanish due to its unsharpness, as described in Eq. (2), we obtain entropic form of UR lower bounded by device uncertainty characterizing unsharpness of C such that

$$H_{\rho}(A,B) \ge D_{\rho}(C) \ge \min_{\rho} D_{\rho}(C) \equiv \mathcal{D}_1.$$
 (5)

Let us take an example of successively measuring two qubit observables Z at first and $X(\theta)$ later in \mathcal{H}_2 described by $\hat{Z}_{\pm} = (\hat{I} \pm s\hat{\sigma}_z)/2$ and $\hat{X}_{\pm}(\theta) = \{\hat{I} \pm t(\sin\theta\hat{\sigma}_x + \cos\theta\hat{\sigma}_z)\}/2$ respectively, where unsharp parameters are denoted by $0 \leq s, t \leq 1$. Additionally, we assume the Lüders instrument for Z, which means the overall observable S is described by $\hat{S}_{\mu\nu} = \sqrt{\hat{Z}_{\mu}}\hat{X}_{\nu}(\theta)\sqrt{\hat{Z}_{\mu}}$ for $\mu, \nu = \pm 1$. In this case, we plot the lower bounds \mathcal{D}_1 and the incompatibility $c = -\log \max_{\mu,\nu} \|\sqrt{\hat{Z}_{\mu}}\sqrt{\hat{X}_{\nu}(\theta)}\|$ versus the angle θ in Fig.2.

3 Joint observables obtained via SM

Both observables A and B' obtained via the second scenario may have their own unsharpness, so that an amount of uncertainties about A and B' may not vanish due to



Figure 3: Graph illustrates device uncertainties D(Z), D(X') and their summation D(Z) + D(X') with respect to the unsharp parameter s.

the unsharpness of them. As formulating this fact, we obtain entropic URs in the form of

$$H_{\rho}(A) + H_{\rho}(B') \ge D_{\rho}(A) + D_{\rho}(B')$$

$$\ge \min_{\alpha} \left[D_{\rho}(A) + D_{\rho}(B') \right] \equiv \mathcal{D}_{2}.$$
(6)

Here, an important point is that the second measurement B may be perturbed to be B' because of disturbance caused by the first measurement A, while A is preserved.

We assume to implement the Lüders instrument for Zand a measurement of X successively in \mathcal{H}_2 described by $\hat{Z}_{\pm} = (\hat{I} \pm s\hat{\sigma}_z)/2$ and $\hat{X}_{\pm} = (\hat{I} \pm \hat{\sigma}_x)/2$ respectively. In this case, the SM is equivalent to measure a pair of jointly measurable observables Z and X', where X' is given as $\hat{X}'_{\pm} = (\hat{I} \pm t\hat{\sigma}_x)^2$ with the unsharp parameter $t = \sqrt{1 - s^2}$. Thus, we cannot avoid unsharpness, and there is the trade-off between the unsharpness of Z and X' such that the more sharpness of Z, the more unsharpness of X'. This behavior can be found in Fig. 3

4 Conclusion

In the present work we have suggested entropic URs for successive generalized measurement within two distinctive scenarios. In both scenarios, it is identified that measuring incompatible observables via SM scheme imposes unavoidable uncertainty, as illustrated in Figs. 2 and 3. Additionally, we note that the entropic UR (6) derived in the second scenario is applicable to any pair of jointly measurable observables, since Heinosaari *et al.* have proved that we can obtain any pair of jointly measurable observables via SM scheme.

References

- K. Baek; T. Farrow; W. Son, Optimized entropic uncertainty for successive projective measurements *Phys. Rev. A*, 89, 032108, 2016.
- [2] K. Baek, W. Son, Unsharpness of generalized measurement and its effects in entropic uncertainty relations. *Sci. Rep.*, 6, 30228, 2016.
- [3] K. Baek, W. Son, Entropic uncertainty relations for successive generalized measurements *Mathematics*, 4, 41, 2016.
- [4] M. Krishna, K.R. Parthasarathy, An entropic uncertainty principle for quantum measurements, *Indian J. Stat. Ser. A*, 64, 842, 2002.

Fault-tolerant quantum computation using a maximum-likelihood decoder with the GKP code states

Kosuke Fukui¹ * Akihisa Tomita¹ † Atsushi Okamoto¹ ‡

¹ Graduate School of Information Science and Technology, Hokkaido University, Kita14-Nishi9, Kita-ku, Sapporo 060-0814, Japan

Abstract. In this paper, utilizing continuous variable nature of the GKP code states effectively, we propose a decoder using maximum-likelihood for concatenated Calderbank-Shor-Steane codes. In particular, we perform numerical simulation with the C4/C6 code proposed by Knill. A numerical calculations for a decoding of C4/C6 confirmed the effectiveness of our method in terms of error-tolerance and the threshold for concatenation.

Keywords: GKP code states, continuous variables, maximum-likelihood decoder

1 Introduction

Quantum computers have a great deal of potential, but to realize that potential, they need some sort of protection from noise to construct a large scale quantum computation. Optical continuous variable states are promising candidates for building blocks to implement scalable quantum computation and communication [1,2]. However, the finite squeezing limits the scale of the quantum computation by inducing noise, which destroys the quantum information even with the perfect experimental apparatus[3]. Nevertheless, it has been shown that an infinite length fault-tolerant quantum computation is possible using qubit encoding of an oscillator introduced by Gottesman, Kitaev, and Preskill (so called the GKP code states) in 2014 [4]. In this paper, we propose a maximum-likelihood scheme for concatenated Calderbank-Shor-Steane (CSS) codes with the GKP code states. In particular, we perform numerical simulation with the C_4/C_6 code proposed by Knill [5].

2 Likelihood for the GKP code states

We start by explaining the GKP code states where the qubit is protected against small shifts in phase space [6]. GKP proposed to use states whose q quadrature wave function is composed of a series of Gaussian peaks of width Δ contained in a larger Gaussian envelope of width $1/\Delta$. The approximated logical states $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ are given by

$$\begin{aligned} |\widetilde{0}\rangle &\propto \sum_{t=-\infty}^{\infty} \int e^{-2\pi\Delta^2 t^2} e^{-(q-2t\sqrt{\pi})^2/(2\Delta^2)} |q\rangle \, dq \\ |\widetilde{1}\rangle &\propto \sum_{t=-\infty}^{\infty} \int e^{-\pi\Delta^2 (2t+1)^2/2} e^{-(q-(2t+1)\sqrt{\pi})^2/(2\Delta^2)} |q\rangle \, dq \end{aligned}$$
(1)

The bit values 0 and 1 of the GKP code states can be determined by measurement of the variable q. Although in case of $\Delta \rightarrow 0$ (infinite squeezing) the state becomes

the perfect code states, the approximate states are not orthogonal, and there are some probability of misidentify a 0 state $|\widetilde{0}\rangle$ as a 1 state $|\widetilde{1}\rangle$ and vise versa. Measurement on the approximated states $|\widetilde{0}\rangle$ ($|\widetilde{1}\rangle$) yields an outcome q_m around the nearest bit value $q_k = (2t + k)$ (t = 0, $\pm 1, \pm 2, \dots, k = 0, 1$). In practice, because we don't know the true state, we need to guess the true bit value is k from the measurement result q_m . We define the measurement shift by $\Delta q_m = |q_m - q_k|$ for the logical state $|\widetilde{k}\rangle$. If Δq_m is less than $\sqrt{\pi}/2$, the true shift $\overline{\Delta}$ is equal to Δq_m . On the other hand, if Δq_m is between $\sqrt{\pi}/2$ and $\sqrt{\pi}$, the true shift $\overline{\Delta}$ is equal to $-\Delta q_m$. We notice that Δ obeys the following Gaussian probability distribution $f(\overline{\Delta})$ with the average 0 and the variance Δ^2 ,

$$f(\overline{\Delta}) = \frac{1}{\sqrt{2\pi\Delta^2}} e^{-\overline{\Delta}^2/(2\Delta^2)}$$
(2)

In our method we regard the function $f(\overline{\Delta})$ as a likelihood function and combine the discrete variables k, which refer to the degree of freedom for the logical level, with the continuous variables $\overline{\Delta}$, the degree of freedom for the physical level to improve our guess on k.

3 Maximum-likelihood decoder

To give the idea of our maximum-likelihood method, we briefly describe our method by three-qubit bit flip error code. The three-qubit code encodes a single logical qubit into three physical qubits to correct a single bit flip error. Suppose the three physical qubits are labeled by 1, 2, and 3. The two logical states $|0\rangle$ L and $|1\rangle$ L are defined as $|0\rangle$ L = $|000\rangle$ 123 and $|1\rangle$ L= $|111\rangle$ 123, so that an arbitrary single qubit state $|\Psi\rangle = \alpha |0\rangle + \beta |0\rangle$ is mapped to $\alpha |0\rangle L + \beta |0\rangle L = \alpha |000\rangle 123 + \beta |0\rangle 123 = |\Psi\rangle L$. In a conventional manner, the three-qubit code will correct a state such as $|100\rangle_{123}$ ($|011\rangle_{123}$) to $|000\rangle_{123}$ ($|111\rangle_{123}$) by a majority voting. In our maximum-likelihood manner, we compare two maximum-likelihood functions which are corresponding to the case with a single error and double errors. If the error syndrome shows that the first qubit is 0 (or1) and other two qubits are 11(or 00), we compare the function $F_1 = f(\Delta_{m1}) \times f(-\Delta_{m2}) \times f(-\Delta_{m3})$ with $F_2 = f(-\Delta_{m1}) \times f(\Delta_{m2}) \times f(\Delta_{m3})$, where the Δ_{mi} is

^{*}fukui.opt@gmail.com

[†]tomita@ist.hokudai.ac.jp

[‡]ao@optnet.ist.hokudai.ac.jp



Figure 1: Error-correcting teleportation with the maximum-likelihood decoding for C_4/C_6 code.

the measurement shift of *i*-th qubit. Because the function $F_1(F_2)$ is a likelihood, in the case of $F_1 > F_2$, we decide that a single error occurs on the first qubit. In the case of $F_1 < F_2$, we decide that two error occur on the second and third qubits. In our method the three-qubit code can correct two errors, whereas in the conventional method the code corrects only a single error.

We apply the likelihood function to our maximumlikelihood method for concatenated CSS codes and confirm the validity of our method by a numerical calculation for the specific case of C_4/C_6 code based on teleportation. As in the figure.1, which shows the decoder of the C4/C6 code, the encoded data qubit $|\Psi\rangle$ in is teleported to the fresh encoded qubit of the ancilla Bell state $|\Psi\rangle_{\rm out}$ using maximum-likelihood decoding (MLD). The outcome of the encoded Bell measurement, b_x and b_z , provides the syndrome information and error-detecting or error-correcting operation is performed by teleportation. The C4/C6 code is composed of a concatenation of two codes, C4 and C6. At level-1, a qubit pair is encoded into four physical qubits, which refers to C4. At more than level-1, a level-l qubit pair is encoded into three level-(l-1) qubit pairs $(l=2,3,4,\cdots)$. To evaluate the performance of the proposed decoder, we examined the error-tolerance for a Gaussian channel which leads to errors of displacements in the q and p quadrature, which is dipicted as GC in figure.1. By considering the displacement which follows Gaussian distribution, we evaluate the influence as the decreasing of the squeezing level of the encoded data qubit. In this simulation, we assumed that errors occur only on the channel and the other operations (encoding, Bell-state preparation, decoding, and Bell measurement) are performed without any errors. In figure. 2, the error probabilities are plotted as a function of the squeezing level of the encoded data qubit for the levels l = 1,2,3 after the channel for 11 dB of the encoded Bell pair's squeezing level. In figure.2, for example, the error probability is improved from about 0.25 to 0.05 at squeezing level of 6.7 dB for level-3, by use of our maximum-likelihood method. Moreover, the threshold for concatenation of C_4/C_6 by use of the proposal are improved by a little less than 1 dB. The simulation results show our method improves the error rate and the thresholds effectively.

4 Conclusion

Towards efficient fault-tolerant quantum computation with the GKP code states, we introduced a maximumlikelihood method for concatenated Calderbank-Shor-Steane codes and applied for the C4/C6 code proposed by Knill. In our method, we use a hybrid quantum informa-



Figure 2: The error probabilities of the decoding with (a) Knill's conventional method, and (b) our maximum-likelihood method for the levels l = 1,2,3.

tion processing, where discrete degree of freedom of a bit value are combined with continuous degree of freedom of a shift value for enhancing noise resistance. A numerical calculations for a decoding of C4/C6 confirmed the effectiveness of our method in terms of error-tolerance and the threshold for concatenation. Moreover, the method will reduce resources required for fault-tolerant quantum computation. The enhanced power results from the continuous variable nature of the oscillators combined with discretization on decoding.

Acknowledgement : This work was partly supported by ImPACT "Advanced Information Society Infrastructure Linking Quantum Artificial Brains in Quantum Network".

References

- M. Pysher, Y. Miwa, R. Shahrokhshahi, R. Bloomer and O. Pfister, In *Phys. Rev. Lett.* 107, 030505, 2011.
- [2] M. Chen, N. C. Menicucci and O. Pfister, *Phys. Rev. Lett.*, 112, 120505, 2014 McGraw-Hill, 1999.
- [3] M. Ohliger, K. Kieling and J. Eisert, *Phys. Rev. A* 82, 042336, 2010.
- [4] N. C. Menicucci, Phys. Rev. Lett., 112, 120504, 2014.
- [5] E, Knill, Nature, 434, 39-44, 2005.
- [6] D. Gottesman, A. Kitaev and J. Preskill, *Phys. Rev.* A, 64, 012310, 2001.

Generation and Characterization of Quantum Cluster States using Surface Acoustic Waves

MG Majumdar, CHW Barnes (Dated: April 15, 2016)

Abstract. Cluster State Generation and Use

Keywords. Cluster State, GHZ States, Entanglement Monogamy

We describe a method of generation of four-qubit and six-qubit cluster states using electrons in Quantum One-Dimensional Channels (Q1DC), driven by Surface Acoustic Waves (SAWs).

Section 1 is on the generation of the cluster state using electrons in quantum one-dimensional channels, driven by Surface Acoustic Waves. Section 2 is on measures for characterization of N-particle entanglement. Section 3 is on the results and discussion of the entanglement generation and characterization.

I. INTRODUCTION

One-way quantum computation, also known as Cluster State Quantum Computation, provides a robust and efficient tool to perform universal quantum computation using only single-qubit projective measurements, given a highly entangled cluster state. The cluster-state approach to quantum computation also leads to certain practical advantages such as robustness against errors.

The cluster state is generated on a basis defined by electrons in Quantum One-Dimensional Channels (Q1DCs), driven by Surface Acoustic Waves [1]. The setup for the generation consists of Copper interdigitated transducers on a Silicon substrate with layers of Silicon Dioxide and Zinc Oxide, to reinforce the piezoelectric effect on the substrate. The transducers are placed on either sides of a centrally-placed etched region with an Electron Gas. When a high frequency AC signal is applied, Surface Acoustic Waves are generated, by the principle of piezoelectricity. As the SAW propagates through the etched region, the travelling potential it creates carries the electrons from the electron gas with it.

A typical SAW frequency of 3 GHz and an applied power of 10 dBm produces a measurable current in the nano-ampere range, as shown by *Barnes, et al* [1]. One-qubit rotations and controlled two-qubit gates can be implemented on this system. The primary gate in our generation-protocol is the Root of Swap gate.

Interchannel and intra-channel, two-instance swap

operations form the primary building blocks of the given generation-protocol. Owen et al [2] demonstrated how two particles that are interacting in a harmonic potential generate maximally entangled states, which are created simply through the quantum dynamics of the system and possessing a high entanglement delity (F > 0.98). The underlying operation is essentially a root-of-SWAP operation. Bayer et al [3] demonstrated coupling and entanglement of quantum states in a pair of vertically aligned quantum dots by studying the emission of an interacting exciton in a single dot molecule as a function of the separation between the dots. The electron-hole complex was shown to be equivalent to entangled states of two interacting spins.

II. SURFACE ACOUSTIC WAVES

Surface-acoustic waves (SAWs) are sound waves that travel parallel to the surface of an elastic material. The displacement amplitude decays into the material and therefore these waves are confined to within roughly a wavelength of the surface. In a piezoelectric material, mechanical deformations associated with the SAW produce electric fields.

For non-piezoelectric materials, Hooke's law states that the mechanical stress field experienced by a body is proportional to the strain field:

$\sigma_{ij} = c_{ijkl} \epsilon_{kl}$

where σ_{ij} and ϵ_{kl} are components of the stress and strain fields respectively, and c_{ijkl} is a component of the 4th rank 'elastic' tensor. The electric displacement for nonpiezoelectric materials is proportional to components of the electric field, with components of the permittivity tensor being the proportionality constants.

For piezeolectric materials, the electric displacement depends on the applied electric field and mechanical strain, and the stresses depend on both the applied mechanical strain and the electric field.

$$D_i = \epsilon_{ij}^S + e_{ijk}\epsilon_{jk}$$

$$\sigma_{ij} = -e_{kij}E_k + c_{ijkl}^E\epsilon_{kl}$$

Here superscripts S and E denote that the quantities are measured under constant strain and electric field

respectively.

A SAW can be generated by applying an oscillating signal to a suitably designed set of interdigitated transducer based surface gates on a piezoelectric substrate. Small localized displacements of the uid will propagate as an acoustic wave, also known as a compressional wave. When a SAW passes beneath a SAW transducer of the appropriate pitch, an alternating potential is generated across the transducer.

III. THE SETUP

In our setup, by bringing the channels close to each other, we allow for Coulombic interaction to take place between the electrons travelling in the channels. As seen, with a high fidelity, this generates an entangled state using the 'Root-of-Swap' operation. One can also use a magnetic field, oriented in a certain direction to implement single qubit rotations, which constitute an essential part of the Universal Quantum Gates set.



Figure 1: Setup, comprising of Quantum One-Dimensional Channels with electrons driven by Surface Acoustic Waves (SAWs)

IV. CHARACTERIZATION OF ENTANGLEMENT

We wish to characterize the entanglement in multipartite qubit states. A pure n-qubit state is called unentangled if its wave function may be written as an n-fold tensor product of individual qubits. A state is globally entangled if it cannot be written as a tensor product of any set of subsystems.

There are several ways of quantifying entanglement. Measures of entanglement can be been used that are constant on locally equivalent states. These must be entanglement monotones i.e. they must be non-increasing under Local Operations and Classical Communication (LOCC). One can also have observables whose expectation values are positive (negative) on unentangled states and negative (positive) on entangled states.

Partial Density Matrices

The density operator ρ for the ensemble or mixture of states $|\psi_i\rangle$ with probabilities p_i is given by

$$\rho = \sum_{i} p_i |\psi_i\rangle \langle \psi_i |$$

The reduced density operator describes the properties of measurements of a sub-system A, when the other subsystem(s) is(are) left unobserved, by tracing them out.

Peres [4] showed that a necessary condition for seperability in a system is that a matrix obtained using partial transposition of the density matrix of the system has only non-negative eigenvalues.

Concurrence

As defined by *Carvalho et al* [5], for an N-partite quantum system, one can define $2^N - 2$ reduced density matrices and an associated concurrence measure:

$$C_N = 2^{1-\frac{N}{2}} \sqrt{(2^N - 2)(\langle \psi | \psi \rangle)^2 - \sum_{\alpha} Tr \rho_{\alpha}^2}$$

where α labels all the reduced density matrices.

V. RESULTS AND DISCUSSION



Figure 2: Gate Combination with interchannel and intrachannel Root-of-Swap Operations

For this setup, we consider the various input states and the concurrence measures for the entanglement generated by the setup in the process.

Case 1: Input comprises of $|00\rangle$ and $|00\rangle$

 $C_4 = 0$

Case 2: Input comprises of $|11\rangle$ and $|11\rangle$

$$C_4 = 0$$

Both these cases are expected to have vanishing entanglement concurrence-measures, as the Root-of-Swap operation leaves the $|11\rangle/|00\rangle$ combinations unaltered. In this case, a seperable input composite state is unaffected by the *setup-entanglers*.

Case 3:

Input comprises of $ 00\rangle$ and $ 01\rangle$
Input comprises of $ 00\rangle$ and $ 10\rangle$
Input comprises of $ 01\rangle$ and $ 00\rangle$
Input comprises of $ 10\rangle$ and $ 00\rangle$
Input comprises of $ 11\rangle$ and $ 10\rangle$
Input comprises of $ 11\rangle$ and $ 01\rangle$
Input comprises of $ 10\rangle$ and $ 11\rangle$
Input comprises of $ 01\rangle$ and $ 11\rangle$

 $C_4 = 1.479$

In these cases, there is one flipped spin, with respect to the remaining qubit subsystem. As a result, the entanglement capacity for each of these systems is equal.

Case 4:

Input comprises of $|00\rangle$ and $|11\rangle$ Input comprises of $|11\rangle$ and $|00\rangle$

 $C_4 = 1.458$

The first inter-channel entangling Root-of-Swap operation has no effect on the input state since they are $|11\rangle/|00\rangle$ combinations. However, the subsequent intra-channel entanglers give rise to entanglement in the state.

Case 5:

Input comprises of $|01\rangle$ and $|01\rangle$ Input comprises of $|10\rangle$ and $|10\rangle$

$$C_4 = 1.620$$

This is the case when both interchannel and intrachannel entanglers contribute to the generation of entanglement.

Case 6:

Input comprises of $|01\rangle$ and $|10\rangle$ Input comprises of $|10\rangle$ and $|01\rangle$

$C_4 = 1.225$

This is an interesting case wherein the entanglers contribute to the generation of entanglement, much like in Case 5. However, the concurrence measure is much lower in this case.



Figure 3: Concurrence Plot

We hypothize that the dip in the plot (*Case 6*) is because of the concept of *Entanglement Monogamy*. Once the entanglement is generated by the interchannel entanglers, the intrachannel entanglers entangle the states further, though this essentially reduces entanglement between subsystems and we obtain a cluster state.



Figure 4: Polar Plot of Concurrence Measures



Figure 5: Gate Combination with intrachannel and interchannel Root-of-Swap Operations

In this case, we have vanishing concurrence (implying seperability) for input comprising of $|00\rangle|00\rangle$ and $|11\rangle|11\rangle$, as in the previous setup.

This is due to the entanglers not generating entanglement for this particular input state, given a Root-of-Swap based generator setup, irrespective of the order of the entanglers: first intra- and then inter-channel entanglers, or first inter- and then intra-channel entanglers.

For the case with one spin flipped, with respect to other qubits in the system, we have the same result as for the previous setup. The concurrence remains The concurrence measure and the amount at 1.479. of entanglement remains unchanged due to the fact that after the first entangler operation in both circuits. entanglement is generated only in a single two-qubit subsystem while the remaining two-qubit subsystem remains in a composite state. This step remains unchanged due to the symmetry of this particular kind of four-qubit input state. Eventually, the second entangler generates entanglement in the entire system by generating quantum correlations between one part of the entangled two-qubit subsystem and one half of the composite subsystem of qubits.



Figure 6: Polar Plot of Concurrence Measures

The concurrence for the $|00\rangle|11\rangle/|11\rangle|00\rangle$ and the $|01\rangle|01\rangle/|10\rangle|10\rangle$ states are interchanged, with respect to the case for the inter-intrachannel combination. The former has a concurrence of 1.620 while the latter has a concurrence of 1.458. This is because the switch in the entangler combination and sequence is countered by the rearrangement of input qubits for the respective matching concurrence measures in the two setup-cases. For the $|01\rangle|10\rangle/|10\rangle|01\rangle$, the concurrence remains at 1.225.



Figure 7: Special Gate Combination ('Cross-Arm Mobius')

In this case, for same-spin qubit input, concurrence vanishes, while for the case with one spin flipped, with respect to other qubits in the system, we have a higher concurrence than the previous case. The value of concurrence for this input combination and the setup (Figure 7) is 1.571.

The concurrence for the $|00\rangle|11\rangle/|11\rangle|00\rangle$ and the $|01\rangle|01\rangle/|10\rangle|10\rangle$ states are higher or equal to the previous setup-cases. The former has a concurrence of 1.894 while the latter has a concurrence of 1.620.

For the $|01\rangle|10\rangle/|10\rangle|01\rangle$, the concurrence value is 1.785. The possible cause for higher concurrence for all input combinations is viewed in the entanglement within the various subsystem partitions. Previously, there was a trade-off between the contribution of an entangled partition-class and the seperability of remaining subsystem partition-classes. In this setup, the entanglement is present across the various partitions and subsystems. Thus this setup, named as the 'Cross-Arm Mobius', is a good generator of entanglement in SAW-driven electrons.



Figure 8: Density Matrix for $|0110\rangle$ case and inter-intrachannel setup)

VI. CONCLUSION

We have developed a scheme for the generation of entanglement and cluster states on a basis defined by electrons in Quantum One Dimensional Channels (Q1DCs), driven by Surface Acoustic Waves (SAWs).

VII. ACKNOWLEDGEMENTS

We would like to thank the Nehru Trust for Cambridge University (NTCU), Trinity College - Cambridge, the Hitachi Cambridge Laboratory and the Thin Film
5

Magnetism group of Cavendish Laboratory, University of Cambridge for their support in the pursuit of this project.

VIII. REFERENCES

[1] Barnes, C. H. W., J. M. Shilton, and A. M. Robinson. "Quantum computation using electrons trapped by surface acoustic waves." Physical Review B 62.12 (2000): 8410.

[2] Owen, E. T., M. C. Dean, and C. H. W. Barnes. "Generation of entanglement between qubits in a onedimensional harmonic oscillator." Physical Review A 85.2 (2012): 022319.

[3] Bayer, M., et al. "Coupling and entangling of quantum states in quantum dot molecules." Science 291.5503 (2001): 451-453.

[4] Peres, Asher. "Separability criterion for density matrices." Physical Review Letters 77.8 (1996): 1413.

[5] Carvalho, Andr RR, Florian Mintert, and Andreas Buchleitner. "Decoherence and multipartite

entanglement." Physical review letters 93.23 (2004): 230501.

[6] Rungta, Pranaw, et al. "Universal state inversion and concurrence in arbitrary dimensions." Physical Review A 64.4 (2001): 042315.

[7] Hill, Scott, and William K. Wootters. "Entanglement of a pair of quantum bits." Physical review letters 78.26 (1997): 5022.

[8] Bennett, Charles H., et al. "Mixed-state entanglement and quantum error correction." Physical Review A 54.5 (1996): 3824.

[9] Horodecki, Micha, Pawe Horodecki, and Ryszard Horodecki. "Limits for entanglement measures." Physical Review Letters 84.9 (2000): 2014.

[10] Wong, Alexander, and Nelson Christensen. "Potential multiparticle entanglement measure." Physical Review A 63.4 (2001): 044301.

Generation and evaluation of entanglement using multiple single photon sources and linear optics

Jun-Yi Wu¹ Holger F. Hofmann¹

¹ Graduate School of Advanced Sciences of Matter, Hiroshima University, Japan

Abstract. We study the experimentally accessible properties of multi-photon entanglement generated by single photon sources and beam splitters. As the photon number increases, it is possible to observe a rich variety of structures in the photon distributions obtained after linear optics transformations. In this presentation, we focus on the patterns obtained from the unbiased interference of all modes that is described by a discrete Fourier transformation of the light field amplitudes and show how the entanglement can be characterized using the correlations of photon statistics observed in the two multi-mode outputs.

Keywords: Multi-photon entanglement, entanglement generation, entanglement evaluation

1 Introduction

Nowadays, the development of reliable single photon sources opens up new possibilities of quantum information processing using an increasing number of single photon inputs. It is well-known that splitting a single photon into two output modes by a beam splitter can generate a Bell state with entanglement between the modes (singlerail encoded entanglement). Although the single-rail encoded entanglement of single photon Bell states can be accessed by linear optics and photon detection with extra ancillary photons [1, 2, 3], we restrict ourself on the Fock spaces of the entangled states themselves without any ancilla. Under this constraint, the single-rail encoded entanglement of two modes is not more accessible. By scaling up the single photon entanglement between a pair of modes to multi-photon entanglement between pairs of multiple modes, more possible local unitaries are implementable by linear optics and photon number detection, such that the multi-photon entanglement is then accessible without ancillas. An entanglement criterion for a specific type of multi-photon entangled states which can be implemented by discrete Fourier transformations and photon number detection without ancillas will be derived.

2 Generation and evaluation of multiphoton entanglement

To tackle the limits on the unitary transformations in the Fock space of a single mode, we scale the system up to multiple single photon sources. As it is shown in Fig. 1, M photons in M input modes are split by M beam splitters and redistributed into two separate output ports A and B. In this manner, one obtains a state represented by a coherent superposition of all possible photon number states satisfying the condition that here is only one photon in each mode m, and this photon is found either in port A or in port B, i.e.

$$|\psi_M\rangle = \sum_{n_m \le 1} |\boldsymbol{n}\rangle_A \, |\bar{\boldsymbol{n}}\rangle_B \,, \tag{1}$$

Since we only consider linear optics and photon detection, the local measurements will not be sensitive to quantum coherence between different total photon numbers.



Figure 1: Entanglement generation from M single photons. The modes are indexed by 0, ..., M - 1.

Therefore, we should consider the different partitions of photon number between A and B separately, assigning a different entangled state to each. Post-selecting the output states $|\psi_M\rangle$ with fixed photon number partitions $(1_A: M - 1_B), ..., (M - 1_A: 1_B)$ between A and B, one can obtain (M - 1) entangled states $|\phi_{N,M-N}\rangle$ which are the binomially distributed components of the coherent superposition of the total output state given by Eq. (1), i.e.

$$|\psi_M\rangle = \frac{1}{2^{M/2}} \sum_{N=0}^{M} \sqrt{\binom{M}{N}} |\phi_{N,M-N}\rangle$$
(2)

with

$$|\phi_{N,M-N}\rangle = \frac{1}{\sqrt{\binom{M}{N}}} \sum_{n_m \le 1, |\boldsymbol{n}| = N} |\boldsymbol{n}\rangle |\bar{\boldsymbol{n}}\rangle.$$
 (3)

Here the sum in Eq. (3) runs over all patterns of N photons that have zero or one photon in each mode and the bar over the photon number distribution in B indicates the complementary correlation $\mathbf{n}^{(A)} + \mathbf{n}^{(B)} = (1, ..., 1)$. Increasing total photon number M, one can generate an increasing number of entangled states $|\phi_{N,M-N}\rangle$, all of which have their own entanglement structures.

To access this multi-photon entanglement by photon detection, one needs to implement certain local unitaries U_A and U_B to transform the photon number state basis \mathcal{E} to another basis system \mathcal{K} on the subsystems A

and B, such that one can perform measurements sensitive to the quantum coherences between the complementarily correlated Fock states (Fig. 1). The best unitary transformation for entanglement evaluation would be the one that maps the photon number state basis \mathcal{E} into its MUB. However, due to the large number of possible photon distributions compared to the much lower number of modes, such a unitary cannot be implemented via linear optics transformations of modes at photon numbers greater than one. Instead of the perfect MUBsmapping in the whole post-selected Fock space, the next best choice is the discrete Fourier transformation (DFT) U_F , which transforms a single optical input mode into a mutually unbiased superposition of all M output modes, i.e.

$$b_{k}^{\dagger} = \hat{U}_{F} a_{k}^{\dagger} \hat{U}_{F}^{\dagger} = \sum_{m=0}^{M-1} \frac{1}{\sqrt{M}} e^{i\frac{2\pi}{M}km} a_{m}^{\dagger}.$$
 (4)

In general, the combinations of creation operators in the multi-photon statistics results in a non-trivial bias in the statistics of the multi-photon output distributions. However, we can identify specific translational patterns \boldsymbol{p} , such that the DFT transforms each input pattern into a superposition of mutually unbiased output patterns related to each other by cyclic mode shifts \hat{S} . The pattern class $\mathcal{E}_{\boldsymbol{p}}$ of \boldsymbol{p} are generated from the cyclic mode shifts \hat{S} from the origin photon number state \boldsymbol{p} , i.e.

$$\mathcal{E}_{\boldsymbol{p}} = \{ \hat{S}^m \, | \boldsymbol{p} \rangle \}_{m=0,\dots,M-1}. \tag{5}$$

The MUB $\mathcal{K}_{p} = \{|k_{p}\rangle\}_{k}$ of the translational pattern class \mathcal{E}_{p} is then given by

$$|k_{\boldsymbol{p}}\rangle := \frac{1}{\sqrt{d_{\boldsymbol{p}}}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}km} \hat{S}^m |\boldsymbol{p}\rangle.$$
(6)

where $d_{\mathbf{p}}$ is the cardinality of the **p**-pattern class $\mathcal{E}_{\mathbf{p}}$. In the $\mathcal{K}_{\mathbf{p}}$ basis the the state $|\phi_{N,M-N}\rangle$ is correlated by $(k^{(A)}, -k^{(B)})$, i.e.

$$|\phi_{N,M-N}\rangle = \frac{1}{\sqrt{\binom{M}{N}}} \sum_{\boldsymbol{p},k} |k_{\boldsymbol{p}}\rangle |-k_{\bar{\boldsymbol{p}}}\rangle.$$
(7)

The k-values of $|k_p\rangle$ states can be displaced by DFTs in the output patterns n of photon number detections. We call this property the K-readout rule of DFTs, which says

$$\langle \boldsymbol{n} | U_F | k_{\boldsymbol{p}} \rangle = 0, \text{ for all } K(\boldsymbol{n}) \neq k$$
 (8)

with

$$K(\boldsymbol{n}) = \sum_{m=0,\dots,M-1} n_m m \pmod{M} \tag{9}$$

being the *M*-modulus total mode index of the photon number state $|n\rangle$, which we call the displacement of the output pattern n. The *K*-readout rule implies that the correlations of *k*-values of in the k_p -basis will be displaced in the correlations of *K*-values in the photon number detection after local DFTs. According to Eq. (7), the output patterns of photon number detection after local DFTs of the target entangled state $|\phi_{N,M-N}\rangle$ exhibits therefore perfect (K, -K)-correlations. That means for the state $|\phi_{N,M-N}\rangle$, the probability $\mathcal{P}(K, -K)$ of (K, -K)-correlations in the output patterns of photon number detection after local DFTs is 100%. In the naturally photon number state basis, the probability $\mathcal{P}(n, \bar{n})$ of the complementary correlations (n, \bar{n}) is also 100% for the state $|\phi_{N,M-N}\rangle$. In general, the sum of the two probabilities for correct correlations $((n, \bar{n})$ - and (K, -K)correlations) has an upper bound for separable states, which is smaller than 2. The upper bound can be derived with the help of the separable inequality of correlation functions in MUBs [4]. As a result, we can then derive a separability inequality as follows.

$$\mathcal{P}(\boldsymbol{n}, \bar{\boldsymbol{n}}|\rho_{\text{sep.}}) + \mathcal{P}(K, -K|U_F^{\otimes 2}\rho_{\text{sep.}}U_F^{\dagger \otimes 2}) \le \frac{3}{2}.$$
 (10)

Note that, while this is by no means the optimal bound for DFTs, it does provides a sufficient criterion for the experimental verification of multi-photon entanglement in our system. We have therefore demonstrated the possibility of detecting the multi-photon entanglement of the post-selected state $|\phi_{N,M-N}\rangle$ using linear optics (specifically the DFTs) and photon detection.

3 Conclusion

We consider the generation of entangled multi-photon states using multiple single photon sources and linear optics. The resulting state exhibit a highly non-trivial structure in their photon number statistics. After postselection of fixed photon number partitions with respect to the subsystems A and B the entanglement of each output state can be evaluated by linear optics and photon detection. Specifically, we show that the mode transformation known as the discrete Fourier transformation (DFT) can be used to evaluate the correlations in two different photon number bases, where the identification of mutually unbiased subspaces permits us to formulate a criterion for entanglement detection based on the sum of the probabilities of measuring the correct correlations in both photon detection measurements. For separable states, the bound of this sum of two probabilities is 3/2, while the entangled state generated by beam splitting ideally exhibits both correlations with probability 1. Experimentally, it should therefore be possible to verify this entanglement using DFTs by observing correlations that exceed this bound.

- [1] E. Knill. Phys. Rev. A, 66:052306, 2002.
- [2] A. P. Lund and T. C. Ralph. Phys. Rev. A, 66:032307, 2002.
- [3] T. C. Ralph, A. P. Lund, and H. M. Wiseman. Journal of Optics B: Quantum and Semiclassical Optics, 7(10):S245, 2005.
- [4] C. Spengler, M. Huber, S. Brierley, et al. *Phys. Rev.* A, 86:022311, 2012.

Geometrical distance on quantum channels

Haidong Yuan

Department of Mechanical and Automation Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong*

Chi-Hang Fred Fung

Canada Research Centre, Huawei Technologies Canada, Ontario, Canada[†]

(Dated: July 21, 2016)

We propose a metric on the space of quantum channels and show how this metric determines the prefect discrimination between quantum channels and the ultimate precision limit for quantum parameter estimation, it thus provides a unified framework for these two related, but so far largely separated fields. New insights can then be gained for studies in both fields, which we demonstrate with two examples: first we derive a lower bound on the minimum number of uses needed for perfect discrimination of two quantum channels, which can be seen as the counterpart of the Heisenberg limit in quantum parameter estimation; second we show that sequential strategy has advantage over parallel strategy in quantum parameter estimation by providing an example inspired by quantum channel discrimination. We remark that our metric is efficiently computable using semi-definite programming.

PACS numbers:

Quantum channel discrimination and quantum parameter estimation are two active fields in quantum information science, quantum channel discrimination studies how to identify a quantum channel among a discrete set of channels[4–9] whereas quantum parameter estimation focus on identifying a channel among a continuous set of channels that characterized by some parameters[10–28]. Intuitively they are all related to the distinguishability of quantum channels, which are determined by the distance between the channels. Despite their similar nature, studies in these two fields are largely separated, as it lacks of a common measure of the distances on quantum channels.

We propose a distance measure on general quantum channels which can be seen as an extension of Bures metric on quantum states to quantum channels. We first show how this distance measure provide a general framework for quantum parameter estimation which relates the ultimate precision limit directly to the underlying dynamics, this provides efficient methods for computing the ultimate precision limit. It also provides an analytical formula of the precision limit with arbitrary pure input states, which does not need any optimization over equivalent Kraus operators as required in previous studies[20, 21]. We further demonstrate the power of the framework by deriving a sufficient condition on when ancillary systems are not useful for improving the precision limit. We then show this distance measure bridges the studies in quantum channel discrimination and quantum parameter estimation, and show how new insights can be gained on studies of both fields through two examples: first we derive a lower bound on the minimum number of evaluations needed for perfect discrimination between two quantum channels, this lower bound is a counterpart of the Heisenberg limit in quantum parameter estimation; second we show sequential strategy can outperform parallel strategy in quantum parameter estimation by providing an example inspired by quantum channel discrimination, which sheds light on a conjecture in quantum parameter estimation.

- [1] H.D. Yuan, & C.-H. F. Fung, arXiv: 1506.01909 (2015).
- [2] H.D. Yuan, & C.-H. F. Fung, arXiv: 1506.00819 (2015).
- [3] H.D. Yuan, & C.-H. F. Fung, Phys. Rev. Lett. 115, 110401 (2015).
- [4] A. Acín. Statistical distinguishability between unitary operations. *Physical Review Letters*, 87(17):177901, 2001.
- [5] R. Y. Duan, Y. Feng, and M. S. Ying, "Entanglement is Not Necessary for Perfect Discrimination between Unitary Operations", Phys. Rev. Lett. 98, 100503 (2007).
- [6] R. Y. Duan, Y. Feng, and M. S. Ying, Phys. Rev. Lett. 100, 020503 (2008).
- [7] G. Chiribella, G. D'Ariano, and P. Perinotti. Memory effects in quantum channel discrimination. *Physical Review Letters*, 101, 180501, 2008.

^{*}Electronic address: hdyuan@mae.cuhk.edu.hk

[†]Electronic address: chffung.app@gmail.com

- [8] R. Duan, Y. Feng, and M. Ying. Perfect distinguishability of quantum operations. Phys. Rev. Lett. 103, 210501 (2009).
- [9] Aram W. Harrow, Avinatan Hassidim, Debbie W. Leung, and John Watrous, Phys. Rev. A 81, 032339 (2010).
- [10] Helstrom, C. W., Quantum Detection and Estimation Theory. (Academic Press, New York, 1976).
- [11] Holevo, A. S., Probabilistic and Statistical Aspect of Quantum Theory. (North-Holland, Amsterdam, 1982).
- [12] Giovannetti, V., Lloyd, S. & Maccone, L. Nature Photonics. 5, 222 (2011).
- [13] Giovannetti, V., Lloyd, S. & Maccone, L., Quantum metrology. Phys. Rev. Lett. 96, 010401 (2006).
- [14] Wineland, D. J., Bollinger J. J., Itano, W. M. & Moore, F.L., Phys. Rev. A 46, R6797-R6800 (1992).
- [15] Caves, C. M., Phys. Rev. D 23, 1693-1708 (1981).
- [16] Lee H., Kok P. & Dowling, J.P., J. Mod. Opt. 49, 2325-2338 (2002).
- [17] Braunstein, S. L., Phys. Rev. Lett. 69, 3598 (1992).
- [18] Braunstein, S. L. & Caves, C. M., Statistical distance and the geometry of quantum states. Phys. Rev. Lett. 72, 3439 (1994).
- [19] Braunstein, S. L., Caves, M. C. & Milburn, G. J., Generalized Uncertainty Relations: Theory, Examples, and Lorentz Invariance. Annals of Physics 247, 135-173 (1996).
- [20] Fujiwara, A.& Imai, H., J. Phys. A: Math. Theor. 41, 255304 (2008).
- [21] Escher, B.M., de Matos Filho, R.L. & Davidovich, L., Nature Phys. 7, 406 (2011).
- [22] M. Tsang, Quantum metrology with open dynamical systems. New J. Phys. 15, 073005 (2013)
- [23] Demkowicz-Dobrzański, R., Kołodyński, J. & Guta, M. Nature Comm. 3, 1063 (2012).
- [24] Knysh, S., Smelyanskiy, V. N., & Durkin, G. A., Phys. Rev. A. 83, 021804 (2011).
- [25] Knysh, S., Chen, E. & Durkin, G., arxiv:1402.0495 (2014).
- [26] Kołodyński, J. & Demkowicz-Dobrzański, R., New Journal of Physics 15, 073043 (2013).
- [27] Demkowicz-Dobrzański, R. & Maccone, L., Phys. Rev. Lett. 113, 250801 (2014).
- [28] Alipour, S., Mehboudi, M., & Rezakhani, A.T. Phys. Rev. Lett. 112, 120405 (2014).
- [29] Chau, H. F., Quant. Inf. Compu. 11, 0721 (2011).
- [30] Fung, C.-H. F. & Chau, H. F., Phys. Rev. A 88, 012307 (2013).
- [31] Fung, C.-H. F. & Chau, H. F., Phys. Rev. A 90, 022333 (2014).
- [32] Fung, C.-H. F., Chau, H. F., Li, C.K. & Sze, N.S., Quantum Information and Computation, Vol. 15, No. 7&8, 0685-0693 (2015).
- [33] A. Childs, J. Preskill, and J. Renes. Quantum information and precision measurement. Journal of Modern Optics, 47(2– 3):155–176, 2000.
- [34] Uhlmann, A., Rep. Math. Phys. 9, 273-279 (1976).
- [35] M.A. Nielsen, I.L. Chuang, Quantum Information and Quantum Computation, (Cambridge University Press, 2000).
- [36] Masahito Hayashi, Communications in Mathematical Physics, Vol. 304, No. 3, 689-709 (2011);
- [37] Masahito Hayashi, Progress of Informatics, No.8 81-87 2011
- [38] Masahito Hayashi, Sai Vinjanampathy, L. C. Kwek, arXiv:1602.07131 (2016).

Group covariance of q-ary PSK coherent-state signals coded by codes over extension field \mathbb{F}_q

Minami TANAKA¹ * Asuka OHASHI² [†] Tsuyoshi Sasaki USUDA¹ [‡]

 ¹ School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan
 ² College of Science and Engineering, Ritsumeikan University,

1-1-1 Noji-Higashi, Kusatsu-shi, Shiga, 525-8577, Japan

Abstract. The formula of the channel matrix for group covariant signals in classical-quantum communication has been studied to calculate the channel matrix analytically. However, the derived formula cannot be applied to coded q-ary phase shift keing (PSK) signals by the codes over extension field \mathbb{F}_q despite its importance. In this study, using coding by group codes over \mathbb{F}_4 and \mathbb{F}_8 , we demonstrate that coded 4PSK and 8PSK signal sets can be narrow sense group covariant with respect to \mathbb{F}_4 and \mathbb{F}_8 , respectively.

Keywords: Quantum information theory, Extension field, Gram matrix, Channel matrix

1 Introduction

In classical-quantum communication[1], the computation of the channel capacity in finite codeword length is difficult even though finite codeword length is used in actual communication. For example, when Square-Root Measurement (SRM)[2] is used, the channel matrix is calculated by the square root of the Gram matrix of the quantum signal set. However, due to computational complexity, it is difficult to calculate using a universal algorithm if there are many signals.

Therefore, we have studied formulas to calculate the channel matrix analytically, and formula of channel matrix for narrow sense group covariant signals[4] has been derived[3]. However, the formula cannot be applied to quantum signal sets coded by codes over extension field $\mathbb{F}_{p^k} = \mathbb{F}_q$ despite its importance. Here, p is a prime number and k is a natural number. Thus, we now focus on the group covariance of q-ary Phase Shift Keying (PSK) coherent-state signals coded by codes over \mathbb{F}_q .

In this paper, with coding by codes over \mathbb{F}_4 and \mathbb{F}_8 , we show that coded 4PSK and 8PSK signal sets can be narrow sense group covariant with respect to \mathbb{F}_4 and \mathbb{F}_8 respectively.

2 Group covariant signals

Definition 1 ([5]) Let $(G; \circ)$ be a finite group and a set of parameters that characterize pure quantum-state signals $\{|\psi_i\rangle \mid i \in G\}$. The set of signals is called $(G; \circ, \hat{\chi})$ covariant if there exist unitary operators $U_k(k \in G)$ such that

$$U_k |\psi_i\rangle = \hat{\chi}(k, i) |\psi_{k \circ i}\rangle, \ \forall i, k \in G, \tag{1}$$

where $\hat{\chi}$ is a map from $G \times G$ into $\mathbb{U} = \{x \in \mathbb{C} \mid |x| = 1\}.$

If $\hat{\chi}(i, j) = 1$ ($\forall i, j \in G$), the set of signals is referred to as narrow sense group covariant.

Proposition 2 ([3]) A set of pure quantum-state signals $\{|\psi_i\rangle \mid i \in G\}$ is $(G; \circ, \hat{\chi})$ -covariant if and only if, for any $i, j \in G$,

$$\langle \psi_{k\circ i} | \psi_{k\circ j} \rangle = \hat{\chi}(k,i) \hat{\chi}(k,j) \langle \psi_i | \psi_j \rangle, \qquad (2)$$

for all $k \in G$.

Next, we give another proposition for $(G; \circ, \hat{\chi})$ covariant signals, which is used in Section 3.

Proposition 3 ([6]) Let G be an additive group. A set $\{v \mid v \in C\}$ of coded $(G; +, \hat{\chi})$ -covariant signals by a group code $C(\subseteq G^n)$ over G is $(C; +, \hat{\chi}')$ -covariant. Here, $\hat{\chi}'$ is defined as follows:

$$\hat{\chi}'(\boldsymbol{v}, \boldsymbol{w}) = \prod_{i=1}^{n} \hat{\chi}(v_i, w_i), \qquad (3)$$

for $v = (v_1, \ldots, v_n), w = (w_1, \ldots, w_n) \in C.$

3 Group covariance of coded PSK signals

3.1 Coded 4PSK signals by codes over \mathbb{F}_4

We show an example wherein 4PSK signals can be narrow sense group covariant with respect to \mathbb{F}_4 by coding, and a construction method of narrow sense group covariant codes of length 2n over $\mathbb{F}_{2^2} = \mathbb{F}_4$ from arbitrary group codes over \mathbb{F}_4 .

In the following, we use quaternary vector representation $\{0, 1, 2, 3\}$ for elements of \mathbb{F}_4 rather than $\{0, 1, \omega, \omega + 1\}(\omega^2 + \omega + 1 = 0)$.

Proposition 4 The set of coded 4PSK signals by the (2,1) code

$$C_{(2,1)} := \{00, 13, 22, 31\}$$

over \mathbb{F}_4 is narrow sense group covariant with respect to $C_{(2,1)}$ (and \mathbb{F}_4).

This proposition is proven using Proposition 2.

To prepare to demonstrate the method, we define a map $f_4: \mathbb{F}_4 \to \mathbb{F}_4$ as follows:

$$f_4(a) = \begin{cases} a & \text{if } a \in \{0, 2\}, \\ a+2 & \text{if } a \in \{1, 3\}. \end{cases}$$
(4)

^{*}im153006@cis.aichi-pu.ac.jp

[†]a-ohashi@fc.ritsumei.ac.jp

[‡]usuda@ist.aichi-pu.ac.jp

Definition 5 For code C over \mathbb{F}_4 of length n, consider the codes $C_{(2,1)}^{ex}(C) \subset \mathbb{F}_4^{2n}$ constructed by adding redundant symbols as follows:

$$C_{(2,1)}^{\text{ex}}(C) := \{ (\boldsymbol{a}|\boldsymbol{b}) \mid \boldsymbol{a} = (a_1, \dots, a_n) \in C \\ \boldsymbol{b} = (f_4(a_1), \dots, f_4(a_n)) \in \mathbb{F}_4^n \}. (5)$$

We refer to $C_{(2,1)}^{ex}$ as the extended code of C by $C_{(2,1)}$.

From Proposition 3, we obtain the following proposition for codes $C_{(2,1)}^{\text{ex}}$.

Proposition 6 A set of coded 4PSK signals $\{|w_i\rangle | w_i \in C_{(2,1)}^{ex}\}$ is narrow sense group covariant with respect to $C_{(2,1)}^{ex}$ if C is a group.

3.2 Coded 8PSK signals by codes over \mathbb{F}_8

Here, we show an example of symmetrization of 8PSK signals by coding and a construction method of narrow sense group covariant codes of length 8n over $\mathbb{F}_{2^3} = \mathbb{F}_8$ from arbitrary group codes over \mathbb{F}_8 .

In the following, we use an octonary vector representation $\{0, 1, 2, 3, 4, 5, 6, 7\}$ for elements of \mathbb{F}_8 rather than $\{0, 1, \omega, \omega+1, \omega^2, \omega^2+1, \omega^2+\omega, \omega^2+\omega+1\}(\omega^3+\omega+1=0)$. Furthermore, note that the eight letters correspond to 8PSK signals in the order 0, 4, 1, 6, 2, 7, 3 from the first signal.

Proposition 7 The set of coded 8PSK signals by the (8,1) code

$$C_{(8,1)} := \{0000000, 13131313, 2222222, 3131313144576675, 57447566, 66754457, 75665744\}$$

over \mathbb{F}_8 is narrow sense group covariant with respect to $C_{(8,1)}$ (and \mathbb{F}_8).

This proposition is proven using Proposition 2.

To demonstrate the method, we define a map $f_8 : \mathbb{F}_8 \to \mathbb{F}_8^7$ as follows:

$$f_8(a) = \begin{cases} (0,0,0,0,0,0,0) & \text{if } a = 0, \\ (3,1,3,1,3,1,3) & \text{if } a = 1, \\ (2,2,2,2,2,2,2,2) & \text{if } a = 2, \\ (1,2,1,2,1,2,1) & \text{if } a = 3, \\ (4,5,7,6,6,7,5) & \text{if } a = 4, \\ (7,4,4,7,5,6,6) & \text{if } a = 5, \\ (6,7,5,4,4,5,7) & \text{if } a = 6, \\ (5,6,6,5,7,4,4) & \text{if } a = 7. \end{cases}$$
(6)

Definition 8 For code C over \mathbb{F}_8 of length n, consider the code $C_{(8,1)}^{ex}(C) \subset \mathbb{F}_8^{8n}$ constructed by adding redundant symbols as follows:

$$C_{(8,1)}^{\text{ex}}(C) := \left\{ (\boldsymbol{a}|\boldsymbol{b}) \mid \boldsymbol{a} = (a_1, \dots, a_n) \in C \\ \boldsymbol{b} = (f_8(a_1), \dots, f_8(a_n)) \in \mathbb{F}_8^{7n} \right\}.(7)$$

We refer to $C_{(8,1)}^{ex}$ as the extended code of C by $C_{(8,1)}$.

From Proposition 3, we obtain following proposition for the codes $C_{(8,1)}^{ex}$.

Proposition 9 A set of coded 8PSK signals $\{|w_i\rangle | w_i \in C_{(8,1)}^{ex}\}$ is narrow sense group covariant with respect to $C_{(8,1)}^{ex}$ if C is a group.

4 Example

Here, we give an example of our method. Let $C = \{000, 121, 232, 313\}$. Gram matrix of the coded 4PSK signals by C is

$$\Gamma_{C} = \begin{pmatrix} 1 & e^{(-4+2\mathbf{i})N_{\rm S}} & e^{(-5-\mathbf{i})N_{\rm S}} & e^{(-3-\mathbf{i})N_{\rm S}} \\ e^{(-4-2\mathbf{i})N_{\rm S}} & 1 & e^{(-3+3\mathbf{i})N_{\rm S}} & e^{(-5-\mathbf{i})N_{\rm S}} \\ e^{(-5+\mathbf{i})N_{\rm S}} & e^{(-3-3\mathbf{i})N_{\rm S}} & 1 & e^{(-4+2\mathbf{i})N_{\rm S}} \\ e^{(-3+\mathbf{i})N_{\rm S}} & e^{(-5+\mathbf{i})N_{\rm S}} & e^{(-4-2\mathbf{i})N_{\rm S}} & 1 \\ \end{pmatrix}$$

$$(8)$$

and it is obvious that this code does not comprise group covariant signals. However, the Gram matrix of the coded 4PSK signals by the code

$$C_{(2,1)}^{\text{ex}}(C) = \{000000, 132213, 223122, 311331\}$$
(9)

which is a group code over \mathbb{F}_4 but is not a group code over \mathbb{Z}_4 is

$$\Gamma_{C_{(2,1)}^{ex}(C)} = \begin{pmatrix} 1 & e^{-8N_{\rm S}} & e^{-10N_{\rm S}} & e^{-6N_{\rm S}} \\ e^{-8N_{\rm S}} & 1 & e^{-6N_{\rm S}} & e^{-10N_{\rm S}} \\ e^{-10N_{\rm S}} & e^{-6N_{\rm S}} & 1 & e^{-8N_{\rm S}} \\ e^{-6N_{\rm S}} & e^{-10N_{\rm S}} & e^{-8N_{\rm S}} & 1 \end{pmatrix}.$$
(10)

This signal set is narrow sense group covariant with respect to $C_{(2,1)}$ (and \mathbb{F}_4) from Proposition 3.

5 Conclusion

We have shown codes over extension fields \mathbb{F}_4 and \mathbb{F}_8 with which coded 4PSK signal sets and coded 8PSK signal sets are applicable to the channel matrix formula.

Our method is simple; however we think it proposes a type of symmetrization method of non-symmetric signals using "coding". Therefore, in future study, we will consider symmetrization of quadrature-amplitude modulation (QAM) signals by coding. Note that QAM signals are important but are not group covariant in any sense.

Acknowledgment: This work has been supported in part by KAKENHI (Grant Numbers 24360151 and 16H04367).

- [1] C.W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, (1976).
- [2] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, Phys. Rev. A54, pp.1869-1876, (1996).
- [3] T.S. Usuda and K. Shiromoto, AIP Conf. Proc. 1363,
 T. Ralph and P.K. Lam (Eds.), pp.97-100, (2011).
- [4] T.S. Usuda and I. Takumi, QCMC2, Plenum Press, New York, pp.37-43, (2000).
- [5] T.S. Usuda, Y. Ishikawa, and K. Shiromoto, AIP Conf. Proc. 1633, H.-J. Schmiedmayer and P. Walther (Eds.), pp.201-203, (2014).
- [6] M. Tanaka, T. Sogabe, K. Shiromoto, and T.S. Usuda, Proc. of ISITA2014, p.348, (2014).

Intensity fluctuation suppression in a decoy-state quantum key distribution transmitter

Kensuke Nakata¹ *

Akihisa Tomita¹ Yu Kadosawa¹[†]

Kazuhisa Ogawa¹

Atsushi Okamoto¹

¹ Graduate School of Information Science and Technology, Hokkaido University, Kita14-Nishi9, Kita-ku, Sapporo 060-0814, Japan

Abstract. In decoy-BB84 quantum key distribution (QKD) protocol, intensity fluctuation of the transmitted optical pulses reduce secure key rate. The main factors of intensity fluctuation are a light source and an intensity modulator (IM). In this study, we focus an IM and show that fluctuation of modulation signals affect intensity fluctuation. Furthermore, we propose a robust IM with Nested Modulator (NM) for suppressing influence of fluctuation of modulation signals and experimentally confirm that the influence is greatly suppressed by NM

Keywords: Quantum key distribution, security certification

1 Introduction

It is rather recent that quantum key distribution (QKD) systems have shown enough performances for practical use, in terms of key generation speed and stability. Currently, state-of-arts QKD systems generate key at several hundred kb/s through an installed fiber of more than 10-dB loss[1]. The automatic control on the QKD systems enables unmanned operation for months without severe disruption. People are now seriously considering deployment of QKD systems. Still, there are a number of obsessions on the social deployment, one of which is the lack of security certification on a working system. In fact, security of the QKD protocol, particularly decoy-BB84, has been fully established in theory. However, such security proofs would be of no use without the certification that QKD equipment works properly under the practical conditions. In terms of security certification, "working properly" refers that the system satisfies the assumptions of the security proof.

An important issue for the decoy protocol is that the intensities of the transmitted pulses should be set precisely and kept stable. Since the estimation of the leakage information to the eavesdropper (Eve) depends on the intensities of the pulses, errors in the pulse intensities prevent us from accurate calculation of the amount of sacrifice bits, and thus affect the security of the final key. Recent studies suggested that the error of the pulse intensity should be kept smaller than 5 % [2, 3]. Therefore, it is necessary for the transmitters to stabilize the intensity within this range.

Experimentally, the intensity varies by several reasons, such as fluctuation of laser intensity, drift and fluctuation in the intensity modulation, and alteration of the loss in the passive components. Among these mechanisms, the effects from passive components would be smaller than others. We here focus on the intensity modulator, and propose a novel intensity modulator to reduce the intensity fluctuation. We consider a LiNbO₃ (LN) based intensity modulator (IM) used for high speed QKD systems. Since decoy method requires to change the intensity pulse by pulse, the IM should operate as fast as the clock frequency. The LN modulators are often employed for decoy method, because high speed modulators up to 20 GHz band width are commercially available. The intensity fluctuation originates from the fluctuation of the drive voltage. Actually, the drive voltage may fluctuate for high frequency operation. As well-known, the band width of the drivers should be much larger than the clock frequency to conserve the rectangular pulse shape. Otherwise, the waveform of the pulse is deformed and the signal varies by timing. The pulse jitter then results in the fluctuation of the applied voltage to alter the modulation.

2 Intensity fluctuation in a conventional modulator

Dual-drive Modulators (DDM) are often used for IM in QKD systems [4]. Figure 1(a) shows the schematic structure of the DDM. The intensity of the output is given by the phase shifts θ_1 and θ_2 through the upper and lower arms, as

$$I_{out}(\theta_1, \theta_2) = \frac{1}{2} \left(1 + \cos(\theta_1 - \theta_2) \right) I_{in}.$$
 (1)

For two-decoy method, three different intensities I_S , I_D , and I_0 are used, where the phases are set to $(\theta_1, \theta_2) = (0, 0), (\theta, 0), and(0, \pi)$ for I_S , I_D , and I_0 , respectively. If the applied voltage deviates from the designed value, the phase shift error results in the intensity error. Suppose the phase shift error appears in the upper arm $\theta_1 \rightarrow \theta_1 + \Delta$, the intensity error $I(\Delta) = [I(\theta_1 + \Delta, \theta_2) - I(\theta_1, \theta_2)]/I(\theta_1, \theta_2)$ grows proportionally to Δ^2 for I_S and I_0 , but to Δ for I_D . Therefore, decoy intensity is more sensitive to the phase error than other intensities I_S and I_0 . We measured the fluctuation of the decoy intensity for $(\theta_1 = \pi?2, \theta_2 = 0)$. As shown in Fig. 1(b), intensity distribution is broaden at the DDM output. If we evaluate the fluctuation by $3\sigma/\mu$, with the

^{*}nakata@optnet.ist.hokudai.ac.jp

[†]username3@domainname3

average intensity μ and the standard deviation σ , the range of the fluctuation $3\sigma/\mu$ increased from 4.4 % to 7.5 % by the IM.



Figure 1: (a) A schematic structure of a Dual-Drive Modulator (DDM,) (b) Intensity distribution of decoy pulses at the DDM output.

3 Reduction of the intensity fluctuation by a nested modulator

We observed that the large intensity fluctuation comes from the linear dependence of the intensity on the phase error for the decoy pulses. Therefore, we can reduce the intensity fluctuation by changing the linear dependence to the square dependence. To this end, we introduce a novel intensity modulator structure to the QKD transmitter. This type of the modulator, called a nested modulator (NM) [5] contains two Mach-Zehnder interferometer, as shown in Fig. 2(a). Though the phases θ_1 , θ_2 , θ_3 , and θ_4 can be controlled independently, we fix θ_3 and θ_4 to zero. Then, the output intensity is given by

$$I_{out}(\theta_1, \theta_2) = \frac{1}{8} \left(3 + 2\cos\theta_1 + 2\cos\theta_2 + \cos(\theta_1 - \theta_2) \right) I_{in}$$
(2)

We obtain signal and two decoys by setting θ_1 and θ_2 as $I_S = I_{out}(0,0) = I_{in}$, $I_D = I_{out}(0,\pi) = I_{in}/4$, and $I_0 = I_{out}(\pi,\pi) = 0$. By applying phase error as in the DDM $\theta_1 \rightarrow \theta_1 + \Delta$, we observe the intensity errors grows proportional to Δ^2 for all I_S , I_D , and I_0 . Therefore, NM output should be robust to the phase error, i.e., error of the applied voltage. Figure 2 (b) shows the measured intensity distribution of the NM output. The fluctuation was estimated to be $3\sigma/\mu = 4.9$ %, which was almost equal to the input fluctuation.



Figure 2: (a) A schematic structure of a Nested Modulator (NM,) (b) Intensity distribution of decoy pulses at the NM output.

4 Conclusion

We have shown that the intensity of the modulator output may fluctuate largely by the change of the applied voltage. The change may originate from the deformation of the electric pulses due to the limited band width of the driver, which become serious for the high speed QKD systems. We propose the use of nested modulators (NMs) to decoy-QKD transmitter. The output intensities from the NM vary as a quadratic function of the phase error, so that the intensities are little affected by the drive voltage fluctuation, if the operation point is properly set. The decoy intensity from the nested modulator should be fixed to 0.25 I_{in} to achieve the robustness to the applied voltage fluctuation. However, this value is often used in decoy-BB84 system, so that the effect on the final key rate would be small.

Acknowledgement This work was partly supported by NICT contract research project 157-B, and ImPACT "Advanced Information Society Infrastructure Linking Quantum Artificial Brains in Quantum Network."

- M. Sasaki, et al. Opt. Express, 19, 10387–10409 (2011).
- [2] M. Hayashi and R. Nakayama. New J. Phys. 16, 063009 (2014).
- [3] Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki. *Phys. Rev. A* 93, 042325 (2016).
- [4] A. Tanaka, et al. IEEE J. Quant. Electron. 48, 542– 550 (2012).
- [5] J. Ichikawa, et al. U.S. patent US20080212915 A1 (04, September, 2008)

Measurement based quantum computation and Quantum Error correction codes

Abhishek Sharma¹, Divyanshi Bhatnagar² and Atipriya Bajaj³

¹SRM University, NCR Campus, Ghaziabad 201204, India <u>er.abhishek01@gmail.com</u>

² Student, SRM University, NCR Campus, Ghaziabad 201204, India <u>divyanshi.db@gmail</u>

³ Student, SRM University, NCR Campus, Ghaziabad 201204, India <u>atipriyabajaj19@qmail.com</u>

ABSTRACT: Quantum Computing is the new hope in the field of computation. In one way quantum computation, an incredible technological advancement in the field of quantum computation, the previously prepared entangled state is computed via measurements. This article studies the basic concepts of measurement-based quantum computation, error correcting codes and fault tolerant system. Qubits, the building unit of Quantum Computation are prone to errors and are affected by the environment. However, fault tolerant algorithms can be designed for better performance. This paper presents a theoretical schema of large scale quantum computation.

Keywords: Measurement based quantum computation, error correcting codes, decoherence, topological code

1. INTRODUCTION

Information processing technology is largely based on the physics of classical electromagnetic dynamics. The processing of computers and networks is based on this principle. This principle has 20^{th} blossomed in century as electronics. Digital computers operate on data including magnitudes, symbols and letters i.e. in the form of binary digits 0 and 1. Each information is encoded in using different combinations of these digits. By comparing, counting and manipulating different combinations of these digits as per instructions digital computers perform tasks. These tasks include controlling industrial processes, regulating operations of machines, stimulating dynamic systems, analyzing and organizing vast business data etc. A new principle of physics is on focus since late 20th century. This new principle of information processing is based on quantum physics. Entering the realms of atoms opens up enormous powerful opportunities where processors work a million times faster than the ones we use today. A quantum computer has a sequence of qubits. A qubit can have any value 0, 1 or any quantum superposition of these two qubit states. If there are n qubits then 2ⁿ states can be represented by it simultaneously. A QC is a step ahead of classical computer in computation of prime

Factorization, secure communication, and teleportation of quantum information. However this information processing is not easy to realize because the quantum states are not stable (easily decoherence) for long time and difficult to manipulate. Vigorous efforts are going for the realization quantum information processing.

This article is review on the newcomputational model of quantum computers called measurement based quantum computation. Section 2 describes the basic concepts of Measurement based quantum computation and comparison with conventional computation models i.e. the circuit model. Section 3 describes errors and quantum error correcting codes. Section 4 is about fault tolerant topological quantum computer.

2. MEASUREMENT BASED QUANTUM COMPUTATION

From the beginning the realization of quantum computing has been considered on the basis of circuit model (fig 1). Circuit model has few basic gates such as single qubit rotation gates and two qubit interaction gate: the controlled not gate.Controlled NOT gate is one of the main difficulty in realization of QC. To obtain proper interaction between the particles is quite difficult.

In 2000s a new paradigm for quantum computers started. Researchers began to re-examine the computational model to utilize the feature of quantum physics. Since classical physics is completely different form quantum physics they thought of a new model for computation. Quantum states can exist in entanglement state. This feature leads to new model described by Gottesman and Chuang. As per their model quantum gates operate by the means of quantum teleportation. In Teleportation, quantum information is transmitted from one location to another with the help of classical computing and quantum entanglement between the sending and receiver location. Output of controlled -NOT is obtained by using entangled state by operating quantum teleportation. (Fig.2). The entangled state can be regarded as a computational resource for the quantum gate. Further modified computation model of teleportation is One way quantum computation. Prepare a cluster state that is entangled.Next stepis to perform single-qubit measurement on the cluster state. After this perform universal quantum computation. Major role is played by entangled cluster state in quantum gate and information flow. Creating an entangled state is a lot easier than measurement because target is already known. We utilize a non deterministic gate that has low success probability in order to generate the entangled resource. Once the resource of entangled state is created it is easy to perform one qubit interaction rather than two qubit interactions gates, so the new computational model decreases the difficulty of realizing quantum computers.



Figure 1 Circuit Model



Figure 2 Teleportation Based Gate



Figure 3 Measurement based quantum computation

3. ERRORS AND QUANTUM ERROR CORRECTING CODES

Qubits are prone to errors. They can be affected by heat,noise in the environment or by stray electromagnetic couplings. Usually there is bit flip error in classical computing i.e. 0 is mistakenly flipped to 1 or vice versa. Whereas in case of qubits there can be bit flip as well as phase errors. In case of phase error the sign of phase relation between 0 and 1 flips.

There are two main differences between classical error correction and quantum error correction. First is non cloning theorem it states that it is impossible to perfectly copy an unknown quantum state. This means there is no operation that satisfies this $U |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle$ for an unknown $|\psi\rangle$. Therefore, we are unable to protect arbitrary quantum states against errors by simply making multiple copies. It is possible to spread information of one qubit into highly entangled state of several qubits. Peter Shor discovered this methodto formulating a *quantum error correcting code* by storing the information of one qubit onto a highly entangled state of nine qubits.

Secondly, measurement of any unknown quantum state will collapse the wave function describing the state. Quantum information is destroyed while trying to measure certain subset of encoded state.

Classical error correction is the base of quantum error correction but still we need to define codes in slightly different manner. This is due both to the restrictions of what we can theoretically do with quantum information, but also due to the possible errors that can affect qubits. As stated earlier classical bits experience only bit flip but qubits experience both bit flip and phase errors. The errors are mostly continuous .such as rotation around X axis by some phase angle or some incoherent error caused by interaction with the outside world.

We introduce additional measurement qubit or syndrome measurement to diagnose which error corrupts an encoded state. A series of quantum measurement and data combination is used to diagnose. We then reverse an error by applying a corrective operation based on the syndrome. A syndrome measurement can determine whether a qubit has been corrupted or not. And if it is so thenwhich one had been corrupted. The outcome not only tells which bit was affected but also in which several ways it was affected. The syndrome measurement does not tell us about the value that is stored in the logical qubit as the measurement will destroy soit. It is better to store information in 9 qubits than in 1 qubit.

We only present formalism for coherent errors that can be represented by unitary gate.

Error operator E acting on a qubit $|\psi\rangle$ can be decomposed into linear superposition of X gates, Z gates and Y= iXZ

The detection occurs by redundant encoding with two classical codes. One code will detect X errors and other will detect Z errors without having to necessarily decode the code space. The simplest example is the bit flip code $|0\rangle_L = |0\rangle^{\otimes^N}$ and $|1\rangle =$ $|1\rangle^{\otimes^N}$ where the $^{\otimes^N}$ means N copies of the qubit. The number of physical flips needed to turn $|0\rangle L \leftrightarrow |1\rangle L$ scales linearly with N. In quantum we cannot directly measure the subset of the code block. Therefore we need some different method to spot errors. In bit flip code, there exists a certain property y that for both basis states, pair wise bit-parity in the code block is even (i.e. calculating the parity of any two bits via modulo addition for the $|0\rangle L$ and $|1\rangle L$ state is even). If the result of comparison is an odd value, we know an error has occurred without actually knowing if we started with the |0iL or |1iL state. This is what we need. Therefore, we need a way to calculate the parity of any two qubits in the code block without directly measuring the qubits themselves. The circuit introduces anancillary bit that interacts with the qubits and measured. The result will determine the parity of the two qubits (even or odd) and also force them to be in one of the parity if it is not beforehand. The principle of codespace is to construct encoded codewords that always have well defined parity regardless of the state of encoded information.

Returning to the example , the two encoded states are of even parity states of any pair wise Z operators. . i.e. applying the operator ZiZj for any i,j \in N returns the same state, ZiZj $|0, 1\rangle L = |0, 1\rangle L$. Bit flip errors result in states which violate this condition. For example, a bit-flip on qubit one of the encoded block will result in Z1Zj $|0, 1\rangle L = -|0, 1\rangle L$, $\forall j$. If we measure the parity of any of these operators and we find an odd result, we know that some type of error has occurred. Location and number of unique errors depend on the size of code block N. The parity of pair wise checks of the $Z_i Z_{i+1}$ operator will help us do so.

In case of quantum phase flip works in same way as bit flip. Therefore a full quantum error correction includes two classical codes one for bit flip and other for phase errors.

In Shor code one redundancy code is embedded into another. The code encodes a single qubit of information into nine physical qubits. The basis states are given by,

$$\begin{split} |0\rangle_L &= \frac{1}{\sqrt{2}} \quad (|000\rangle \ + \ |111\rangle)(|000\rangle \ + \\ |111\rangle)(|000\rangle + |111\rangle) \end{split}$$

$$|1\rangle_{L} = \frac{1}{\sqrt[2]{2}} (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle |111\rangle)$$

We have three blocks of three qubits that effectively act as a distance three redundancy code to correct bit flips. This allows us to correct a single bit flip error in any one of the three blocks.

3.1 SUBSYSTEM CODES

3.1.1 Bacon-Shor Codes

A new approach to implement quantum error correction is the quantum subsystem. In subspace codes, The information is encoded ina coding subspace of some large multiqubit system in a subspace code. Subspaces of the multi gubitare identified by the Subsystem and are considered to be equivalent. Bacon-Shor Code is of general nature. It has the ability to perform dynamical code switching in a fault-tolerant manner. The flexibility of BS codes is its strength. BS codes are stabilizer codes and are now defined over a square lattice. The lattice dimensions represent the X and Z error correction properties .Commenting on the size of the lattice in either of these two dimensions dictates the total number of errors the code can correct. In general, a C(n1,n2) BS code is defined over a $n1 \times n2$ square lattice which encodes one logical qubit into n1n2 physical qubits with the ability to correct at least (n1-1)/2 Z errors and at least (n2-12) X errors.

3.1.2 Topological Codes

Topological code's structure is defined on a lattice as in the case of subsystem code and the scaling of the code is done in such a way that more errors are corrected. In topological coding schemes the protection afforded to logical information relies on the unlikely application of error chains which define non-trivial topological paths over the code surface. The two ways of approaching areFirst is to treat topological codes as a class of stabilizer codes over qubit system. Second is to construct a physical Hamiltonian model based on the structure of the topological code or choose systems which appear to exhibit topological order. As a result more complicated field on anyonic quantum computation occurs.

Toric code is a topological quantum error correcting code and example to stabilizing code.



Figure 4 Concatenated Code

4. FAULT TOLERANT TOPOLOGICAL QUANTUM COMPUTER

We need to protect quantum computing form decoherence and different kinds of noise.Error correction codes are available for quantum computers and we can perform fault-tolerant quantum computing by applying an error correction procedure appropriately during computation. A fault tolerant system based on circuit model used quantum linear code and concatenated codes. A standard quantum linear encodes a single qubit into several qubits. It can handle single bit flip and phase flip error but if more than one occurs error correction does not work well. Concatenated coding works well for this. It recursively uses linear code. It provides greater error tolerance if the error rate per basic computational unit is less than a certain threshold. By the usage of codeof concatenation of sufficient depth with the error rate below the threshold then reliable computing can be executed. It is assumed here that any quantum gate can be achieved between widely separated particles, but with the increase in distance interaction between particles becomes weak.Code of quantum gate can be rewritten. And is written between spatially separate particles into combinations of quantum gates between nearest-neighbour sites, the number of consumed gates becomes larger in that case and the threshold of the fault-tolerant system becomes significantly small. At some point of time there was shortage of concatenated codes for fault tolerant systems so new topological or surface codes were proposed. Topological code uses the concept of nearest interactions. This is a realistic model than circuit model.A toric code is a quantum error correcting and an example of stabilizer code defined on a 2- D spin lattice. The edges of 2D lattice represents the qubits. The qubits are in entangled state as in topological code. The qubits that are on the endpoints of the 2D lattice are identical/similar to ones that are on the other side. The 2D lattice is on the surface of a torus, which provides us with the degrees of freedom that is used in encoding logical qubits. The entanglement and error correction can be performed on the nearest neighbourinteractions. Theencoding size can be enlarged by expanding the lattice. Toric code can also be rewritten on a square lattice with boundaries by constructing the equivalent for the hole of the torus and introducing the same topology. This makes easier to prepare multiple logical qubits. There exists a special form of 3D cluster state which becomes a resource Error correction. Toric code 0 1 2 3 2' 0' 6 7 6' 5 4 1' In this case, we can perform fault-tolerant quantum computing with only single-qubit measurements after preparing the 3D cluster states. The thresholds can be

improved by devising better encoding and decoding methods . Recently, the important realistic case of errors with a high loss rate and of nondeterministic entangling gates has also been investigated.

5. FUTURE OUTLOOK

Having reviewed the concepts and features of measurement based quantum computation and fault tolerant system we would like to mention the outlook for future research. As per theory, we need to find more realistic physical model for realization of measurement based quantum computation. There have been studies for finding Hamiltonians whose states are universal resources ground for On measurement based quantum computation. experimental sides some demonstrations of MBQC have been performed. However, it is prone to errors. One of the main problems is to obtain scalability in quantum computers. As per further research, optical quantum computation a new high efficiency single photon source is necessary. Ultra cold atomic gas in an optical lattice can be used for preparing large entangled resource for measurement based quantum computation. Another important candidate is the use of solid state artificial atoms such as quantum dots or dopants in solids for stationary qubits and the use of atoms photon interaction with cavity quantum electrodynamics for quantum gates. To conclude, measurement based quantum computation provides great hope towards realising quantum computers.

REFERENCES

[1] Morimae ,Tomoyuki"Basics and applications of measurement-based quantum computing" Information Theory and its Applications (ISITA), 2014 International Symposium on. IEEE,2014.

[2]Paler, Alexandru, and Simon J. Devitt."*Proceedings of the* 52^{nd} *Annual Design Automation Conference.ACM*, 2015.

[3]Feinstein,David Y.,S.S. Nair and Mitchell A.Thornton."Advances in Quantum Computing Fault Tolerance and Testing." *null*.IEEE,2007.

[4]Devitt, Simon. J., William J. Munro, and KaeNemoto. "Quantumerror correction for beginners." *Reports on Progress in Physics* 76.7(2013).

[4]RaussendorfRobert , and Hans J. Briegel."A oneway quantum computer." *Physical Review Letters* 86.22(2001): 5188

[5]<u>https://www.ntt-</u> review.jp/archive/ntttechnical.php?contents=ntr2012 09fa1.html

[6]https://quantiki.org/wiki/error-correction-0

[7]Duncan,Ross.*Types for quantum computing*. University of Oxford,2006

[8]<u>http://www.mind.ilstu.edu/curriculum/nature/com</u> <u>puter_types.php</u>

Multipartite key distribution in networks

Stefan Bäuml¹ *

Koji Azuma¹[†]

¹ NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa 243-0198, Japan

Abstract. The ability to distribute entanglement to be used as cryptographic key over complex quantum networks is an important step towards a quantum version of the Internet. Most attention so far has been given to the distribution of bipartite entanglement. In this work we derive bounds on the rate at which multipartite private states, such as GHZ states, can be distributed using a given network architecture. Our bounds are particular interest for possible applications of multi-receiver cryptography or quantum secret sharing.

Keywords: Quantum networks, QKD, Secret sharing

An important prerequisite for the application of quantum protocols such as quantum key distribution (QKD) to real world communication problems is the distribution of entanglement over long distances. The simplest way to do so is to create an entangled state locally and send part of it over a quantum channel. As the channel typically introduces noise, it is usually necessary to send many copies of the state via the channel and perform local operations and classical communication (LOCC) in order to distill the desired resource state.

For point to point communication, it has recently been shown [1] that the rate at which a secret key can be transmitted via asymptotically many uses of a channel assisted by LOCC is upper bounded by the squashed entanglement of the channel. The protocol used here is adaptive in the sense that after each channel use a round of LOCC is performed, determining which state will be inserted into the channel next.

The limitations of point to point transmission of entanglement can be overcome by use of quantum repeaters. While quantum repeaters allow for distribution of entanglement over arbitrarily large distances, the use of quantum protocols in a future version of the Internet will require entanglement to be distributed over complex networks rather than just a chain of nodes. In [2], the upper bound on the bipartite key rate given in [1] has been generalised from only a single quantum channel to an arbitrary network consisting of ancillary nodes and quantum channels. In [3] a lower bound for arbitrary networks is presented.

Another important generalisation towards the quantum Internet is to go beyond a one-sender and one-receiver model. This can be achieved using a GHZ state or a multipartite private state [4]. Another cryptographic protocol involving many parties is secret sharing, where two or more parties have to come together in order to decrypt a message. It has been shown that this can be achieved using a GHZ state [5].

In the present work, we present an upper bound on the rate at which GHZ states and multipartite private states can be distributed between an arbitrary number of parties, who are connected by an arbitrary network consisting of quantum broadcast channels and ancillary nodes. The scenario considered here is a generalisation of [6] in that it contains a network of broadcast channels rather than just a single broadcast channel and it is a generalisation of [2] in that it considers multipartite key distribution rather than bipartite one and broadcast channels rather than single receiver ones. We also discuss how the lower bound presented in [3] can be generalised to the multipartite case.

We consider the following setup: There are m nodes $A_1...A_m$ held by the m parties as well as an arbitrary number of ancillary nodes. The nodes are connected by an arbitrary network of quantum broadcast channels of $\mathcal{N}^e: X^e \to Y_1^e...Y_{r_e}^e$. The network can be described by a hypergraph with party and ancillary nodes as vertices and broadcast channels \mathcal{N}^e as hyperedges. In addition the nodes are connected by a network of classical communication, such as the conventional Internet. Initially, the quantum state ρ^0 of the system is fully separable between all nodes. It is our goal to establish an m-partite private state $\gamma_{A_1...A_m}$, as defined in [4], between the parties $A_1...A_m$. A special case of such a private state is the GHZ state.

In order to achieve this goal, an adaptive protocol is performed. The protocol begins with application of broadcast channel $\mathcal{N}^{e_0} : X^{e_0} \to Y_1^{e_0} \dots Y_{r_{e_0}}^{e_0}$ followed by a round of (probabilistic) LOCC, the outcome k_1 of which determines which broadcast channel $\mathcal{N}^{e_{k_1}} : X^{e_{k_1}} \to Y_1^{e_{k_1}} \dots Y_{r_{e_{k_1}}}^{e_{k_1}}$ is used next. Outcome k_1 is obtained with probability $p(k_1)$. After the channel use another round of LOCC is performed, resulting in k_2 . The outcomes $\mathbf{k}_2 = (k_1, k_2)$, which are obtained with probability $p(\mathbf{k}_2) = p(k_2|k_1)p(k_1)$, determine which channel $\mathcal{N}^{e_{\mathbf{k}_2}} : X^{e_{\mathbf{k}_2}} \to Y_1^{e_{\mathbf{k}_2}} \dots Y_{r_{e_{\mathbf{k}_2}}}^{e_{\mathbf{k}_2}}$ is used next and so on. After l channel uses we arrive at state $\rho^{\mathbf{k}_l}$ with probability $p(\mathbf{k}_l)$, such that $\left\| \rho_{A_1 \dots A_m}^{e_{\mathbf{k}_l}} - \gamma_{A_1 \dots A_m}^{d_{\mathbf{k}_l}} \right\|_1 \leq \epsilon$ for some m-partite private state $\gamma^{d_{\mathbf{k}_l}}$.

Our main result is an upper bound on the key dimension $d_{\mathbf{k}_l}$, averaged over all possible outcomes of the *l*round protocol. Before stating the theorem, let us introduce some notation: We call \mathcal{P} a partition of the nodes

^{*}stefan.bauml@lab.ntt.co.jp

[†]azuma.koji@lab.ntt.co.jp

into disjoint classes $\mathcal{G}_1...\mathcal{G}_m$ such that each class contains one party node. In general, some branches of a broadcast channel will remain within the class containing the sender whereas some branches cross the boundaries to other classes. Given channel $\mathcal{N}^e: X^e \to Y_1^e...Y_{r_e}^e$, we denote by $\mathcal{G}_X^e \in \{\mathcal{G}_1...\mathcal{G}_m\}$ the class containing the sender node and by $\mathcal{G}_{(1)}^e...\mathcal{G}_{(n_e)}^e \in \{\mathcal{G}_1...\mathcal{G}_m\}$ the other classes containing receiving nodes. Given partition \mathcal{P} , we denote by $\mathrm{ext}(\mathcal{P})$ the set of indices e, such that channels \mathcal{N}^e crosses at least one boundary between classes. Let us also define $\mathcal{Y}_X^e, \mathcal{Y}_{(1)}^e, ..., \mathcal{Y}_{(n_e)}^e$ as products of all output systems Y_j^e of \mathcal{N}^e going to a node in classes $\mathcal{G}_X^e, \mathcal{G}_{(1)}^e, ..., \mathcal{G}_{(n_e)}^e$, respectively.

If after $l = \sum_e l^e$ rounds of an adaptive protocol as described above the state of $A_1...A_m$ is ϵ -close to an *m*-partite private state $\gamma_{A_1...A_m}^{d_{\mathbf{k}_l}}$, it holds

$$m \left\langle \log d_{\mathbf{k}_l} \right\rangle_{\mathbf{k}_l} \le \min_{\mathcal{P}} \frac{1}{1 - c\epsilon} \left(\sum_{e \in \text{ext}(\mathcal{P})} \left\langle l^e \right\rangle_{\mathbf{k}_l} E_{\text{sq}}^{(\mathcal{P})} \left(\mathcal{N}^e \right) + f(\epsilon) \right)$$

where the minimisation is over all partitions \mathcal{P} , l^e is the number of uses of channel \mathcal{N}^e and the averaging is over all outcome vectors \mathbf{k}_l . Further $c \in \mathbb{Z}^+$ and $f(\epsilon) \to 0$ as $\epsilon \to 0$. $E_{sq}^{(\mathcal{P})}(\mathcal{N}^e)$ denotes the multipartite squashed entanglement as introduced in [7], w.r.t. the partitions given by \mathcal{P} and \mathcal{N}^e .

Let us now discuss how the lower bound on the key rate presented in [3] can be generalised to the multipartite setting. They have derived a lower bound on the key rate that can be achieved by using each channel \mathcal{N}^e with given frequency \bar{f}^e . The bound is achieved by means of a so-called aggregated quantum repeater protocol. The protocol involves distribution of $|\bar{f}^e Q^{\leftrightarrow}(\mathcal{N}^e)|$ copies of Bell states $|\Phi^+\rangle$ via each channel \mathcal{N}^e . The resulting network of Bell states is then used to distribute the maximal entanglement between Alice and Bob by means of entanglement swapping. The network of Bell states can be seen as an undirected graph. The amount of key obtainable in this way depends on the number of edge disjoint paths between Alice and Bob. By Menger's theorem [8], this number is equal to the minimum number of edges in any cut between Alice and Bob. In the case of multipartite key distribution the problem of finding an achievable rate becomes more involved. We will restrict ourselves to the simpler case where all channels in the communication network have only a single sender and a single receiver and discuss general broadcast channels in future work.

As in the bipartite case we use an aggregated quantum repeater protocol. We begin by creating a network of Bell states $|\Phi^+\rangle$, that can be described by a graph $\mathcal{G}^{\text{Bell}}$. The Bell state network is then used to establish a number of (qubit) GHZ state among A_1, \ldots, A_m . The number of qubits of the GHZ state then provides us with a lower bound on the multipartite key rate. Finding the maximal number of GHZ-entangled qubits, however, is a more difficult task as in the bipartite case, where we can use Menger's theorem.

In [9] it has been shown that GHZ states can be connected by an operation similar to entanglement swap-

ping: Assuming we have an n-partite GHZ state and an *m*-partite GHZ state, application of a projection onto two parties results in an n + m - 1 partite GHZ state of the remaining parties. In particular two Bell states can be connected into a 3-partite GHZ state. If necessary, party A_i can also be removed by a measurement in the σ_x eigenbasis and a local application of σ_z depending on the output, resulting in an n + m - 2 partite GHZ state of the remaining parties, which can be seen as a direct generalisation of entanglement swapping to GHZ states. In a general Bell state network we can create a GHZ state between parties $A_1...A_m$ if the corresponding graph contain a *tree* spanning vertices $A_1...A_m$, i.e. if there exists an acyclic subgraph connecting all vertices $A_1...A_m$. A tree that spans a subset of vertices of a graph is referred to as a Steiner tree. Hence, in order to determine the number of GHZ states that can be established between $A_1...A_m$ by means of generalised entanglement swapping, we need to compute the number of edge-disjoint Steiner trees spanning $A_1...A_m$ in the graph corresponding to the Bell network, which is another generalisation of Menger's Theorem.

For general graphs the problem of finding the number of edge-disjoint Steiner trees spanning a subset S of vertices, also known as *Steiner tree packing* has been shown to be NP complete [10]. There are, however, polynomial algorithms, that can provide us with lower bounds on the number of edge-disjoint Steiner trees in a graph [11].

- M. Takeoka, S. Guha, and M. M. Wilde, Nature communications 5 (2014).
- [2] Azuma, A. Mizutani, and H.-K. Lo, arXiv preprint arXiv:1601.02933 (2016).
- [3] K. Azuma and G. Kato, arXiv preprint arXiv:1606.00135 (2016)
- [4] R. Augusiak and P. Horodecki, Physical Review A 80, 042307 (2009).
- [5] M. Hillery, V. Buzek, and A. Berthiaume, Physical Review A 59, 1829 (1999).
- [6] K. P. Seshadreesan, M. Takeoka, and M. M. Wilde, arXiv preprint arXiv:1503.08139 (2015).
- [7] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, Information Theory, IEEE Transactions on 55, 3375 (2009).
- [8] K. Menger, Fundamenta Mathematicae 10, 96 (1927).
- [9] J. Wallnofer, M. Zwerger, C. Muschik, N. Sangouard, and W. Dur, arXiv preprint arXiv:1604.05352 (2016).
- [10] Petteri Kaski. Information processing letters, 91(1):1?5, 2004.
- [11] Lap Chi Lau, Foundations of Computer Science, 2004. Proceedings. 45th Annual IEEE Symposium on, pages 61-70. IEEE, 2004.

Permutation-invariant quantum codes from polynomials

Yingkai Ouyang¹ *

¹ Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372

Abstract. A qudit code is a subspace of the state space of a fixed number of qudits. Such a code is permutation-invariant if it is unchanged under the swapping of any pair of the underlying qudits. Prior permutation-invariant qubit codes encode a single qubit while correcting t arbitrary errors, and their logical codewords have two important properties. First, the Dicke states over which the logical codewords are superposed over have weights spaced a constant number apart. Second, the probability of observing each logical codeword as a given Dicke state is proportional to a binomial coefficient. We design permutation-invariant qudit codes encoding a single qubit with logical codewords that need not have the above two properties, while still allowing the correction of t arbitrary errors. Polynomials govern the structure of the Dicke states and the probabilities in our construction.

The promise offered by the fields of quantum cryptography [1, 2] and quantum computation [3] has fueled recent interest in quantum technologies. To implement such technologies, one needs a way to reliably transmit quantum information, which is inherently fragile and often decoheres because of unwanted physical interactions. If a decoherence-free subspace (DFS) [4] of such interactions were to exist, encoding within it would guarantee the integrity of the quantum information. Indeed, in the case of the spurious exchange couplings [5], the corresponding DFS is just the symmetric subspace of the underlying qubits. In practice, only approximate DFSs are accessible because of small unpredictable perturbations to the dominant physical interaction [6], and using approximate DFSs necessitate a small amount of error correction. When the approximate DFS is the symmetric subspace, permutation-invariant codes can be used to negate the aforementioned errors [7, 8, 9].

Permutation-invariant codes are particularly useful in correcting errors induced by quantum permutation channels with spontaneous decay errors, with Kraus decomposition $\mathcal{N}(\rho) = \mathcal{A}(\mathcal{P}(\rho)) = \sum_{\alpha,\beta} A_{\beta} P_{\alpha} \rho P_{\alpha}^{\dagger} A_{\beta}$, where \mathcal{P} and \mathcal{A} are quantum channels satisfying the completeness relation $\sum_{\alpha} P_{\alpha}^{\dagger} P_{\alpha} = \sum_{\beta} A_{\beta}^{\dagger} A_{\beta} = \mathbb{1}$ and $\mathbb{1}$ is the identity operator on m qubits. The channel \mathcal{P} has each of its Kraus operators P_{α} proportional to $e^{i\theta_{\alpha}\hat{a}_{\alpha}}$, where θ_{α} is the infinitesimal parameter and the infinitesimal generator \hat{a}_{α} is any linear combination of exchange operators. By a judicious choice of θ_{α} and \hat{a}_{α} , the channel \mathcal{P} can model the stochastic reordering and coherent exchange of quantum packets as well as out-of-order delivery of classical packets [10].The channel \mathcal{A} on the other hand models spontaneous decay errors, otherwise also known as amplitude damping errors, where an excited state in each qubit independently relaxes to the ground state with probability γ . Our permutation-invariant code is inherently robust against the effects of channel \mathcal{P} , and can suppress all errors of order γ introduced by channel \mathcal{A} , and is hence approximately robust against the composite noisy permutation channel \mathcal{N} .

The possibility of error correction in permutationinvariant codes [7, 8, 9, 11] is a useful feature, particularly when exchange errors or random permutation errors are the dominant errors afflicting the system. Permutationinvariant codes that can correct even a single qubit error are necessarily non-stabilizer codes, and hence the design of such codes is non-trivial and necessarily uses techniques beyond the stabilizer formalism. Permutation-invariant codes with error correction capabilities are also necessarily highly entangled, and may be of interest to further the theory the entanglement of symmetric states [12, 13, 14, 15, 16, 17].

The first example of a permutation-invariant code which encodes one qubit into 9-qubits while being able to correct any single qubit error was given by Ruskai over a decade ago [7]. A few years later, Ruskai and Pollatshek found 7-qubit permutation invariant codes encoding a single qubit which correct arbitrary single qubit errors [8]. Recently permutation-invariant codes encoding a single qubit into $(2t+1)^2$ qubits that correct arbitrary t-qubit errors has been found [9]. In Ref. [11], permutation-invariant codes encoding more than a qubit while correcting spontaneous decay errors to leading order have also been studied. In Ref. [18], the similarity of permutation-invariant quantum codes and bosonic codes has also been explored, and further advance in the theory of either one of these theories might have important implications for the other.

Here, we extend the theory of permutation-invariant quantum codes, while still retaining the ability to correct t arbitrary errors. The full technical details of this submission is available on the arXiv in Ref. [19]. Prior permutation-invariant qubit codes that encode a single qubit while correcting t arbitrary errors, have logical codewords with two important properties. First, the Dicke states over which the logical codewords are superposed over have weights spaced a constant number Second, the probability of observing each apart. logical codeword as a given Dicke state is proportional to a binomial coefficient. We design permutationinvariant qudit codes encoding a single qubit with logical codewords that need not have the above two properties,

^{*}yingkai_ouyang@sutd.edu.sg

while still allowing the correction of t arbitrary errors. Polynomials govern the structure of the Dicke states and the probabilities in our construction.

We also note that unlike prior permutation-invariant quantum codes that have been restricted to systems comprised of solely qubits, we extend our theory to permutation-invariant qudit codes. For N-qubit systems, the symmetric subspace is spanned by Dicke states with weights from 0 to N. Here, a Dicke state of weight w is a uniform superposition over all computation basis states with exactly w excitations, and we denote it as $|D_w^N\rangle$.

To describe permutation-invariant codes over qudits, we elucidate the basis of the symmetric subspace of Nqudits, where each qudit is of dimension q. We denote $\mathcal{T}_{N,q}$ to be the set of all q-tuples with components that are non-negative integers that sum to N. For each $\boldsymbol{\tau} =$ $(\tau_0, \ldots, \tau_{q-1}) \in \mathcal{T}_{N,q}$, we necessarily have $\tau_0 + \cdots + \tau_{q-1} =$ N, and we wish to define a Dicke state of type $\boldsymbol{\tau}$, which we denote as $|D[\boldsymbol{\tau}]\rangle$. Each $|D[\boldsymbol{\tau}]\rangle$ is a superposition over all computational basis states $|\mathbf{x}\rangle = |x_1\rangle \otimes \cdots \otimes |x_m\rangle$ such that each $|\mathbf{x}\rangle$ is a tensor product of exactly $p_j |j\rangle$'s for $0 \leq j \leq q-1$.

We construct permutation-invariant codes encoding a single qubit into N qudits that correct arbitrary t qudit errors using polynomials p_0, \ldots, p_{q-1} in the variable z and f in the variable x. We assume that the polynomial $f(x) = \sum_{z=0}^{n} f_z x^z$, has real coefficients f_z , and $(p_0(z), \ldots, p_{q-1}(z)) \in \mathcal{T}_{N,q}$ for every $0 \leq z \leq n$, with $f_n \neq 0$. Now let

$$\mathcal{F}_0 = \{ 0 \le z \le n : f_z > 0 \}, \mathcal{F}_1 = \{ 0 \le z \le n : f_z < 0 \},$$
(1)

denote the index sets for which f_z is positive and negative respectively, and let $|f| = |f_0| + \cdots + |f_n|$. Our permutation-invariant codes have basis vectors

$$|0_L\rangle = \sqrt{\frac{2|f_n|}{|f|}} \sum_{z \in \mathcal{F}_0} \sqrt{\frac{|f_z|}{|f_n|}} |D[(p_0(z), \dots, p_{q-1}(z))]\rangle,$$

$$|1_L\rangle = \sqrt{\frac{2|f_n|}{|f|}} \sum_{z \in \mathcal{F}_1} \sqrt{\frac{|f_z|}{|f_n|}} |D[p_0(z), \dots, p_{q-1}(z)]\rangle.$$
(2)

Notice that the logical codewords in Eq. (2) are independent of the choice of nonzero f_n , and we can without loss of generality consider a constant nonzero f_n such as $f_n = 1$. For all $0 \le z \le n$, we denote the classical codes

$$C_{z} = \{ \mathbf{x} \in \{0, \dots, N\}^{N} : \operatorname{wt}_{j}(\mathbf{x}) = p_{j}(z), 0 \le j \le q - 1 \},$$
(3)

and define the pair-wise minimum distance between these codes as

$$\Delta = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in \mathcal{C}_z, \mathbf{y} \in \mathcal{C}_{z'}, 0 \le z < z' \le n\}, (4)$$

where $d(\mathbf{x}, \mathbf{y}) = |\{1 \leq i \leq N : x_i \neq y_i\}|$ denotes the Hamming distance between the vectors \mathbf{x} and \mathbf{y} . Theorem 1 gives sufficient conditions for which the permutation-invariant code spanned by the logical vectors given in Eq. (2) corrects t arbitrary qudit errors. **Theorem 1** Let p_0, \ldots, p_{q-1} be polynomials of degree at most θ . Let f(x) be a non-zero polynomial with real coefficients having a root at x = 1 with multiplicity m. Then the code spanned by Eq. (2) corrects at least $t = \min\{\lfloor \frac{\Delta-1}{2} \rfloor, \lfloor \frac{m-1}{2\theta} \rfloor\}$ arbitrary qudit errors.

Theorem 1 implies that if

$$m \ge (\Delta - 1)\theta + 1,\tag{5}$$

the number of errors that can be corrected is $t = \lfloor \frac{\Delta - 1}{2} \rfloor$. In this scenario, evaluating t becomes a combinatorial problem which depends only on Δ .

The amplitudes $\sqrt{\frac{2}{|f|}}\sqrt{|f_z|}$ of our permutationinvariant code that arise in Eq. (2) depend crucially on our choice of the polynomial f(x) with real coefficients. When the degree of f(x) is equal to the multiplicity of its root at x = 1, that is when n = m, we uniquely have $f(x) = f_n(x-1)^n$ and $f_z = f_n(-1)^{n-z} {n \choose z}$. This choice of f(x) gives rise to the amplitudes that are crucial in the specification of certain permutation-invariant codes [7, 9, 11] and certain bosonic codes [18]. When n > m, we must have

$$f(x) = f_n (x-1)^m \left(x^{n-m} + \sum_{j=0}^{n-m-1} a_j x^j \right), \quad (6)$$

where a_j are arbitrary real constants for $0 \leq j \leq n-m-1$. Hence the set of all polynomials of the form in Eq. (6) is isomorphic to \mathbb{R}^{n-m} , while the set of all monic polynomials f(x) of degree n with real coefficients is isomorphic to \mathbb{R}^n . Random choices of f_z typically yield polynomials f(x) inconsistent with Eq. (6), and the combinatorial identity

$$\sum_{z=0}^{n} f_z z^j = 0, \text{ for every } 0 \le j \le m-1,$$
 (7)

required in the proof of Theorem 1 need not hold. Here we take the convention where $0^0 = 1$. In view of this, requiring f(x) to have a root at x = 1 with multiplicity m is non-trivial.

To complete the specification of our code, apart from the polynomial f(x), the polynomials p_0, \ldots, p_{q-1} appearing in Eq. (2) are also required. In particular, to correct one error, the Ruskai code [7, 9] has logical codewords

$$|0_L\rangle = \frac{1}{2}(|D_0^9\rangle + \sqrt{3}|D_6^9\rangle) |1_L\rangle = \frac{1}{2}(|D_3^9\rangle + \sqrt{3}|D_9^9\rangle).$$
(8)

With our current construction, to correct one error we can for example use $p_1(z) = 1+3z$, $f(x) = (1+x)(x-1)^5$ and N = 19 to obtain a permutation-invariant code with logical codewords

$$|0_L\rangle = \frac{\sqrt{4}|D_4^{19}\rangle + \sqrt{5}|D_{13}^{19}\rangle + |D_{19}^{19}\rangle}{\sqrt{10}} |1_L\rangle = \frac{|D_1^{19}\rangle + \sqrt{5}|D_7^{19}\rangle + \sqrt{4}|D_{16}^{19}\rangle}{\sqrt{10}},$$
(9)

where the weight distribution for the Dicke states are linearly shifted, and the square of the amplitudes do not follow the binomial distribution.

Theorem 1 implies that the polynomials p_0, \ldots, p_{q-1} can be non-linear. For example for q = 3, $f(x) = (1 + x)(x-1)^5$ and $p_1(z) = 3z^2$, $p_2(z) = 0$, $p_1(z) = N - p_1(z)$ and N = 108, we have

$$|0_L\rangle = \frac{\sqrt{4}|D[105,3,0]\rangle + \sqrt{5}|D[60,48,0]\rangle + |D[0,108,0]\rangle}{\sqrt{10}}$$
$$|1_L\rangle = \frac{|D[108,0,0]\rangle + \sqrt{5}|D[96,12,0]\rangle + \sqrt{4}|D[33,75,0]\rangle}{\sqrt{10}}$$
(10)

The code spanned by Eq. (10) also corrects one error. Clearly many other choices of polynomials p_0, \ldots, p_{q-1} are also feasible within the framework of our construction.

To prove Theorem 1, we first state the key lemmas.

Lemma 2 Let $P \in \mathcal{P}_q^{\otimes N}$ have weight w where $w \leq 2t$. Let $\tau_0, \ldots, \tau_{q-1}$ be polynomials in the variable z of degree at most θ . Let $\boldsymbol{\tau} = (\tau_0, \ldots, \tau_{q-1}) \in \mathcal{T}_{N,q}$. Then $\langle D[\boldsymbol{\tau}]|P|D[\boldsymbol{\tau}] \rangle$ is a polynomial of degree at most $2t\theta$ in the variable z.

Lemma 3 Let $f(x) = \sum_{z=0}^{n} f_z x^z$ be a non-zero polynomial with real coefficients f_z and a root at x = 1 with multiplicity m. Then Eq. (7) holds.

it then suffices to show for every N-qudit Pauli operator of weight at most 2t (i) the non-deformation conditions $\langle 0_L | P | 0_L \rangle = \langle 1_L | P | 1_L \rangle$ and (ii) the orthogonality conditions $\langle 0_L | P | 1_L \rangle = 0$ [20]. Having $t \geq \lfloor \frac{\Delta - 1}{2} \rfloor$ immediately implies that the orthogonality conditions (ii) hold. Hence it remains to prove (i), or equivalently the non-deformation condition

$$\sum_{z=0}^{n} f_z \langle D[\mathbf{p}(z)] | P | D[\mathbf{p}(z)] \rangle = 0, \qquad (11)$$

where we denote $\mathbf{p}(z) = (p_0(z), \dots, p_{q-1}(z))$. The proof of Eq. (11) has two ingredients: (i) the polynomials $\langle D[\mathbf{p}(z)]|P|D[\mathbf{p}(z)]\rangle$ have degree no more than $2t\theta$ in the variable z as given in Lemma 2, and (ii) the combinatorial identity Eq. (7) as given in Lemma 3. Note that condition (i) implies that

$$\langle D[\mathbf{p}(z)]|P|D[\mathbf{p}(z)]\rangle = \sum_{j=0}^{2t\theta} \alpha_j z^j,$$
 (12)

for some constants $\alpha_j \in \mathbb{C}$. Hence

$$\sum_{z=0}^{n} f_{z} \langle D[\mathbf{p}(z)] | P | D[\mathbf{p}(z)] \rangle = \sum_{z=0}^{n} f_{z} \sum_{j=0}^{2t\theta} \alpha_{j} z^{j}$$
$$= \sum_{j=0}^{2t\theta} \alpha_{j} \left(\sum_{z=0}^{n} f_{z} z^{j} \right). \quad (13)$$

But the bracketed term in Eq. (13) is always zero because of condition (ii) and $m > 2t\theta$, and this completes the proof of the non-deformation condition Eq. (11). Hence our code can correct at least t arbitrary qudit errors.

- C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, New York, 1984.
- [2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661– 663, Aug 1991.
- [3] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, second ed., 2000.
- [4] P. Zanardi and M. Rasetti, "Noiseless Quantum Codes," *Phys. Rev. Lett.*, vol. 79, pp. 3306–3309, Oct. 1997.
- [5] S. Blundell, Magnetism in Condensed Matter. Great Clarendon Street, Oxford OX2 6DP: Oxford master series in condensed matter physics, first rnote ed., 2003.
- [6] D. A. Lidar, D. Bacon, and K. B. Whaley, "Concatenating decoherence-free subspaces with quantum error correcting codes," *Phys. Rev. Lett.*, vol. 82, pp. 4556–4559, May 1999.
- [7] M. B. Ruskai, "Pauli Exchange Errors in Quantum Computation," *Phys. Rev. Lett.*, vol. 85, pp. 194– 197, July 2000.
- [8] H. Pollatsek and M. B. Ruskai, "Permutationally invariant codes for quantum error correction," *Linear Algebra and its Applications*, vol. 392, no. 0, pp. 255–288, 2004.
- [9] Y. Ouyang, "Permutation-invariant quantum codes," *Physical Review A*, vol. 90, no. 6, p. 062317, 2014.
- [10] V. Paxson, "End-to-end internet packet dynamics," SIGCOMM Comput. Commun. Rev., vol. 27, pp. 139–152, Oct. 1997.
- [11] Y. Ouyang and J. Fitzsimons *Phys. Rev. A*, vol. 93, p. 042340, Apr 2016.
- [12] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, "Entanglement of multiparty-stabilizer, symmetric, and antisymmetric states," *Phys. Rev. A*, vol. 77, p. 012104, Jan 2008.
- [13] R. Hübener, M. Kleinmann, T.-C. Wei, C. González-Guillén, and O. Gühne, "Geometric measure of entanglement for symmetric states," *Physical Review A*, vol. 80, no. 3, p. 032324, 2009.
- [14] L. Chen, H. Zhu, and T.-C. Wei, "Connections of geometric measure of entanglement of pure symmetric states to quantum state estimation," *Physical Review A*, vol. 83, no. 1, p. 012305, 2011.

- [15] L. Arnaud and N. J. Cerf, "Exploring pure quantum states with maximally mixed reductions," *Phys. Rev. A*, vol. 87, p. 012319, Jan 2013.
- [16] D. Baguette, T. Bastin, and J. Martin, "Multiqubit symmetric states with maximally mixed one-qubit reductions," *Phys. Rev. A*, vol. 90, p. 032314, Sep 2014.
- [17] K. Feng, L. Jin, C. Xing, and C. Yuan, "Multipartite entangled states, symmetric matrices and errorcorrecting codes," 2015. arXiv:1511.07992v1.
- [18] M. H. Michael, M. Silveri, R. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. Girvin, "New class of quantum error-correcting codes for a bosonic mode," arXiv preprint arXiv:1602.00008, 2016.
- [19] Y. Ouyang, "Permutation-invariant qudit codes from polynomials," arXiv preprint arXiv:1604.07925, 2016.
- [20] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, "Approximate quantum error correction can lead to better codes," *Phys. Rev. A*, vol. 56, p. 2567, 1997.

Quantum algorithm for association rules mining

Chao-Hua Yu^{1 2 *} Fei Gao^{1 †} Qiao-Yan Wen¹

 State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
 ² State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China

State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100818, China

Abstract. Association rules mining (ARM) is one of the most important problems in knowledge discovery and data mining. Given a transaction database that has a large number of transactions and items, the task of ARM is to acquire consumption habits of customers by discovering the relationships between itemsets (sets of items). In this paper, we propose a quantum algorithm for the key procedure of ARM, finding out frequent itemsets from the candidate itemsets and acquiring their supports. Specifically, for the case in which there are $M_f^{(k)}$ frequent k-itemsets in the $M_c^{(k)}$ candidate k-itemsets $(M_f^{(k)} \leq M_c^{(k)})$, our algorithm can efficiently mine these frequent k-itemsets and estimate their supports by using parallel amplitude estimation and amplitude amplification with complexity $\mathcal{O}(\frac{k\sqrt{M_c^{(k)}M_f^{(k)}}}{\epsilon})$, where ϵ is the error for estimating the supports. Compared with the classical counterpart, classical sampling-based algorithm, whose complexity is $\mathcal{O}(\frac{kM_c^{(k)}}{\epsilon^2})$, our quantum algorithm quadratically improves the dependence on ϵ , and also improves the dependence on $M_c^{(k)}$ to some degree which depends on the practical scale of $M_f^{(k)}$ relative

to $M_c^{(k)}$.

Keywords: AQIS, template

1 Introduction

As one of the most important problems in data mining, association rules mining (ARM) is to discover the consumption habits of customers by finding out relationships between pairs of itemsets (sets of items) from a big transaction database [1]. The transaction database is a large set of a large number of transactions which is denoted by $\mathcal{T} = \{T_0, T_1, \cdots, T_{N-1}\}$ for N transactions, each one being a subset of an overall set of items denoted by $\mathcal{I} = \{I_0, I_1, \cdots, I_{M-1}\}$ for M items, i.e., $T_i \subseteq \mathcal{I}$. It can also be represented by a $N \times M$ binary matrix, denoted by D, in which the element $D_{ij} = 1(0)$ means that the item I_i is (not) contained in the transaction T_i . The task of ARM can be reduced to that of mining all the frequent itemsets [1]. Here an itemset X is called frequent if its support, defined by the percentage of transactions that contain X and denoted by supp(X), is not less than a preset threshold *min_supp*.

In classical regime, there are various algorithms [1] for mining frequent itemsets, the most famous one being the *Apriori* algorithm [2]. Based on the important *Apriori* property stating that all nonempty subset of a frequent itemset must also be frequent, Apriori algorithm employs an iterative approach known as a level-wise search to discover all the frequent itemsets. In the kth iteration of the algorithm, two procedures are executed:

• (P1) Given the set of candidate k-itemsets $C^{(k)}$ which is determined by the frequent (k-1)-itemsets when k > 1 or is just \mathcal{I} when k = 1, the supports of all the elements in $C^{(k)}$ are examined by passing every transaction of database and the frequent elements are pick out to form the set of all frequent k-itemsets $\mathcal{F}^{(k)}$.

• (P2) Generate the set of candidate (k+1)-itemsets $\mathcal{C}^{(k+1)}$ from $\mathcal{F}^{(k)}$.

In practice, in each iteration (P1) dominant the time complexity of whole process [3]. Therefore, how to efficiently executing (P1) of each iteration, namely finding out frequent itemsets from candidate ones, is of great importance. In the following section, we provide a quantum algorithm to implement (P1) for each iteration that can significantly reduce the time complexity in contrast to the classical algorithms.

2 Quantum algorithm

Our quantum algorithm is to find out frequent itemsets from the candidate itemsets in the procedure (P1) of each iteration shown above. Our algorithm is based on the basic quantum oracle O that access the element of the database binary matrix D, namely, $O|i\rangle|j\rangle|a\rangle =$ $|i\rangle|j\rangle|a \oplus D_{ij}\rangle$. $\Theta(k)$ basic oracles O together with the generalized CNOT operation [4] can be used to construct the quantum oracle $O^{(k)}$ that can identify whether an arbitrary transaction contain a k-itemset in in the way that

$$O^{(k)}|i\rangle|X\rangle = (-1)^{\tau(i,X)}|i\rangle|X\rangle,$$

where $\tau(i, X) = 1$ if $X \subseteq T_i$ and $\tau(i, X) = 0$ otherwise. Corresponding to $O^{(k)}$, we define a "big" Grover operator as

$$G^{(k)} = \left((2|\mathcal{X}_N\rangle \langle \mathcal{X}_N| - \mathbb{I}_N) \otimes \mathbb{I}_{M^k} \right) O^{(k)},$$

where $|\mathcal{X}_N\rangle = \frac{\sum_{i=0}^{N-1} |i\rangle}{\sqrt{N}}$ and \mathbb{I}_N is the identity operator with dimension N.

^{*}quantum.ych@gmail.com

[†]gaof@bupt.edu.cn

we suppose $\mathcal{C}^{(k)}$ has $M_c^{(k)}$ elements $\mathcal{C}^{(k)} = \{C_j^{(k)} | j = 1, 2, \cdots, M_c^{(k)}\}$ where $C_j^{(k)} = \{I_{c_{jl}^{(k)}} | l = 1, 2, \cdots, k, c_{jl}^{(k)} \in \mathbb{Z}_M\}$, $\mathcal{F}^{(k)}$ has $M_f^{(k)}$ elements and $\mathcal{F}^{(k)} \subseteq \mathcal{C}^{(k)}$. To mine the $M_f^{(k)}$ frequent k-itemsets from $M_c^{(k)}$ candidate k-itemsets, it requires computing the supports of all the candidate k-itemsets and then picking out the frequent k-itemsets. Our quantum algorithm will propose a new kind of amplitude estimation [5], parallel amplitude estimation, to generate a state approximating

$$\frac{\sum_{j=1}^{M_c^{(k)}} |s_j^{(k)}\rangle \langle s_j^{(k)}| \otimes |C_j^{(k)}\rangle \langle C_j^{(k)}|}{M_c^{(k)}},$$

where $s_j^{(k)}$ denote the supports of $C_j^{(k)}$, and then use the amplitude amplification [5] on the state to search for $s_j^{(k)} \ge min_supp$. Finally, measuring the state after amplitude amplification reveals the frequent k-itemsets and their supports. The details of our algorithm for mining frequent k-itemsets are described as follows.

Algorithm 1 Mining frequent k-itemsets $\mathcal{F}^{(k)}$ and their supports from candidate k-itemsets $\mathcal{C}^{(k)}$

Input: $\mathcal{C}^{(k)}, G^{(k)}, k, T;$

Output: $\mathcal{F}^{(k)}$ and the supports of elements in $\mathcal{F}^{(k)}$; 1: Prepare three registers in the state

$$\left(\frac{\sum_{t=0}^{T-1}|t\rangle}{\sqrt{T}}\right)\left|\mathcal{X}_{N}\right\rangle\left(\frac{\sum_{j=1}^{M_{c}^{(k)}}|C_{j}^{(k)}\rangle}{\sqrt{M_{c}^{(k)}}}\right).$$

- 2: Perform the unitary operation $\sum_{y=0}^{T-1} |y\rangle \langle y| \otimes (G^{(k)})^y$ on the state.
- Perform the inverse Fourier transformation F[†]_T on the first register. Then the third register encodes all the candidate k-itemsets, while the first register encoding their corresponding supports.
- 4: Search in the first register of the state for the terms $y \text{ satisfying } \sin^2(\frac{\pi y}{T}) \geq \min_supp \text{ or } \sin^2(\frac{\pi(T-y)}{T}) \geq \min_supp \text{ by using amplitude amplification and then the state of the first and third register}$

$$\sim \frac{\sum_{j=1, \operatorname{supp}(C_j^{(k)}) \ge \min_supp} |s_j^{(k)}\rangle \langle s_j^{(k)}| \otimes |C_j^{(k)}\rangle \langle C_j^{(k)}|}{M_f^{(k)}}$$

5: Measure the first and third register for $\mathcal{O}(M_f^{(k)})$ times to reveal all the $M_f^{(k)}$ frequent k-itemsets (i.e., $\mathcal{F}^{(k)}$) and their supports.

3 Complexity

We take the basic oracle O as the query complexity. The comparison of our quantum algorithm and classical algorithms are given in the TABLE 1. The Apriori algorithm directly calculate the supports of candidate kitemsets by scanning every transaction in a deterministic way, while the classical sampling-based algorithm estimates the supports by sampling the database and thus is non-deterministic. It is shown that our algorithm is significantly faster than the classical algorithms.

Table 1: Comparisons of our quantum algorithm, classical sampling-based algorithm and the classical Apriori algorithm for mining $\mathcal{F}^{(k)}$ from $\mathcal{C}^{(k)}$.

algorithm	determinacy	query complexity
Quantum Sampling-based Apriori	non-deterministic non-deterministic deterministic	$\mathcal{O}(rac{k\sqrt{M_c^{(k)}M_f^{(k)}}}{rac{\epsilon}{\epsilon^2}}) \ \mathcal{O}(rac{kM_c^{(k)}}{\epsilon^2}) \ \mathcal{O}(kM_c^{(k)}N)$

4 Conclusions

We provide a quantum algorithm for the core procedure of implementing ARM, mining frequent itemsets from the candidate itemsets. Specifically, by subtly using amplitude estimation and amplitude amplification, our algorithm can efficiently find out the frequent k-itemsets from candidate k-itemsets and estimate their supports. Complexity analysis shows our algorithm is faster than the classical counterpart, classical sampling-based algorithm, in the sense that the complexity of our algorithm is at least quadratically improved in the dependence on the error. We hope our quantum algorithm for ARM can help better understanding the power of quantum computing and inspire more quantum algorithms for big data mining tasks.

- J. W. Han, M. Kamber, and J. Pei, *Data mining:* Concepts and Techniques (Morgan Kaufmann, 2011) 3rd ed..
- [2] R Agrawal, R Srikant, Fast algorithms for mining association rules, in *Proceedings of the 1994 international conference on very large data bases (VLDB94)*, Santiago, Chile, 1994, p. 487.
- [3] H. Mannila, H. Toivonen, A. I. Verkamo, Efficient algorithms for discovering association rules, in *KDD*-94: AAAI workshop on Knowledge Discovery in Databases, Seattle, Washington, 1994, p. 181.
- [4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum compution, Phys. Rev. A 52, 3457 (1995).
- [5] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, *Quantum Amplitude Aplification and Estimation*, Contemporary Mathematics Series Millenium Volumn **305** (AMS, New York, 2002).

Quantum Chinese Chess

Chan Ming Shen¹, Jei Wei Chang¹, Wei- Kai Lin², Yanlin Chen², YiKe Huang³, and Li-Yi Hsu¹

¹Department of Physics, Chung Yuan Christian University, Chungli 320, Taiwan, Republic of China ²Institute of Information Science, Academia Sinica ³Department of Computer Science & Information Engineering, National Taiwan University

Abstract. For the pedagogical and entertaining purposes, we are projecting the quantum Chinese chess. Some additional chess rules are put as simile or metaphor of quantum superposition, entanglement, and measurement. Our short-term goal is to build an online platform for the chess players. As the long-term goal, we want to investigate the effect of the quantum moves on quantum Chinese chess. So far it is still unknown how to evaluate the power quantum moves in the chess play.

Keywords: quantum game, quantum entanglement, q

1 Introduction

The idea of quantum chess was originally proposed for the study of quantum chromodynamics. Therein, the space-time is pretended as a chessboard [1]. Maybe quantum tic-tac-toe was the first game play developed as a metaphor for the counterintuitive nature in quantum physics [2]. In 2010, Akl and Wismath proposed quantum chess to put "humans and computers on an ostensibly equal footing when faced with the uncertainties of quantum physics" [3]. Early in this year, Chris Cantwell has successfully raised funds for Quantum Chess on the Kickstarter [4]. Now everyone can see Hawking and Rudd playing the quantum chess on YouTube, and there even are apps for quantum chess.

Here we propose the quantum version of Chinese chess, also known as Xiangqi, which is a popular pastime in the Eastern world. For the pedagogical purpose, we eventually hope to propose quantum Chinese chess accessible and understandable for kids and young adult across the Taiwan Strait.

2 Rules

Among quantum tic-tac-toe, quantum chess, and Xiangqi, three quantum properties: the superposition, entanglement, and quantum measurement are well exploited. To demonstrate how it can be done, three "quantum" moves are put in addition to the traditional ones. (1) (Superposition) In addition to the regular move, the quantum move can move the regular move twice and make a supposition. Fig. 1 shows the quantum move of the "red Cannon". (2) (Entanglement) Based on (1), one can make entanglement between two or more chess pieces. For example, Fig.2 shows the entanglement between "red Cannon" and "red Chariot". Notably, the entanglement is made because the superposition of Cannon seems to "block" the moving way of Chariot. Fig. 2 (c) and (d) show two possible conditions after the measurement. (3) (Quantum measurement) If one want to



Figure 1: (a) Before the quantum move. The arrows each show the corresponding regular moves. (b) After the quantum move. The slashes indicate that "state" in superposition rather than a "real object" of the piece.

capture and remove the opponent piece with the superposition, one has to perform measurement both on this piece and his own. For example, the red Chariot wants to demolish the "black Cannon" in Fig. 3 (a). The probability of this event can occur with the probability 0.25, where the red Chariot and the black Cannon must be collapsed into the position as shown in Fig. 3(b) In addition, one can ask for the measurement on the specific opponent pieces in some circumstance. For example, in Fig. (4), the player with the red pieces can ask for the measurement on the black Canon.

The development of quantum Chinese chess is still in a very early stage. So far, we can play quantum Chinese chess on PC. Our goal is to put quantum Chinese chess on network platform such as twitch. As for the academic study, there are many interesting open questions. One of them is "Do quantum moves really useful?" Based on our chess experience with the low-level strength, we give a very rough answer: It largely depends on how the players recognize the probability on the board.

Traditionally, through the chess play, two players usually seek the balance of terror on the board and start the attacks afterward. Essentially a quantum move can move twice the regular move or make no move with the equal probability. As for the mind-reading, a conserva-

^{*}a6a018@yahoo.com.tw

[†]fairycat1150gmail.com

[‡]wklin@iis.sinica.edu.tw

 $[\]frac{1}{2}$ jackervator@gmail.com

[¶]lyhsu@cycu.edu.tw



Figure 2: (a) To form the entanglement, the red Chariot make a quantum move. (b) The entanglement between the red Chariot and the red Canon. The quantum measurement on these two pieces results in the cases either (c) or (d).

tive player may recognize the quantum move as a null move, while an aggressive player may recognize it as a quick one. Moreover, if the piece under its superposition can remove the opposite pieces with at most the probability 0.5. In this case, quantum moves are exploited to make a "not-so-real" threaten or a bluff. It is feasible that aggressive quantum moves may not be encouraged for a traditional player.

3 Discussion

In the chessboard of Xiangqi, there are 32 chess pieces distributed during 90 standing points. In the setup, the opposite soldiers are divided only a very narrow "river and boundary". The board looks more crowded than that in quantum chess. The legal regular moves are very limited. Moreover, in the initial game play, two players each usually take several regular moves to achieve the layout/ composition for the following defense and offense. In this process, it does not pay to make a quantum move, which will just delay layout completion. Finally, it could be useful that the pieces can escape from be captured and removed using the quantum move. To sum up, quantum Chinese chess is a good game as a metaphor of basic concept in quantum theory. We are looking forward to the collaboration for the further development of quantum Chinese chess.



Figure 3: (a) The red Chariot wants to capture the black Canon. To make this happen, the red Chariot ask for the quantum measurement on these two pieces. The capture can become real if the pieces are collapsed into the case (b).

4 Acknowledge

The authors acknowledge national support from the Ministry of Science and Technology of the Republic of China under Contract No. 102-2112-M-033 -006 -MY3.

- [1] New Scientist, 2137, 32 (1998).
- [2] Allan Goff: American Journal of Physics 74, 962 (2006).
- [3] S. G. Akl, Parallel Process. Letters, 20, 275 (2010).
- [4] http://quantumrealmgames.com/

Quantum Coherence - Their origin and trade-off relations

R. Chandrashekar^{1 2 *} P. Manikandan³ J. Segar^{3 †} Tim Byrnes^{1 2 4 5 ‡}

¹ New York University, 1555 Century Avenue, Pudong, Shanghai 200122, China

² NYU-ECNU Institute of Physics at NYU Shanghai, 3663 Zhongshan Road North, Shanghai 200062, China

³ Department of Physics, Ramakrishna Mission Vivekananda College, Mylapore, Chennai 600004, India

⁴ Department of Physics, New York University, New York 10002, USA

⁵ National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

Abstract. Quantum coherence is investigated using a new measure with metric properties and entropic nature and decomposed into local and intrinsic contributions. The trade-off relation between these contributions as well as their distribution properties are studied for simple tripartite systems and the more complex spin chain model.

Keywords: Quantum coherence, Local and Intrinsic coherence, Monogamy of coherence.

1 Introduction

Quantifying coherence using methods of quantum information science was introduced in [1]. Apart from the introduction of definitions corresponding to incoherent states, incoherent operations and maximally coherent states, the set of properties a functional should satisfy to be considered as a coherence measure were discussed in [1]. For a coherence measure C they are as follows: (i) $\mathcal{C} \geq 0$ and $\mathcal{C} \equiv 0$ iff $\rho \in \mathcal{I}^{(b)}$, where $\mathcal{I}^{(b)}$; is the set of incoherent states. (ii) $\mathcal{C}(\rho)$ is invariant under unitary transformations, *(iii)* $\mathcal{C}(\rho)$ is monotonic under incoherent completely positive trace preserving (ICPTP) map, as well as under selective incoherent measurements on average. (iv) $\mathcal{C}(\rho)$ is convex i.e., does not increase under mixing of quantum states. Two measures of coherence namely the relative entropy of coherence and the ℓ_1 norm were introduced in [1]. The former is an entropic measure, whereas the later is a geometric measure with each of them having their own advantages. To be a distance property a function d over a set X should satisfy the following properties: (i) $d(x, y) > 0 \forall x \neq y$ and d(x, x) = 0(Positivity) (ii) d(x, y) = d(y, x) (Symmetry). In addition if d satisfies $d(x, y) + d(y, z) \ge d(x, z)$ i.e., the triangle inequality, then d is a metric over the space X. We introduce a new coherence measure based on the quantum version of the Jensen-Shannon divergence (QJSD) [2, 3]

$$\mathcal{J}(\rho, \sigma) = \frac{1}{2} [S(\rho \| (\rho + \sigma)/2) + S(\sigma \| (\rho + \sigma)/2)].$$
(1)

which combines the features of both distance property and entropic nature. The QJSD is a distance but it is not a metric i.e., it does not satisfy the triangle inequality. To overcome this we use the square root of the QJSD as our distance measure, since it satisfies the triangle inequality.

2 Inter-qubit, Intra-qubit and Total Coherence

The total coherence of a given system is defined using the square root of the QJSD using the following expression

$$\mathcal{C}(\rho) \equiv \min_{\sigma \in \mathcal{I}^{(b)}} \sqrt{\mathcal{J}(\rho, \sigma)}, \tag{2}$$

where $\mathcal{I}^{(b)}$ is the set of incoherent states in a particular basis *b*. This measure (2) satisfies the properties outlined in Ref. [1] and hence qualifies as a coherence quantifier. But coherence can have its origin to intra-qubit and interqubit correlations. We propose the following measure of coherence to distinctly measure the intra-qubit and the inter-qubit coherences through the following equations

$$\mathcal{C}_{I}(\rho) \equiv \min_{\sigma_{S} \in \mathcal{I}_{S}} \mathcal{D}(\rho, \sigma_{S}), \qquad (3)$$

$$\mathcal{C}_L(\rho) \equiv \mathcal{D}(\sigma_S^{\min}, \rho^d). \tag{4}$$

Here C_I is the inter-qubit coherence and refer to it as intrinsic coherence and C_L is the Local coherence which computes the contribution of the intra-qubit coherence. As an illustrative example we consider a two qubit transverse Ising model which has the Hamiltonian

$$H = \lambda \sigma_1^x \sigma_2^x + J(\sigma_1^x + \sigma_2^x) + \epsilon \lambda (\sigma_1^z + \sigma_2^z).$$
 (5)

The parameters J and λ are the the coupling parameters and ϵ is a symmetry breaking term. A numerical estimation of the values of C_L , C_I and C are given in Fig 1 (a). The local coherence and the intrinsic coherence are complementary. In the limit $J \ll \lambda$ the coherence is intrinsic in nature since the ground state approaches a Bell state in the J = 0 and $\epsilon \to 0$ limit. In the limit $J \ll \lambda$ the coherence is localized with each spin since for $\lambda = 0$ the ground state is $(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$.

3 Distribution and Shareability of quantum coherence

The quantum coherence in a tripartite system ρ_{123} may be decomposed in any one of the following forms

 $\begin{array}{rcl} \mathcal{C}_{123} & \leq & \mathcal{C}_1 + \mathcal{C}_2 + \mathcal{C}_3 + \mathcal{C}_{1:2:3}, \\ \mathcal{C}_{123} & \leq & \mathcal{C}_1 + \mathcal{C}_2 + \mathcal{C}_3 + \mathcal{C}_{2:3} + \mathcal{C}_{1:23}. \end{array}$ (6)

^{*}cr2442@nyu.edu

[†]segar@imsc.res.in

[‡]tim.byrnes@nyu.edu



Figure 1: Coherence measured using QJSD for (a) N = 2site Ising model with $\epsilon = 0.2$; (b) Werner GHZ state (c) W state with $\theta = \pi/4$; (d) N = 10 site XXZ spin chain model with J = 1. Inset: Monogamy of the XXZ spin chain.

where C_n is the local coherence of the nth subsystem obtained from the reduced density matrix ρ_n and $C_{1:2:3}$ is the intrinsic coherence i.e., $C_I(\rho_{123})$. There are many such equivalent decompositions from which can conclude that

$$\mathcal{C}_{1:2:3} \simeq \mathcal{C}_{2:3} + \mathcal{C}_{1:23} \simeq \mathcal{C}_{1:2} + \mathcal{C}_{12:3} \simeq \mathcal{C}_{1:3} + \mathcal{C}_{13:2}.$$
 (7)

The above decomposition gives us an idea about how coherence is shared between the subsystems of various orders in a composite system. Similar to monogamy of entangled states [4, 5] we define the monogamy of coherence. In a maximally coherent tripartite system ρ_{123} , the coherence between the system 1 and the bipartition 23 is related to the coherence between the subsystems 1 and 2 as well the coherence between 1 and 3 through the inequality

$$C_{1:23} \ge C_{1:2} + C_{1:3}.\tag{8}$$

If the inequality is obeyed the system is called monogamous and if not it is referred to as polygamous system. For a multipartite system the inequality is $C_{1:2...N} \geq \sum_{n=1}^{N} C_{1:n}$ and we define the measure

$$M = \sum_{n=2}^{N} C_{1:n} - C_{1:2...N}$$
(9)

which is monogamous for $M \leq 0$ and polygamous M > 0. Thus from the monogamy concept we get to know whether the coherence is distributed in a bipartite fashion or in a multipartite fashion.

4 Investigation of Multipartite systems

The tripartite states can be divided into two classes namely GHZ and the W class. These two classes are unrelated under local operations and classical communication [6]. The Local coherence of the systems in these two kinds of states is zero and hence the intrinsic coherence is equal to the total coherence. For the pure mixed tripartite states the coherence and its distribution is given through Fig 1 (b) and Fig 1 (c).

To understand complex multipartite systems we investigate the Heisenberg XXZ spin chain. The Hamiltonian of the spin chain is

$$H = J \sum_{n} (\sigma_{n}^{x} \sigma_{n+1}^{x} + \sigma_{n}^{y} \sigma_{n+1}^{y} + \Delta \sigma_{n}^{z} \sigma_{n+1}^{z}), \qquad (10)$$

where J is the nearest neighbor spin coupling and Δ is the anisotropy parameter. The total quantum coherence shown in Fig 1 (d) is found to vary with the anisotropy parameter. The monogamy of coherence is shown in the inset of Fig 1 (d) shows that Δ switches the coherence from bipartite to multipartite nature.

5 Conclusion

A new coherence measure with both distance properties and entropic nature is proposed. The total coherence in the system is decomposed into contributions which arise from Local and Intrinsic contributions. It is found that the coherence transforms from the local to intrinsic nature in a Ising model depending on the interaction parameter. In the case of the Heisenberg spin chain there is a change from the monogamous behavior which is a highly multipartite coherence to the polygamous nature which is more bipartite in nature. Further applications in quantum metrology [7] may lead to interferometric advantages.

6 Acknowledgments

The work is supported by the Shanghai Research Challenge Fund, New York University Global seed Grants for Collaborative Research, National Natural Science Foundation of China Grant No. 61571301, and the Thousand Talents Program for Distinguished Young Scholars.

- T. Baumgratz, M. Cramer and M.B. Plenio, Phys. Rev. Lett. 113, 140401 (2014).
- [2] A.P. Majtey, P.W. Lamberti and D.P. Prato, Phys. Rev. A 72 052310 (2005).
- [3] P.W. Lamberti, A.P. Majtey, A. Borras, M. Casas and A. Plastino, Phys. Rev. A 77 052311 (2008).
- [4] V. Coffman, J. Kundu and W.K. Wootters, Phys. Rev. A 61, 052306 (2000).
- [5] T.J. Osborne and F. Verstraete, Phys. Rev. Lett. 96, 220503 (2006).
- [6] W. Dür, G. Vidal and J.I. Cirac, Phys. Rev. A 62, 062314 (2000).
- [7] J. Sahota and N. Quesada, Phys. Rev. A 91, 013808 (2015).

Quantum homomorphic encryption from quantum codes

Yingkai Ouyang and Si-Hui Tan

Singapore University of Technology and Design, 8 Somapah Road, Singapore*

Joseph Fitzsimons

Singapore University of Technology and Design, 8 Somapah Road, Singapore^{*} and Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore

Homomorphic encryption has been recognised as an important primitive for building secure delegated computation protocols for many decades [1]. It provides a processing functionality for encrypted data which stays secret during the evaluation, and a scheme is fullyhomomorphic if it allows for arbitrary computation. Despite widespread interest in this problem, it was not until 2009 that the first computationally secure classical scheme for fully homomorphic encryption (FHE) was discovered [2], with many improvements following rapidly from this initial discovery [3, 4], and has recently drawn attention within the quantum information community One might wonder if quantum cryptosystems [5-12].might offer unconditionally secure homomorphic encryption schemes and whether the privacy homomorphisms could be extended to allow for evaluation of quantum circuits.

Like their classical counterparts, quantum homomorphic encryption (QHE) schemes comprise of four parts: key generation, encryption, evaluation, and decryption. Unlike blind quantum computation [13], in which the computation to be performed forms part of the secret, QHE schemes do not have secret circuit evaluations. They serve to obscure only the information that is contained within the state to be processed using the chosen circuit. The extent to which a scheme is secure depends on its specifics, and in previous work has varied depending on the precise nature of the computation which can be performed on the encrypted input. QHE schemes described in Refs. [9, 10] offer some information theoretic security, but this is only in the form of a gap between the information accessible with and without the secret key, a notion of security which does not imply the stronger notion of security under composition. These schemes are also limited in the set of operations that can be performed on the encrypted data. The scheme in [9] only allows computations in the BosonSampling model, while that in [10] is not known to support encoded universal quantum computing. Broadbent and Jeffrey's scheme [11] enables quantum homomorphic encryption of fixed depth circuits by bootstrapping onto a classical fully homomorphic encryption scheme and as such is only computationally secure. Recently Dulek, Schaffner and Speelman [12] used the garden-hose model of computation with Broadbent and Jeffrey's quantum homomorphic schemes to allow the evaluation of polynomial-depth circuits. Several other

schemes for computing on encrypted data have previously been introduced which offer universal quantum computation, but require interactions between the client and evaluator [5–8]. This requirement for interaction places them outside of the formalism of homomorphic encryption, although confusingly several of these schemes use that terminology [5, 6].

The difficulty in creating a perfectly secure quantum fully homomorphic encryption (QFHE) scheme persists, and is in line with the no-go result provided by [14] that perfect information-theoretic security whilst enabling arbitrary processing of encrypted data is impossible, unless the size of the encoding grows exponentially. Nonetheless, given the growing interest in QHE schemes and the multitude of possibilities, Broadbent and Jeffrey set out to provide a rigorous framework for defining QHE schemes [11], basing their security definitions on the requirement for indistinguishability of codewords under chosen plaintext attack with additional computation assumptions. Broadbent and Jeffery also require that a quantum *fully* homomorphic encryption satisfies two properties: correctness and compactness. Perfect correctness occurs when the evaluated output on the cipherstate after decryption is exactly the correct evaluated input.

Here we present a quantum encryption scheme which is homomorphic for arbitrary classical and quantum circuits which have at most some constant number of non-Clifford gates. Unlike classical schemes, the security of the scheme we present is information theoretic, satisfying entropic security definitions, and hence independent of the computational power of an adversary. The QHE scheme we present builds on constructions taken from quantum error correction codes to provide gates for universal quantum computation. The block of qubits that contains the code is embedded in a much larger set of qubits that are initialized in a maximally mixed state. The qubits are then shuffled in a specific but random way to hide the qubits that contain that code. Our protocol guarantees that the trace distance between ciphertexts corresponding to any two quantum inputs is exponentially suppressed. This is a significantly stronger security guarantee than previous homomorphic encryption schemes presented in [9]. Moreover the computation power of our scheme is similar to that of Broadbent and Jeffrey's while avoiding bootstrapping on the classical ho-



FIG. 1: Figure shows qubits arranged on a grid with shaded circles representing data qubits. Within the x-th row, the n data qubits are in a code encoded by U_x . The unshaded circles are ancilla qubits which are in the completely mixed state. There are r sets of codes, and b copies of such sets. A random permutation of the columns completes the encryption procedure of our quantum homomorphic encryption scheme.

momorphic encryption scheme.

Our QHE scheme takes as its input a r-qubit state ρ_{input} , and t independent copies of the magic state $|T\rangle\langle T| = \frac{I}{2} + \frac{X-Y}{2\sqrt{2}}$, all arranged in a single column (See Figure 1). We then introduce (2n-1) more columns of maximally mixed qubits to obtain a grid of qubits with r+t rows and 2n columns. Here, we choose n to such that $\frac{n-1}{4}$ is a non-negative integer. Of the new columns introduced, n-1 of them will be incorporated as data qubits while the remaining n columns will be used as ancillae in the encryption. An encoding quantum circuit $U = U_1 \otimes \cdots \otimes U_{r+t}$ is applied row-wise on the first n columns. Applying U spreads the quantum input from just the first column to the first n columns. Since every qubit not residing on the first column is maximally mixed, the encoding circuit on each row encodes the quantum data on the first column into a random quantum code, the resultant quantum information of which resides in a random codespace on the first ncolumns. Encryption is then achieved via randomly permuting the 2n columns with a permutation κ . Permuting the columns brings the quantum information to be processed from the first *n* columns to the columns k_1, \ldots, k_n , where $1 \leq k_1 < \cdots < k_n \leq 2n$. For the decryption algorithm, one performs the inverse permutation κ^{-1} of the columns, followed by the inverse unitary U^{\dagger} on the first n columns of the grid. Finally every qubit in the rows r+1 to r+t are measured in the computation basis. The quantum output of our scheme is then located on the first r rows of the first column of our grid of qubits.

To evaluate the circuit, the evaluator operates independently and identically (i.i.d) on not n but 2n columns of qubits, n columns of which are the maximally mixed state. The i.i.d structure of the evaluator's operations allows these operations to commute with any secret permutation of the columns of the qubits on the grid. In addition, the evaluators' operations necessarily leave



FIG. 2: Figure shows the encoding quantum circuit U_x that is applied on the first *n* qubits in the *x*-th row. Each line represents one qubit and the gates are applied in the order from left to right.

the n columns of qubits initialized in the maximally mixed state unchanged, thereby implementing i.i.d quantum operations on only the columns containing the encoded quantum data. Hence the evaluator, by applying transversal gates on the 2n columns, achieves the application of the corresponding transversal gates on the ncolumns with the quantum data without requiring knowledge of the location of the columns containing the encoded quantum information.

The circuit to be evaluated can always be written as $V = V_d \dots V_1$, where the evaluator is to apply privacy homomorphisms of the gates V_1 to V_d sequentially. Here, each V_i applies either a Clifford gate or a T gate locally on a single qubit, or applies a CNOT locally on a pair of qubits.

When V_i is a unitary operation that applies a Clifford gate G locally on the x-th qubit, the evaluator can apply the logical G-gate on our random code on the x-th row without any knowledge of the data columns k_1, \ldots, k_n . To do so, the evaluator simply applies the unitary $G^{\otimes 2n}$ on the 2n qubits located on the x-th row on each copy. Since any unitary operation leaves a maximally mixed qubit state unchanged, the evaluator effectively only applies the unitary $G^{\otimes n}$ on the qubits in the encrypted data columns k_1, \ldots, k_n on the x-th row, which is the logical G-gate on the x-th row.

When V_i is a unitary operation that applies a CNOT gate with control on the x-th qubit and target on the y-th qubit, denoted as $CNOT_{x,y}$, the evaluator can also apply the corresponding logical CNOT gate on our random code on the x-th and y-th row without any knowledge of the data columns k_1, \ldots, k_n . To do so, the evaluator simply applies a CNOT with control qubit on the x-th row and the *j*-th column and target qubit on the *y*-th row and the *j*-th column for every j = 1, ..., 2n. Since any unitary operation on two qubits leaves a maximally mixed two-qubit state unchanged, the evaluator effectively only applies the unitary $CNOT^{\otimes n}$ on the qubits in the encrypted data columns k_1, \ldots, k_n with control qubits on the x-th row and target qubits on the y-th row, which is the correct logical CNOT-gate, which we denote as $\overline{\text{CNOT}}_{x,y}$.

When V_i is a unitary operation that applies the kth non-Clifford gate T on the x-th qubit, the evaluator has to perform gate teleportation [15, 16]. Now consider gate teleportation of a single-qubit gate T. Omitting the correction operation required by gate teleportation allows this procedure to succeed with probability $\frac{1}{2}$ as depicted in Figure 3. The required measurement can be deferred until decryption due to the principle of deferred measurement [17].

To implement gate teleportation of the logical T operation, the evaluator applies privacy homomorphism for $\text{CNOT}_{x,r+k}$ followed by the privacy homomorphism for $\text{CNOT}_{r+k,x}$. Because of the ancilla columns being in the maximally mixed state, the unitary $\overline{\text{CNOT}}_{x,r+k}$ followed by the the unitary $\overline{\text{CNOT}}_{r+k,x}$ are effectively applied on the data columns k_1, \ldots, k_n .

$$\begin{array}{c} TH|0\rangle & \fbox{Z meas} \\ |\psi\rangle & \fbox{T}|\psi\rangle \text{ with probability } \end{array}$$

FIG. 3: Gate teleportation of the T-gate without correction.

Our scheme satisfies the correctness and compactness condition of Broadbent and Stacey. Each copy of our scheme yields the correct quantum output with constant probability 2^{-t} . Extra copies simply amplify the probability of success. Thus although each instance of our scheme implements T non-deterministically, it can be said to have *heralded* perfect completeness: namely, $b = \lfloor \sqrt{\frac{\alpha}{2}} + 1 \rfloor^2 2^{2t}$ copies of our scheme yields the correct output in at least one copy with probability at least $1 - e^{-\alpha}$, and we know which of the b copies yield the correct output. An arbitrarily large α brings the success probability arbitrarily close to unity. Since t, b are constant, and the total number of gates required for decryption is independent of the depth of the circuit to be evaluated. Hence, our scheme is compact for circuits with a constant maximum number of T gates and unbounded Clifford gates.

Randomly permuting the columns of qubits obfuscates the subset of columns where the quantum information resides, thereby encrypting the quantum data. The maximum trace distance between any two outputs is exponentially suppressed in n, with value at most $e\left(\frac{4n}{\pi}\right)^{1/4} 4^{b(r+t)}2^{-n}$, which is exponentially suppressed in n for constant r and t. For full details, see Ref. [18].

This material is based on research supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01. JFF and ST acknowledges support from the Air Force Office of Scientific Research under AOARD grant FA2386-15-1-4082.

- R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations* of secure computation, vol. 4, no. 11, pp. 169–180, 1978.
- [2] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-first Annual ACM* Symposium on Theory of Computing, STOC '09, (New York, NY, USA), pp. 169–178, ACM, 2009.
- [3] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in Advances in cryptology-EUROCRYPT 2010, pp. 24–43, Springer, 2010.
- [4] C. Gentry, S. Halevi, and N. Smart, "Fully homomorphic encryption with polylog overhead," in Advances in Cryptology EUROCRYPT 2012 (D. Pointcheval and T. Johansson, eds.), vol. 7237 of Lecture Notes in Computer Science, pp. 465–482, Springer Berlin Heidelberg, 2012.
- [5] M. Liang, "Symmetric quantum fully homomorphic encryption with perfect security," *Quantum Information Processing*, vol. 12, no. 12, pp. 3675–3687, 2013.
- [6] M. Liang, "Quantum fully homomorphic encryption scheme based on universal quantum circuit," *Quantum Information Processing*, pp. 1–11, 2015.
- [7] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, "Quantum computing on encrypted data," *Nat. Commun.*, vol. 5, 01 2014.
- [8] A. M. Childs, "Secure assisted quantum computation," Quantum Info. Comput., vol. 5, pp. 456–466, Sept. 2005.
- [9] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, "Quantum walks with encrypted data," *Phys. Rev. Lett.*, vol. 109, p. 150501, Oct 2012.
- [10] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, "A quantum approach to fully homomorphic encryption," arXiv prnote arXiv:1411.5254, 2014.
- [11] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low *T*-gate complexity," arXiv prnote arXiv:1412.8766, 2014.
- [12] Y. Dulek, C. Schaffner, and F. Speelman, "Quantum homomorphic encryption for polynomial-sized circuits," 2016. arXiv:1603.09717v1.
- [13] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on, pp. 517–526, Oct 2009.
- [14] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Limitations on information-theoretically-secure quantum homomorphic encryption," *Phys. Rev. A*, vol. 90, p. 050303, Nov 2014.
- [15] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390–393, 1999.
- [16] X. Zhou, D. W. Leung, and I. L. Chuang, "Methodology for quantum logic gate construction," *Phys. Rev. A*, vol. 62, p. 052316, Oct 2000.
- [17] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, second ed., 2000.
- [18] Y. Ouyang, S.-H. Tan, and J. Fitzsimons, "Quantum homomorphic encryption from quantum codes," arXiv preprint arXiv:1508.00938, 2015.

^{*} Electronic address: vingkai_ouvang@sutd.edu.sg

Quantum information approach to Bose-Einstein condensation of composite bosons

Su-Yong Lee^{1 2 *} Jayne Thompson² Sadegh Raeisi^{3 2} Paweł Kurzyński^{4 2} Dagomir Kaszlikowski^{2 5} Jaewan Kim¹

¹ School of Computational Sciences, Korea Institute for Advanced Study, Hoegi-ro 85, Dongdaemun-gu, Seoul 02455, Korea

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

Singapore

 3 Institute for Theoretical Physics II, Friedrich-Alexander-Universitt Erlangen-Nrnberg

⁴ Faculty of Physics, Adam Mickiewicz University, Umultowska 85, 61-614 Poznań, Poland

⁵ Department of Physics, National University of Singapore, 2 Science Drive 3, 117542 Singapore, Singapore

Abstract. We consider composite bosons (cobosons) comprised of two elementary particles, fermions or bosons, in an entangled state. First, we show that the effective number of cobosons implies the level of correlation between the two constituent particles. For the maximum level of correlation, the effective number of cobosons is the same as the total number of cobosons, which can exhibit the original Bose-Einstein condensation (BEC). In this context, we study a model of BEC for indistinguishable cobosons with a controllable parameter, i.e., entanglement between the two constituent particles. Furthermore we consider its application in entanglement of macroscopic states.

Keywords: BoseEinstein condensation, composite boson, entanglement, macroscopic state

We consider a simple model of BEC with composite bosonic particles. In particular, we assume that neither the composite particles nor their constituents interact, such that the internal structure of composite particles is stable and temperature independent.

Of course, the bound states between constituent particles have to result from their interaction. However, here we assume that once the constituents form a composite particle state, they do not interact anymore. Physically, this may correspond to a dilute gas of composite particles for which energy scales of a binding interaction potential between constituents are much greater than energy scales of the confining trap. As an example, one may think of an atomic hydrogen gas in which ionization temperature is much higher than the standard temperatures required to obtain BEC. Such a simplified model allows us to focus on the fundamental problem of how BEC depends on the internal state of composite particles, while neglecting other physical properties.

Imagine a pair of distinguishable fermionic or bosonic particles. The system is described by the creation operators \hat{a}_k^{\dagger} and \hat{b}_l^{\dagger} , where the indices $k, l = 0, 1, \ldots, \infty$ label different modes that can be occupied by the two particles. These modes can, for example, correspond to different energy/momentum states. The wave function of the system is of the form

$$\sum_{k,l=0}^{\infty} \alpha_{k,l} \hat{a}_k^{\dagger} \hat{b}_l^{\dagger} |0\rangle, \qquad (1)$$

where $\alpha_{k,l}$ is the probability amplitude that particle a is in mode k and particle b is in mode l, and $|0\rangle$ is the vacuum state. Using insights from entanglement theory,

the mathematical procedure known as the Schmidt decomposition allows us to rewrite the above state as [1]

$$\sum_{m=0}^{\infty} \sqrt{\lambda_m} \hat{a}_m^{\dagger} \hat{b}_m^{\dagger} |0\rangle \equiv \hat{c}^{\dagger} |0\rangle, \qquad (2)$$

where the modes labeled by m are superpositions of the previous modes k and l and $\sqrt{\lambda_m}$ are probability amplitudes that both particles occupy mode m. Note that despite the fact that \hat{a}^{\dagger}_m and \hat{b}^{\dagger}_m share the same label, physically these modes might be totally different. What is important is that, the modes labeled by m give rise to the internal structure of a composite particle.

We introduce a composite boson creation operator \hat{c}^{\dagger} , that creates a pair of particles. Note that this operator resembles the one for Cooper pairs [2]. The entanglement between particles is encoded in the amplitudes $\sqrt{\lambda_m}$. In particular, one can introduce a measure of entanglement known as *purity*

$$P = \sum_{m=0}^{\infty} \lambda_m^2, \quad 0 < P \le 1.$$
(3)

For P = 1 the particles are disentangled, whereas in the limit $P \rightarrow 0$ the entanglement between particles goes to infinity. The degree of entanglement can be also expressed via the so called Schmidt number K = 1/P. Intuitively, K estimates the average number of modes that are taken into account in the internal structure of a composite boson.

The bosonic properties of \hat{c}^{\dagger} can be studied in many ways. For example, the commutation relation gives $[\hat{c}, \hat{c}^{\dagger}] = 1 + \xi \sum \lambda_m (\hat{a}_m^{\dagger} \hat{a}_m + \hat{b}_m^{\dagger} \hat{b}_m)$, where $\xi = -1$ if *a* and *b* are fermions, or $\xi = +1$ if they are bosons. On the other hand, following the approach in [1] one may

^{*}papercrane79@kias.re.kr

study the ladder properties of this operator

$$|n\rangle \equiv \chi_n^{-1/2} \frac{(\hat{c}^{\top})^n}{\sqrt{n!}} |0\rangle,$$

$$\hat{c}|n\rangle = \sqrt{\frac{\chi_n}{\chi_{n-1}}} \sqrt{n} |n-1\rangle + |\epsilon_n\rangle, \ \langle n-1|\epsilon_n\rangle = 0,$$

$$\langle \epsilon_n |\epsilon_n\rangle = 1 - n \frac{\chi_n}{\chi_{n-1}} + (n-1) \frac{\chi_{n+1}}{\chi_n},$$
(4)

where $|n\rangle$ are states of n composite bosons, parameters χ_n are normalization factors, such that $\langle n|n\rangle = 1$, and $|\epsilon_n\rangle$ are unnormalized states that can result from subtracting a single composite particle from a state $|n\rangle$. The states $|\epsilon_n\rangle$ do not correspond to n-1 composite bosons of the same type, but rather to a complicated state of n-1 pairs of particles a and b. The ladder structure of operators \hat{c}^{\dagger} and \hat{c} starts to approach those of ideal bosons if $\frac{\chi_{n+1}}{2} \to 1$ for all n.

To simplify our model, we assume BEC in Gaussian states which are represented by a combination of coherent, thermal, and squeezed states. Assuming that composite bosons are in a thermal state or in a harmonic trap, we can describe the composite bosons with a Gaussian state. Thus, the Gaussian formula of the composite bosons is represented by the following modified operator that is based on the one studied in [1]

$$\hat{c}_{r}^{\dagger} = \sum_{m=0}^{\infty} \sqrt{(1-x)x^{m}} \hat{a}_{m,r}^{\dagger} \hat{b}_{m,r}^{\dagger}, \qquad (5)$$

where the double indices refer to internal (m) and to external degrees of freedom (r). The internal index mmay represent their position values. In our case r labels the energy levels of the trap in which the BEC takes place. Moreover, as we assumed in the beginning, the internal structure parameters $\lambda_m = (1-x)x^m$ (for $0 \le x < 1$) are independent of r. The internal structure parameter λ_m is equivalent to the coefficient of a two-mode squeezed vacuum (TMSV) state, $|TMSV\rangle = \sum_{m=0}^{\infty} \sqrt{(1-r)r^m} |m\rangle_a |m\rangle_b$, which is a typical two-mode Gaussian state. The above operator has desirable properties, since it is possible to analytically evaluate the factors χ_n and one can control the entanglement between constituents a and b via the parameter x [1]. For x = 0 the system is separable and in the limit $x \to 1$ entanglement goes to infinity. In addition

$$0 \le \left(\frac{\chi_{n+1}}{\chi_n}\right)_F = \frac{x^n(n+1)(1-x)}{(1-x^{n+1})} < 1 \tag{6}$$

for a pair of fermions [1] and

$$1 < \left(\frac{\chi_{n+1}}{\chi_n}\right)_B = \frac{(n+1)(1-x)}{(1-x^{n+1})} \le n+1 \tag{7}$$

for a pair of bosons [1].

It is known that the effective number of cobosons is related to the level of correlation between the two constituent particles. For the maximum level of correlation, the effective number of cobosons is the same as the total number of cobosons. For the weak level of correlation, the effective number of cobosons is smaller (larger) than the total number of cobosons while each constituent fermion (boson) exhibits its own property.

We showed how much the coboson BEC deviates from the behavior of a BEC comprised of ideal bosons, using a controllable parameter, i.e., entanglement between the two constituent particles. We specifically considered bi-fermions trapped in a 3D isotropic harmonic system. By the Pauli exclusion principle between bi-fermions, we found that the effective number of bi-fermions can be smaller than the total number of bi-fermions, regardless of system. Thus we demonstrated that the effective number of bi-fermions in the ground state increases with the degree of entanglement between a pair of fermions. Correspondingly, we found that the transition temperature for the 3D isotropic harmonic system, i.e., the temperature at which all the bi-fermions moved to the excited states, increased with increasing entanglement.

Moreover, we discussed coboson BEC, where each coboson is a bi-boson. Due to the bunching effect from each constituent boson, the effective number of bi-bosons can be greater than the total number of bi-bosons. Thus it was shown that the effective number of bi-bosons in the ground state decreases with the degree of entanglement between a pair of bosons. Correspondingly, the transition temperature for the 3D isotropic harmonic system decreased with increasing entanglement. When the entanglement between a pair of bosons becomes sufficiently small, the bi-boson pairs are dissociated, increasing the bunching effect in the effective number of bi-bosons. Consequently the coboson operator is represented by the direct product of each component field operator.

All the details are given in Ref. [3]. Furthermore, we show that BEC of composite bosons can be applied to quantum indistinguishability using macroscopic states [4].

Acknowledgments This research was partly supported by the IT R&D program of MOTIE/KEIT [1004346 (2012)].

- C.K. Law. Quantum entanglement as an interpretation of bosonic character in composite two-particle systems. *Phys. Rev. A* 71; 034306, 2005.
- [2] M. Combescot. "Commutator formalism" for pairs correlated through Schmidt decomposition as used in Quantum Information. *Europhys. Lett.* 96; 60002, 2011.
- [3] S.-Y. Lee, J. Thompson, S. Raeisi, P. Kurzynski, and D. Kaszlikowski. Quantum information approach to BoseEinstein condensation of composite bosons. *New J. Phys.*, 17; 113015, 2015.
- [4] S.-Y. Lee, C.-W. Lee, P. Kurzynski, D. Kaszlikowski, and J. Kim. Duality in entanglement of macroscopic states of light. arXiv :1606.01613.

Quantum key distribution without monitoring signal disturbance by using heralded pair-coherent sources

Le Wang¹ Shengmei Zhao¹ *

¹ Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications(NUPT), Nanjing 210003, China

Abstract. Recently, a new type of quantum key distribution (QKD) without monitoring signal disturbance, named the round-robin differential-phase-shift (RRDPS) QKD, was proposed. However, the current RRDPS-QKD schemes with the weak coherent pulses (WCPs) have low key generation rates and short transmission distances due to the vacuum component of sources of these schemes are significant large. In this paper, we propose to implement the heralded pair-coherent source into the RRDPS-QKD scheme to provide a longer transmission distance comparing with the scheme with WCPs.

Keywords: Round-robin differential-phase-shift quantum key distribution, Heralded pair-coherent sources, weak coherent pulses

1 Introduction

Quantum key distribution (QKD) allows two remote users, called Alice and Bob, to securely exchange cryptographic keys despite that in the presence of an eavesdropper (Eve), and it has been theoretically proved to be unconditionally secure. However, if there exists the disturbances caused by the imperfect quantum channel or eavesdroppers, the keys might not be identical or secure. Hence, it is essential to guarantee protection against the eavesdropping by monitoring the signal disturbances during the transmission of the quantum signals.

Recently, a new QKD scheme, named the round-robin differential phase-shift (RRDPS) QKD [1], was proposed, which does not need monitoring of disturbances to guarantee the security. Hence, the RRDPS-QKD could tolerate a high bit error rate, up to almost 50%, which is significantly higher than that of the traditional QKD schemes. Since the RRDPS-QKD was proposed, it has been studied from both theoretically [1,2] and experimentally [3,4]. However, the current RRDPS-QKD schemes with the weak coherent pulses (WCPs) have low key generation rate and short transmission distance due to the vacuum component of WCPs is significant large.

On the other hand, the heralded pair-coherent source (HPCS) can remove the shortcomings of the WCPs because the vacuum component of the HPCS is much lower than that of the WCPs. Hence, it shows excellent behaviors when the applications of the HPCS to the traditional QKD schemes [5,6]. In this paper, we propose to implement the HPCS into the RRDPS-QKD scheme. In addition, a tighter and more reasonable bound of the phase error rate proposed by [2] is adopted. By comparing the performances of the current RRDPS-QKD scheme with the WCPs, the transmission distance of the our scheme with HPCS is significantly longer than that of the current scheme with WCPs.

2 The RRDPS-QKD scheme with HPCS

The schematic diagram of the RRDPS-QKD with the HPCS is shown in Fig.1, and the proposed scheme runs as follows:



Figure 1: A schematic diagram of the RRDPS-QKD with the HPCS. PCS: pair-coherent source. ATT: attenuator. PM: phase modulator. BS: beam splitter. RNG: random number generator.

Step 1: Alice employs the HPCS to generate a series of pulse trains, where each pulse train contains L pulses. The HPCS is realized by the photon-heralding technique on the pair-coherent source (PCS) [7] that uses one mode of a two-mode correlated coherent state from the PCS as a trigger to encode the behavior of the other mode and the other mode as a carrier to transmit the quantum signals to Bob. Then Alice generates a random L-bit sequence, s_1, s_2, \dots, s_L , where $s_i \in \{0, 1\}$ by a random number generator (RNG). Subsequently, Alice encodes the random L-bit sequence into the phase of the L-pulse train, 0 according by $s_i = 0$ or π according by $s_i = 1$, by a phase modulator (PM).

Step 2: Alice uses an attenuator (ATT) to attenuate the pulse trains into the signals with the average intensity μ . Then, Alice sends the pulse trains to Bob through a quantum channel.

Step 3: Upon receiving an *L*-pulse train, Bob splits the pulse train into two pulse trains with a 50:50 beam splitter (BS). Then Bob shifts one of the pulse trains by *r* pulses with a Variable Delay, which is controlled by a RNG. The RNG is used to generate a number $r \in \{-L+1, \dots, -2, -1, 1, 2, \dots, L-1\}$.

Step 4: Bob measures the interference between two L-

^{*}zhaosm@njupt.edu.cn

pulse trains. If Bob obtains a detection result on position i and j in the unshifted pulse train and the shifted pulse train, respectively, where i and j satisfy $j = i \pm r \pmod{L}$, Bob records a key bit s_A according to the relative phase $s_B = s_i \oplus s_j$. Otherwise, Bob regards the transmission as a failure.

Step 5: Bob announces the indices $\{i, j\}$ to Alice through a classic channel, and Alice could compute $s_A = s_i \oplus s_j$ to obtain a sifted key s_A .

By using the photon-heralding technique on the PCS, one mode of the PCS can be locally triggered and used to encode the behavior of the other mode. Then the *n*photon number probability of the encoded pulse can be expressed as [5,6]

$$P_n(\mu) = \frac{1}{\sqrt{I_0(2\mu)}} \frac{\mu^{2n}}{(n!)^2} [1 - (1 - \eta_A)^n + d_A], \quad (1)$$

where μ is the average intensity of the pulses, $I_0(x)$ is the modified Bessel's function of the first kind, η_A and d_A represent the detection efficiency and the dark count rate of the triggering detector of Alice, respectively.

The key generation rate per pulse for the proposed scheme can be written as the following [2]

$$R = \frac{1}{L}Q_{L\mu}[1 - fH(e_{bit}) - H_{PA}],$$
 (2)

where $Q_{L\mu}$ is the overall gain when the average intensity of the pulse trains is $L\mu$, f denotes the efficiency of the error correction, and $H(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is a binary Shannon entropy. e_{bit} is the bit error rate and H_{PA} is the ratio of the key rate loss in the privacy amplification.

3 Results discussion

In this section, we discuss the performance of the proposed protocol by numerical simulations.

Fig.2 shows the key generation rate performance of the RRDPS-QKD with the HPCS against the transmission distance, in comparison with that of the RRDPS-QKD with the WCPs with the same experimental parameters [2] when L = 32, $\eta_A = 75\%$ and $d_A = 5 \times 10^{-8}$. The results show that the key generation rate performance of proposed scheme is much better than that of the current scheme with the WCPs. The transmission distance of the our scheme with HPCS is significantly longer than that of the current scheme with WCPs. That is because the vacuum component of the HPCS is significant lower than that of the WCPs.

In this paper, we have presented to implement the HPCS into the RRDPS-QKD scheme. In addition, a tighter and more reasonable bound of the phase error rate proposed by is adopted. It has been shown that the transmission distance of the our scheme with HPCS is significantly longer than that of the current scheme with WCPs.



Figure 2: The key generation rate performance of the RRDPS-QKD with the HPCS against the transmission distance, in comparison with that of the RRDPS-QKD with the WCPs.

- T. Sasaki et. al. Practical quantum key distribution protocol without monitoring signal disturbance. Nature, 509, 475, 2014.
- [2] Z. Zhang et. al. Round-robin differential-phase-shift quantum key distribution. arXiv, 1505.02481.
- [3] J. Y. Guan et. al. Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution. *Phys. Rev. Lett.*, 114, 180502, 2015.
- [4] H. Takesue et. al. Experimental quantum key distribution without monitoring signal disturbance. Nat. Photonics, 9, 827-831, 2015.
- [5] S. L. Zhang et. al. A universal coherent source quantum key distribution. *Chin. Sci. Bull.*, 54, 1863-1871, 2009.
- [6] F. Zhu et. al. Enhancing the performance of the measurement-device-independent quantum key distribution with heralded pair-coherent sources. *Phys. Lett. A*, 380, 1408-1413, 2016.
- [7] G. S. Agarwal et. al. Generation of pair coherent states and squeezing via the competition of four-wave mixing and amplified spontaneous emission. *Phys. Rev. Lett.*, 57, 827, 1986.

Spin blockade of Heavy-Holes in Double Quantum Dots

Jo-Tzu Hung,¹ * Bin Wang,¹ ² Alexander R. Hamilton,¹

Dimitrie Culcer¹

¹School of Physics, The University of New South Wales, Sydney NSW 2052, Australia ²University of Science and Technology of China, Hefei, Anhui, 230026, China

Abstract. Spin-orbit interaction plays a crucial role in manipulating hole-spin qubits, and its coupling strength may be extracted from Pauli spin blockade. We investigate Pauli spin blockade for two heavy holes in a double quantum dot in an in-plane magnetic field. We include relevant spin-orbit interactions as well as complex Zeeman interaction, and calculate blockade leakage as a function of the in-plane field strength and direction. The leakage is anisotropic in the in-plane field direction. We further compare the spin-orbit coupling strength by extracting the relation between the leakage current and the field strength.

Keywords: spin qubit, quantum dot, hole, spin blockade

1 Lower-dimensional hole system

Holes, often symbolized as an alternate representation of electrons in the valence band, have the effective spin $J = \frac{3}{2}$ [see Fig. 1(a).] Owing to the atomic *p*-orbital, holes suffer from less spin-spin coupling to the nuclei and is expected to have a strong spin-orbit (SO) interaction[1]. Hole qubits then promise a less noisier magnetic environment and a purely electric control due to the strong SO mixture in the hole qubit [see Fig. 1(b).]

The $J = \frac{3}{2}$ Hilbert space comprises a heavy hole (HH) with a secondary quantum number $m_J = \pm \frac{3}{2}$ and a light hole (LH) with $m_J = \pm \frac{1}{2}$. For two-dimensional holes, when the HH-LH splitting is relatively large, the HH and LH states can be considered weakly coupled, and one may perform a unitary rotation to block-diagonalize the $J = \frac{3}{2}$ matrix[2]. In gated QDs, the ground state usually have a strong HH character and can be treated as a pseudospin.



Figure 1: (a) The effective spin of bulk conduction band (CB) and valence band (VB) with $J = \frac{1}{2} \oplus 1$. The red and blue curves correspond to the HH and LH. (b) Both the logicals $|\uparrow\rangle$ and $|\downarrow\rangle$ in a HH are an strong SO mixture and can be driven by electric control E(t). (c) PSB in a two-HH double QD. Practically, the spin of the left HH is unknown. PSB is often employed in quantum computing because it permits spin-selective charge readouts.

2 Spin-orbit lifted Pauli spin blockade

We theoretically investigate hole SO interaction by studying Pauli spin blockade [PSB, see Fig. 1(c)] of two HHs confined by coupled QDs in a magnetic field $\mathbf{B} = B(\cos\theta, \sin\theta, 0)$. θ is measured from the x axis.

We adapt the Pauli matrices $\vec{\sigma}$ to describe a HH pseudospin. The in-plane Zeeman interaction is given by $\hat{H}_Z = \hat{H}_{Zq} + \hat{H}_{[001]} + \hat{H}_{Zc}$, where $\hat{H}_{Zq} = -\frac{3}{2}q\mu_B B(e^{i\theta}\sigma_+ + e^{-i\theta}\sigma_-)$, and $\hat{H}_{[001]} = \frac{-f}{\hbar^2}\mu_B B(e^{-i\theta}\sigma_+p_-^2 + e^{i\theta}\sigma_-p_+^2)$ and $\hat{H}_{Zc} = F(\mu_B B)^3(e^{-3i\theta}\sigma_+ + e^{3i\theta}\sigma_-)$, with $\sigma_{\pm} = \frac{1}{2}(\sigma_x \pm i\sigma_y)$ and p_{\pm} being the raising (lower) operator of the spatial momentum. μ_B denotes the Bohr magneton, q is a dimensionless, material-dependent quantity, and both of f and F are subject to the dot confinement. The SO interaction $\hat{H}_{SO} = \hat{H}_R + \hat{H}_D$ includes Rashba and Dresselhaus couplings, with $\hat{H}_R = i\alpha(\sigma_+p_-^3 - \sigma_-p_+^3)$ and $\hat{H}_D = -\beta_3(\sigma_+p_-p_+p_-+\sigma_-p_+p_-p_+) - \beta_1(\sigma_+p_-+\sigma_-p_+)$.

Figure 1(c) shows a HH PSB from (1, 1) to (0, 2), where (N_L, N_R) labels the number of HHs on the left and right. The two dots are coupled by a spin-perserving coupling t_0 , and the lowest energy state is $|S_{02}\rangle$, a (0, 2) singlet. Due to the Pauli exclusion principle, the left spin, if it is parallel to the right spin, will be blocked. In the presence of the SO interaction, such PSB may be lifted[3].



Figure 2: Individual DQD spin splittings (a) $2|E_Z(B)|$ with the dot radius $R_0 = 30$ nm and (b) $2|E_Z(R_0)|$ at B = 0.1 T, due to \hat{H}_{Zq} , $\hat{H}_{[001]}$ and \hat{H}_{Zc} , respectively.

We denote by $|S_{11}\rangle$ the (1,1) singlet and by $|T_0\rangle$ the

^{*}jo-tzu.hung@unsw.edu.au

Table 1: The θ -dependent $\Delta_+(\theta)$ and $\Delta_0(\theta)$, with $t_{R(D)} \equiv \langle S_{02} | \hat{H}_{R(D)} | \downarrow \downarrow \rangle$ being the Rashba (Dresselhaus) coupling parameter.



Figure 3: Individual PSB leakage currents $I(\theta)$ at B = 1T when (a) only the *B*-linear terms in \hat{H}_Z are included, and when (b) only \hat{H}_{Zc} is included. The oscillation period in (b) is three times more than that in (a). *e* is the elementary charge, and we set the (1, 1) relaxation rate $\Gamma_0 = 3$ MHz and $t_R = 0.3t_0 \gg t_D$. $t_0 = 200 \ \mu\text{eV}$.

(1,1) unpolarized triplet, and by $|T_{\pm}\rangle$ the (1,1) polarized triplet. In the basis $\{S_{02}, M, M_{\perp}, T_{+}, T_{-}\}$, the effective tunneling Hamiltonian reads

$$\hat{H} = \begin{bmatrix} 0 & 0 & N_M(\theta) & \Delta_+(\theta) & -\Delta_+(\theta) \\ 0 & 0 & 0 & 0 & 0 \\ N_M(\theta) & 0 & 0 & 0 & 0 \\ \Delta_+^*(\theta) & 0 & 0 & E_Z & 0 \\ -\Delta_+^*(\theta) & 0 & 0 & 0 & -E_Z \end{bmatrix},$$
(1)

Here we have used the superpositions of $|S_{11}\rangle$ and $|T_0\rangle$: $|M\rangle \equiv \frac{1}{N_M} [\Delta_0(\theta) |S_{11}\rangle - t_0 |T_0\rangle]$ and $|M_{\perp}\rangle = \frac{1}{N_M} (t_0 |S_{11}\rangle + \Delta_0^*(\theta) |T_0\rangle)$ with $N_M = \sqrt{t_0^2 + |\Delta_0(\theta)|^2}$. The in-plane Zeeman terms split the triplet by E_Z , whereas $\Delta_+(\theta)$ and $\Delta_0(\theta)$ correspond to the SO tunneling element between $|T_{\pm}\rangle$ and $|S_{02}\rangle$, and between $|T_0\rangle$ and $|S_{02}\rangle$. We list $\Delta_+(\theta)$ and $\Delta_0(\theta)$ in Table 1 by considering individual Zeeman terms.

3 Main Results

We diagonalize Eq. (1) and calculate the PSB leakage by solving the steady-state kinetic equations: $-\sum_{\sigma} W_{k\sigma} P_k - \sum_{k' \neq k} \Gamma_k P_k + \sum_{k' \neq k} \Gamma_{k'} P_{k'} + \sum_{\sigma} U_{\sigma k} P_{\sigma} = 0$ and $-\sum_k U_{\sigma k} P_{\sigma} + \sum_k W_{k\sigma} P_k = 0$. Here P_k and P_{σ} correspond to the probabilities in the eigenstate $|k\rangle$ and in (0,1) with the spin σ . $W_{k\sigma}$ $(U_{\sigma k})$ denotes the transition rate from $|k\rangle$ $[(0,1)_{\sigma}]$ to $(0,1)_{\sigma}$ $(|k\rangle)$, and Γ_k is the (1,1) relaxation rate out of $|k\rangle$.

Figure 2 shows individual spin splittings in a double QD due to the three terms in \hat{H}_Z . As expected, the two *B*-linear terms are significant at low and intermediate fields, whereas \hat{H}_{Zc} is dominating at large



Figure 4: Individual PSB leakage currents I(B) at $\theta = 0$ for (a) $t_R = 0.3t_0 \gg t_D$ and $(b)t_R = 0.6t_0 \gg t_D$.

fields. Figure 3 compares individual $I(\theta)$ at B = 1 T with a fixed SO coupling. The qualitative difference in $I(\theta)$ between the *B*-linear and *B*-cubic cases provides an indication of the power of the dominating in-plane Zeeman term in hole QDs. In Fig. 4, we find at low fields, where the *B*-linear terms dominates, the larger |dI/dB|, the stronger the SO coupling. To compare with electron PSB[4], we assume $t_R \ll t_0$ and $|E_Z| < t_0$, we obtain $I(B) \sim e\Gamma_{\rm DL}P_M E_Z^2 \gamma^2 / (E_Z^2 + \frac{t_0^4}{|\Delta_+|^2} \gamma^2)$, with Γ_{DL} the transition rate between the dot and lead, and $\gamma^2 = \Gamma_0/\Gamma_{DL}$.

4 Conclusion

We have found that (i) the $I(\theta)$ behavior suggests that the SO mixture in the hole qubit can be tuned by adjusting the field direction θ , and (ii) the slope of I(B) can be used in comparing the SO coupling strength.

Acknowledgement This work is supported by the ARC through the DP scheme.

- C. Kloeffel and D. Loss. Prospects for spin-based quantum computing in quantum dots Annu. Rev. Condens.Matter Phys. 4:51–81, 2013.
- [2] R. Winkler et al. Spin orientation of holes in quantum wells. Semicond. Sci. Technol. 23:114017, 2008.
- [3] R. Li et al. Pauli spin blockade of heavy holes in a silicon double quantum dot. *Nano Lett.*, 15:7314–7318, 2015; D. Q. Wang et al. Anisotropic Pauli spin blockade in GaAs double hole quantum dots. manuscript in preparation.
- [4] J. Danon and Y. V. Nazarov. Pauli spin blockade in the presence of strong spin-orbit coupling. *Phys. Rev.* B. 80:041301, 2009.
- [5] J. -T. Hung et al. Spin blockade of heavy holes in gate-defined quantum dots. manuscript in preparation.

Unified View of Quantum Correlations and Quantum Coherence

Kok Chuan Tan¹ *

Hyukjoon Kwon¹[†]

Chae-Yeun Park^{1 ‡}

Hyunseok Jeong^{1 §}

¹Center for Macroscopic Quantum Control, Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea

Abstract. We present arguments that quantum coherence in a bipartite system can be contained either locally or in the correlations between the subsystems. The portion of quantum coherence contained within correlations can be viewed as a kind of quantum correlation which we call correlated coherence. We demonstrate that the framework provided by correlated coherence allows us to retrieve the same sets of quantum correlations as defined by the asymmetric and symmetric versions of quantum discord as well as quantum entanglement, thus providing a unified interpretation of these correlations. We also prove that correlated coherence can be formulated as an entanglement monotone, thus demonstrating that entanglement may be viewed as a specialized form of coherence.

Keywords: Quantum Coherence, Quantum Correlations, Quantum Discord, Entanglement

1 Introduction

Following the quantitative theories of entanglement, Baumgratz et al. [2] recently proposed a resource theory of quantum coherence. They first postulate a set of axioms that a measure of quantum coherence should satisfy, and then went on to demonstrate that several intuitive measures of quantum coherence satisfy these properties. Recent developments have since uncovered interesting connections between quantum coherence and correlation, such as their interconversion with each other [3, 4] as well as trade-off relations [5]. At the same time, it is well known in quantum information theory that within quantum theory, the set of all possible correlations can be categorized either as "classical" or "quantum". Here, we provide some arguments [1] to suggest that the "quantumness" of quantum correlations can be interpreted in terms of the language of the resource theory of quantum coherence, thus providing a bridge between the two concepts.

2 Preliminaries

We will frequently refer to a bipartite quantum state which we denote ρ_{AB} , where A and B refer to local subsystems held by different laboratories. Following convention, we say the subsystems A and B are held by Alice and Bob respectively. The local state of Alice is obtained by performing a partial trace on ρ_{AB} , and is denoted by $\rho_A = \text{Tr}_B(\rho_{AB})$, and $\{|i\rangle_A\}$ is a complete local basis of Alice's system. Bob's local state and local basis are also similarly defined. In general, the systems Alice and Bob holds may be composite, such that $A = A_1 A_2 \cdots A_N$ and $B = B_1 B_2 \cdots B_M$ so the total state may identically be denoted by $\rho_{A_1 A_2 \cdots A_N B_1 B_2 \cdots B_M}$.

We will adopt the axiomatic approach for coherence measures as shown in Ref. [2]. For a fixed basis set $\{|i\rangle\}$, the set of incoherent states \mathcal{I} is the set of quantum states

with diagonal density matrices with respect to this basis. Then a reasonable measure of quantum coherence \mathcal{C} should satisfy following properties: (C1) $C(\rho) \geq 0$ for any quantum state ρ and equality holds if and only if $\rho \in \mathcal{I}$. (C2a) The measure is non-increasing under incoherent completely positive and trace preserving maps (ICPTP) Φ , i.e., $C(\rho) \geq C(\Phi(\rho))$. (C2b) Monotonicity for average coherence under selective outcomes of ICPTP: $C(\rho) \geq \sum_n p_n C(\rho_n)$, where $\rho_n = \hat{K}_n \rho \hat{K}_n^{\dagger} / p_n$ and $p_n = \text{Tr}\hat{K}_n \rho \hat{K}_n^{\dagger}$ for all \hat{K}_n with $\sum_n \hat{K}_n \hat{K}_n^{\dagger} = \mathbb{1}$ and $\hat{K}_n \mathcal{I} \hat{K}_n^{\dagger} \subseteq \mathcal{I}.$ (C3) Convexity, i.e. $\lambda C(\rho) + (1-\lambda)C(\sigma) \geq$ $C(\lambda \rho + (1 - \lambda)\sigma)$, for any density matrix ρ and σ with $0 \leq \lambda \leq 1$. Here, we will employ the l_1 -norm of coherence, which is defined by $\mathcal{C}(\rho) \coloneqq \sum_{i \neq j} |\langle i | \rho | j \rangle|$, for any given basis set $\{|i\rangle\}$ (otherwise called the reference basis). It can be shown that this definition satisfies all the properties mentioned [2].

3 Results

Consider a bipartite state ρ_{AB} , with total coherence $\mathcal{C}(\rho_{AB})$ with respect to local reference bases $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$. Then $\mathcal{C}(\rho_A)$ and $\mathcal{C}(\rho_B)$ can be interpreted as the coherence that is local to A and B respectively. In general, the sum of the total local coherences is not necessarily the same as the total coherence in the system. It is therefore reasonable to suppose that a portion of the quantum coherences are not stored locally, but within the correlations of the system itself. This motivates the following definition:

Definition 1 With respect to local reference bases $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$, the correlated coherence for a bipartite quantum system is the local coherences subtracted from the total coherence:

$$\mathcal{C}_{cc}\left(\rho_{AB}\right) \coloneqq \mathcal{C}\left(\rho_{AB}\right) - \mathcal{C}\left(\rho_{A}\right) - \mathcal{C}\left(\rho_{B}\right)$$

where ρ_A and ρ_B are the reduced density matrices of A and B respectively.

In general, the above quantity is basis dependent. However, it can be made a state dependent property by

^{*}bbtankc@gmail.com

[†]tera900@snu.ac.kr

[‡]kaeri@gmail.com

[§]h.jeong37@gmail.com
choosing the local basis to be the the local eigenbasis. For every bipartite state ρ_{AB} , the reduced density matrices ρ_A and ρ_B have eigenbases $\{|\alpha_i\rangle\}$ and $\{|\beta_i\rangle\}$, respectively. In the even of degeneracy, where multiple local eigenbases exists, we will choose the basis that minimizes the total coherence. By choosing these local bases, ρ_A and ρ_B are both diagonal so the local coherences are zero. The implication of this is that for such a choice, the coherence in the system is stored entirely within the correlations and the correlated coherence becomes a state dependent property. We will assume that this choice of local bases will always be made.

Correlated coherence has many interesting properties. For instance, the following theorems suggests that it can properly define the set of states with symmetric/asymmetric quantum discord or quantum entanglement:

Theorem 2 (Symmetric Quantum Discord) For a given state ρ_{AB} , $C_{cc}(\rho_{AB}) = 0$ iff $\rho_{AB} = \sum_{i,j} p_{i,j} |i\rangle_A \langle i| \otimes |j\rangle_B \langle j|.$

Theorem 3 (Asymmetric Quantum Discord)

For a given state ρ_{AB} , let $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ be the the eigenbases of ρ_A and ρ_B respectively. Define the measurement on A onto the local basis as $\Pi_A(\rho_{AB}) \coloneqq$ $\sum_i (|i\rangle_A \langle i| \otimes I_B) \rho_{AB}(|i\rangle_A \langle i| \otimes I_B)$. Then, with respect to these local bases, $C_{cc}(\rho_{AB}) - C_{cc}(\Pi_A(\rho_{AB})) = 0$ iff $\rho_{AB} = \sum_i p_i |i\rangle_A \langle i| \otimes \rho_B^i$, where ρ_B^i is some normalized density matrix and $\{|i\rangle_A\}$ is some set of orthonormal vectors.

Theorem 4 (Entanglement) Let $\rho_{AA'BB'}$ be some extension of a bipartite state ρ_{AB} and choose the local bases to be the eigenbases of $\rho_{AA'}$ and $\rho_{BB'}$ respectively. Then with respect to these local bases, $\min C_{cc} (\rho_{AA'BB'}) = 0$ iff $\rho_{AB} = \sum_i p_i |\alpha_i\rangle_A \langle \alpha_i| \otimes |\beta_i\rangle_B \langle \beta_i|$ for some set of normalized vectors $|\alpha_i\rangle$ and $|\beta_i\rangle$ that are not necessarily orthogonal and may repeat. The minimization is over all possible extensions of ρ_{AB} of the form $\rho_{AA'BB'}$.

The above results already suggest a non-trivial relationship between coherence and quantum correlations. This relationship can be pushed further. We also demonstrate that it is possible to construct a new entanglement monotone from the coherence measure, suggesting that entanglement itself is a specialized form of coherence. This new entanglement monotone is first constructed by considering what we call unitarily symmetric extensions:

Definition 5 (Unitarily Symmetric Extensions)

Let $\rho_{AA'BB'}$ be an extension of a bipartite state ρ_{AB} . The extension $\rho_{AA'BB'}$ is said to be unitarily symmetric if it remains invariant up to local unitary operations on AA' and BB' under a system swap between Alice and Bob.

More formally, let $\{|i\rangle_{AA'}\}$ and $\{|j\rangle_{BB'}\}$ be complete local bases on AA' and BB' respectively. Define the swap operator $U_{\text{swap}}|i,j\rangle_{AA'BB'} \coloneqq |j,i\rangle_{AA'BB'}$. Then $\rho_{AA'BB'}$ is unitarily symmetric if there exists local unitary operations $U_{AA'}$ and $U_{BB'}$ such that $U_{AA'} \otimes U_{BB'}$ ($U_{\text{swap}}\rho_{AA'BB'}U_{\text{swap}}^{\dagger}$) $U_{AA'}^{\dagger} \otimes U_{BB'}^{\dagger} = \rho_{AA'BB'}$. It is possible then to define our entanglement measure:

Definition 6 Let $\rho_{AA'BB'}$ be some unitarily symmetric extension of a bipartite state ρ_{AB} and choose the local bases to be the eigenbases of $\rho_{AA'}$ and $\rho_{BB'}$ respectively. Then the entanglement of coherence is defined to be:

$$E_{cc}(\rho_{AB}) \coloneqq \min \mathcal{C}_{cc} \left(\rho_{AA'BB'} \right)$$

The minimization is over all possible unitarily symmetric extensions of ρ_{AB} of the form $\rho_{AA'BB'}$.

From the above definition, it can then be shown that the above quantity satisfies the basic requirement of all entanglement measures:

Theorem 7 (Entanglement monotone) The entanglement of coherence E_{cc} is an entanglement monotone in the sense that it satisfies:

- *i.* $E_{cc}(\rho_{AB}) = 0$ iff $E_{cc}(\rho_{AB})$ is separable.
- ii. $E_{cc}(\rho_{AB})$ is invariant under local unitaries on A and B.
- iii. $E_{cc}(\rho_{AB}) \geq E_{cc}(\Lambda_{\text{LOCC}}(\rho_{AB}))$ for any LOCC procedure Λ_{LOCC} .

4 Conclusion

The framework of the correlated coherence allows us to identify the same non-classical correlations as those of (both symmetric and asymmetric) quantum discord and quantum entanglement. We also provide the first direct proof that entanglement can be viewed as a type of coherence by constructing an entanglement monotone through correlated coherence. The successful interpretation of quantum discord and entanglement in terms of the language of coherence suggests that tasks enabled by them actually derive their quantum advantage from a common source. This connection may eventually allow for the development of a new set of common tools in the treatment of various forms of quantum correlations and quantum coherence.

References

- K. C. Tan, H. Kwon, C.Y. Park and H. Jeong, arXiv. 1603.01958 (2016).
- [2] T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).
- [3] J. Ma, B. Yadin, D. Girolami, V. Vedral, and M. Gu, arXiv. 1510.06179 (2015).
- [4] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Phys. Rev. Lett. **115**, 020403 (2015).
- [5] Z. Xi, Y Li and H. Fan, Sci. Rep. 5, 10922 (2015).