Posters

August 31, 2023 (Thu.) [Poster Session III]

Entanglement witness and multipartite quantum state discrimination

Donghoon Ha[1] Jeong San Kim[1] *

[1] *Department of Applied Mathematics and Institute of Natural Sciences, Kyung Hee University, Yongin 17104, Republic of Korea*

Abstract. We consider multipartite quantum state discrimination and show that the minimum-error discrimination by separable measurements is closely related to the concept of entanglement witness. Based on the properties of entanglement witness, we establish some necessary and/or sufficient conditions on minimum-error discrimination by separable measurements. We also provide some conditions on the upper bound of the maximum success probability over all possible separable measurements. Our results are illustrated by examples of multidimensional multipartite quantum states. Finally, we provide a systematic way in terms of the entanglement witness to construct multipartite quantum state ensembles showing nonlocality in state discrimination.

Keywords: minimum-error discrimination, separable measurement, entanglement witness

Quantum state discrimination is one of the fundamental concepts used in various quantum information and computation theory [1–4]. In general, we can always perfectly discriminate orthogonal quantum states using appropriate measurement. However, nonorthogonal quantum states cannot be perfectly discriminated by means of any measurement. For this reason, various state discrimination strategies have been studied for optimal discrimination of nonorthogonal quantum states, such as minimum-error discrimination, unambiguous discrimination and maximum-confidence discrimination [5–9].

Entanglement witness(EW) is an important tool to detect the existence of entanglement inherent in a multipartite quantum state [10–13]. Mathematically, EW is a Hermitian operator having non-negative mean value for every separable state, but negative for some entangled states. As EW provides an useful methodology to detect entanglement that is an important quantum nonlocality, it is natural to ask whether EW can also be used to characterize other nonlocal phenomenon of multipartite quantum states.

Quantum nonlocal phenomenon also arises in discriminating multipartite quantum states; quantum nonlocality occurs when optimal state discrimination cannot be realized only by *local operations and classical communication*(LOCC) [14–17]. However, characterizing local discrimination of quantum states is a hard task and very little is known due to the lack of good mathematical structure for LOCC.

Here, we establish a specific relation between the properties of EW and separable measurements, a mathematically well-structured set of measurements having LOCC measurements as a special case [18]. We show that the minimum-error discrimination of multipartite quantum states using separable measurements strongly depends on the existence of EW. More precisely, we establish conditions on minimum-error discrimination by separable measurements in terms of EW. We also provide conditions on the upper bound of the maximum success probability over all possible separable measurements. We illustrate our results using examples of multidimensional multipartite quantum states. Finally, we provide a systematic way in terms of EW to construct multipartite quantum state ensembles showing nonlocality in state discrimination [18].

Let us consider the situation of discriminating n *multipartite* quantum states $\rho_1, \ldots, \rho_n$ in which the state ρ_i is prepared with the probability η_i. We denote this situation as an ensemble,

$$\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n. \tag{1}$$

We use $p_{\mathrm{G}}(\mathcal{E})$ to denote the optimal success probability in the minimum-error discrimination of $\mathcal{E}$, that is,

$$p_{\mathrm{G}}(\mathcal{E}) = \max_{\text{Measurement}} \sum_{i=1}^n \eta_i \mathrm{Tr}(\rho_i M_i). \tag{2}$$

When the available measurements are limited to separable measurements, we denote the maximum success probability by

$$p_{\mathrm{SEP}}(\mathcal{E}) = \max_{\substack{\text{Separable} \\ \text{measurement}}} \sum_{i=1}^n \eta_i \mathrm{Tr}(\rho_i M_i). \tag{3}$$

Similarly, we denote

$$p_{\mathrm{L}}(\mathcal{E}) = \max_{\substack{\text{LOCC} \\ \text{measurement}}} \sum_{i=1}^n \eta_i \mathrm{Tr}(\rho_i M_i). \tag{4}$$

From the definitions, we trivially have

$$p_{\mathrm{L}}(\mathcal{E}) \leqslant p_{\mathrm{SEP}}(\mathcal{E}) \leqslant p_{\mathrm{G}}(\mathcal{E}). \tag{5}$$

For a multipartite quantum state ensemble $\mathcal{E}$, we define $\mathbb{H}_{\mathrm{SEP}}(\mathcal{E})$ as

$$\begin{aligned} \mathbb{H}_{\mathrm{SEP}}(\mathcal{E}) = \{&H \in \mathbb{H} \,| \\ &H - \eta_i \rho_i \in \mathbb{SEP}^* \ \forall i = 1, \ldots, n\}, \end{aligned} \tag{6}$$

where $\mathbb{H}$ is the set of all Hermitian operators and $\mathbb{SEP}^*$ is the set of all block-positive operators. We further define

$$\begin{aligned} \mathbb{H}_{\mathrm{EW}}(\mathcal{E}) = \{&H \in \mathbb{H}_{\mathrm{SEP}}(\mathcal{E}) \,| \\ &H - \eta_j \rho_j \text{ is a EW for some } j \in \{1, \ldots, n\}\}. \end{aligned} \tag{7}$$

*freddie1@khu.ac.kr

Now, let us consider the minimum quantity

$$q_{\rm SEP}(\mathcal{E}) = \min_{H\in\mathbb{H}_{\rm SEP}(\mathcal{E})} {\rm Tr}H, \tag{8}$$

which is an upper bound of $p_{\rm SEP}(\mathcal{E})$ [19], that is,

$$p_{\rm SEP}(\mathcal{E}) \leqslant q_{\rm SEP}(\mathcal{E}). \tag{9}$$

Theorem 1 *For a multipartite quantum state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$,

$$p_{\rm SEP}(\mathcal{E}) = q_{\rm SEP}(\mathcal{E}). \tag{10}$$

For a given ensemble $\mathcal{E}$, the following theorem provides a necessary and sufficient condition for a separable measurement $\{M_i\}_{i=1}^n$ and $H \in \mathbb{H}_{\rm SEP}(\mathcal{E})$ to realize $p_{\rm SEP}(\mathcal{E})$ and $q_{\rm SEP}(\mathcal{E})$, respectively.

Theorem 2 *For a multipartite quantum state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$, *a separable measurement* $\{M_i\}_{i=1}^n$ *and* $H \in \mathbb{H}_{\rm SEP}(\mathcal{E})$, $\{M_i\}_{i=1}^n$ *realizes* $p_{\rm SEP}(\mathcal{E})$ *and* H *provides* $q_{\rm SEP}(\mathcal{E})$ *if and only if*

$${\rm Tr}[M_i(H - \eta_i\rho_i)] = 0 \quad \forall i = 1, \ldots, n. \tag{11}$$

We note that $H \in \mathbb{H}_{\rm SEP}(\mathcal{E})$ providing $q_{\rm SEP}(\mathcal{E})$ is generally not unique. However, the following corollary states the case that $H \in \mathbb{H}_{\rm SEP}(\mathcal{E})$ providing $q_{\rm SEP}(\mathcal{E})$ is unique.

Corollary 3 *For a multipartite quantum state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$, *we have*

$$p_{\rm SEP}(\mathcal{E}) = \eta_1, \tag{12}$$

if and only if

$$\eta_1\rho_1 - \eta_i\rho_i \in \mathbb{SEP}^* \quad \forall i = 2, \ldots, n. \tag{13}$$

In this case, $\eta_1\rho_1$ *is the only element of* $\mathbb{H}_{\rm SEP}(\mathcal{E})$ *providing* $q_{\rm SEP}(\mathcal{E})$.

When Eq. (12) of Corollary 3 holds, the maximum success probability $p_{\rm SEP}(\mathcal{E})$ can be achieved without the help of measurement, simply by guessing ρ_1 is prepared. The choice of ρ_1 in Corollary 3 can be arbitrary. That is, any of $\{\rho_i\}_{i=1}^n$ can be used to play the role of ρ_1 in Corollary 3.

For a given ensemble $\mathcal{E}$, the minimum-error discrimination can be realized by separable measurements if and only if

$$p_{\rm SEP}(\mathcal{E}) = p_{\rm G}(\mathcal{E}). \tag{14}$$

Theorem 4 *For a multipartite quantum state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$, *if there exists separable measurement* $\{M_i\}_{i=1}^n$ *satisfying*

$$\sum_{i=1}^n \eta_i\rho_i M_i \in \mathbb{H}_{\rm EW}(\mathcal{E}), \tag{15}$$

then

$$p_{\rm SEP}(\mathcal{E}) = \sum_{i=1}^n \eta_i {\rm Tr}(\rho_i M_i) < p_{\rm G}(\mathcal{E}). \tag{16}$$

Thus, non-existence of such separable measurement $\{M_i\}_{i=1}^n$ satisfying Condition (15) is a necessary condition for $p_{\rm SEP}(\mathcal{E}) = p_{\rm G}(\mathcal{E})$.

Example 1 *For any integers* $m, d \geqslant 2$, *let us consider the* m*-qudit state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^{d+2}$ *consisting of* $d+2$ *states,*

$$\begin{aligned}
&\eta_i = \frac{1}{d^m + d},\ \rho_i = |i-1\rangle\langle i-1|^{\otimes m},\ i = 1, \ldots, d,\\
&\eta_{d+1} = \frac{d^m - d}{d^m + d},\ \rho_{d+1} = \frac{1}{d^m - d}\Big(\mathbb{1} - \sum_{j=0}^{d-1} |j\rangle\langle j|^{\otimes m}\Big),\\
&\eta_{d+2} = \frac{d}{d^m + d},\ \rho_{d+2} = |\Phi\rangle\langle\Phi|,
\end{aligned} \tag{17}$$

where

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes m}. \tag{18}$$

For a separable measurement $\{M_i\}_{i=1}^{d+2}$ with

$$\begin{aligned}
&M_i = |i-1\rangle\langle i-1|^{\otimes m},\ i = 1, \ldots, d,\\
&M_{d+1} = \mathbb{1} - \sum_{j=0}^{d-1} |j\rangle\langle j|^{\otimes m},\ M_{d+2} = 0_{\mathbb{H}},
\end{aligned} \tag{19}$$

we show that Condition (15) holds with respect to the ensemble in Eq. (17). It is straightforward to verify that

$$\begin{aligned}
&\sum_{j=1}^{d+2} \eta_j\rho_j M_j - \eta_i\rho_i \succeq 0,\ \ i = 1, \ldots, d+1,\\
&\sum_{j=1}^{d+2} \eta_j\rho_j M_j - \eta_{d+2}\rho_{d+2} = \frac{1}{d^m + d}\big(\mathbb{1} - d\,|\Phi\rangle\langle\Phi|\,\big)\\
&\qquad\qquad \in \mathbb{SEP}^*.
\end{aligned} \tag{20}$$

Furthermore, a straightforward calculation leads us to

$$\langle\Phi|\left(\sum_{j=1}^{d+2} \eta_j\rho_j M_j - \eta_{d+2}\rho_{d+2}\right)|\Phi\rangle < 0. \tag{21}$$

Thus, Theorem 4 leads us to

$$p_{\rm SEP}(\mathcal{E}) = \sum_{i=1}^{d+2} \eta_i {\rm Tr}(\rho_i M_i) = \frac{d^m}{d^m + d} < p_{\rm G}(\mathcal{E}). \tag{22}$$

Theorem 5 *For a multipartite quantum state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$, $p_{\rm SEP}(\mathcal{E}) = p_{\rm G}(\mathcal{E})$ *if and only if there exists* $H \in \mathbb{H}_{\rm SEP}(\mathcal{E})$ *such that it provides* $q_{\rm SEP}(\mathcal{E})$ *but does not satisfy*

$$H \in \mathbb{H}_{\rm EW}(\mathcal{E}). \tag{23}$$

If $p_{\rm SEP}(\mathcal{E}) = p_{\rm G}(\mathcal{E})$, Theorem 5 implies that there must exist $H \in \mathbb{H}_{\rm SEP}(\mathcal{E}) \setminus \mathbb{H}_{\rm EW}(\mathcal{E})$ providing $q_{\rm SEP}(\mathcal{E})$. In this case, there possibly exists another Hermitian operator H' satisfying $H' \in \mathbb{H}_{\rm EW}(\mathcal{E})$ and ${\rm Tr}H' = q_{\rm SEP}(\mathcal{E})$.

Corollary 6 *For a multipartite quantum state ensemble* $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$ *with Condition* (13), $p_{\rm SEP}(\mathcal{E}) < p_{\rm G}(\mathcal{E})$ *if and only if there exists an EW in* $\{\eta_1\rho_1 - \eta_i\rho_i\}_{i=2}^n$.

Example 2 *For any integers $m, d \geqslant 2$, let us consider the m-qudit state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^{d+1}$ consisting of $d+1$ states,*

$$\begin{aligned} \eta_1 &= \frac{1}{2},\ \rho_1 = \frac{1}{d^m}\mathbb{1}, \\ \eta_i &= \frac{1}{2d},\ \rho_i = \frac{d^2-d}{d^m-d}\left|\Phi_i\right\rangle\!\left\langle\Phi_i\right| + \frac{d^m-d^2}{d^m(d^m-d)}\mathbb{1}, \\ & \qquad i = 2, \ldots, d+1, \end{aligned} \tag{24}$$

where

$$\left|\Phi_j\right\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\exp\left(\frac{\mathrm{i}2\pi jk}{d}\right)\left|k\right\rangle^{\otimes m}. \tag{25}$$

For each $i = 2, \ldots, d+1$, a straightforward calculation leads us to

$$\eta_1\rho_1 - \eta_i\rho_i = \frac{d-1}{2d(d^m-d)}(\mathbb{1} - d\left|\Phi_i\right\rangle\!\left\langle\Phi_i\right|) \in \mathbb{SEP}^*. \tag{26}$$

Furthermore, a straightforward calculation leads us to

$$\left\langle\Phi_i\right|\Big(\eta_1\rho_1 - \eta_i\rho_i\Big)\left|\Phi_i\right\rangle < 0 \quad \forall i = 2, \ldots, d+1. \tag{27}$$

From Eqs. (26) and (27), $\eta_1\rho_1 - \eta_i\rho_i$ is an EW for any $i = 2, \ldots, d+1$. Thus, Corollary 6 leads us to

$$p_{\mathrm{SEP}}(\mathcal{E}) = \frac{1}{2} < p_{\mathrm{G}}(\mathcal{E}). \tag{28}$$

Now, we provide a systematic way in terms of EW to construct multipartite quantum state ensembles showing nonlocality in state discrimination, that is, $p_{\mathrm{L}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$. For a given EW W, let us consider the multipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^{2}$ where

$$\begin{aligned} \eta_1 &= \frac{\mathrm{Tr}(P+W)}{\mathrm{Tr}(2P+W)},\ \rho_1 = \frac{P+W}{\mathrm{Tr}(P+W)}, \\ \eta_2 &= \frac{\mathrm{Tr}P}{\mathrm{Tr}(2P+W)},\ \rho_2 = \frac{P}{\mathrm{Tr}P}, \end{aligned} \tag{29}$$

with any positive-semidefinite operator $P \succeq 0$ satisfying

$$P + W \succeq 0. \tag{30}$$

Since $\eta_1\rho_1 - \eta_2\rho_2$ is proportional to the EW W, $p_{\mathrm{SEP}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$ holds from Corollary 6. Thus, Inequality (5) leads us to $p_{\mathrm{L}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$.

Corollary 6 can also be used to construct a multipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^{n}$ with $n > 2$ showing nonlocality in quantum state discrimination. For a set of EWs $\{W_i\}_{i=2}^{n}$, let us consider the multipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^{n}$ where

$$\begin{aligned} \eta_1 &= \frac{\mathrm{Tr}\mathbb{1}}{\mathrm{Tr}(n\mathbb{1} - \sum_{j=2}^{n}\lambda_j W_j)},\ \rho_1 = \frac{\mathbb{1}}{\mathrm{Tr}\mathbb{1}}, \\ \eta_i &= \frac{\mathrm{Tr}(\mathbb{1} - \lambda_i W_i)}{\mathrm{Tr}(n\mathbb{1} - \sum_{j=2}^{n}\lambda_j W_j)},\ \rho_i = \frac{\mathbb{1} - \lambda_i W_i}{\mathrm{Tr}(\mathbb{1} - \lambda_i W_i)}, \\ & i = 2, \ldots, n, \end{aligned} \tag{31}$$

with any set of positive real numbers $\{\lambda_i\}_{i=2}^{n}$ satisfying

$$\mathbb{1} - \lambda_i W_i \succeq 0 \quad \forall i = 2, \ldots, n. \tag{32}$$

Because $\eta_1\rho_1 - \eta_i\rho_i$ is proportional to W_i for any $i \in \{2, \ldots, n\}$, $p_{\mathrm{SEP}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$ holds from Corollary 6. Thus, Inequality (5) leads us to $p_{\mathrm{L}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$.

Quantum nonlocality is a key ingredient making quantum states outperform the classical ones in various quantum information processing tasks such as quantum teleportation and quantum cryptography [20, 21]. It is also known that quantum nonlocality plays an important role in quantum algorithms which are more powerful than any classical ones [22, 23]. As the violation of the conditions in Theorem 5 implies $p_{\mathrm{SEP}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$, which consequently means $p_{\mathrm{L}}(\mathcal{E}) < p_{\mathrm{G}}(\mathcal{E})$, our results provides a useful methodology to guarantee the occurrence of nonlocality in state discrimination.

Our results establish a specific relation between the properties of EW and minimum-error discrimination by separable measurements, therefore it is natural to investigate the relationship between EW and other measurements. It is also an interesting future work to construct good conditions, in terms of EW, for optimal state discrimination in other state discrimination strategies.

References

[1] A. Chefles. Quantum state discrimination. *Contemp. Phys.* 41: 401, 2000.

[2] S. M. Barnett and S. Croke. Quantum state discrimination. *Adv. Opt. Photon.* 1: 238, 2009.

[3] J. A. Bergou. Discrimination of quantum states. *J. Mod. Opt.* 57: 160, 2010.

[4] J. Bae and L.-C. Kwek. Quantum state discrimination and its applications. *J. Phys. A: Math. Theor.* 48: 083001, 2015.

[5] C. W. Helstrom. Quantum detection and estimation theory. *J. Stat. Phys.* 1: 231, 1969.

[6] I. D. Ivanovic. How to differentiate between nonorthogonal states. *Phys. Lett. A* 123: 257, 1987.

[7] D. Dieks. Overlap and distinguishability of quantum states. *Phys. Lett. A* 126: 303, 1988.

[8] A. Peres. How to differentiate between nonorthogonal states. *Phys. Lett. A* 128: 19, 1988.

[9] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson and J. Jeffers. Maximum Confidence Quantum Measurements. *Phys. Rev. Lett.* 96: 070401, 2006.

[10] M. Horodecki, P. Horodecki and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* 223: 1, 1996.

[11] B. M. Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A* 271: 319, 2000.

[12] M. Lewenstein, B. Kraus, J. I. Cirac and P. Horodecki. Optimization of entanglement witnesses. *Phys. Rev. A* 62: 052310, 2000.

[13] D. Chruściński and G. Sarbicki. Entanglement witnesses: construction, analysis and classification. *J. Phys. A: Math. Theor.* 47: 483001, 2014.

[14] A. Peres and W. K. Wootters. Optimal detection of quantum information. *Phys. Rev. Lett.* 66: 1119, 1991.

[15] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin and W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A* 59: 1070, 1999.

[16] S. Ghosh, G. Kar, A. Roy, A. Sen(De) and U. Sen. Distinguishability of Bell States. *Phys. Rev. Lett.* 87: 277902, 2001.

[17] E. Chitambar and M.-H. Hsieh. Revisiting the optimal detection of quantum information. *Phys. Rev. A* 88: 020302(R), 2013.

[18] D. Ha and J. S. Kim. Entanglement witness and multipartite quantum state discrimination. arXiv:2301.05420, 2023.

[19] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous and N. Yu. *IEEE Trans. Inf. Theory* 61: 3593, 2015.

[20] A. K. Ekert. Limitations on Separable Measurements by Convex Optimization. *Phys. Rev. Lett.* 67: 661, 1991.

[21] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* 70: 1895, 1993.

[22] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A* 439: 553, 1992.

[23] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. the 35th Annual Symposium on Foundations of Computer Science (IEEE)*, pages 124–134, 1994.

Higher-order quantum transformations of Hamiltonian dynamics

Tatsuki Odake[1] * Hlér Kristjánsson[1] † Akihito Soeda[2] ‡ Mio Murao[1] §

[1]*Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo, Japan*
[2]*National Institute of Informatics, Hitotsubashi 2-1-2, Chiyoda-ku, Tokyo, Japan*

Abstract. We present a quantum algorithm to achieve higher-order transformations of Hamiltonian dynamics. Namely, the algorithm takes as input a finite number of queries to a black-box seed Hamiltonian dynamics to simulate a desired Hamiltonian. Our algorithm efficiently simulates linear transformations of any local seed Hamiltonian, making use of only controlled-Pauli gates and time-correlated randomness. This algorithm is an instance of quantum functional programming, where the desired function is specified as a concatenation of higher-order quantum transformations. By way of example, we demonstrate the simulation of negative time-evolution and time-reversal, and perform a Hamiltonian learning task. This contribution is based on arXiv:2303.09788.

Keywords: Higher-order transformation, Hamiltonian dynamics, functional programming, qDRIFT

1 Introduction and Summary

Efficiently simulating the dynamics of complex quantum systems is often stated as one of the main motivations of quantum computing. While such simulation is considered hard on classical computers, a range of efficient quantum algorithms have been developed for simulating Hamiltonian dynamics [1, 2, 3, 4, 5, 6, 7]. The core principle behind the standard Hamiltonian simulation algorithms is that the desired Hamiltonian dynamics can be well-approximated by a series of (arguably) simpler quantum operations. These algorithms rely on having a classical description of the desired Hamiltonian, which can often be used for obtaining a decomposition into a sum of easily implementable terms. This limits the way we can develop large-scale, complex quantum programs for dynamics simulation. Quantum algorithms which do not require detailed descriptions of quantum resources have a higher flexibility in quantum software development. This issue also touches on a fundamental problem in quantum algorithms as to how much quantum algorithms rely on classical descriptions of their input to achieve quantum advantages in information processing.

In this work, we study which Hamiltonian dynamics can be implemented given a seed Hamiltonian H, without using a classical description of H. We present a quantum algorithm that simulates the dynamics of $f(H)$ where f is any physically realizable linear function of H, given a description of f and using a classically unknown H as the seed. This algorithm is an instance of a higher-order quantum transformation on the unitary operation realized by the seed Hamiltonian dynamics. The functions that the algorithm can implement include both the negative time-evolution and the time-reversal of an unknown Hamiltonian evolution by considering $f(H) = -H$ and $f(H) = H^T$ (transposition of H in terms of the computational basis), respectively. Such general transformations have applications ranging from fundamental physics simulations to potential improvements in state-of-the-art algorithms, such as the Hamiltonian singular value transformation [8]. We also show an application of our algorithm for Hamiltonian learning [9], in particular, a task of efficiently estimating a parameter of a multi-parameter Hamiltonian using Hamiltonian dynamics by appropriately choosing $f(H)$.

Our work constitutes the first systematic study of higher-order quantum transformations in the context of Hamiltonian dynamics. Higher-order quantum transformations have attracted significant attention in recent years in the context of quantum circuit transformations, and are also known as superchannels, supermaps, quantum combs and process matrices [10, 11, 12, 13, 14, 15]. Higher-order algorithms for quantum computation can be seen as an analogue of functional programming in classical computing, where the possible inputs to an algorithm are quantum channels (for example, unitaries) specified "operationally" by their input-output description only (i.e. as black boxes).

Previous works on this topic have focused on the possible transformations that can be achieved when the input channels are taken to be a finite sequence of quantum gates [10, 16, 17, 18, 19, 20, 21, 22, 23, 15, 24]. Yet, the resources available in a given computation are not always best described by a finite sequence of gates, but rather by a continuously parameterized Hamiltonian evolution. In fact, it is known that certain functions such as controllization, which cannot be implemented on black box unitaries [25, 26, 27, 28], can in fact be implemented if access to the underlying Hamiltonian evolution is given [29, 17]. This is because it is possible to apply an arbitrary fractional power of an unknown Hamiltonian evolution by changing the evolution time, whereas applying a fractional power is not possible for black box unitaries.

Our algorithm is a starting point of the emerging field of black box Hamiltonian simulation. One possible future direction is to extend higher-order quantum transformations of Hamiltonian dynamics to the Hamiltonian transformations beyond hermitian-preserving linear transformations.

*tatsuki.odake@phys.s.u-tokyo.ac.jp
†hler.kristjansson@outlook.com
‡soeda@nii.ac.jp
§murao@phys.s.u-tokyo.ac.jp

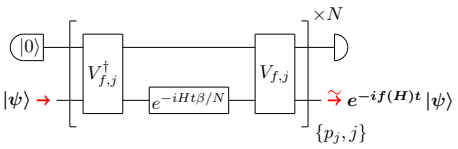


Figure 1: A circuit representation of Algorithm 1 implementing the transformation $e^{-iH\tau} \mapsto e^{-if(H)t}$ for an arbitrary hermitian-preserving linear map $f : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ satisfying $f(I) \propto I$. The unitary $e^{-if(H)t}$ is simulated deterministically and approximately, for an arbitrary input state $|\psi\rangle \in \mathcal{H}$ and the auxiliary qubit initialized in the state $|0\rangle \in \mathcal{H}_c$. The number N on the top-right of the bracket refers to the number of iterations while $t\beta/N$ is the Hamiltonian evolution time of each iteration. For each iteration, an index $j = (\vec{v}, \vec{v}', \vec{u}, \vec{w})$ is randomly chosen from the probability distribution $p_j = p^{(1)}_{\vec{v},\vec{v}'} p^{(2)}_{\vec{u},\vec{w}}$, to perform the j-dependent circuit inside the square brackets.

2 Algorithm

We now present our algorithm (see Algorithm 1). We represent Hilbert spaces of an n-qubit quantum system and a single-qubit auxiliary system by $\mathcal{H}$ and $\mathcal{H}_c$, respectively. We assume that we can invoke the Hamiltonian evolution $e^{-iH\tau}$ of a seed Hamiltonian $H \in \mathcal{L}(\mathcal{H})$ for any time $\tau > 0$. Given a hermitian-preserving linear map $f : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ represented in terms of the Pauli transfer matrices γ [30] as in Eq. (1), our algorithm simulates the Hamiltonian evolution $e^{-if(H)t}$ for any $t > 0$ representing the time for the transformed Hamiltonian dynamics up to an error $\epsilon > 0$ and variance 8ϵ. For convenience, we make two assumptions without loss of generality. (a) We assume that H is normalized as $||H||_{\rm op} = 1$, which can be satisfied by appropriately adjusting the timescale τ. (b) We impose that $f(I) \propto I$, which ensures that the resulting evolution $e^{-if(H)t}$ preserves the invariance under the global phase of $e^{-iH\tau}$. This class of f covers all physically realizable linear transformations of H.

In Algorithm 1, the gate sequence $V_{f,j}$ is constructed only from Clifford gates. The only element which may be non-Clifford is the black box dynamics $e^{-iH\tau}$. Dependence on the transformation f is specified only through the probability distribution $p^{(2)}_{\vec{u},\vec{w}}$ in choosing $(\vec{u}, \vec{w})$ in Step 4 and through the gate X^{s_f} in Step 5. The total runtime $O(\beta^2 t^2 n/\epsilon)$ is calculated by multiplying the number of iterations N with the runtime $O(n)$ for implementing the controlled-Pauli gates in $V_{f,j}$ using CNOT gates and single-qubit Clifford gates. The procedure of Algorithm 1 is summarized in Figure 1. The gate sequence of $\sum_{\vec{v},\vec{v}'} V_{f,j}(I \otimes e^{-iHt\beta/N})V_{f,j}^\dagger$ can be viewed as constructed in a functional programming approach, namely, by concatenations of a series of higher-order transformations (see the accompanied paper).

Algorithm 1 Simulating $e^{-if(H)t}$

Input:

- A finite number of queries to a black box Hamiltonian dynamics $e^{-iH\tau}$ of a seed Hamiltonian H with $\tau > 0$ on an n-qubit system $\mathcal{H}$
- Hermitian-preserving linear map $f : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ satisfying $f(I) \propto I$, which can always be represented by the Pauli transfer matrix elements $\gamma_{\vec{w},\vec{u}}$ as

$$f = \sum_{\substack{\vec{w}\in\{0,1,2,3\}^n \\ \vec{u}\in\{0,1,2,3\}^n\setminus(0,\ldots,0)}} \gamma_{\vec{w},\vec{u}}\, f_{\vec{w},\vec{u}}\,, \qquad (1)$$

  for some $\gamma_{\vec{w},\vec{u}} \in \mathbb{R}$ and functions $f_{\vec{w},\vec{u}}$ defined by $f_{\vec{w},\vec{u}}(\sigma_{\vec{v}}) := \delta_{\vec{v},\vec{u}}\sigma_{\vec{w}}$, for any tensor products of Pauli operators $\sigma_{\vec{v}} := \sigma_{v_1} \otimes \cdots \otimes \sigma_{v_n}$, where $\sigma_0 = I,\ \sigma_1 = X,\ \sigma_2 = Y,\ \sigma_3 = Z$ and $\vec{u},\ \vec{v},\ \vec{w} \in \{0,1,2,3\}^n$ are the Pauli index vectors.
- Input state $|\psi\rangle \in \mathcal{H}$
- Allowed error $\epsilon > 0$
- Time $t > 0$

Output: A state approximating $e^{-if(H)t}|\psi\rangle$ with an error less than ϵ (measured by the 1-norm)

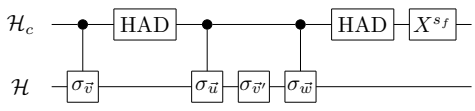
Runtime: $O(\beta^2 t^2 n/\epsilon)$ for $\beta := 2\sum_{\vec{w},\vec{u}} |\gamma_{\vec{w},\vec{u}}|$
Used Resources:
System: $\mathcal{H}$ and one auxiliary qubit $\mathcal{H}_c$
Gates: $e^{-iH\tau}$ $(\tau > 0)$ and Clifford gates on $\mathcal{H}_c \otimes \mathcal{H}$

Procedure:

1: Compute $N := \text{ceil}\left[\max\left(\frac{5\beta^2t^2}{\epsilon}, \frac{5}{2}\beta t\right)\right]$
2: Initialize:
$|\text{current}\rangle \leftarrow |0\rangle \otimes |\psi\rangle$
3: **for** $m = 1, \ldots, N$ **do**
4: Randomly choose

- $(\vec{v}, \vec{v}') \in (\{0,1,2,3\}^n)^2$ with prob. $p^{(1)}_{\vec{v},\vec{v}'} := \frac{1}{16^n}$
- $(\vec{u}, \vec{w}) \in (\{0,1,2,3\}^n)^2$ with prob. $p^{(2)}_{\vec{u},\vec{w}} := \frac{2|\gamma_{\vec{u},\vec{w}}|}{\beta}$

5: Prepare the gate sequence [with $j = (\vec{v}, \vec{v}', \vec{u}, \vec{w})$]

$V_{f,j} :=$ 

where $s_f := \frac{1-\text{sgn}(\gamma_{\vec{u},\vec{w}})}{2}$ (all gates other than X^{s_f} are independent of f) and HAD refers to the Hadamard gate
6: $|\text{current}\rangle \leftarrow V_{f,j}(I \otimes e^{-iHt\beta/N})V_{f,j}^\dagger |\text{current}\rangle$
7: **end for**
8: Trace out $\mathcal{H}_c$ of $|\text{current}\rangle$
9: **Return** $|\text{current}\rangle$

3 Applications of the algorithm

We describe three applications of our algorithm: the negative time-evolution of Hamiltonian dynamics $e^{-iH\tau} \mapsto e^{iHt}$ $(\tau, t > 0)$, the time-reversal of Hamiltonian dynamics $e^{-iH\tau} \mapsto e^{-iH^T t}$ $(\tau, t > 0)$, and a Hamiltonian learning task of estimating a parameter represented by a Pauli coefficient $c_{\vec{v}}$ ($|c_{\vec{v}}| \leq 1$, $\vec{v} \in \{0,1,2,3\}^n$) of a Hamiltonian $H = \sum_{\vec{u}} c_{\vec{u}} \sigma_{\vec{u}}$ with Heisenberg-limited precision scaling using its dynamics $e^{-iH\tau}$ $(\tau > 0)$. The operator norm $\|H\|_{\mathrm{op}}$ of the first two applications are assumed to be 1, while $\|H\|_{\mathrm{op}}$ can be of an arbitrary value but its upper bound should be known in advance for Hamiltonian learning. In general, all three applications can be performed even if the dynamics $e^{-iH\tau}$ is given as a black box apart from knowledge of $\|H\|_{\mathrm{op}}$. However, given the knowledge that H belongs to a subspace of $\mathcal{L}(\mathcal{H})$ spanned by the set $\{\sigma_{\vec{v}}\}_{\vec{v}\in J}$ for some $J \subset \{0,1,2,3\}^n$, negative time-evolution and time-reversal can be performed in a runtime of $O(\mathrm{poly}(|J|))$. This property is useful when the Hamiltonian is known to be k-local for some $k \ll n$, in which case $J = \{\vec{w} \ : ||\vec{w}||_0 \leq k\}$ satisfies $|J| \sim O(n^k)$, which is polynomial in n.

In quantum algorithms that make direct use of Hamiltonian dynamics, both the positive and negative time-evolution are often assumed to be readily accessible. For example, this is required in the recent Hamiltonian singular value transformation [8]. However, in practice, a Hamiltonian evolution being native to a given hardware does not automatically guarantee that the same is true for the corresponding negative time-evolution. Therefore, the ability to efficiently simulate the negative time-evolution of any Hamiltonian given as a black box can decrease the resources required for such algorithms. On the more foundational side, given access to a black box Hamiltonian evolution, one might be interested in simulating the corresponding time-reversed evolution. For example, the evolution of an antiparticle is described by the time-reversal of the corresponding particle evolution.

The simulations of both negative time-evolution and time-reversal are performed by choosing the function f as $f^{\mathrm{neg}}(H) := -H$ and $f^{\mathrm{rev}}(H) := H^T$, respectively, which are specified by

$$\begin{aligned} \gamma^{\mathrm{neg}}_{\vec{w},\vec{u}} &:= -\delta_{\vec{w},\vec{u}} \\ \gamma^{\mathrm{rev}}_{\vec{w},\vec{u}} &:= (-1)^{s_{\vec{w}}} \delta_{\vec{w},\vec{u}}, \end{aligned} \tag{2}$$

where $s_{(w_1,\ldots,w_n)} := |\{j \in \{1,\ldots,n\} \mid w_j = 2\}|$. In the definition of $\gamma^{\mathrm{rev}}_{\vec{w},\vec{u}}$, the fact that $I^T = I$, $X^T = X$, $Y^T = -Y$, and $Z^T = Z$ are used.

In both of these cases, $\beta = 2\sum_{\vec{w},\vec{u}} |\gamma_{\vec{w},\vec{u}}| = 2(4^n - 1)$, thus the runtime $O(\beta^2 t^2 n/\epsilon)$ is exponential in n in general. However, when H is in a subspace of $\mathcal{L}(\mathcal{H})$ spanned by the set $\{\sigma_{\vec{v}}\}_{\vec{v}\in J}$, we can define

$$\gamma^{\mathrm{neg}}_{\vec{w},\vec{u}} := \begin{cases} -\delta_{\vec{w},\vec{u}} & (\vec{u} \in J) \\ 0 & (\text{otherwise}) \end{cases} \tag{3}$$

$$\gamma^{\mathrm{rev}}_{\vec{w},\vec{u}} := \begin{cases} (-1)^{s_{\vec{w}}} \delta_{\vec{w},\vec{u}} & (\vec{u} \in J) \\ 0 & (\text{otherwise}) \end{cases}, \tag{4}$$

since $f(H)$ does not depend on values of $\gamma_{\vec{w},\vec{u}}$ for $\vec{u} \notin J$. In this case, β is calculated as $\beta = 2|J|$ and the runtime $O(\beta^2 t^2 n/\epsilon)$ can be reduced depending on the size of J. We note that the runtime scales as t^2, meaning that in order to perform the time-reversal or negative time-evolution by this algorithm, the dynamics is slowed down quadratically.

Finally, we consider an application of our algorithm to Hamiltonian learning [9]. Estimation techniques of parameters of unknown Hamiltonians for Hamiltonian learning have many applications in quantum sensing [31], analyzing properties of quantum many-body physics [32], and quantum device calibration [33]. Recently, an estimation technique achieving the Heisenberg limit for the precision scaling in the estimation of parameters of a *low-interaction Hamiltonian* has been proposed [34]. Our algorithm can be used to extend this technique to a more general class of n-qubit Hamiltonians. In particular, given access to the dynamics $e^{-iH\tau}$ with an arbitrary time $\tau > 0$ of any Hamiltonian $H = \sum_{\vec{v}\in\{0,1,2,3\}^n} c_{\vec{v}} \sigma_{\vec{v}}$ where each coefficient satisfies $|c_{\vec{v}}| \leq 1$, but is not necessarily positive as in the case of [34], and an upper bound of its operator norm $\|H\|_{\mathrm{op}}$ is known, we can find an estimate $\hat{c}_{\vec{v}}$ of a *single* parameter represented by a Pauli coefficient $c_{\vec{v}}$ for a chosen $\vec{v} \in \{0,1,2,3\}^n$ with a standard deviation smaller than or equal to $s > 0$ in a total evolution time $O(1/s)$. According to the Chebyshev inequality, the task of this protocol can be regarded as an estimation of $c_{\vec{v}}$ with an error smaller than or equal to $\epsilon = ks$ with the failure probability smaller than or equal to $1/k^2$ for an arbitrary $k > 0$.

Our estimation algorithm consists of two steps. The first step simulates $e^{-if_{\vec{v}}(H)t}$ $(t > 0)$ using the Hamiltonian dynamics $e^{-iH\tau}$ $(\tau > 0)$ where $\vec{v}$ specifies $c_{\vec{v}}$ that we want to estimate and $f_{\vec{v}}$ is a hermitian preserving linear map chosen as $f_{\vec{v}}(H) = c_{\vec{v}} Y \otimes I \otimes \cdots \otimes I$. This function $f_{\vec{v}}$ "filters" to keep only the coefficient $c_{\vec{v}}$ and changes all other coefficients to be zero and then sends the coefficient $c_{\vec{v}}$ to the coefficient of $Y \otimes I \otimes \cdots \otimes I$, which is chosen for the convenience of the second step. The corresponding γ is given by $\gamma_{\vec{w}\vec{u}} := \delta_{\vec{w},(2,0,\ldots,0)} \delta_{\vec{u},\vec{v}}$. The second step performs robust phase estimation [35] using $e^{-if_{\vec{v}}(H)t}$ similarly to the technique in [34] to obtain an estimate for $c_{\vec{v}}$, by measuring only the first qubit in our algorithm.

References

[1] M. Suzuki, Fractal decomposition of exponential operators with applications to many-body theories and Monte Carlo simulations, Physics Letters A **146**, 319 (1990).

[2] M. Suzuki, General theory of fractal path integrals with applications to many-body theories and statistical physics, Journal of Mathematical Physics **32**, 400 (1991).

[3] E. Campbell, Random compiler for fast Hamiltonian simulation, Physical Review Letters **123**, 070503 (2019).

[4] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma, Simulating Hamiltonian dynamics with a truncated Taylor series, Physical Review Letters **114**, 090502 (2015).

[5] G. H. Low and I. L. Chuang, Optimal Hamiltonian simulation by quantum signal processing, Physical Review Letters **118**, 010501 (2017).

[6] G. H. Low and I. L. Chuang, Hamiltonian simulation by qubitization, Quantum **3**, 163 (2019).

[7] A. M. Childs, D. Maslov, Y. Nam, N. J. Ross, and Y. Su, Toward the first quantum simulation with quantum speedup, Proceedings of the National Academy of Sciences **115**, 9456 (2018).

[8] S. Lloyd, B. T. Kiani, D. R. Arvidsson-Shukur, S. Bosch, G. De Palma, W. M. Kaminsky, Z.-W. Liu, and M. Marvian, Hamiltonian singular value transformation and inverse block encoding, arXiv preprint arXiv:2104.01410 (2021).

[9] C. E. Granade, C. Ferrie, N. Wiebe, and D. G. Cory, Robust online hamiltonian learning, New Journal of Physics **14**, 103013 (2012).

[10] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Quantum circuit architecture, Physical Review Letters **101**, 060401 (2008).

[11] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Transforming quantum operations: Quantum supermaps, Europhysics Letters **83**, 30004 (2008).

[12] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Theoretical framework for quantum networks, Physical Review A **80**, 022339 (2009).

[13] A. Bisio and P. Perinotti, Theoretical framework for higher-order quantum theory, Proceedings of the Royal Society A **475**, 20180706 (2019).

[14] E. Chitambar and G. Gour, Quantum resource theories, Reviews of Modern Physics **91**, 025001 (2019).

[15] O. Oreshkov, F. Costa, and Č. Brukner, Quantum correlations with no causal order, Nature Communications **3**, 1092 (2012).

[16] J. Miyazaki, A. Soeda, and M. Murao, Complex conjugation supermap of unitary quantum maps and its universal implementation protocol, Physical Review Research **1**, 013007 (2019).

[17] Q. Dong, S. Nakayama, A. Soeda, and M. Murao, Controlled quantum operations and combs, and their applications to universal controllization of divisible unitary operations, arXiv preprint arXiv:1911.01645 (2019).

[18] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Probabilistic exact universal quantum circuits for transforming unitary operations, Physical Review A **100**, 062339 (2019).

[19] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Reversing unknown quantum transformations: Universal quantum circuit for inverting general unitary operations, Physical Review Letters **123**, 210502 (2019).

[20] S. Yoshida, A. Soeda, and M. Murao, Reversing unknown qubit-unitary operation, deterministically and exactly, arXiv preprint arXiv:2209.02907 (2022).

[21] G. Chiribella and H. Kristjánsson, Quantum Shannon theory with superpositions of trajectories, Proceedings of the Royal Society A **475**, 20180903 (2019).

[22] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Quantum computations without definite causal structure, Physical Review A **88**, 022318 (2013).

[23] F. A. Pollock, C. Rodríguez-Rosario, T. Frauenheim, M. Paternostro, and K. Modi, Non-markovian quantum processes: Complete framework and efficient characterization, Physical Review A **97**, 012127 (2018).

[24] G. Bai, Y.-D. Wu, Y. Zhu, M. Hayashi, and G. Chiribella, Efficient algorithms for causal order discovery in quantum networks, arXiv preprint arXiv:2012.01731 (2020).

[25] Z. Gavorová, M. Seidel, and Y. Touati, Topological obstructions to implementing controlled unknown unitaries, arXiv preprint arXiv:2011.10031 (2020).

[26] M. Araújo, A. Feix, F. Costa, and Č. Brukner, Quantum circuits cannot control unknown operations, New Journal of Physics **16**, 093026 (2014).

[27] A. Soeda, *Limitations on quantum subroutine designing due to the linear structure of quantum operators* (Talk at the International Conference on Quantum Information and Technology (IC- QIT), 2013).

[28] N. Friis, V. Dunjko, W. Dür, and H. J. Briegel, Implementing quantum control for unknown subroutines, Physical Review A **89**, 030303 (2014).

[29] S. Nakayama, A. Soeda, and M. Murao, Quantum algorithm for universal implementation of the projective measurement of energy, Physical Review Letters **114**, 190501 (2015).

[30] J. M. Chow, J. M. Gambetta, A. D. Corcoles, S. T. Merkel, J. A. Smolin, C. Rigetti, S. Poletto, G. A. Keefe, M. B. Rothwell, J. R. Rozen, *et al.*, Universal quantum gate set approaching fault-tolerant thresholds with superconducting qubits, Physical review letters **109**, 060501 (2012).

[31] M. de Burgh and S. D. Bartlett, Quantum methods for clock synchronization: Beating the standard quantum limit without entanglement, Physical Review A **72**, 042301 (2005).

[32] N. Wiebe, C. Granade, C. Ferrie, and D. Cory, Quantum hamiltonian learning using imperfect quantum resources, Physical Review A **89**, 042314 (2014).

[33] N. Boulant, T. F. Havel, M. A. Pravia, and D. G. Cory, Robust method for estimating the lindblad operators of a dissipative quantum process from measurements of the density operator at multiple time points, Physical Review A **67**, 042322 (2003).

[34] H.-Y. Huang, Y. Tong, D. Fang, and Y. Su, Learning many-body hamiltonians with heisenberg-limited scaling, arXiv preprint arXiv:2210.03030 (2022).

[35] S. Kimmel, G. H. Low, and T. J. Yoder, Robust calibration of a universal single-qubit gate set via robust phase estimation, Physical Review A **92**, 062315 (2015).

Higher-order Trotterization against total errors in digitial quantum simulation

Sangjin Lee[1] Sung-yeop Lim[1 2] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Korea*
[2] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Korea*

Abstract. Trotter errors are unavoidable in digital quantum simulations (DQS) due to the decomposition of the unitary evolution of the Hamiltonian into finite number of Trotter steps. Decoherence also causes additional errors which may significantly harms the performance of DQS. In this work, we introduce and analyze a higher-order Trotterization scheme for digital quantum simulations to suppress both errors from the Trotterization and decoherence. Motivated from the advanced schemes of dynamical decoupling for higher-order error suppression, we design the sequences of operations for Trotterization to reduce both the Trotter errors and the physical errors simultaneously. We expect that our scheme provides an efficient tool to develop practical digital quantum simulators.

Keywords: Digital quantum simulations, Trotterization, Dynamical decoupling

1 Introduction

A quantum simulation is a natural-born tool for an exploration to complex and many-body physics in which conventional computation techniques such as an exact diagonalization suffers from exponentially large Hilbert space. Concerning large Hilbert space, a numbers of constructed quantum simulators even with small number of qubits already start to benchmark standard known results: energy levels of molecules, phase diagram of lattice gauge theories[1, 2]. Even though many quantum simulations already done, we still need an efficient algorithm to be implemented to existing quantum simulation platforms because of restricted resources and practical errors.

Regarding to quantum simulations, there are two types of quantum simulations: analog and digital quantum simulations (DQS). Those two types of quantum simulations have pros and cons respectively. In spite of its advantage in controllability, DQS is inevitably contaminated by so called Trotter errors. The Trotter errors in principle can be arbitrary reduced if the number of Trotter steps is sufficiently large. However, in the presence of physical errors caused by decoherence or gating errors the performance of DQS is also significantly reduced. Therefore, in the realistic implementation of DQS, an efficient strategy to suppress both the Trotter errors and physical errors is essential.

A Suzuki formula [3] provides a way to achieve arbitrary precisions with the cost of exponential precisions of gate-timing and exponentially many number of gates. While such a scheme provides a way to suppress arbitrary high-order Trotter errors, a more systematic approach of the Trotterization is required in realistic situations regarding the gate-timing and operation cost. Moreover, in order to efficiently mitigate nontrivial errors induced by the correlation between the Trotter and physical errors, a sophisticated design of higher-order Trotterization would be necessary. In this work, we introduce and analyze schemes to suppress both the Trotter and physical errors simultaneously up to higher-order. Based on the analysis of the total errors in Trotterization including both Trotter and physical errors as well as their correlations [4], we apply a higher-order scheme to suppress the total errors. Motivated from the advanced schemes of dynamical decoupling for higher-order error suppression [5], we design the sequences of operations for Trotterization to reduce the total errors efficiently up to higher order. We expect that our work provides an efficient tool to design the Trotterization in developing practical digital quantum simulators.

*swleego@gmail.com

2 Total errors in Trotterization

The system Hamiltonian H to simulate can be decomposed into L elements as $H = \sum_{j=1}^{L} H_j$, while the total Hamiltonian evolution time, t, is divided into r steps. Each evolution of the segmented Hamiltonian for the time interval t/r, i.e., $\{e^{-iH_j t/r}\}_j$, is implemented in terms of gate operations. The simulation is then represented through the evolution of the effective Hamiltonian $\tilde{H}$ which is defined as

$$e^{-i\tilde{H}t/r} = \prod_{j=1}^{L} e^{-iH_j t/r}. \quad (1)$$

The form of the effective Hamiltonian can be recasted by using Baker-Campbell-Hausdorff(BCH) formula into

$$\tilde{H} = H - \frac{i}{2}\sum_{\nu=\mu+1}^{L}\sum_{\mu=1}^{L}[H_\nu, H_\mu](t/r) + O(t^2/r^2). \quad (2)$$

The Trotter error can be then obtained by expanding the Hamiltonian time evolution operator and is bounded as

$$\left\| e^{-iHt} - e^{-i\tilde{H}t} \right\| \leq \left\| -\frac{it^2}{2r}\sum_{\mu<\nu}^{L}[H_\nu, H_\mu] + O(t^3/r^2) \right\|. \quad (3)$$

Physical errors also harms DQS during the evolution in realistic situations. First, we can assume the physical

errors that are not correlated with the Trotter errors. The total simulating channel is then given as

$$\mathcal{E} = \bigcirc_{j=1}^{r} \mathcal{E}' \circ \mathcal{V}, \tag{4}$$

where $\mathcal{V}$ indicates one Trotter step evolution, $\mathcal{E}'$ is a noisy quantum channel in Trotter step and $\bigcirc$ denotes the concatenation of channels and $\mathcal{E}'$. For example, we can consider the depolarization quantum channel $\mathcal{E}^{DEPOL}(\rho) = (1-p)\rho + (p/d)I$. Then, the total error can be obtained as [6]

$$D_{DEPOL} \leq (1-p)\mathcal{A}\frac{t^2}{2r} + rp(2 - \frac{2}{d^2}), \tag{5}$$

where

$$\mathcal{A} \propto \left\| \sum_{\mu<\nu} [H_\nu, H_\mu] \right\|. \tag{6}$$

In the assumption that physical error is uncorrelated with the Trotter error, the total error can be given as the form

$$\frac{C}{r} + Dr, \tag{7}$$

with constants C and D which characterize the physical error model. We can then find the optimal Trotter number as $r_{opt} = \sqrt{C/D}$. On the other hand, if any correlation exists between physical and Trotter errors, we arrive at

$$\frac{C(r)}{r} + D(r)r, \tag{8}$$

including nontrivial higher-order terms of the Trotter number r.

3 Higher-order Trotterization

Let us consider the second-order Trotterization, i.e., symmetrized Trotterization. It has been proved that through the design of the symmetrized sequence of operations in Trotter steps the bound of Trotter errors can be recasted into the form as [7]

$$\begin{aligned} \varepsilon &\equiv \left|\left| \prod_{k=1}^{r} \mathcal{C}_k^\dagger S_{\delta t} \mathcal{C}_k - e^{-iHt} \right|\right| \\ &< \left|\left| \frac{1}{2}\left(\frac{t}{r}\right)^2 \left(\sum_k \sum_{\mu<\nu} \mathcal{C}_k^\dagger [H_\mu, H_\nu] \mathcal{C}_k \right) + \mathcal{O}\left(H_\mu^3 \left(\frac{t}{r}\right)^3 \right) \right|\right|, \end{aligned} \tag{9}$$

where $H = \sum_{\mu=1} H_\mu$ and $S_{\delta t} = \prod_\mu e^{-iH_\mu \delta t}$ with $\delta t = t/r$. Here, $\mathcal{C}_k$ is an arbitrary member of symmetry group of the Hamiltonian, *i.e.*, $[\mathcal{C}_k, H] = 0$, at the k-th quantum gate operation. The performance of proposed error bound is also numerically analyzed in Ref. [7].

In this work, we try to propose that systematic sequences to tighten ε. We will exploit the symmetries of Hamiltonian to tame errors from quantum simulations. Our result can be sketched as [8]

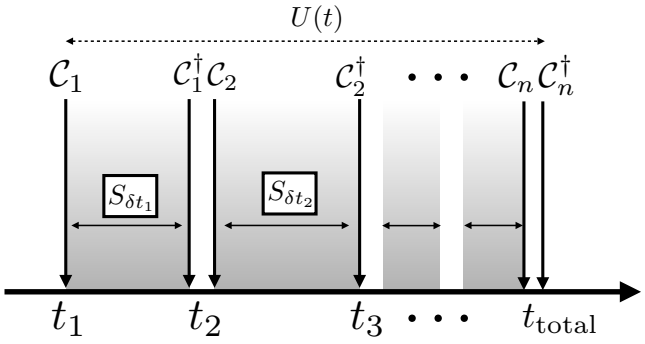


Figure 1: Schematic sequence of symmetry operations for a digital quantum simulation. The simulation time elapses by a designed sequence of $S_{\delta t_{i=1\cdots n}}$. In the middle of idle time between $S_{\delta t_{i=1\cdots n}}$ operations, symmetry operations $\mathcal{C}_i$ is applied to manage errors, which ,in principle, has to preserve initially conserved quantities of simulating Hamiltonian.

Theorem 1 *If target Hamiltonian posses a symmetry group with order 2, then one can design a symmetry operation sequence which gives* $\varepsilon = \mathcal{O}\left(H_\mu^3 \left(\frac{t}{r}\right)^3\right)$ *in Eq. (9).*

This claim can be rephrased as there is a symmetry operation sequence that removes the $\mathcal{O}\left(t^2/r^2\right)$ errors. The basic idea is along the same line with the first-order dynamical decoupling which essentially uses destructive interferences of two wavefunctions with π phase difference.

We note that a symmetry group with order 2 commonly appears over the broad fields of physics such as a parity symmetry in high energy physics and reflection symmetry or continuous U(1) symmetry include order 2 symmetry group as a subgroup which is also symmetry of Hamiltonian.

To go one step further, we focus on symmetries, $\mathcal{C}_n$ with following properties

$$\mathcal{C}_n : H_\mu \to H_{\mathcal{C}(\mu)}, \tag{10}$$

where $H = \sum_\mu H_\mu$ and $(\mathcal{C}_n)^n = \mathbb{1}$. This implies that this operation permutes terms composing of the target Hamiltonian and it can be used to systematically decompose the Hamiltonian up to minimal choice of a set that generates the Hamiltonian.

Armed with this symmetry operations, we design a sequence of symmetry operations, $U(t)$ in a systematic way (See Fig. 1 for schemes),

$$U(t) = \prod_{i=1}^{n} \mathcal{C}_i^\dagger S_{\delta t_i} \mathcal{C}_i, \tag{11}$$

$$\epsilon \equiv \left|\left| U(t) - e^{-iHt} \right|\right| = \mathcal{O}\left(H_\mu^{poly(n)} \left(\frac{t}{r}\right)^{poly(n)} \right) \left|\right|, \tag{12}$$

where $poly(n)$ is a polynomial function of total number of trotter steps n.

It is expected that as the number of symmetry operation increases, a precision of simulations can be improved. Motivated from the advanced schemes of dynamical decoupling for higher-order error suppression [5], we can design the sequence of operations to further suppress the higher-order total errors [8]. Our result will be useful to establish an optimal strategy of Trotterization in DQS for a given target Hamiltonian to simulate under decoherence.

References

[1] S. McArdle, S. Endo, A. Aspuru-Guzik, S. C. Benjamin, & X. Yuan, Quantum computational chemistry, *Rev. Mod. Phys.* **92**, 015003 (2020).

[2] L. Lumia, P. Torta, G. B. Mbeng, G. E. Santoro, E. Ercolessi, M. Burrello, & M. M. Wauters, Two-Dimensional $\mathbb{Z}_2$ Lattice Gauge Theory on a Near-Term Quantum Simulator: Variational Quantum Optimization, Confinement, and Topological Order, *PRX Quantum.* **3**, 020320 (2022)

[3] M. Suzuki, Fractal decomposition of exponential operators with applications to many-body theories and Monte Carlo simulations, *Phys. Lett. A.* **146**, 6 (1990)

[4] S. Lim *et al.*, in preparation (2023).

[5] G. A. Paz-Silva, S.-W. Lee, T. J. Green, L. Viola, Dynamical decoupling sequences for multi-qubit dephasing suppression and long-time quantum memory, *New Journal of Physics*, **18** 073020 (2016).

[6] G. C. Knee, W. J. Munro Optimal trotterization in universal quantum simulators under faulty control, *Phys. Rev. A*, **91** 052327 (2015).

[7] M. C. Tran, Y. Su, D. Carney, J. M. Taylor, Faster digital quantum simulation by symmetry protection, *PRX quantum*, **2** 010323 (2021).

[8] S. Lee *et al.*, in preparation (2023).

The coherent measurement cost of coherence distillation

Varun Narasimhachar[1] *

[1] *Institute of High Performance Computing, Agency for Science, Technology and Research (A*STAR), 1 Fusionopolis Way, Singapore 138632*

Abstract. Quantum coherence is distillable using coherence–non-creating operations. But distillation's coherent *measurement* cost has not previously been estimated. We show that this cost (quantified in Hadamard measurements) is no smaller than the difference between the input's coherence of formation and distillable coherence (the bound achievable in the asymptotic limit). This cost applies to any application whereof coherence distillation is an incidental outcome (e.g. assisted randomness extraction), but the implications are more dramatic if coherence is the only desired outcome: the measurement cost is often higher than the yield, in which case coherence should rather be prepared afresh than distilled.

Keywords: Coherence, resource, distillation, measurement cost, irreversibility

1 Introduction: resource theories of coherence

Coherence—or superposition in wavefunctions—is a cornerstone of quantum mechanics, as well as a valuable resource powering transformative quantum technologies. Various formalizations of the concept of coherence have been explored under the broad umbrella of *resource theories* [1]. A resource theory formalizes the study of a quantum resource by identifying the operational capabilities required to prepare or proliferate it and axiomatically forbidding these. The theory then endeavours to chart out what can and cannot be done using only the remaining, "free" operations. In the resource theories we will consider, the resource is coherence relative to a fixed orthogonal basis ("the *incoherent basis*") of the Hilbert space of a given quantum system, with composite systems inheriting the tensor product of their subsystems' incoherent bases—a form of *speakable coherence* [2]. It is operationally relevant for, e.g., gate-based quantum computing, where every elementary system has a "computational basis".

The free states in these coherence resource theories are density matrices diagonal in the incoherent basis, and the free operations are constrained to be incapable of creating or increasing coherence. There are diverse ways to obey this constraint [1], amongst which we will focus on *incoherent operations* (IO): quantum processes that can be implemented using components that *may detect* coherence (i.e., measure relative to coherent bases) but *must not create* coherence on incoherent inputs [3].

2 Distillation of coherence-resource

Resource distillation—converting an arbitrary resource state to a standard form—is an essential part of applications. For example, coherence distillation is crucial to the task of incoherent or assisted randomness extraction [4]. The standard form of coherence-resource is a pure state containing a uniform superposition of some number of incoherent basis elements, e.g. $|\Psi_M\rangle := M^{-1/2}\sum_{m=0}^{M-1}|m\rangle$. In the *asymptotic* or *independent and identically-distributed* (i.i.d.) limit of the resource theory, where the free operations act on large numbers of independent copies of identical states, the standard coherent states of different M values admit reversible (to leading order) exchange at a rate proportional to $\log_2 M$, which is the equivalent number of standard coherent bits (or *cobits*) $|\Psi_2\rangle$.

The IO resource theory is asymptotically *universally distillable*: copies of *any* coherent state—pure or mixed—can be converted (albeit *not* reversibly—more on this later) by IO to cobits at a rate that is maximal in a resource-theoretic sense [5].

3 What powers coherence distillation?

Strictly incoherent operations (SIO) are the sub-class of IO that use only components that *cannot even detect* coherence [6]. This restriction ends up breaking the asymptotic universal distillability of IO. Indeed, SIO exhibit a particularly severe form of non-distillable, or "bound", coherence [7]. In summary, the *unbounded* coherence-detecting power of IO enables universal distillation, while the strictly coherence–non-detecting SIO are too constrained to distill universally. But what lies between these two extremes? Our paper is an attempt to understand this intervening operational landscape, by answering questions such as:

1. How much coherence-detecting power (quantified in a way that will be discussed later) is necessary to recover the full extent of asymptotic distillability afforded by IO—i.e., to distill at the *maximal* asymptotic rate? How much is sufficient?

2. Given a coherent measurement budget less than the cost of maximal distillation, what (non-maximal) distillation rate can be attained?

3. How does this coherent measurement cost behave away from the asymptotic limit?

*varun.achar@gmail.com

4 Irretrievable coherence

Given a state ρ, its *relative entropy of coherence* is defined as

$$C_r(\rho) = \min\left\{S\left(\rho\|\sigma\right) :\ \Delta[\sigma] = \sigma\right\}, \tag{1}$$

where $\Delta(\cdot)$ denotes the diagonal part (in the incoherent-basis representation) of the argument. Thus, the minimization is over all free states σ. Meanwhile, ρ's *coherence of formation* $C_f(\rho)$ is the *convex-roof extension* of C_r. Operationally, $C_r(\rho)$ is the asymptotic (regularized, per-copy) *distillable coherence* under IO, defined as the maximum asymptotic rate at which cobits can be distilled from copies of ρ by IO. Likewise, $C_f(\rho)$ is the asymptotic *coherence cost* under IO: the minimum asymptotic rate at which cobits must be *consumed* to *prepare* copies of ρ by IO, in the task of *resource dilution*. For almost all states ρ (in a measure-theoretic sense), C_f is strictly larger than C_r [3]. Hence, the coherence distillable by IO from a given input is generically smaller than that required to prepare the same input—an instance of *irreversibility* [8, 9].

In our main results, these two coherence measures feature in the form of their difference $\ell(\rho) := C_f(\rho) - C_r(\rho)$. Because of its connection with irreversibility, we christen it the *irretrievable coherence*. It has, in fact, been encountered (though not named) in the literature in a different operational context: it quantifies the difference between the quantum and the classical *intrinsic randomness* of a state [10, 11].

5 Clues in the literature

Winter and Yang [3] constructed an IO protocol achieving the maximal asymptotic distillation rate $r = C_r(\rho)$. A high-level examination of the protocol already hints at connections between asymptotic irreversibility and the coherent measurement cost. Crucially, the protocol consists (apart from asymptotically-inconsequential measurements) of just a unitary transformation of the input followed by a partial trace. Considering the purity required of the output, the effect of the protocol before the final partial trace is approximately $\rho^{\otimes n} \equiv \varrho_n^{\mathrm{A}} \overset{U}{\longmapsto} \tau^{\mathrm{S}} \otimes \Psi_M^{\mathrm{M}}$, where A labels the input system, M the output system, and S the part that will be traced out. The coherent measurement cost translates to how coherently this unitary U must act. Since no additional systems are involved, the systems' dimensionalities satisfy $A = SM$. Let us now make some heuristic estimates for these numbers, appealing to (a crude form of) asymptotic typicality [12]; qualifiers like "approximate" and "typical part" are implicit in the following.

Firstly, consider the input $\varrho_n \equiv \rho^{\otimes n}$: its rank (by unitarity, also the rank of τ) is $S_0 := \exp_2\left[n\, S(\rho)\right]$. Considering the diagonal part $\Delta\left(\varrho_n\right)$, which is in fact $[\Delta(\rho)]^{\otimes n}$, the relevant dimensionality (covering all the incoherent basis labels with nonzero amplitudes) is $A = \exp_2\left[n\, S\left(\Delta[\rho]\right)\right]$. Finally, the size of the distillate is $M = \exp_2\left[n\, C_r(\rho)\right] = \exp_2\left[n\left(S\left[\Delta(\rho)\right] - S[\rho]\right)\right]$. Notice that $M = A/S_0$, and therefore, $S_0 = S$. Noting that the input's spectrum must be flat, we conclude that τ must be maximally mixed.

In particular, this means that S is discarded in an incoherent state, uncorrelated with M. Now let us view the protocol in reverse: we take Ψ_M, append to it an auxiliary system S in the *incoherent* state τ, and apply the unitary $U^\dagger$ to map the composite SM to $\varrho_n^{\mathrm{A}\equiv\mathrm{SM}}$. How much coherence must $U^\dagger$ generate for this? Considering that it has the Ψ_M to begin with, it still needs to account for the rest of ϱ_n's coherence—a hint at irreversibility.

To be sure, the Winter–Yang IO protocol's reversal is not in IO or any of the other classes of incoherent operations defined in the literature. Besides, their protocol is but one possibility; in general, a protocol may use auxiliary systems. A further difficulty is that there is not yet an operational understanding of IO in terms of their *dilations*, unlike SIO [6]. These complications notwithstanding, the hint inspires us to consider a non-asymptotic idealization of the above "crudely-typicalized" case of maximal distillation, yielding a result (Theorem 1 below) that leaves us within sniffing distance of the corresponding asymptotic result (Theorem 2).

6 Summary of main results

As mentioned above, we approach the problem of estimating the coherent measurement cost of asymptotic distillation by first considering a certain single-shot (i.e., finite-sized and non-asymptotic) variant containing idealized versions of the typicality-related features encountered in maximal asymptotic distillation:

Theorem 1 *Any incoherent operation (IO) that deterministically maps an input state ρ with rank S and incoherent alphabet size A to a standard coherent resource Ψ_M with $M = A/S$ must involve coherent measurements over at least $M^{-1}\exp_2\left[C_f\left(\tau_\rho\right)\right] \geq \exp_2 \ell\left(\tau_\rho\right)$ elements of the input's classical basis, where $\tau_\rho := \mathbb{1}_{\mathrm{supp}\rho}/S$.*

We also establish approximate and non-maximal versions of the above result, but omit these from this summary. Next, we look at distillation in the asymptotic limit. Here the irretrievable coherence $\ell(\cdot)$ plays an even more essential role, as the lower bound of the foregoing results turns out also to be *achievable* in the asymptotic limit:

Theorem 2 *A sequence $\mathcal{E}_n$ of incoherent operation (IO) channels that respectively distill (with asymptotically vanishing error) from $\varrho_n \equiv \rho^{\otimes n}$ at the maximal asymptotic rate of $C_r(\rho)$ must involve coherent measurements over at least L_n elements of the input's classical basis, with $\log_2 L_n \in \Omega\left[n\,\ell\left(\rho\right)\right]$. Conversely, for any given ρ there exists a sequence of maximally-distilling IO channels achieving this scaling.*

The proof of the necessity of the L_n cost in this case proceeds very similarly to the approximate single-shot case, with the approximation threshold dictated by n-dependent parameters associated with asymptotic equipartition. Essentially, we show that with increasing n the task gets closer to the idealized maximal instance of Theorem

1—a formalization of the observations we made in Section 5. The achievability direction turns out to be more involved, requiring putting together several pieces:

1. A construction for a decomposition of ϱ_n that
   - asymptotically approaches the defining bound of the coherence of formation and
   - possesses some symmetries (thanks to the asymptotic typicality properties of ϱ_n) whereby the coherence of each component in the decomposition approaches the overall average value (i.e. ϱ_n's coherence of formation).
2. A sequence of maximally-distilling IO subchannels $\mathcal{F}_n$ based on
   - filtering the above decomposition to further "typicalize" or "flatten" the coherence in each pure component,
   - truncating parts that are more coherent than a threshold that asymptotically scales favourably, and
   - adapting from Winter and Yang's IO distillation protocol [3] a certain "pooling" of the classical labels that (we prove) maps *any* decomposition of ϱ_n to an asymptotically maximally-distilling IO.

   By virtue of the above truncation, the resulting subchannels $\mathcal{F}_n$ use measurement coherence bounded by the claimed scaling.
3. Showing that, despite the above filtering and truncation, the IO subchannel sequence $\mathcal{F}_n$ asymptotically converges towards trace preservation, so that the maximal distillate it produces is asymptotically deterministic.
4. Finally, showing that the (asymptotically negligible but nonzero) trace deficit remaining can be fulfilled by completing each $\mathcal{F}_n$ to a full channel $\mathcal{E}_n = \mathcal{F}_n + \mathcal{G}_n$ using a subchannel $\mathcal{G}_n$ that, like $\mathcal{F}_n$,
   - is also IO and
   - can also be implemented with measurement coherence suitably bounded.

Turning to *non*-maximal distillation in the asymptotic limit, we adapt our achievability result from the maximal case to put an *upper* bound on the requisite coherent measurement cost (we do not reproduce this result here, since it involves cumbersome technical detail). Based on the symmetries that emerge in the asymptotic limit, we conjecture that this upper bound is optimal; settling the conjecture is left for future work.

Apart from the results summarized above, we make some observations on the connection between coherence distillation and certain linear-algebraic structures that we call *decoupling schemes*. We explore this connection

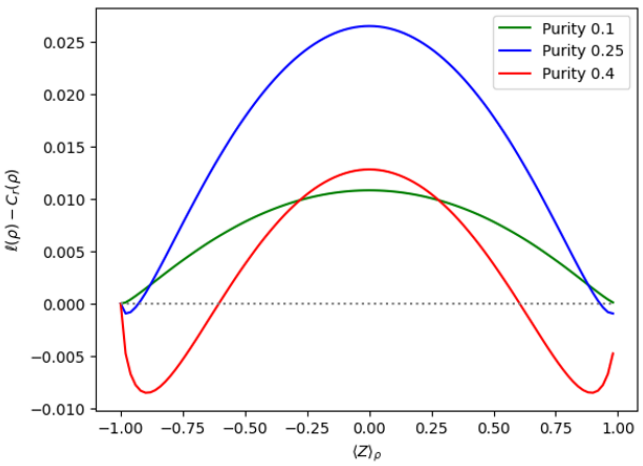


Figure 1: Difference between the asymptotic coherent measurement cost $\ell(\rho)$ and the distillable coherence $C_r(\rho)$ for a section of the qubit Bloch ball: notice that the cost exceeds the yield for a nonzero measure of states.

insofar as it proves useful in deriving the above results (and some variants with nonuniformly-superposed outputs). But decoupling schemes could be of independent interest for future research, with possible connections to established notions of decoupling [13, 14].

7 Discussion

We showed that distilling all of the coherence in a given resource costs a number of Hadamard-like measurements no smaller than the resource's *irretrievable coherence*: the difference between its distillable coherence and coherence of formation. This cost is also achievable in the asymptotic limit. Our results imply that for a nonzero measure of instances (see Fig. 1 for an illustration in the qubit case), the cost of coherence distillation in terms of coherent gates is higher owing to the requisite measurements than the final distilled yield itself! In such instances, it is more prudent to use the available coherent gates to simply prepare fresh coherent states, rather than to distill from the given noisy resource. Open problems for the future include similar cost estimation for non-maximal distillation and other variants (including multipartite tasks like assisted randomness extraction [4] and entanglement distillation under local coherence constraints [15]). An open question of possible wider resource-theoretic significance is: Is the appearance of the irretrievable coherence (a measure of distillation–dilution irreversibility) in our results a coincidence, or does it indicate a systematic connection between irreversibility and ancillary (or otherwise hidden) costs of resource distillation?

References

[1] Alexander Streltsov, Gerardo Adesso, and Martin B Plenio. Colloquium: Quantum coherence as a resource. *Reviews of Modern Physics*, 89(4):041003, 2017.

[2] Iman Marvian and Robert W Spekkens. How to quantify coherence: Distinguishing speakable and unspeakable notions. *Physical Review A*, 94(5):052324, 2016.

[3] Andreas Winter and Dong Yang. Operational resource theory of coherence. *Physical review letters*, 116(12):120404, 2016.

[4] Masahito Hayashi, Kun Fang, and Kun Wang. Finite block length analysis on quantum coherence distillation and incoherent randomness extraction. *IEEE Transactions on Information Theory*, 67(6):3926–3944, 2021.

[5] Fernando GSL Brandao and Gilad Gour. Reversible framework for quantum resource theories. *Physical review letters*, 115(7):070503, 2015.

[6] Benjamin Yadin, Jiajun Ma, Davide Girolami, Mile Gu, and Vlatko Vedral. Quantum processes which do not use coherence. *Physical Review X*, 6(4):041028, 2016.

[7] Ludovico Lami, Bartosz Regula, and Gerardo Adesso. Generic Bound Coherence under Strictly Incoherent Operations. *Phys. Rev. Lett.*, 122:150402, 2019.

[8] Ludovico Lami and Bartosz Regula. No second law of entanglement manipulation after all. *Nature Physics*, 19(2):184–189, 2023.

[9] Ludovico Lami, Bartosz Regula, and Alexander Streltsov. Catalysis cannot overcome bound entanglement. *arXiv preprint arXiv:2305.03489*, 2023.

[10] Xiao Yuan, Hongyi Zhou, Zhu Cao, and Xiongfeng Ma. Intrinsic randomness as a measure of quantum coherence. *Physical Review A*, 92(2):022124, 2015.

[11] Xiao Yuan, Qi Zhao, Davide Girolami, and Xiongfeng Ma. Quantum coherence and intrinsic randomness. *Advanced Quantum Technologies*, 2(11):1900053, 2019.

[12] Claude E Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[13] Francesco Buscemi. Private quantum decoupling and secure disposal of information. *New Journal of Physics*, 11(12):123002, 2009.

[14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(1):251–284, 2014.

[15] Eric Chitambar and Min-Hsiu Hsieh. Relating the resource theories of entanglement and quantum coherence. *Physical review letters*, 117(2):020402, 2016.

Encoded-fusion based quantum computation with photons

Wooyeong Song[1] Nuri Kang[1] Yong-Su Kim[1 2] Seung-Woo Lee[1 *]

[1]*Center for Quantum Information, Korea Institute of Science and Technology, Seoul 02792, Korea*
[2]*Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Korea*

Abstract. Fusion-based quantum computing (FBQC) is a promising new paradigm for quantum computing based on the use of photonic quantum systems. Fusion is a projective entangling measurement for multiple qubits. In FBQC, quantum computation is performed by repeatedly applying fusion on small fixed-sized entangled states, called resource states. Fusion acts as a quintessence of FBQC by generating larger quantum correlations necessary for universal quantum computing. However, fusion is intrinsically non-deterministic, and can be significantly affected by photon loss that is the most detrimental obstacle for scalable photonic quantum computation. Here we propose encoded-qubit based resource states and an encoded-fusion protocol as a solution to overcome both the non-deterministic fusion and the effect of photon loss. We show that FBQC with encoded-fusion is tolerant to loss and can boost the fusion success probability, leading to better fault-tolerance of quantum computation.

Keywords: Photonic quantum computation, Encoded-Fusion, Fusion-based quantum computation

1 Introduction

Fusion-based quantum computing, a recently proposed universal quantum computing scheme, is drawing attention as a model appropriate to be realized by photonic quantum system [1, 2]. FBQC consists of two primitive components: modules that generate small constant-sized entangled resource states (known as resource state generators), and projective entangling measurements (referred to as fusion). Fusion, the core of FBQC, creates larger entanglement by applied on multiple qubits, and it was initially proposed as a method for generating extensive entanglement required for measurement-based quantum computation (MBQC) [3, 4]. Resource state generators (RSGs) and fusion devices are specifically connected to each other to create a network configuration, which is called a fusion network. This configuration of network, together with the modifications of the fusion basis and some single-qubit measurements, implements logical operations for quantum computation.

Both FBQC and MBQC perform computation using quantum entanglements and measurements, but in case of MBQC, the preparation of large entanglements and the measurement process for computation are separated. In contrast, FBQC performs computation while generating extensive entanglement through entangling measurements applied between finite-sized entangled states. Additionally, MBQC considers the resource consumptions due to non-deterministic fusion or fusion error that can occur during the generation process of cluster state as an offline resource (i.e., post-select a successfully generated cluster state prior to computation process). In contrast, FBQC applies quantum operations including all effects of non-deterministic fusion or fusion error, and handles errors resulting from such things together with logical errors at a higher-level encoding. These differences reveal that implementing universal quantum computing using a photonic platform is more suitable through FBQC than MBQC. Although fusing two photonic qubits is non-deterministic, it is relatively easy to implement using elementary linear optics. And there is no need for extensive entanglement to be maintained stable during the computation. The performance of FBQC based on photonic platform is significantly affected by the success probability for fusions and the fact that photons can easily be lost. There is a well-known method for increasing the fusion success probability by using additional ancillary photons [5], however, an increase in the number of photons used leads to an increased risk of photon loss in the system, which might be more harmful than fusion failure. Therefore, it is crucial to boost the fusion success probability while suppressing the detrimental effects of photon loss. We propose a scheme that achieves better tolerance for qubit loss by using additional photons in an apt way, the parity encoding [6], and a higher fusion success probability from an appropriate fusion protocol for the parity-encoded qubits [7, 8]. This will enable us to build an efficient fusion-based quantum computing with a better fault-tolerant threshold.

2 Results

We use encoded resource states in FBQC, which are loaded on the quantum parity code [6]. In specific, it can be written as follows:

$$|0\rangle_L^{(m,n)} = |+^{(m)}\rangle^{\otimes n} \text{ and } |1\rangle_L^{(m,n)} = |-^{(m)}\rangle^{\otimes n}$$

Here, $|\pm^{(m)}\rangle = (|H\rangle^{\otimes m} + |V\rangle^{\otimes m})/\sqrt{2}$. The parity code has photon loss tolerance, as the loss of any one photon consisting the encoded-state only reduces the encoding level by 1. And it can be recovered through fusion with an additional resource. The success probability of the fusion between parity encoded-resource states can be boosted by raising the encoding level. In specific, we utilize a protocol to fuse encoded-resource states in an efficient way [7, 8]. Differing from the scheme that uses additional photon pairs to boost the fusion success rate [1],

*swleego@gmail.com

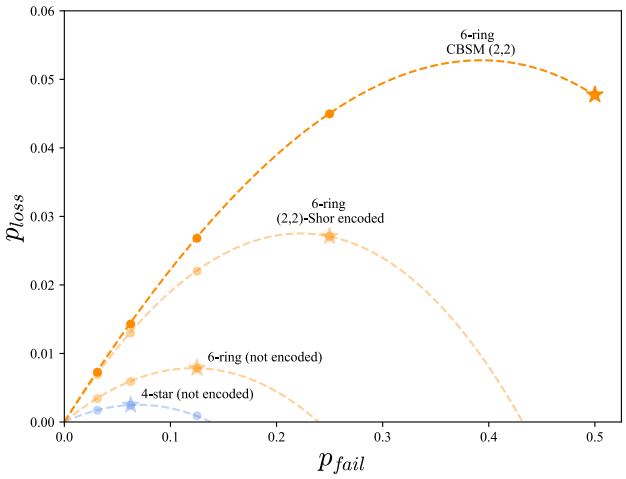


Figure 1: Photon loss threshold for the fusion networks: 4-star (blue) and 6-ring cases (orange) [9]. Here, p_{fail} denotes probabilities to individual fusion fails, and p_{loss} means photon loss threshold derived from the fusion erasure threshold, which is obtained by fusion network simulation [1]. The dim curves show reproduced results from previous work [1], and our result is shown in the curve, 6-ring CBSM (2,2). Our result achieves better loss tolerance than the case using same resource states, (2,2)-Shor, with the fusion boosting using additional photon pairs [5]. For direct comparison, the fusion boosting scheme [5] is considered also in our scheme, but the best result is revealed in $p_{fail} = 0.5$, the case with no boosting.

our scheme has a photon loss tolerance. Even if some photons participating in the fusion are lost, it still has a non-zero success probability. It resolves the issue of the increasing risk of photon loss that occurs with using more photons to boost the fusion success probability.

We replace the existing FBQC architectures (which are based on 4-star resource states and 6-ring resource states) with an encoded-resource state-based one. Then, as in Figure 1, we demonstrate that it achieves better photon loss-tolerance than the structure with the resource states not loaded onto the code [9].

3 Remarks

Fusion-based quantum computation is a method more appropriate for realizing quantum computing using photonic system. This does not require static qubits, instead, it utilizes tools that generate small-entangled state sequentially, and fusion can be leveraged to create larger entanglement necessary for universal quantum computing. Though this is intriguing scheme for the realization of quantum computation based on photonics, the success of FBQC heavily relies on the performance of fusion, which is intrinsically non-deterministic and vulnerable to photon loss. To solve these problems, our work employs the error correction encoding for qubits participating in fusion that are tolerant to errors and qubit loss. Our scheme requires the generation of encoded-resource states, which may be most challenging in the realization of photonic quantum computation as additional resource states. For this, building sub-networks generate encoded-resource state from elementary photonic resource states, such as 3-GHZ states can be considered. Then it allows to construct a fault-tolerant fusion network for computation based on the sub-networks, as resource state generators. We expect that our work paves an efficient way towards fault-tolerant quantum computing based on photonic FBQC architectures.

References

[1] S. Bartolucci et al., Fusion-based quantum computation. *Nat. Comm.*, 14(1), 912, 2023.

[2] H. Bombín et al., Interleaving: Modular architectures for fault-tolerant photonic quantum computing. arXiv:2103.08612, 2021.

[3] D. E. Browne and T. Rudolph, Resource-efficient linear optical quantum computation. Phys. Rev. Lett. 95(1), 010501, 2005.

[4] M. Gimeno-Segovia et al., From three-photon Greenberger-Horne-Zeilinger states to ballistic universal quantum computation. Phys. Rev. Lett. 115(2), 020502, 2015.

[5] W. P. Grice, Arbitrarily complete Bell-state measurement using only linear optical elements. Phys. Rev. A 84(4), 042331, 2011.

[6] T. C. Ralph et al., Loss-tolerant optical qubits. Phys. Rev. Lett. 95(10), 100501, 2005.

[7] S.-W. Lee et al., Nearly deterministic Bell measurement for multiphoton qubits and its application to quantum information processing. Phys. Rev. Lett. 114(11), 113603, 2015.

[8] S.-W. Lee et al., Fundamental building block for all-optical scalable quantum networks. Phys. Rev. A 100(5), 052303, 2019.

[9] W. Song et al., to be submitted (2023)

Design of three-qubit system with three transmons and single resonator in a transmon-based quantum computer

Jeongsoo Kang[1] * Chanpyo Kim[1] † Younghun Kim[1] ‡ Younghun Kwon[1] §

[1] *Department of Applied Physics, Hanyang University, Ansan, Kyunggi-Do, 425-791, South Korea*

Abstract. The transmon-based quantum computer is known as one of the best promising quantum computer architectures. In this work, we propose a new building block for a transmon-based quantum computer, a three-qubit system consisting of three transmons and a single resonator. The building block differs from the architecture of Google and IBM quantum computers. Using the simulator we constructed, we show that the two-qubit gate fidelities, such as CNOT in the three-qubit system consisting of three transmons and a single resonator, can be larger than 0.96.

Keywords: Transmon, quantum computing, quantum gate

1 Introduction

The superconducting circuit is one of promising ingredients for quantum computing. Specially, the transmon-based quantum computer is known as one of the best promising ingredients for quantum computing[1, 2]. When one uses transmons for building a quantum computer, there can be different architectures. In this work, we propose a new building bolck to the architecture for a quantum computer. The new building block is composed of three transmon and single resonator, which implies three qubit system. We show that by obtaing the suitable pulse parameters, the average fidelities of the three qubit system are above 0.96.

2 Method

2.1 Hamiltonian

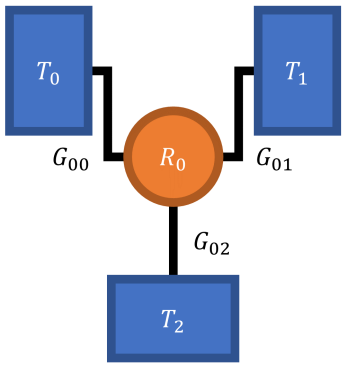
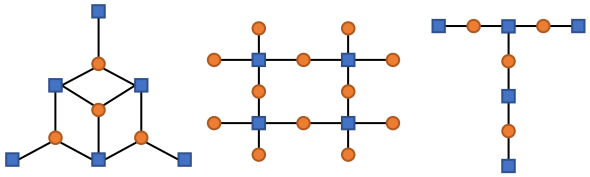


Figure 1: Three qubit system with three transmons and single resonator. Here R, T, and G_{ri} denote resonator, transmon, and connection energy, respectively. The blue(red) color indicates a tranmon(resonator).

In this work, we consider three-qubit system with three-transmon($N_T = 3$) and single resonator($N_R = 1$) in transmon-based quantum computer(Fig. 1). Here we call this system *three-transmon system*. In the three-transmon system, every transmon is connected and CNOT gate between any two transmons can be possible. And two transmons are connected indirectly through a resonator. The three-transmon system with three-transmon and single resonator can be used a new building block for transmon-based quantum computer. Fig. 2 shows the difference among our system, Google system and IBM system.



(a) (b) (c)

Figure 2: (a) Six-transmon system consisting of our building block. (b) Google machine(transmon system in the lattice structure[12]). (c) IBM machine(transmon system in T-shape[13]).

Table 1: The specification of hardware in three-transmon system. The unit of energy is GHz.

	R_0	T_0	T_1	T_2
$\omega/2\pi$	7.0	-	-	-
$E_{C,i}/2\pi$	-	0.30783	0.30902	0.31040
$E_{J,i}/2\pi$	-	11.914	11.412	10.993
$G_{0i}/2\pi$	-	0.07	0.07	0.07

The hamiltonian H of the system consists of the resonator hamiltonian H_R, the transmon hamiltonian H_R, and the interaction hamiltonian as follows:

$$H(t) = H_R + \sum_{i=0}^{2} H_{T,i}(t) + H_I \tag{1}$$

$H_{T,i}$ denotes the hamiltonian of i-th transmon. The energy gap of the resonator is determined by the resonator frequency ω.

$$H_R = \omega a^\dagger a \tag{2}$$

*jskang1202@hanyang.ac.kr
†freezeticket@hanyang.ac.kr
‡hpoqh@hanyang.ac.kr
§yyhkwon@hanyang.ac.kr

Here we use $\hbar = 1$. And time and energy is expressed in terms of the unit of ns and GHz, respectively. $a(a^\dagger)$ denotes the annihilation(creation) operator of the resonator. The energy level and anharmonicity of transmon are determined by E_C and $E_{J,i}$[1, 2].

$$H_{T,i}(t) = 4E_{C,i}(n_i - n_{g,i}(t))^2 - E_{J,i}\cos\phi_i \tag{3}$$

n is a number operator to extra Cooper pair in the island of transmon. ϕ is the operator to the phase difference of two Cooper pair between Josepson junctions. $n_g(t)$ is the gate offset number, which is a function to denote the pulse driving a transmon. The interaction hamiltonian is expressed by the exchange between transmon and resonator.

$$H_I = \sum_i G_i(a + a^\dagger)n_i \tag{4}$$

Here G_i is the interaction energy between transmon and resonator.

The operator to transmon and resonator are expressed by matrices of 4×4. This implies that higher energy levels should be included. It is known that the higher energy levels are important in implementing two qubit gates such as CNOT[3].

2.2 Pulse Design

To drive transmon-resonator system, the voltage pulse is applied to transmon. The voltage pulse is expressed by a gate offset number of transmon.

$$n_g(t) = \sum_j \Omega_j(t)\cos(2\pi f_j t - \gamma_j) \tag{5}$$

Here Ω_j and f_j denote a envelope and a frequency of the pulse, which are important elements in performance of gate. γ_j is the initial phase which determines the axis of rotation of transmon.

For the envelope of the pulse, we consider $\Omega_G(t)$ and $\Omega_S(t)$ as follows:

$$\Omega_G(t) = \Omega_X \frac{e^{-(t-T_X/2)^2/2\sigma^2} - e^{-T_X^2/8\sigma^2}}{1 - e^{-T_X^2/8\sigma^2}} \tag{6}$$

$$\Omega_S(t) = \begin{cases} \Omega_S S(t) & (0 \le t < T_{\text{rise}}) \\ \Omega_S & (T_{\text{rise}} \le t < T_{\text{rise}} + T_S) \\ \Omega_S S(t - T_S) & (T_{\text{rise}} + T_S \le t < 2T_{\text{rise}} + T_S) \end{cases} \tag{7}$$

$\Omega_G(t)$ is a function of pulse time T_X, amplitude Ω_X, and thickness $\sigma = T_X/4$. Meanwhile, $\Omega_S(t)$ is a function of pulse time T_S, amplitude Ω_S, and the ratio of increasing period $\varrho = T_{\text{rise}}/T_S$. $S(t)$ is a function given as $S_1(t) = \sin(\pi t/2T_{\text{rise}})$ or $S_2(t) = \sin^2(\pi t/2T_{\text{rise}})$.

2.3 Quantum Gate Optimization

The quantum gates $\mathcal{U}$ in this work can be obtained by applying pulse to total Hamiltonian.

$$\mathcal{U} = \mathcal{T}\exp\left(-i\int_0^T dt H(t)\right) = \mathcal{T}\prod_{n=1}^{N} e^{(-i\tau H((n+1/2)\tau))} \tag{8}$$

Here $\tau = T/N$ is a time interval for numerical approach. The total hamiltonian can be expressed as $H(t) = H_0 + H_1(t)$, where $H_0(H_1(t))$ denotes the diagonal(non-diagonal) matrx, respectively. And $e^{(-i\tau H((n+1/2)\tau))}$ is evaluated by Suzuki-Trotter algorithm[4].

$$e^{(-i\tau H((n+1/2)\tau))} \simeq e^{(-i\tau H_0/2)} V e^{(-i\tau\Lambda(t))} V^\dagger e^{(-i\tau H_0/2)} \tag{9}$$

A diagonalized matrix $\Lambda(t)$ and a symmetric marix V satisfy the relation of $H_1(t) = V\Lambda(t)V^\dagger$. The final stage to obtain the quantum gate is to apply VZ gate $\mathcal{Z}$[5].

$$\mathcal{Z} = \bigotimes_{i=0}^{N_T} R_Z(\theta_i) \tag{10}$$

The performance to quantum gate $\mathcal{U}$ is evaluated by the average fidelity F. The fidelity to pure state $|\psi\rangle$ is given as follows:

$$F_\psi = \langle\psi|U^\dagger\mathcal{U}|\psi\rangle \tag{11}$$

Here, U denotes the ideal quantum gate. In this work, we obtain the average fidelity by using M-number of different $|\psi\rangle$[11].

$$F = \frac{1}{M}\sum_{m=1}^{M} F_{\psi,m} \tag{12}$$

By minimizing the infidelity $1 - F$,the quantum gate $\mathcal{U}(f, T, \Omega, \gamma, ...)$ can be optimized. Here, we use Nelder-Mead algorithm as optimizer[6].

3 Result

In this section we explain the result of design of three-qubit system made of three transmons and single resonator. The specification of hardware is listed in the Table 1. In the case of single qubit gates, we can easily obtain the best parameters of pulses for the single qubit gates. The most important gate to two-qubit gates is CNOT. To build CNOT gate, cross-resonance(CR) pulses are used[7, 3, 10]. CR pulse is the pulse applying the qubit frequency of target qubit to control qubit. And according to the state of the control qubit, the resonance responce to target qubit varies. The completion of CNOT gate is obtained by CR pulse and adding pulse to target qubit.

$$n_{g,C}(t) = \Omega_S(t)\cos(2\pi f_1 t - \gamma_1) \tag{13}$$

$$n_{g,T}(t) = \Omega_G(t - T_S)\cos(2\pi f_2(t - T_S) - \gamma_2) \tag{14}$$

Here $C(T)$ denotes a control(target) qubit. And $f_{1,2}$ is in general the qubit frequency of target qubit. To improve the performance of the gate, $f_{1,2}$ can be detuned. The adding pulse starts at the end of CR pulse. Therefore, CNOT gate can be expressed by two unitary gates $\mathcal{U}_{\text{CR}}$ and $\mathcal{U}_a$.

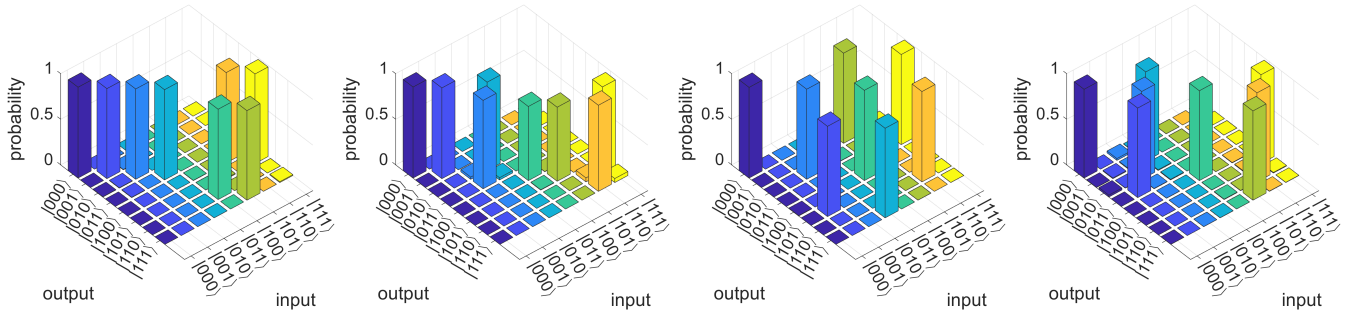
$$\text{CNOT}_{ij} = \mathcal{Z}\mathcal{U}_{a,j}\mathcal{U}_{\text{CR},i} \tag{15}$$

Here, $i(j)$ denotes the number of control(target) qubit. In the design of a quantum gate, the most important process is to find the vector of pulse parameters. The vector of pulse parameters can be expressed by 12-dimensional real vector as follows:

$$(f_1, f_2, T_X, T_S, \Omega_X, \Omega_S, \varrho, \gamma_1, \gamma_2, \theta_1, \theta_2, \theta_3)^T \tag{16}$$

Table 2: The pulse parameters of CNOT gate and the average fidelity in three-transmon system.

Gate	f_1	f_2	T_X	T_S	Ω_X	S, Ω_S
CNOT_{01}	4.9783	4.9783	10	130	0.0055	S_2, 0.07
CNOT_{12}	4.8895	4.8895	10	120	0.01	S_1, 0.05
CNOT_{20}	5.0851	5.0841	8.5	190	0.035	S_1, 0.08
CNOT_{21}	4.9783	4.9783	10	170	0.025	S_1, 0.05
ϱ	γ_1	γ_2	θ_1	θ_2	θ_3	F
0.25	0	2.2007	0.6959	0	0.1001	0.9956
0.3	0	-1.5708	0	3.1416	0	0.9619
0.2	0	-1.2566	0.1571	0	2.6704	0.9938
0.3	0	-1.8850	0	0	1.5708	0.9867



(a) (b) (c) (d)

Figure 3: The success probability of CNOT gate of three qubit system in computational basis. (a) The gate success probability of CNOT_{01}. (b)The gate success probability of CNOT_{12}. (c)The gate success probability of CNOT_{20}. (d)The gate success probability of CNOT_{21}.

The first step to design $\mathcal{U}_{\text{CR}}$ is to select a suitable $S(t)$. Atfer the process, we need to find f_1, T_S, Ω_S, ϱ, and γ_1. Then to design $\mathcal{U}_a$, we select a suitable value for f_2, T_X, Ω_X, γ_2. Table 2 shows the pulse parameters for performing CNOT_{01}, CNOT_{12}, CNOT_{20}, and CNOT_{21}. And Fig. 2 shows the success probabilities of them in the computational basis. The average fidelities for them are above 0.96. Specially, in the case of CNOT_{01} and CNOT_{21} the average fidelities are beyond 0.99.

4 Conclusion

Many promising quantum computer architectures are based on transmon quantum computer. In this work, we proposed a new building block which consists of three transmons and a single resonator. Using the new building block, we can build a quantum computer with the new structure. We showed that the average success probabilities of CNOT gates are beyond 0.96.

Acknowledgment

This work is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF2022R1F1A1064459) and Creation of the Quantum Information Science R&D Ecosystem (Grant No. 2022M3H3A106307411) through the National Research Foundation of Korea (NRF) funded by the Korean government (Ministry of Science and ICT).

References

[1] Nakamura Y., Y.A. Pashkin, and J. Tsai. Coherent control of macroscopic quantum states in a single-Cooper-pair box. *Nature*, 398(6730): p. 786-788, 1999.

[2] Koch J., et al. Charge-insensitive qubit design derived from the Cooper pair box. *Physical Review A*, 76(4): p. 042319, 2007.

[3] Magesan E. and J.M. Gambetta. Effective Hamiltonian models of the cross-resonance gate. *Physical Review A*, 101(5): p. 052308, 2020.

[4] Suzuki M. Decomposition formulas of exponential operators and Lie exponentials with some applications to quantum mechanics and statistical physics. *Journal of mathematical physics*, 26(4): p. 601-612, 1985.

[5] McKay D. C., Wood C. J., Sheldon S., Chow J. M., and Gambetta J. M. Efficient Z gates for quantum computing. *Physical Review A*, 96(2): p. 022330, 2017.

[6] Nelder J.A., and R. Mead. A simplex method for function minimization. *The computer journal*, 96(2): 7(4): p. 308-313, 1965.

[7] Kirchhoff S., et al. Optimized cross-resonance gate for coupled transmon systems. *Physical Review A*, 97(4): p. 042348, 2018.

[8] Schlör, S., et. al. Correlating decoherence in transmon qubits: Low frequency noise by single fluctuators. *Physical review letters*, 123(19): p. 190502, 2019.

[9] Niu S., and Todri-Sanial A. Pulse-level noise mitigation on quantum applications. *arXiv preprint*, arXiv:2204.01471, 2022.

[10] Rigetti C., and Devoret M. Fully microwave-tunable universal gates in superconducting qubits with linear couplings and fixed transition frequencies. *Physical Review B*, 81(13): p. 134507, 2010.

[11] Nielsen, M. A. A simple formula for the average gate fidelity of a quantum dynamical operation. *Physics Letters A*, 303(4): p. 249-252, 2002.

[12] Arute F., et. al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779): p. 505-510, 2019.

[13] IBM Quantum, `ibmq_quito`. https://quantum-computing.ibm.com/.

Generic Decoherence Free subspace of Non-Interacting Open Quantum System

Mi-Jung So[1] Dongni Chen[1] Mahn-Soo Choi[1] *

[1] *Department of Physics, Korea University, Seoul 02841, South Korea.*

Abstract. We consider a non-interacting open quantum system that has permutation symmetry, and found the decoherence free subspace that the relative capacity asymptotically approaches one.

Keywords: Non-interacting open quantum system, Weak symmetry, Decoherence free subspace

1 Introduction

Decoherence free subspace(DFS)[1] approach is a powerful method to avoid specific decoherence mechanism. It is identified by the symmetry of the interaction between system and the environment. The approach is used in quantum communication without shared reference frame[2], where the transmission process is collective and the operators form a unitary group, so that it has exchange symmetry. In the open Heisenberg XXZ spin 1/2 chain they expanded to the symmetry of Liouvillian superoperator[3]. However they consider specific symmetry that is the commutation of only one superoperator. In our case we combine the exchange symmetry feature and the symmetry of Liouvillian superoperator.

In this paper, we consider open quantum system with exchange symmetry and non-interacting Hamiltonian. We present the systematic way to find the optimal DFS to encode quantum information by the structure of Liouvillian superoperator of the quantum master equation.

2 General model

Quantum master equation is a quantum operation as a differential equation.

$$\dot{\hat{\rho}} = \mathcal{L}\hat{\rho}(t) \equiv -i[\hat{H}, \hat{\rho}(t)] + \sum_{\mu} \Big(\hat{L}^{\mu} \hat{\rho}(t) \hat{L}^{\mu\dagger} - \frac{1}{2} \{ \hat{L}^{\mu\dagger} \hat{L}^{\mu}, \hat{\rho}(t) \} \Big). \tag{1}$$

Here the $\hat{\rho(t)}$ is the system density operator, the super operator $\mathcal{L}$ is called the Liouvillian. The Hermitian operator $\hat{H}$ is effective Hamiltonian and the $\hat{L}^{\mu}$ are quantum jump operators.

For the non-interacting Hamiltonian, the Hamiltonian becomes sum of identical single qubit Hamiltonians, therefore the total Liouvillian $\mathcal{L}$ of n qubit system can be expressed as the sum of single qubit Liouvillian $\mathcal{L}_j$ for jth qubit as,

$$\dot{\hat{\rho}} = \mathcal{L}\hat{\rho} = \Big(\sum_{j=1}^{n} \mathcal{L}_j \Big) \hat{\rho}, \tag{2}$$

where the ρ is the density operator for total system. This Liouvillian has the weak permutation symmetry, which is defined as the commutation between the Liouvillian of number of n qudits and the permutation superoperators $\mathcal{S}_k$ given by

$$\mathcal{S}_k \mathcal{L} = \mathcal{L} \mathcal{S}_k, \quad \mathcal{S}_k(\hat{x}) \equiv \hat{\pi}_k \hat{x} \hat{\pi}_k^{\dagger}, \quad k = 1, 2, ..., n!, \tag{3}$$

where the $\hat{\pi}_k$ are the operator representation of the n permutation group. From the next section we introduce how to calculate the decoherence free subspace or subsystem of the total Liouvillian by the structure of the single qubit Liouvillian matrix representation.

3 Non-degenerate case

Here is a case of single qubit Liouvillian with the Pauli operator $\hat{\sigma}_z$ for the Hermitian part and $\hat{\sigma}_+$, $\hat{\sigma}_-$, $\hat{\sigma}_z$ for the jump operators.

$$\begin{aligned} \mathcal{L}_j \hat{\rho}(t) = & -i \left[h^z \hat{\sigma}_j^z, \hat{\rho} \right] \\ & + \Gamma^+ \left(\hat{\sigma}_j^+ \hat{\rho} \hat{\sigma}_j^{+\dagger} - \frac{1}{2} \hat{\sigma}_j^{+,\dagger} \hat{\sigma}_j^+ \hat{\rho} - \frac{1}{2} \hat{\rho} \hat{\sigma}_j^{+,\dagger} \hat{\sigma}_j^+ \right) \\ & + \Gamma^- \left(\hat{\sigma}_j^- \hat{\rho} \hat{\sigma}_j^{-,\dagger} - \frac{1}{2} \hat{\sigma}_j^{-,\dagger} \hat{\sigma}_j^- \hat{\rho} - \frac{1}{2} \hat{\rho} \hat{\sigma}_j^{-,\dagger} \hat{\sigma}_j^- \right) \\ & + \Gamma^z \left(\hat{\sigma}_j^z \hat{\rho} \hat{\sigma}_j^{z,\dagger} - \frac{1}{2} \hat{\sigma}_j^{z,\dagger} \hat{\sigma}_j^z \hat{\rho} - \frac{1}{2} \hat{\rho} \hat{\sigma}_j^{z,\dagger} \hat{\sigma}_j^z \right) \end{aligned} \tag{4}$$

All coefficients h^z, Γ^+, Γ^-, Γ^z are real and Γ^+, Γ^-, Γ^z are positive.

There are four Eigenvalues of the Liouvillian as,

$$\left\{ 0,\ -2\tilde{\Gamma},\ -\tilde{\Gamma} - 2\Gamma^z - 2ih^z,\ -\tilde{\Gamma} - 2\Gamma^z + 2ih^z \right\}, \tag{5}$$

where $\tilde{\Gamma} \equiv \frac{\Gamma^+ + \Gamma^-}{2}$.

For the number of n qubits, the eigenvalues of the Liouvillian are summation of the eigenvalues of single qubit Liouvillian. There are degenerate eigenvalues and the superposition between the degenerate states of the Liouvillian conserves during time evolution so that the subspace of the degenerate states is decoherence free subspace.

For the general non-degenerate single qubit Liouvillian, the eigenvalue $-(n + \Gamma^z)\tilde{\Gamma}$ has the maximum number of degenerate corresponding eigenstates and we denote the number as $D^{(n)}$.

$$D^{(n)} = \frac{n! 2^{\frac{n}{2}}}{\frac{n}{4}! \frac{n}{4}! \frac{n}{2}!}. \tag{6}$$

*username3@domainname3

To represent general 1 qubit information, we need 4 operator basis to encode 1 qubit quantum information to include the superposition. Therefore, total $\log_4 D^{(n)}$ qubits of information can be stored in the DFS. The relative capacity of the DFS $\frac{1}{n}\log_4 D^{(n)}$ is represented in the figure 1. The relative capacity asymptotically approaches 1 as $1-\frac{3}{2n}\log_4 n+\mathcal{O}(\frac{1}{n})$ for large n.

4 Without Γ_z transition

For the Liouvillian in equation (4), if the $\Gamma^z=0$, the eigenvalues are,

$$\left\{0,\ -2\tilde{\Gamma},\ -\tilde{\Gamma}-2ih^z,\ -\tilde{\Gamma}+2ih^z\right\}. \tag{7}$$

These eigenvalues are still non-degenerate however for the n qubit Liouvillian there is a additional degeneracy that the sum of first two eigenvalues are same as the sum of the rest. Therefore the maximum number of degenerate corresponding eigenstates $D^{(n)}_{\Gamma^z=0}$ is the number of eigenstates with eigenvalue $-n\tilde{\Gamma}$,

$$D^{(n)}_{\Gamma^z=0}=\binom{n}{\frac{n}{2}}^2 \tag{8}$$

By the structure of the single qubit eigenstates, $D^{(n)}_{\Gamma_z=0}\geq D^{(n)}$. The relative capacity of the DFS $\frac{1}{n}\log_4 D^{(n)}_{\Gamma_z=0}$ is represented in figure 1. The relative capacity asymptotically approach 1 as $1-\frac{1}{n}\log_4 n+\mathcal{O}(\frac{1}{n})$.

5 degenerate case

For the case when the single qubit Liouvillian in equation (4) has degenerate energy levels, that is $h^z=0$, two eigenvalues are degenerate.

$$\left\{0,\ -2\tilde{\Gamma},\ -\tilde{\Gamma}-2\Gamma^z,\ -\tilde{\Gamma}-2\Gamma^z\right\}. \tag{9}$$

In this case, for the number of N qubits, also the eigenvalue $-N(\tilde{\Gamma}+\Gamma^z)$ has the maximum number of degenerate corresponding eigenstates which is denoted as $D^{(n)}_{h^z=0}$,

$$D^{(n)}_{h^z=0}=\frac{n!2^{\frac{n}{2}}}{\frac{n}{4}!\frac{n}{4}!\frac{n}{2}!} \tag{10}$$

Degenerate Liouvillian has larger DFS than the non-degenerate cases, $D^{(n)}_{h^z=0}\geq D^{(n)}_{\Gamma^z=0}$. The relative capacity of the DFS $\frac{1}{n}\log_4 D^{(n)}_{h^z=0}$ is represented in figure 1. The relative capacity also asymptotically approach 1 as $1-\frac{1}{n}\log_4 n+\mathcal{O}(\frac{1}{n})$.

6 Degenerate case without Γ_z

For the case when the single qubit Liouvillian in equation (4) has degenerate energy levels, that is $h^z=0$, and also without Γ^z term, the two eigenvalues are degenerate.

$$\left\{0,\ -2\tilde{\Gamma},\ -\tilde{\Gamma},\ -\tilde{\Gamma}\right\}. \tag{11}$$

There is a similar structure as in section 4, that the sum of the first two eigenvalues are same as the sum of the rest. In this case, for the number of N qubits, also the eigenvalue $-N\tilde{\Gamma}$ has the maximum number of degenerate corresponding eigenstates which is denoted as $D^{(n)}_{h^z,\,\Gamma^z=0}$,

$$D^{(n)}_{h^z,\,\Gamma^z=0}=\frac{4^n(n-\frac{1}{2})!}{\sqrt{\pi}n!} \tag{12}$$

This case has larger DFS than other cases, $D^{(n)}_{h^z,\,\Gamma^z=0}\geq D^{(n)}_{h^n=0}$. The relative capacity of the DFS $\frac{1}{n}\log_4 D^{(n)}_{h^z,\,\Gamma^z=0}$ is represented in figure 1. The relative capacity also asymptotically approach 1 as $1-\frac{1}{2n}\log_4 n+\mathcal{O}(\frac{1}{n})$.

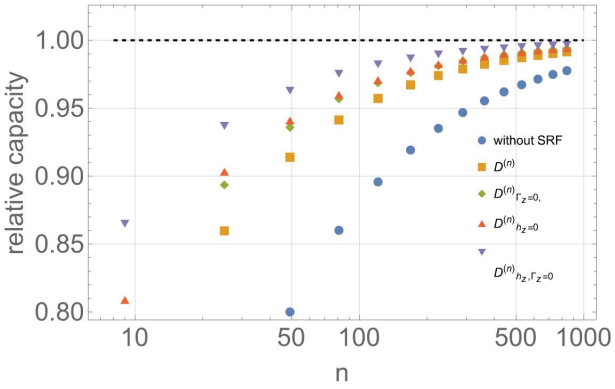


Figure 1:

7 Conclusion

We have considered a non interacting open quantum system with exchange symmetry and showed the systematic way to find the optimal decoherence free subspace(DFS). Here we have taken a specific model with Pauli Z Hamiltonian, and we give exact formulas of the dimension of the DFS and the eigenvalue that the states are correlated.

References

[1] Kempe, Julia, et al. Theory of decoherence-free fault-tolerant universal quantum computation. Phys.Rev.A 63.4 (2001):042307

[2] Bartlett, Stephen D., Terry Rudolph, and Robert W. Spekkens. Classical and quantum communication without a shared reference frame. Phys.Rev.Lett 91.2 (2003):027901

[3] Buča, Berislav, and Tomaž Prosen. Buča, Berislav, and Tomaž Prosen. "A note on symmetry reductions of the Lindblad equation: transport in constrained open spin chains. New J. Phys 14.7 (2012):073007

Non-destructive quantum state discrimination

Youngrong Lim[1] Minki Hhan[2] Hyukjoon Kwon[1] *

[1] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*
[2] *Quantum Universe Center, Korea Institute for Advanced Study, Seoul 02455, Korea*

Abstract. In conventional state discrimination, the local distinguishability of a set of states might not be directly connected to entanglement. We propose a non-destructive quantum state discrimination to reveal a such connection. Remarkably, for any set of orthogonal maximally entangled states, our scheme shows that any classical strategy cannot beat random guessing. Furthermore, we suggest a fully non-destructive discrimination scheme for a set of maximally entangled stabilizer states and compute the entanglement cost for perfect discrimination. We find a set of maximally entangled stabilizer states exhibiting *entanglement earning*, where one can gain a positive net entanglement via the discrimination task.

Keywords: Quantum state discrimination, Stabilizer formalism

1 Introduction

Quantum state discrimination is a task distinguishing a set of quantum states, which is related to the foundation of quantum theory and has various applications in quantum communications and cryptography [1, 2]. Basically, a set of orthogonal quantum states can be perfectly distinguished without any restriction on measurements. When distant parties can only perform local operations and classical communications (LOCC), however, the task becomes highly nontrivial and has been extensively studied. For example, one can construct a set of orthogonal product states that cannot be perfectly distinguished using LOCC, so-called *nonlocality without entanglement* [3]. On the other hand, any two pure orthogonal states can be perfectly discriminated via local measurements [4], whether the states are entangled or not. These results imply that entanglement in a set of quantum states might not be directly related to their local distinguishability.

In this work, we propose a non-destructive quantum state discrimination (NDSD) task to reveal a connection between entanglement in a set of quantum states and their local distinguishability. In this setup, the task succeeds when the classical answer indicating the right state and the quantum answer confirming the non-disturbance of the initial state are both correct. Consequently, it also demands not destroying the entanglement in the initial state, which can restrict the power of local discrimination. This modification leads to a drastic change in the success probability of the discrimination between classical and quantum strategies. Especially for a set of maximally entangled states (MESs), we show that the success probability of the strategy with no shared entanglement cannot be higher than random guessing, which is not guaranteed in the conventional state discrimination task without non-disturbance condition [5].

We also investigate entanglement cost to perform perfect NDSD. While a naïve approach is applying conventional discrimination via teleportation followed by repreparation of the initial state, we find a more efficient scheme for maximally entangled stabilizer states (MESSs) by implementing a syndrome measurement using pre-shared entanglement. We demonstrate that the entanglement cost of the proposed scheme is always equal or less than the teleportation-and-repreparation strategy and provide explicit cases that yield a strict gap between two strategies. Interestingly, we find a set of MESSs exhibiting *entanglement earning*, where one can possess more entanglement after the discrimination than consumed in the task. This phenomenon is certainly distinct from the result in which one can distinguish a set of MESSs using entanglement as a catalyst by the teleportation-and-repreparation method, where the net change of entanglement is zero [6].

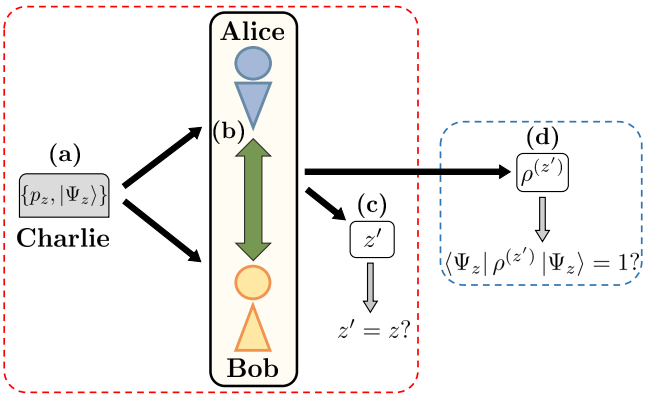


Figure 1: Schematic of conventional state discrimination task (red dashed box) and NDSD task (red dashed + blue dashed boxes). (a) Charlie chooses a state from the ensemble $\{p_z, |\Psi_z\rangle\}$ and distributes it to Alice and Bob. (b) Alice and Bob perform (local) operations including measurements. (c) A classical answer z' is determined from the measurement outcomes. If $z' = z$, the task succeeds. (d) For NDSD, Alice and Bob output the classical answer z' and the quantum state $\rho^{(z')}$ after performing their operations. The nondisturbance of the state can be checked by Charlie, and the NDSD succeeds when both $z' = z$ and $\langle\Psi_z|\rho^{(z')}\,|\Psi_z\rangle = 1$ are satisfied.

*hjkwon@kias.re.kr

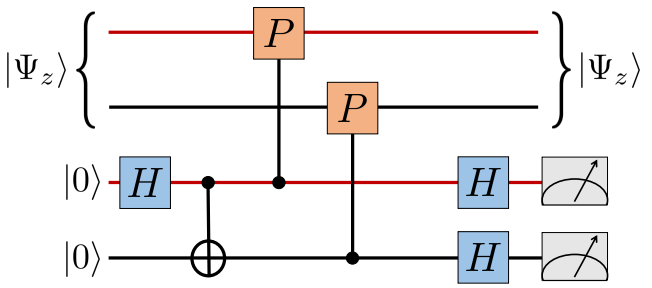


Figure 2: Circuit diagram for determining the sign information of the stabilizer PP. Using additional MES $1/\sqrt{2}(|00\rangle + |11\rangle)$, one can perform controlled Pauli operations in the local parties Alice (red horizontal lines) and Bob (black horizontal lines). If the outcomes of the local measurements in the basis $|\pm\rangle$ match, the measurement effect is $\frac{\mathbb{I}_4+PP}{2}$. If it does not match, $\frac{\mathbb{I}_4-PP}{2}$ is acted.

2 Results

2.1 Non-destructive state discrimination

Our non-destructive state discrimination scheme is depicted in Fig. 1. In a conventional state discrimination, Alice and Bob produce a classical answer z', and Charlie check whether $z' = z$. On the other hands, in the proposed scheme, they send the final quantum state $\rho^{(z')}$ to Charlie for confirming non-destructiveness. This modification leads an interesting results as follows:

Theorem 1 *Suppose there are k bipartite MESs with equal probability. Then any classical strategy (separable operation) for local NDSD has no advantage over random guessing.*

Note that this result holds for separable operations, which strictly include LOCC, so it is also valid for LOCC. We highlight that the success probability does not depend on the local dimension. Therefore, even two MESs in any dimension cannot be locally discriminated in a non-destructive way, and the optimal success probability of a classical strategy is $1/2$. Since any two orthogonal pure states can be perfectly distinguished with LOCC [4], the condition of non-destructiveness makes a large discrepancy between quantum and classical strategies. In comparison, for a conventional (destructive) state discrimination, the upper bound of the classical success probability can reach d/k, which scales by the local dimension d [5].

2.2 Entanglement cost for non-destructive state discrimination

We propose a totally non-destructive method for a perfect NDSD using stabilizer formalism and syndrome measurement [7] and compute the entanglement cost for a perfect NDSD. First, we consider a subset of MESs called MESSs constructed as

$$\rho_{\mathrm{MESS}} = \frac{1}{4^n}\prod_{i=1}^{n}\left(\mathbb{I}_{4^n} \pm (ZZ)^i\right)\left(\mathbb{I}_{4^n} \pm (XX)^i\right)_{A_iB_i}, \quad (1)$$

where $(PP)^i = \mathbb{I}_4^1 \otimes \cdots \otimes (PP)^i \otimes \cdots \otimes \mathbb{I}_4^n$ are two-qubit Pauli operators acting on A_iB_i qubits. Then we can obtain 4^n MESSs by choosing the signs of $(ZZ)^i$ and $(XX)^i$. In other words, we have a representation for 4^n MESSs by a set of $2n$ sign elements $\{+,-\}^{2n}$. Next, we introduce a method of determining the signs of the MESSs non-destructively. Namely, since four Bell states are considered as those that have undergone local bit flip X error or phase error Z on the Φ^0, we can detect the errors by syndrome measurements. This can be done by consuming an additional 1 ebit, Φ^0 (Fig. 2). Specifically, the state after controlled-P operations is given by

$$\frac{1}{\sqrt{2}}\left(|00\rangle_{A'B'}|\Psi_z\rangle_{AB} + |11\rangle_{A'B'}P\otimes P|\Psi_z\rangle_{AB}\right), \quad (2)$$

where $|\Psi_z\rangle$ is one of four Bell states. If the outcomes of the local measurements in the basis $|\pm\rangle$ coincide, the measurement effect is $\frac{\mathbb{I}_4+PP}{2}$, and if not, $\frac{\mathbb{I}_4-PP}{2}$. Therefore we can decide the sign of PP as $+$ for matched outcomes and $-$ for unmatched ones, without destructing $|\Psi_z\rangle$. In fact, our method is at least as good as the teleportation-and-repreparation for NDSD of MESSs.

Theorem 2 *For an NDSD task for a given set of MESSs, the teleportation-and-repreparation method can be simulated by the stabilizer method with the same entanglement cost.*

Our interest then moves to find an example showing a strict gap between two strategies. The following examples demonstrate such gaps.

2.3 Examples

We provide explicit examples, where the stabilizer method is strictly better than the teleportation scheme in a perfect NDSD of MESSs. The first example is the discrimination of three Bell states. Let us consider uniformly distributed three Bell states $\{|\Phi^0\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle), |\Phi^1\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle), |\Phi^2\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)\}$. Since the optimal entanglement cost of the perfect conventional state discrimination is 1 ebit [8], the cost of the teleportation-and-repreparation method is 2 ebit. For exploiting the stabilizer method, let us represent the three Bell states as a sign table such that

	ZZ	XX
$\|\Phi^0\rangle$	$+$	$+$
$\|\Phi^1\rangle$	$+$	$-$
$\|\Phi^2\rangle$	$-$	$+$

If we measure the sign of the first generator, ZZ, $-$ comes out with probability $1/3$ and $+$ with $2/3$. In the former case, we can determine the received state as $|\Psi^2\rangle$, thus the procedure is terminated. In the latter case, we need to obtain the sign of the second generator, XX, by using another ebit. Thus the average entanglement cost is given by $\frac{1}{3}\times 1 + \frac{2}{3}\times 2 = \frac{5}{3}$ (ebits). In fact, this cost is optimal for the sign table because for distinguishing them, we can minimally assign one bit to $|\Psi^2\rangle$ as 0, and two bits for the

others, $\left|\Psi^0\right\rangle$ with 10 and $\left|\Psi^1\right\rangle$ with 01. We can interpret the correspondence between the quantum states and the strings as a *uniquely decodable code* or *prefix code*. The optimality of this scheme among the stabilizer method is ensured by the Kraft-McMillan inequality from the coding theory [9, 10]. We call this cost $\{1, 2, 2\}$, and then the entanglement cost is $\{2, 2, 2\}$ for the teleportation-and-repreparation method. In other words, the stabilizer method can use the sign information of each column in the sign table, but the teleportation method has to read the signs of two columns at once, so there exists a gap in average entanglement cost between the two strategies, 1/3 ebits. The next example shows a more interesting situation even considering the LOCC equivalence, in which a positive net entanglement remains on average after the discrimination task. Suppose we have a set of 6 MESSs such that

$$\{\Phi^0\Phi^1\Phi^2, \Phi^0\Phi^2\Phi^1, \Phi^1\Phi^0\Phi^2, \Phi^1\Phi^2\Phi^0, \Phi^2\Phi^0\Phi^1, \Phi^2\Phi^1\Phi^0\}, \tag{3}$$

where each state is a product of three Bell states ($n = 3$), and we omit the ket notation. First, let us compute the cost of the teleportation-and-repreparation scheme. Since all states consist of permutation of three Bell states $\{\left|\Phi^0\right\rangle, \left|\Phi^1\right\rangle, \left|\Phi^2\right\rangle\}$, we can choose the first qubit for the teleportation. Then one can determine the first qubit among the three Bell states with 2 ebits non-destructively, and for each result, there are two possibilities. Thus by using another ebit, one can measure the second qubit to determine the state between the two remaining Bell states, so the total cost is 3 ebits. This cost, i.e., $\{3, 3, 3, 3, 3, 3\}$, is not optimal for the set, however, the optimal one is 16/6 ebits, $\{2, 2, 3, 3, 3, 3\}$. We can show that the stabilizer method can render the optimal entanglement cost, thus the gap is 1/3 ebits. We emphasize that this gap holds even if we allow LOCC for the set of states. Interestingly, we can gain extra 1/3 ebits on average per round of the discrimination task, *entanglement earning*. This is a unique feature of the stabilizer method because the qubit teleportation-and-repreparation scheme cannot get a positive net entanglement. Note that in Ref. [6], a set of 4×4 MESSs is introduced, i.e., $\{\Phi^0\Phi^0, \Phi^1\Phi^1, \Phi^1\Phi^2, \Phi^1\Phi^3\}$. Although the set of MESSs cannot be locally distinguishable, the teleportation-and-repreparation scheme gives the optimal cost of 2 ebits ($\{2, 2, 2, 2\}$), owing to the four Bell basis in the second qubit. Consequently, both strategies can achieve the optimal cost, and effectively zero entanglement is consumed as a catalyst. Our example highlights a crucial difference between the two strategies and entanglement gain in the discrimination task.

Moreover, we can find generic sets of MESSs having gaps between the two schemes.

Theorem 3 *Let us construct a set of MESSs as follows. The first qubit is uniformly picked from three Bell states $\{\Phi^i\}_{i=0}^2$, and from the second qubit to n-th qubit, each qubit is uniformly picked from two Bell states $\{\Phi^i\}_{i=0}^1$. This produces a set of $3 \times 2^{n-1}$ MESSs. Then for the perfect NDSD, the stabilizer method can reach the optimal entanglement cost, $n + 2/3$ ebits, but the cost of the teleportation-and-repreparation is $n + 1$ ebits.*

This result includes the previous examples as special cases when $n = 1$ and $n = 2$. Note that we can find generic sets of MESSs exhibiting the constant gap 1/3 ebits between two strategies with considering LOCC equivalence. Moreover, our method can be applied in a more general situation involving a mixed state, where a MESS $|\Psi\rangle$ and its orthogonal complement. In this case, we can check the non-destructive condition by applying the projector of the input state $|\Psi\rangle\langle\Psi|$, which should give 1 for the input state $|\Psi\rangle$ and 0 for its orthogonal complement. Although any two pure orthogonal states can be distinguished by LOCC, this is not the case because one of them is a mixed state.

Theorem 4 *For a MESS $\rho_1 = |\Psi\rangle\langle\Psi|$ and its orthogonal complement $\rho_2 = \frac{\mathbb{I} - |\Psi\rangle\langle\Psi|}{2^{2n}-1}$, the entanglement cost in ebits of the stabilizer method for the perfect NDSD is given by*

$$n + 1 - \frac{n}{2^{2n}-1},$$

and of the teleportation method follows as

$$n + \frac{4}{3} - \frac{n}{2^{2n}-1}.$$

We can figure out that the gap between the two strategies is 1/3 ebits, regardless of the dimension. It has been known that the optimal entanglement cost for standard discrimination of those states for $n = 1$ is 1 ebit [11]. This matches our result of the teleportation scheme, i.e., 2 ebits, where an additional ebit is needed to reconstruct the initial state. For $n \geq 2$, if $\rho_1 \otimes |\alpha\rangle$ and $\rho_2 \otimes |\alpha\rangle$ can be unambiguously discriminated, then the Schmidt number of the ancillary state is $Sch(|\alpha\rangle) \geq 2^n$ for a conventional discrimination task [11].

3 Discussion

We emphasize that our method can be applied to more general cases, for example, high-dimensional systems using qudit stabilizers. A more interesting case is a quantum network involving multipartite entanglement. Since a set of MESSs consists of a target stabilizer state and error-occurred states, NDSD can be a task of detecting and modified the error in the network. In that case, the teleportation and repreparation method is seemingly inefficient. Using our scheme, however, we can locally detect and modify the errors in a quantum network with a low cost of additional entanglement. For instance, if there exists n-party GHZ state in the quantum network as entanglement resource, i.e., $1/\sqrt{2}(|0\cdots0\rangle + |1\cdots1\rangle)$, one can decide the sign of n-qubit stabilizer $P\cdots P$ using the GHZ state as our scheme in Fig. 2. Moreover, a resource entanglement can be a lossy GHZ state or W state for more general situations. Studies in those directions are attractive future works.

References

[1] S. M. Barnett and S. Croke, Quantum state discrimination. Advances in Optics and Photonics, **1**, 238, 2009.

[2] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications. Journal of Physics A: Mathematical and Theoretical, **48**, 083001, 2015.

[3] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. Physical Review A, **59** 1070, 1999.

[4] J. Walgate, A. J. Short, L. Hardy, and V. Vedral. Local distinguishability of multipartite orthogonal quantum states. Physical Review Letters, **85**, 4972, 2000.

[5] M. Nathanson. Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases. Journal of Mathematical Physics, **46**, 062103, 2005.

[6] N. Yu, R. Duan, and M. Ying. Four locally indistinguishable ququad-ququad orthogonal maximally entangled states. Physical Review Letters, **109**, 020506, 2012.

[7] D. Gottesman. Stabilizer codes and quantum error correction. California Institute of Technology, 1997.

[8] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu. Limitations on separable measurements by convex optimization. IEEE Transactions on Information Theory, **61**, 3593, 2015.

[9] L. G. Kraft. A device for quantizing, grouping, and coding amplitude-modulated pulses. Massachusetts Institute of Technology, 1949.

[10] B. McMillan. Two inequalities implied by unique decipherability. IRE Transactions on Information Theory, **2**, 115, 1956.

[11] N. Yu, R. Duan, and M. Ying. Distinguishability of quantum states by positive operator-valued measures with positive partial transpose. IEEE Transactions on Information Theory, **60**, 2069, 2014.

Recovery of entanglement distributed via entanglement swapping over noisy quantum channel

Sewon Jeong[1 2] Hyang-Tag Lim[1] Yongsu-Kim[1] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Korea*
[2] *Department of Physics, Ewha Womans Univeristy, Seoul, 03760, Korea*

Abstract. We propose a scheme to recover the degree of entanglement of the photonic quantum state distributed by entanglement swapping under noise. We define and employ the reversing operation in each qubit mode to reverse the effect of noise and recover the entanglement. We first consider the effect of damping noise with various different scenarios by changing the noise and reversing strength. We found that the optimal reversing operation allows us to recover and increase the distributed entanglement under noisy quantum channel to some extent. We also apply our scheme to recover entanglement against photon loss in entanglement swapping by using the noiseless linear amplification (NLA). We observe the recovery of the entanglement distributed by entanglement swapping over lossy channel. We expect that our scheme can be used as a tool to develop long distance quantum communication via noisy quantum channel.

Keywords: Entanglement swapping, Reversing operation, Noiseless linear amplification, Quantum communication

1 Introduction

Entanglement swapping is essential for realizing long distance quantum communication. However, noises and losses reducing the degree of entanglement inevitably and significantly are the major obstacle towards practical and scalable quantum network.

In this work, we study the effect of noise on the entanglement of photonic states distributed via noisy entanglement swapping, and propose a scheme to recover the degree of entanglement of the state by reversing operation [1]. We define and employ the reversing operation in each qubit mode to reverse the effect of noise. We first consider the effect of damping noise with various different scenarios of entanglement swapping. We change the strength of the damping noise and the reversing operation accordingly. We use the concurrence as a measure of the distributed entanglement. We found that reversing operation allows us to recover and increase the entanglement degree of the quantum states distributed by noisy entanglement swapping to some extent. We also analyze the optimal reversing operation under given noise strength in various different scenarios.

We then also consider the reversal of photon loss, which is the most detrimental factor for building long distance quantum communication channel by entanglement swapping. The noiseless linear amplification (NLA)[2, 3] is one type of experimental scheme for reversing operation against the effect of loss in each photonic qubit modes. We found that the entanglement of photonic qubit states distributed by entanglement swapping over lossy channel can be recovered by applying NLA to some extent and discuss on the optimal NLA operation for a given lossy channel. We expect that our scheme provide an efficient scheme for realizing long distance quantum communication toward scalable quantum network with photons.

*swleego@gmail.com

Figure 1: Entanglement swapping

2 Model

We consider the entanglement swapping of two entangled states (A-B) and (C-D) as illustrated in the Figure 1. Bell state measurement applying on B and C qubits from two entangled pairs (A-B and C-D) serves as the connector between two entangled pairs resulting in an entangled state between A and D. In this work we consider the amplitude damping noise that degrades the degree of entanglement of the final state (A-D). The damping noise can be represented by an operator $|0\rangle\langle 0| + \sqrt{1-D}|1\rangle\langle 1|$, where D is the strength of amplitude damping.

We then consider two different cases: One is O-D-D-O case, in which the node B and C experience amplitude damping, while the other O-D-O-D case in which the node B and D experience amplitude damping. We investigate and compare the effect of damping noise in two cases on the entanglement shared between A and D nodes after the entanglement swapping. In both cases, we observe the degradation of the entanglement, which become significant as increasing the strength of amplitude damping (D), as shown by dotted lines in Figure 2.

3 Reversing the effect of damping noise

Let us apply a reversing operation of quantum measurement [4] to reverse the damping noises on the quantum state. The reversing operation for a given damping noise can be defined by two measurement operators $R_1 = \sqrt{1-R}|0\rangle\langle 0| + |1\rangle\langle 1|$ and $R_2 = \sqrt{R}|1\rangle\langle 0|$, where R is the revering strength.

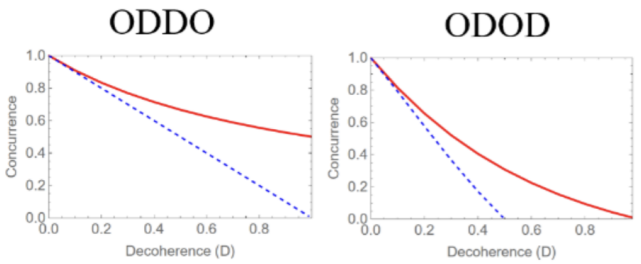


Figure 2: Entanglement distributed between A and D nodes: dotted lines show the concurrence against decoherence strength D, while solid lines are obtained by applying reversing operation with the same strength $R = D$

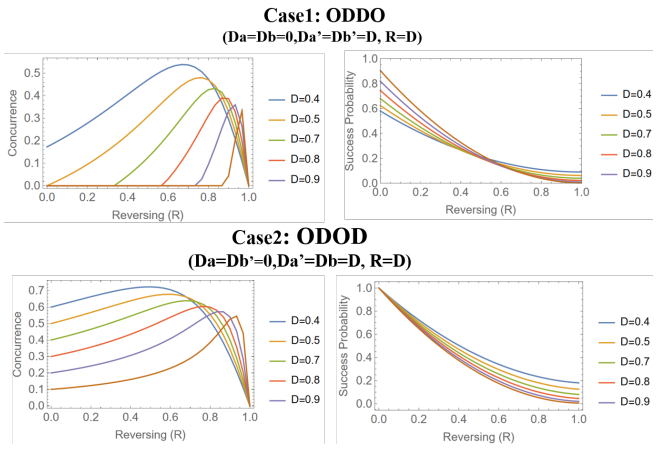


Figure 3: Entanglement recover by reversion operation with different strength R under noise with strength D

We also consider two cases: O-D-D-O and O-D-O-D. We first apply the same strength of reversing operation with the strength of the damping noise on the same node that noise occurs, i.e. $R = D$. The result is given in Figure 2. In both cases, we observe entanglement recovery which becomes more effective when the damping noise strength increases. We also investigate the amount of entanglement recovery by changing the strength of reversing operation R for a fixed strength of damping noise D as shown in the Figure 3. We found that the maximum recovery can be achieved when the the reversing strength is slightly larger than damping strength $R > D$ [6].

4 Reversing the effect of photon loss

We now apply noiseless linear amplification (NLA) as a reversing operation of the effect of photon loss, which can be experimentally realized by a scheme named "Quantum scissor" as illustrated in Figure 4. The output state then can be written as

$$\hat{T}_1|\psi\rangle = \sqrt{\frac{1}{2(g^2+1)}}(c_0|0\rangle + gc_1|1\rangle), \qquad (1)$$

where $g = (1-\eta)/\eta$ is the gain of the amplification [5]. This process can be understood as a teleportation process

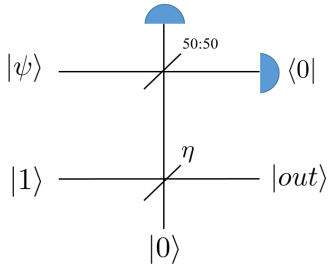


Figure 4: Schematic of the quantum scissor scheme

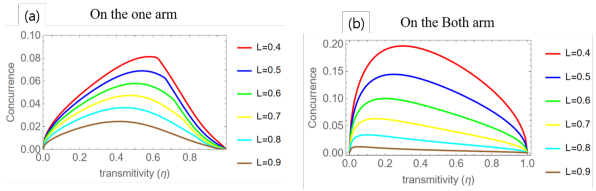


Figure 5: The changes of entanglement of $|\phi^+\rangle$ (a) loss and NLA on one arm, and (b) both arms

via a single photon entangled state $\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$ so that the output state is in the truncated space up to the Fock basis $n = 1$.

We found that the entanglement can be recovered by NLA on the state experiencing when photon loss occurs (a) on the one arm or (b) two arms as shown in Figure 5. We investigate the recovery tendency by changing the transmitivity η of the experimental setup in Figure 4. Based on the result, we can optimize the experimental setup for a given different loss rate L [6].

5 Summary

We have proposed a scheme to recover entanglement of photonic qubits distributed by entanglement swapping over noisy quantum channel [6]. By applying the reversing operation, we have observed significant recovery of entanglement both for the effect of damping noise and losses. Based on our investigations, the reversing operation for a given noisy channel can be optimized to recover the maximum degree of entanglement. We expect that our scheme can be used as an efficient tool to realize long distance quantum communication via noisy quantum channel.

References

[1] Y. W. Cheong and S.-W. Lee. Balance between information gain and reversibility in weak measurement. Phys. Rev. Lett. **109**, 150402(2012).

[2] H. M. Chrzanowski, N. Walk, S. M. Assad,J. Janousek, S. Hosseini, T. C. Ralph , T. Symul, and P. K. Lam. Measurement-based noiseless linear amplification for quantum communication. Nature Photonics **8(4)**, 333-338 (2014).

[3] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde. Heralded noiseless linear amplification and distillation of entanglement. Nature Photonics **4(5)**, 316-319 (2010).

[4] S.-W. Lee, D.-G. Im, Y.-H. Kim, H.Nha, and M. S. Kim. Quantum teleportation is a reversal of quantum measurement. Phys. Rev. Res. **3**, 033119 (2021).

[5] M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph. Generalized quantum scissors for noiseless linear amplification. Phys. Rev. A, **102**, 063715 (2020).

[6] S. Jeong *et al.*, to be submitted (2023).

Exploring Shallow-Depth Boson Sampling for Scalable Quantum Supremacy

Byeongseon Go[1] * Hyunseok Jeong[1] †

[1] *Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea*

Abstract. Boson sampling is a sampling task proven to be hard to classically simulate under plausible assumptions, which makes it an appealing candidate for quantum supremacy. Due to a large noise rate for near-term quantum devices, it is still unclear whether those noisy devices maintain the quantum advantage for much larger quantum systems, and the alternative to evade the issue is to find evidence of hardness at the shallow-depth quantum circuit. We examine the limitation of the hardness argument at this shallow-depth regime for geometrically local architectures. We also propose a shallow-depth linear optical circuit architecture that can resolve those problems.

Keywords: Boson sampling, Quantum computational advantage, Photonic quantum computing

1 Introduction

Boson sampling [1] is a prominent candidate for demonstrating quantum advantage with near-term quantum devices. It is a sampling problem from the random linear-optical circuit instances, which has been complexity-theoretically proven to be hard to efficiently simulate with classical computers under plausible assumptions [1–3]. Ever since the theoretical foundation, there have been plenty of experimental results claiming the first realization of quantum advantage with boson sampling [4–6].

However, it remains unclear whether the quantum advantage can be maintained for larger quantum systems. The major obstacle to the scalability of the quantum advantage is the uncorrected noise on near-term quantum devices. There have been many results about efficient classical algorithms to simulate noisy boson sampling with various noise models, such as photon loss and partial distinguishability of photons [7–16]. Those results suggest that circuits with super-logarithmic circuit depth are vulnerable to noise and thus hinder the scalable quantum advantage. Hence, an obvious way to suppress the effect of noise is to consider shallow-depth circuits and investigate if we can still maintain hardness in shallow-depth circuits.

A crucial factor in proving the classical hardness of boson sampling, using the state-of-the-art technique, is the average-case hardness of output probability approximation within additive imprecision [1–3, 17]. Specifically, to get simulation hardness, most of the output probability instances of most of the linear optical circuits should be hard to approximate. We prove that for geometrically local circuit architectures, there is no average case hardness in the shallow-depth regime, as most of the probability instances are easy to estimate, regardless of circuit ensembles. Besides, if we employ local random circuit ensembles, a typical setup for recent experimental results [4, 5], their diffusive properties make the situation even worse, requiring additional circuit depth to get out the easiness regime.

Following the above examination, we find a linear-optical circuit architecture that can resolve the issues in the shallow-depth regime, using geometrically non-local gates. We numerically examine that the corresponding circuit architecture with each gate drawn from the local random unitary shows a fast convergence toward the global Haar random unitary, the requirement to achieve evidence of the average-case hardness [1], where the rate of convergence is insensitive to increasing system size. Those results demonstrate the potential of the circuit architecture to achieve the average-case hardness in the shallow-depth regime.

2 Limitations of Geometrically Local Architectures

A typical way to construct a random linear-optical network using local interactions is a local parallel circuit architecture, a parallel array of geometrically local beam splitters [18]. More formally, the d-dimensional local parallel circuit with depth D consists of $D/2d$ rounds, where a single round consists of $2d$ steps, 2 steps of the parallel application of local gates for each dimension. We also define the d-dimensional local parallel *random* circuit as a d-dimensional local parallel circuit with each gate drawn from the Haar measure on U(2) independently, where the configuration is motivated by recent experimental setups.

We consider both Fock-state boson sampling (FBS) and Gaussian boson sampling (GBS) schemes, and we consider the FBS scheme first. Let total mode number M, and the input state is N product of the single-photon state. M and N are polynomially related by $M = c_0 N^\gamma$. Using this convention, we prove the following theorem.

Theorem 1 *(Any circuit ensemble) For d-dimensional local parallel circuit of depth $D \leq \mathcal{O}(N^{\frac{\gamma-1}{d}})$ and arbitrarily chosen input mode configuration, most of the outcomes of FBS have zero output probability.*

The theorem implies that for circuits with a depth below a certain threshold, most output instances have zero probabilities, which are easy to approximate, for any input configuration and circuit instance.

*gbs1997@snu.ac.kr
†jeongh@snu.ac.kr

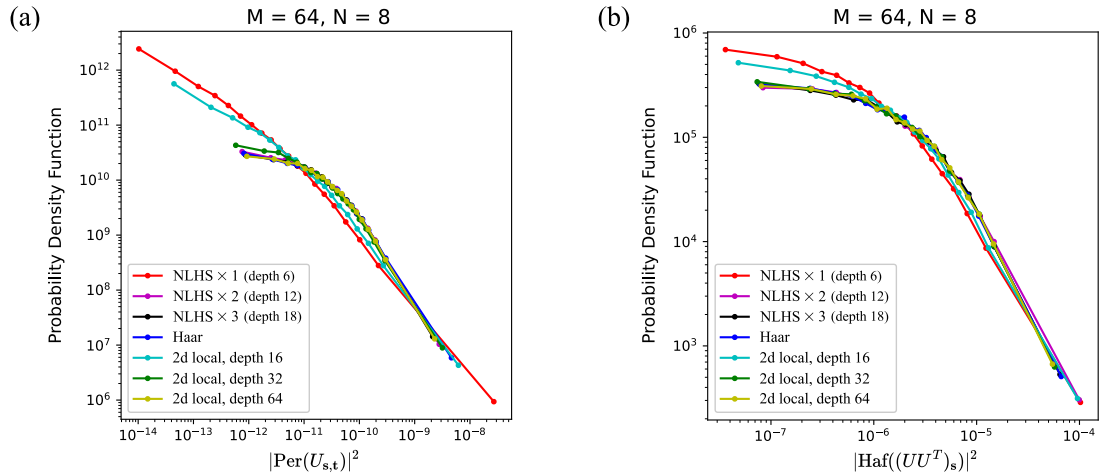


Figure 1: Probability density function for output probabilities of (a) FBS and (b) GBS with $M = 64$ and $N = 8$, for random NLHS circuit with different repetition numbers and $2d$ local parallel random circuit with different depths. The distribution corresponding to the global Haar unitary circuit is also displayed as an ideal case.

Furthermore, if we choose the local random circuit ensembles, which correspond to the d-dimensional local parallel random circuit, we find that additional circuit depth is required to get out of the easiness regime.

Theorem 2 *(Local random ensemble) For d-dimensional local parallel random circuit of depth $D \leq \mathcal{O}(N^{\frac{2(\gamma-1)}{d}-\lambda})$ for any $\lambda > 0$, $0 < \beta < 1$ and input mode configuration, it is easy to estimate the output probabilities of FBS within additive error $\epsilon = poly(N)^{-1}\frac{N!}{M^N}$, for $1-\xi$ portion of output instances with probability $1-\delta$ over the random circuit instances, where ξ and δ are exponentially small with system size.*

For the GBS scheme, we get similar results to the FBS case. Let total mode number M, and now the input state is K product of the single-mode squeezed vacuum states with equal squeezing. We focus on fixed output photon number $2n$, which we will set as mean photon number, and M and n are polynomially related as $M = c_1 n^\gamma$. Using these notations, we prove the following theorem.

Theorem 3 *(Any circuit ensemble) For d-dimensional local parallel circuit of depth $D \leq \mathcal{O}(n^{\frac{\gamma-1}{d}})$, arbitrary K within $n \leq K \leq M$ and arbitrarily chosen input mode configuration, most of the outcomes of GBS have zero output probability.*

Theorem 3 states that regardless of the number of input single-mode squeezed vacuum states and their configuration, most of the outcomes of GBS have zero probabilities which are easy to approximate under a certain degree of polynomial depth, for any circuit instances.

Moreover, for the case of the local random circuit ensembles, we find that the argument from the proof of Theorem 2 also holds for the GBS scheme.

Theorem 4 *(Local random ensemble) For d-dimensional local parallel random circuit of depth $D \leq \mathcal{O}(n^{\frac{2(\gamma-1)}{d}-\lambda})$ for any $\lambda > 0, 0 < \beta < 1$, $n \leq K \leq M$ and input mode configuration, it is easy to estimate the output probabilities of GBS within additive error $\epsilon = poly(n)^{-1}\frac{(2n)!}{M^{2n}}$ for $1-\xi$ portion of output instances with probability $1-\delta$ over the random circuit instances, where ξ and δ are exponentially small with system size.*

3 Geometrically Non-Local Architecture: Hypercubic Structure

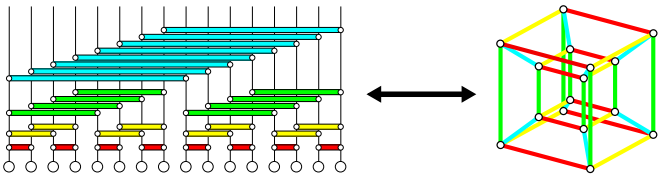


Figure 2: A Schematic of a one-cycle of NLHS circuit for total mode number $M = 2^4$. In this case, the architecture of the circuit can be interpreted as a $4d$ hypercube, also known as a tesseract.

An obvious way to resolve the problems we addressed previously is to consider non-local interactions along modes, i.e., geometrically non-local unitary gates are available. In this case, we find a circuit that can mitigate the problems within logarithmic circuit depth, where the architecture of the circuit was first introduced in [19] in order to implement Fourier matrices. Throughout this section, we refer to the circuit as a non-local hypercubic structure (NLHS) circuit.

A single round of the NLHS circuit is a one-cycle of a hypercubic sequence of parallel applications of unitary gates, and an example of the single round for $M = 2^4$ is illustrated in Figure 2. For random circuit instances, we employ a conventional setup such that all unitary gates composing the NLHS circuit as independently chosen random beam splitters, each drawn from Haar measure on U(2).

We investigate the output probability distribution of FBS and GBS over the random NLHS circuit, with in-

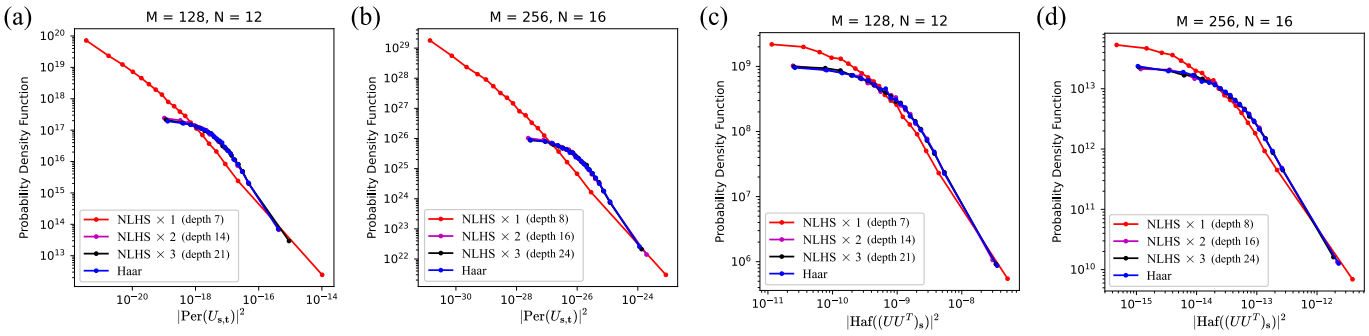


Figure 3: Probability density function for (a-b) FBS and (c-d) GBS, with $M = 128, 256$ and $N = 12, 16$ each.

creasing depth (i.e., repeating a single round of the random NLHS circuit). For the investigation, we employ the probability density function, which is a modified version of the histogram [1].

First, we compare output probability distribution from the random NLHS circuit with $2d$ local parallel random circuit, for mode number $M = 64$ and output photon number $N = 8$, both for FBS and GBS schemes. We sample 10000 unitary matrices for each depth of random NLHS circuits, $2d$ local circuits, and global Haar random circuit as an ideal case. For each unitary matrix, we calculate output probability values (unnormalized for the GBS case) for randomly chosen input/output, and using those values we draw a probability density function (Figure 1). The result shows that an iteration of the random NLHS circuit makes quick convergence to the distribution of the Haar random unitary, compared to the $2d$ local circuit.

Next, we examine how the convergence behavior varies as system size scales. We increase the mode number as $M = 128, 256$ and sample 10000 unitary matrices for each repetition of the random NLHS circuit and from the global Haar measure. We calculate output probability values for randomly chosen input/output for output photon $N = 12, 16$ respectively, and we draw a probability density function (Figure 3). The result shows that the number of repetitions required to imitate the distribution from the global Haar random unitary is insensitive to system size.

We also investigate how entanglement along the modes varies with the repetition of the NLHS circuit. Specifically, we focus on Rényi-2 entropy of reduced states of output states of GBS [20], each evolved by different repetitions of random NLHS circuits or global Haar random unitary. For $M = 256$, we prepare M product of single-mode squeezed vacuum states evolved by randomly sampled 10000 unitary matrices for each circuit, and calculate the average of Rényi-2 entropy with respect to different subsystem sizes (Figure 4). The result shows the entanglement generation with an increasing stacking number, where the distribution converges to the distribution from the global Haar random unitary. It is notable that the required number of repetitions for the convergence is comparably small, similar to the previous results.

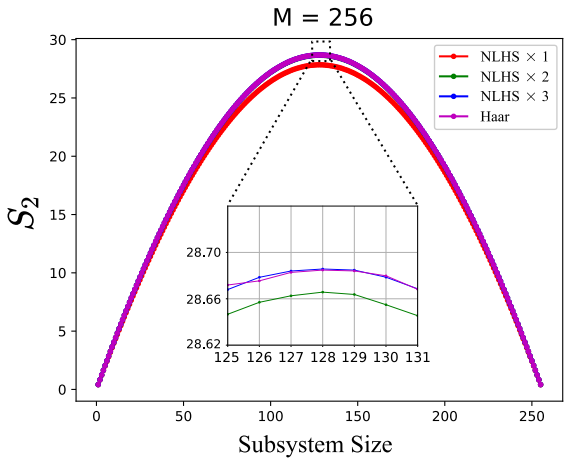


Figure 4: The average of Rényi-2 entropy with respect to different subsystem sizes, for mode number $M = 256$.

4 Conclusion

We examined that for local circuit architectures, there is no average-case hardness below a certain polynomial depth, which implies the limitation for achieving sampling hardness at the shallow depth regime. We proposed geometrically non-local circuit architecture which can restrain the issues we addressed within the shallow depth regime. The corresponding architecture shows quick convergence behavior toward the global Haar random unitary circuit, insensitive to system size. Hence, it has the potential to be used as an approximate Haar measure with shallow depth random circuit and be utilized as an architecture for scalable quantum advantage with boson sampling.

References

[1] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[2] Craig S Hamilton, Regina Kruse, Linda Sansoni, Sonja Barkhofen, Christine Silberhorn, and Igor Jex. Gaussian boson sampling. *Physical review letters*, 119(17):170501, 2017.

[3] Abhinav Deshpande, Arthur Mehta, Trevor Vincent, Nicolás Quesada, Marcel Hinsche, Marios Ioannou,

Lars Madsen, Jonathan Lavoie, Haoyu Qi, Jens Eisert, et al. Quantum computational advantage via high-dimensional gaussian boson sampling. *Science advances*, 8(1):eabi7894, 2022.

[4] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[5] Han-Sen Zhong, Yu-Hao Deng, Jian Qin, Hui Wang, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Dian Wu, Si-Qiu Gong, Hao Su, et al. Phase-programmable Gaussian boson sampling using stimulated squeezed light. *Physical review letters*, 127(18):180502, 2021.

[6] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022.

[7] Gil Kalai and Guy Kindler. Gaussian noise sensitivity and bosonsampling. *arXiv preprint arXiv:1409.3093*, 2014.

[8] Jelmer Renema, Valery Shchesnovich, and Raul Garcia-Patron. Classical simulability of noisy boson sampling. *arXiv preprint arXiv:1809.01953*, 2018.

[9] Jelmer J Renema, Adrian Menssen, William R Clements, Gil Triginer, William S Kolthammer, and Ian A Walmsley. Efficient classical algorithm for boson sampling with partially distinguishable photons. *Physical review letters*, 120(22):220502, 2018.

[10] Valery S Shchesnovich. Noise in boson sampling and the threshold of efficient classical simulatability. *Physical Review A*, 100(1):012340, 2019.

[11] Alexandra E Moylett, Raúl García-Patrón, Jelmer J Renema, and Peter S Turner. Classically simulating near-term partially-distinguishable and lossy boson sampling. *Quantum Science and Technology*, 5(1):015001, 2019.

[12] Daniel Jost Brod and Michał Oszmaniec. Classical simulation of linear optics subject to nonuniform losses. *Quantum*, 4:267, 2020.

[13] Changhun Oh, Liang Jiang, and Bill Fefferman. On classical simulation algorithms for noisy boson sampling. *arXiv preprint arXiv:2301.11532*, 2023.

[14] Michał Oszmaniec and Daniel J Brod. Classical simulation of photonic linear optics with lost particles. *New Journal of Physics*, 20(9):092002, 2018.

[15] Raúl García-Patrón, Jelmer J Renema, and Valery Shchesnovich. Simulating boson sampling in lossy architectures. *Quantum*, 3:169, 2019.

[16] Haoyu Qi, Daniel J Brod, Nicolás Quesada, and Raúl García-Patrón. Regimes of classical simulability for noisy gaussian boson sampling. *Physical review letters*, 124(10):100502, 2020.

[17] Adam Bouland, Bill Fefferman, Zeph Landau, and Yunchao Liu. Noise and the frontier of quantum supremacy. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1308–1317. IEEE, 2022.

[18] William R Clements, Peter C Humphreys, Benjamin J Metcalf, W Steven Kolthammer, and Ian A Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, 2016.

[19] Andrea Crespi, Roberto Osellame, Roberta Ramponi, Marco Bentivegna, Fulvio Flamini, Nicolò Spagnolo, Niko Viggianiello, Luca Innocenti, Paolo Mataloni, and Fabio Sciarrino. Suppression law of quantum states in a 3d photonic fast fourier transform chip. *Nature communications*, 7(1):10469, 2016.

[20] Joseph T Iosue, Adam Ehrenberg, Dominik Hangleiter, Abhinav Deshpande, and Alexey V Gorshkov. Page curves and typical entanglement in linear optics. *arXiv preprint arXiv:2209.06838*, 2022.

Toward Incompatible Quantum Limits on Multiparameter Estimation

Binke Xia[1 2 3 *] Jingzheng Huang[1 2 3 †] Guihua Zeng[1 2 3 ‡]

[1] *State Key Laboratory of Advanced Optical Communication Systems and Networks, Institute for Quantum Sensing and Information Processing, School of Sensing Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[2] *Hefei National Laboratory, Hefei 230088, China*
[3] *Shanghai Research Center for Quantum Sciences, Shanghai 201315, China*

Abstract. Achieving the ultimate precisions for multiple parameters simultaneously is a challenging task in quantum physics. Due to the Heisenberg uncertainty principle, the joint optimal measurements for incompatible parameters is prohibited. In this study[1], we propose a criterion to surpass this constraint by simultaneously increasing the variances of the parameter generators, enabling improved precision. For demonstration, we utilize the high-order Hermite-Gaussian beams for simultaneous estimation of spatial displacement and angular tilt of light. Experimental results achieve precisions of 1.45 nm and 4.08 nrad. Our findings deepen understanding of the Heisenberg uncertainty principle in multiparameter estimation and contribute to quantum metrology applications.

Keywords: Multiparameter estimation, Heisenberg uncertainty relation, Hermite-Gaussian beams

1 Background

Heisenberg's uncertainty principle serves as a fundamental pillar of quantum physics. Due to distinct physical parameters necessitate distinct optimal measurement operators, this principle prohibits the simultaneous execution of optimal measurements for parameters if these measurements are non-commutative[2]. Consequently, one parameter's measurement precision deviates considerably from its theoretical limits when the other parameter approaches its theoretical limits, giving rise to the incompatibility of quantum precision limits in multiparameter estimation. Alleviating this incompatibility enables the simultaneous effective enhancement of overall measurement precisions for the two parameters. This issue has emerged as a central concern in the realm of quantum physics and quantum precision measurement, with the synchronization of measurement precisions for incompatible parameters to quantum limits posing the most formidable challenge. Addressing this challenge holds practical significance in the domains of quantum sensing[3], quantum communication[4], and quantum computing[5].

2 Results

This study addresses the issue of incompatible precision limits in quantum multiparameter estimation and presents theoretical and experimental investigations. The key accomplishments are outlined as follows.

Despite the inability to achieve simultaneous quantum limits for incompatible parameters, a trade-off relation exists, which provides a practical attainable lower bound of precisions for these parameters[6]. Through an analysis of the trade-off relation in the context of incompatible parameters, we establish a theoretical criterion for quantifying the level of incompatibility, which is given as

$$\mathcal{S}_{ij} = \frac{4\langle \Delta \hat{H}_i^2 \rangle \langle \Delta \hat{H}_j^2 \rangle}{\left| \langle [\hat{H}_i, \hat{H}_j] \rangle \right|^2}, \tag{1}$$

where $\hat{H}_i$, $\hat{H}_j$ are the generators of unknown parameters g_i, g_j, respectively. This criterion highlights that

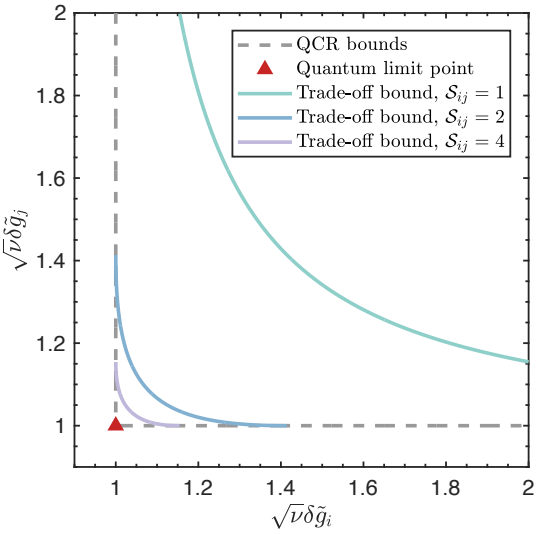


Figure 1: Precision limits of estimating parameters g_i and g_j simultaneously. The x-axis and y-axis are separately the normalized estimation errors of parameters g_i and g_j. The gray dashed lines are the quantum precision limits for parameters g_i and g_j, respectively. The cross point (red triangle in figure) of gray dashed lines is the quantum limit point where both parameters achieve the theoretical ultimate precision. The green solid curve stands for the trade-off bound of parameters g_i and g_j with $\mathcal{S}_{ij} = 1$, which corresponds to the minimum-uncertainty probe state. The blue and purple solid curves are separately the trade-off bounds with $\mathcal{S}_{ij} = 2$ and $\mathcal{S}_{ij} = 4$.

*mogician@sjtu.edu.cn
†jzhuang1983@sjtu.edu.cn
‡ghzeng@sjtu.edu.cn

the incompatibility of precision limits can be mitigated by concurrently increasing the uncertainty of the probe with respect to the generators of incompatible parameters during simultaneous estimation of two parameters in a multi-parameter quantum estimation task. Additionally, this approach enables the enhancement of the overall measurement accuracy for these two parameters. The highlights of this result are illustrated in Fig. 1.

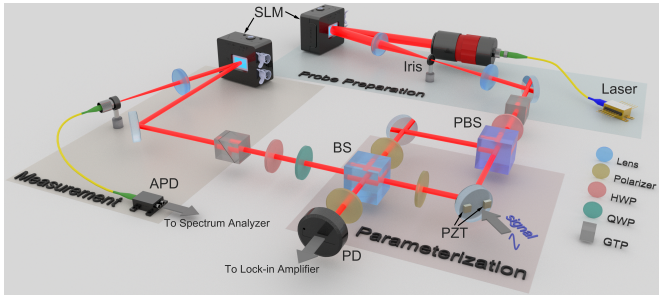


Figure 2: Diagram of experimental setup. The n-order HG beam is converted from a expanded Gaussian beam by a spatial light modulator(SLM) and a spatial filter system. The incompatible parameters (position displacement and momentum kick) are introduced by a piezoelectric driven mirror in the Mach-Zehnder interferometer. The other SLM is used to perform the projective measurements to demodulate the parameters.

In practice, the transverse displacement and angular tilt of light are a pair of typical incompatible parameters. By utilizing the Hermitian-Gaussian mode probe, the measurement precisions of the transverse displacement and angular tilt parameters for a single beam can effectively converge towards their respective quantum limits simultaneously. The experimental setup is depicted in Fig. 2. As a result, we achieve a precision of 1.45 nm for the transverse displacement parameter and a precision of 4.08 nrad for the angular tilt parameter in experiments. The experiments employ the post-selection weak measurement technique to mitigate technical noise. Furthermore, this study demonstrates that increasing the number of Hermite-Gaussian probe modes concurrently enhances the measurement precisions of both parameters. The experimental results are illustrated in Fig. 3, where g_1 and g_2 are the parameters associated with the transverse displacement and the angular tilt of light beams, respectively.

3 Significance

This work holds significant importance as it establishes a comprehensive theoretical criterion to quantify the degree of incompatibility between quantum parameters. This criterion serves as a foundational tool in addressing the challenge of incompatibility in precision limits during quantum multiparameter estimation. Furthermore, this study successfully achieves practical measurements of incompatible parameters for a light beam, attaining simultaneous quantum precision limits that are at the forefront. These results have vast potential in various

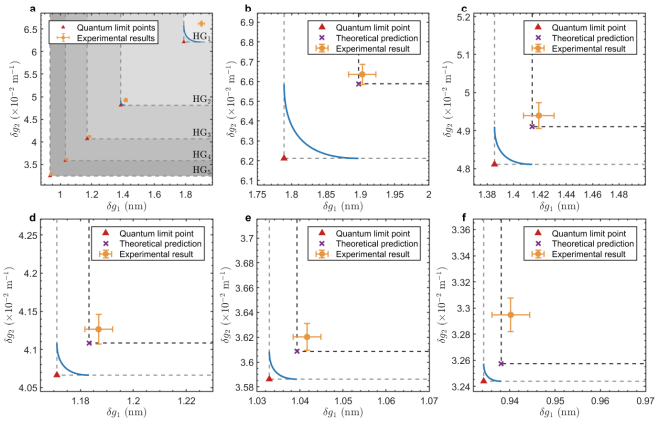


Figure 3: Experimental results of minimum detectable parameters g_1 and g_2, which are illustrated by the yellow points with error bar. The trade-off bounds of parameters g_1 and g_2 with different HG modes are represented by the blue solid curves. **a** Experimental results of HG_1 to HG_5 modes. The different HG regions are distinguished by the gray levels. The gray dashed lines are the quantum precision limits of parameters g_1 and g_2 with different HG modes, and the cross points (red triangles) are the corresponding quantum limit points. **b-f** Specific experimental results of HG_1 to HG_5 modes. The purple cross marks are the theoretical predictions of experimental results.

applications such as polarization measurement, vibration sensing, magnetic field detection, quantum communication, quantum imaging, and quantum computing, etc..

References

[1] **B. Xia**, J. Huang, H. Li, H. Wang, and G. Zeng. Toward incompatible quantum limits on multiparameter estimation. *Nat. Commun.*, 14(1):1021, 2023.

[2] J. Liu, H. Yuan, X.-M. Lu, and X. Wang. Quantum fisher information matrix and multiparameter estimation. *J. Phys. A: Math. Theor.*, 53(2):023001, 2019.

[3] C. L. Degen, F. Reinhard, and P. Cappellaro Quantum sensing. *Rev. Mod. Phys.*, 89(3):035002, 2017.

[4] D. S. Simon, G. Jaeger, and A. V. Sergienko. Quantum communication and cryptography. In *Quantum Metrology, Imaging, and Communication*, pages 201–220, 2017.

[5] V. Gebhart, R. Santagati, A. A. Gentile, et al. Learning quantum systems. *Nat. Rev. Phys*, 5(3):141–156, 2023.

[6] X.-M. Lu, and X. Wang. Incorporating Heisenberg's Uncertainty Principle into Quantum Multiparameter Estimation. *Phys. Rev. Lett.*, 126(12):120503, 2021.

Resource-efficient probabilistic detection of GHZ entanglement with conditional witness

Kwang-Jun Choi[1 2] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Korea*
[2] *Department of Physics, Yonsei University, Seoul 03722, Korea*

Abstract. We propose a resource-efficient scheme for detecting GHZ entanglement by hybridizing existing probabilistic and conditional methods. Our scheme improves the resource efficiency by eliminating the need for a projection operator and reducing the required number of measurement settings compared to previous conditional witness and few-copy method. We derive a new confidence bound based on conditional witness measurements, allowing us to consider all conditional outcomes. We demonstrate that our scheme outperforms previous methods regarding the resource efficiency, which becomes further pronounced when detecting the genuine multipartite entanglement among larger numbers of qubits.

Keywords: Genuine multipartite entanglement, Entanglement witness, Entanglement verification

1 Introduction

Genuine multipartite entanglement (GME) is crucial for the development of scalable quantum computing and quantum network architectures. Traditional approaches to verify GME, such as state tomography and entanglement witness, require a large number of resource states and measurement setups. As the number of qubits increases, these requirements grow exponentially. Hence, it is essential to develop a resource-efficient and reliable method to detect GME for developing large-scale quantum architectures. Recently, some noise-robust and resource-efficient schemes to detect GME have been proposed such as conditional [1] and few-copy detection schemes [4]. However, these have certain limitations, such as the need to use a projection operator [1] or a divergence of the number of resources near the noise bound [4]. In this work, we propose a hybrid scheme that combines the advantages of the conditional witness and few-copy detection methods. Our scheme exhibits resource efficiency even with a larger number of qubits, which is crucial for entanglement verification in large-scale quantum systems.

2 Conditional witness

The localizable entanglement (LE) of a multipartite entangled state is the maximal amount of entanglement that can be concentrated between two subsystems by performing local measurements on the other systems [2]. In other words, it quantifies the ability to concentrate global entanglement to a specific local subsystem. The LE of the bipartition $(x|y)$ for a n-qubit state ρ is given by

$$LE_{x|y}(\rho) = \sup_{M} \sum_{i} p_i E(\rho_{x|y:i}) \tag{1}$$

Here, M represents a local measurement on $(x, y)^c$, i represents the corresponding outcome, and $\rho_{x|y:i}$ is the post-measurement state.

From the fact that entanglement cannot increase via local operations and classical communication (LOCC), $LE_{x|y} > 0$ implies the presence of entanglement in all bipartitions where one partition contains x, another partition contains y, and all possible distributions of the remaining subsystems. Using this, a conditional entanglement witness can be constructed [1]:

$$W_{[x|y]} = |\Phi_+\rangle\langle\Phi_+| \bigotimes_{[x,y]^c} |+\rangle\langle+|, \tag{2}$$

which outperforms the standard witness with respect to noise-robustness and required measurement settings [1]. However, it relies on localizable entanglement, which depends on 2^{n-2} conditional outcomes, obtaining the expected value $\mathrm{Tr}(W_{[x|y]})$ for a fixed conditional outcome requires the use of the projection operator $\bigotimes_{[x,y]^c} |+\rangle\langle+|$. This projection operator necessitates the use of additional ancillary qubits or post-selection, which is inefficient in terms of resource utilization. To post-select $\bigotimes_{[x,y]^c} |+\rangle\langle+|$ from X-basis measurements, it is necessary to discard resources (copies) sampled from $2^{n-2} - 1$ outcomes.

3 Few-copy entanglement detection

A few-copy entanglement detection scheme can be explained as follows: A sequence of random binary local measurements M_i with $i = 1, \ldots, N$ is sampled from a measurement set, where N is the number of copies and each measurement is performed sequentially on the copies. Each binary measurement has outcomes $\{0, 1\}$. The ratio of obtaining a positive outcome (1) for each measurement has an upper bound p_s for all biseparable states ρ_s. The success rate of the test in experiments denoted as p_e, is given by S/N, where S is the number of positive outputs in the measurement sequence. If p_e is greater than p_s, the test is considered successful. The figure of merit is the confidence of the test, $C(\delta) = 1 - P(\delta)$, where $P(\delta)$ is the probability of success of the test for any biseparable state, and δ is the difference between the success rate of the test, $\delta = p_e - p_s$. The upper bound on $P(\delta)$ for all biseparable states ρ_s is given by:

$$P(\delta) \leq e^{D(p_s+\delta|p_s)N}, \tag{3}$$

*swleego@gmail.com

where $D(x|y)$ represents the Kullback-Leibler divergence. In other words, the confidence is lower bounded as:

$$C(\delta) \geq 1 - e^{D(p_s+\delta|p_s)N} \tag{4}$$

and, the maximum number of copies required to get the confidence is given by:

$$N_{max} = \frac{\ln(1 - C(\delta))}{D(p_s + \delta|p_s)} \tag{5}$$

The crucial aspect of this protocol is determining the values of $\{M_i\}$, p_e, and p_s. In [4], the entanglement witness method was employed for a 6-qubit H-shaped cluster state, whose stabilizer witness is local-decomposable. Separable bounds were derived, specifically:

$$\sum_{i=1}^{2^n} \frac{1}{2^n} Tr(M_i^1 \rho_s) \leq \frac{3}{4} = p_s \tag{6}$$

where $M_i^1 = (1 + S_i)/2$. In the noiseless condition, N_{max} for achieving 99% confidence is obtained as 16 copies, while 132 copies are required in an actual experiment. This is a dramatic reduction of resource costs compared to standard approach in which 2^n observables and many copies of states are necessary for obtaining the expectation values. However, if the level of noise approaches the witness bound, p_e turns out to be getting close to p_s so that the required number of copies suddenly diverges [5].

4 Hybrid scheme

We propose a hybrid scheme that combines aforementioned two methods. It does not require the use of a projection operator, unlike the conditional witness [1], and uses fewer measurement settings compared to the few-copy method [4]. We choose n-qubit GHZ state for the target state. We derive a new confidence bound for the few-copy entanglement detection method using a conditional witness. This bound allows us to consider all conditional outcomes, making our scheme more resource-efficient compared to the trivial conditional witness.

Suppose j is the eigenvalue of the conditional measurements. If we measure the other qubits using the Pauli X-basis, except for the two qubits being tested, the n-qubit GHZ state collapses to two possible states:

$$|\Phi^{\pm}\rangle = \begin{cases} \frac{|00\rangle + |11\rangle}{\sqrt{2}} & \text{when } j = 1 \\ \frac{|00\rangle - |11\rangle}{\sqrt{2}} & \text{otherwise} \end{cases} \tag{7}$$

Based on the work [6], the stabilizer witness $W_{\pm}$ for these states is given by:

$$W_{\pm} = \frac{1}{2} I - |\Phi^{\pm}\rangle\langle\Phi^{\pm}| = \frac{1}{2} I - \frac{1}{2^2} \sum_{k=1}^{4} S_k^{\pm} \tag{8}$$

where $S_k^{\pm}$ is the stabilizer of $|\Phi^{\pm}\rangle$. Using (6) and the fact that $S_4^{\pm} = I$ and $Tr(I\rho) = 1$ for any quantum state ρ, we have:

$$\sum_{i=1}^{3} \frac{1}{3} Tr(M_i^{\pm} \rho_s) \leq \frac{2}{3} = p_s^{\pm} \tag{9}$$

where $M_i^{\pm} = \frac{1+S_i^{\pm}}{2}$. This leads to the derivation of the confidence bound for our work.

Theorem 1 *If we measure conditional qubits as X-basis and sample a random measurement operator from sets derived from (8) and process the test, we obtain the same bound as (3).*

Proof. Most of the proof is similar to that of [3]. The difference lies in dividing the sum of binary outcomes into sums based on the 2^{n-2} conditional outcomes. Let X be the sum of binary outcomes E_k from randomly sampled measurement operator M_k. Then, we have $X = \sum_{k=1}^{N} E_k = \sum_{i=1}^{2^{n-2}} \sum_{k=1}^{N_i} E_k^{i^{\pm}}$, where $N = \sum_{i=1}^{2^{n-2}} N_i$, and each $E_k^{i^{\pm}}$ is the binary outcome from $M_k^{\pm}$ corresponding to the i-th conditional outcome among the 2^{n-2} outcomes. For any $t > 0$, $P_{\text{sep}}(\delta) = P_{\text{sep}}(X \geq p_e N) = P_{\text{sep}}(e^{tX} \geq e^{tp_e N}) \leq \frac{<e^{tX}>}{e^{tp_e N}}$, where $\delta = \{\delta^{i^{\pm}}\}$ and $p_e N = \sum_{i=1}^{2^{n-2}} (p_s^{\pm} + \delta^{i^{\pm}}) N_i = \sum_{i=1}^{2^{n-2}} p_e^{i^{\pm}} N_i$. Thus, $\frac{<e^{tX}>}{e^{tp_e N}} = \prod_{i=1}^{2^{n-2}} \prod_{k=1}^{N_i} \frac{<e^{tE_k^{i^{\pm}}}>}{e^{tp_e^{i^{\pm}}}} = \prod_{i=1}^{2^{n-2}} \prod_{k=1}^{N_i} \frac{1 - <E_k^{i^{\pm}}> + <E_k^{i^{\pm}}> e^t}{e^{tp_e^{i^{\pm}}}}$. Since all $< E_k^{i^{\pm}} >$ are $\leq p_s^{\pm}$ for all $1 \leq i \leq 2^{n-2}$, we have $P_{\text{sep}}(\delta) \leq (\frac{1 - p_s^{\pm} + p_s^{\pm} e^t}{e^{tp_e}})^{\sum_{i=1}^{2^{n-2}} N_i} = (\frac{1 - p_s^{\pm} + p_s^{\pm} e^t}{e^{tp_e^{i^{\pm}}}})^N$. Let $f(t) = \frac{1 - p_s^{\pm} + p_s^{\pm} e^t}{e^{tp_e}}$. This function has a minimum at $t_m = \log \frac{(1 - p_s^{\pm}) p_e}{(1 - p_e) p_s^{\pm}}$. Thus, $P_{\text{sep}}(\delta) \leq e^{D(p_e||p_s^{\pm})N}$, where $D(x||y)$ is the Kullback-Leibler divergence. □

We can use the same measurement settings for both collided states since their stabilizer generators are the same. The only difference lies in the phase of g_1, where $g_1^{\pm} = \pm\sigma_x^{\otimes k}$. Therefore, it is sufficient to consider the eigenvalue of the conditional outcomes on the other systems and manipulate the phase of $M_i^{\pm}$. The summary of the process for our work is as follows:

1. Generate an n-qubit GHZ state.
2. Define conditional bipartitions [1, 2], [2, 3], ..., [n-1, n] based on conditional witness.
3. Measure the qubits outside the bipartitions in the Pauli X-basis and record the results.
4. Measure the qubits in the target bipartitions in the basis sampled from $M_i^{\pm}$ based on each conditional outcome.
5. Determine the bound using 1.
6. Repeat steps 1-5 for multiple trials to obtain statistical data.

To simulate our method, we utilized the open-source Python library Qiskit [7]. We constructed noise models following the same approach as [1], which involved incorporating a two-qubit depolarizing error after each CNOT gate and a single-qubit measurement bit-flip error for all qubits. Through simulations, we observed a significant advantage in resource utilization using our method across both noise models. Moreover, this advantage was further

amplified with an increasing number of qubits. The corresponding results are depicted in Figure 1, and 2

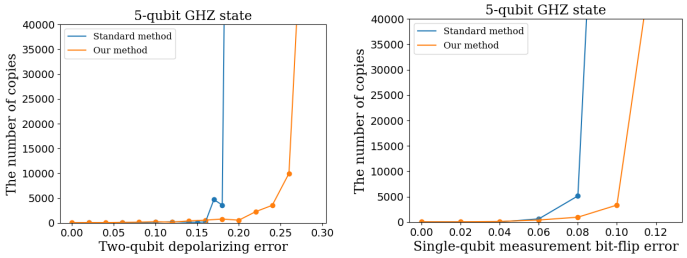


Figure 1: 5-qubit GHZ state in the two noise models

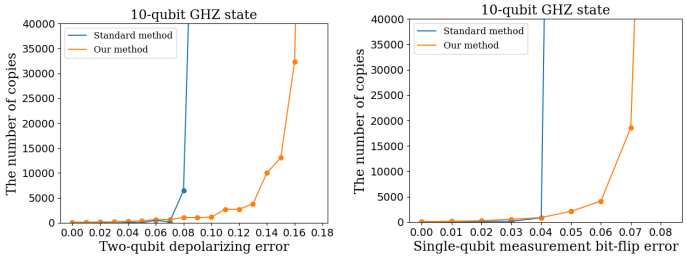


Figure 2: 10-qubit GHZ state in the two noise models

Our results validate the resource efficiency of our hybrid scheme under different noise conditions. Our scheme outperforms existing approaches, especially as the number of qubits increases, regarding resource efficiency and noise robustness. The reduction of the required measurement settings and the elimination of the need for a projection operator make our method more practical and scalable for real-world applications.

References

[1] A. Rodriguez-Blanco et al. Efficient and robust certification of genuine multipartite entanglement in noisy quantum error correction circuits. *PRX quantum*, 2:020304, 2021.

[2] M. Popp et al. Localizable entanglement *Physical Review A*, 71(4):042306, 2005.

[3] A. Dimić and B. Dakić. Single-copy entanglement detection *npj Quantum Information*, 4(1):11., 2018.

[4] V. Saggio et al. Experimental few-copy multipartite entanglement detection. *Nature physics*, 15(9):935-940, 2019.

[5] V. Saggio and Philip Walther. Few-Copy Entanglement Detection in the Presence of Noise *Annalen der Physik*, 534(7), 2022.

[6] J. Sperling and W. Vogel. Multipartite entanglement witnesses *Physical review letters*, 111(11):110503, 2013.

[7] M. Treinish et al. Qiskit: An open-source framework for quantum computing. https://doi.org/10.5281/zenodo.7897504, 2023.

Exploring Toric Code Model: Comparative Performance Analysis of the Parameterized Loop Gas Circuit in Noisy Quantum Systems

Yaswitha Gujju[1] * Rong-Yang Sun[2] † Tomonori Shirakawa[2] ‡ Seiji Yunoki[2] §

[1] *Graduate School of Information Science and Technology, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan*

[2] *Computational Materials Science Research Team, RIKEN Center for Computational Science (R-CCS), Kobe, Hyogo, 650-0047, Japan*

Abstract. In recent years, the interest in topologically ordered states has surged due to their distinct properties and potential applications in quantum computing. The toric code, a variant of the surface code, shows promise for quantum error correction. However, experimental realization of topologically ordered states remains challenging, requiring the generation of long-range entanglement. A recent study successfully implemented a quantum circuit on a superconducting processor to prepare the toric code's ground state [5]. Building upon this, a novel ansatz called the Parameterized Loop Gas Circuit (PLGC) was introduced to accurately represent the ground state and explore its properties[1]. We evaluate the PLGC ansatz's performance in noisy conditions using simulation and a real quantum device, comparing it to a hardware-efficient ansatz. The PLGC ansatz exhibits faster convergence and improved optimal values, highlighting its robustness and scalability potential.

Keywords: Toric code, Variational Eigen Solver, Parameterized loop gas circuit (PLGC), Hardware-efficient ansatz, Noisy quantum systems

1 Introduction

The increasing fascination with topologically ordered states, which exhibit long-range entanglement, has gained considerable momentum in recent years owing to their distinct properties and their impact in quantum computing. The toric code, a variant of the surface code, has emerged as a promising stabilizer code for quantum error correction. The experimental realization of topologically ordered states can be accomplished by identifying quantum systems with preexisting topologically ordered ground states or by engineering a topologically ordered state in a controlled quantum system. The toric code is a fundamental example of a two-dimensional lattice model with topological properties, showcasing what is known as $\mathbb{Z}_2$ topological order. The work in [5] first implemented an efficient quantum circuit on a superconducting quantum processor to prepare the ground state of the toric code ground state on a lattice of 31 superconducting qubits.

Recently, [1] proposed a novel ansatz called the Parameterized Loop Gas Circuit (PLGC) that has shown to offer adequate expressibility for the ground state of non-exactly solvable correlated Hamiltonians while being faithfully evaluable on NISQ devices. It encodes the quantum loop gas state with adjustable loop configurations into an optimized-depth quantum circuit.

The authors note precise reproduction of the ground state of the toric code model in an external magnetic field, encompassing both topologically ordered and ferromagnetically ordered phases. They additionally note that their PQC achieves energy accuracy better than 10^{-2} for the toric code model. This efficient representation of the ground state facilitates the exploration of topologically ordered states and provides valuable insights into their properties. Their work contributes to the advancement of utilizing quantum computers for studying topologically ordered systems, bridging the gap between theory and experimental exploration.

Variational Quantum Eigensolver (VQE) have been widely used to solve the non-exactly solvable quantum many-body problems and are characterized by the usage of a parametrized quantum circuit (PQC) where the parameters are generally optimized using a classical optimizer to minimize a cost function. The choice of the ansatz, cost function, gradient, etc., dictates the overall efficiency of the VQE.

In this work, we study the performance of the PLGC ansatz in the noisy setting using both simulator and the real device provided by [11] using error mitigation techniques. The lattices considered here are 2×1, 3×2, and 3×3. We further compare the performance with an hardware efficient ansatz and see that the PLGC ansatz shows faster convergence rates and better optimal values. This result is consistent under noisy environmant and finite sampling error and shows the robustness of the PLGC ansatz. We also note that the number of parameters that need to be optimized in the Hardware efficient ansatz increases exponentially when compared to the PLGC ansatz thereby showing scope for the scalability of the PLGC ansatz to bigger lattice structures. Nevertheless, the efficacy of these quantum algorithms is contingent upon the classical optimization of a challenging cost function. It is essential to thoroughly evaluate the performance of the various optimizers available through comprehensive benchmarking. Consequently, we compare the performance of different optimizers to gain a deeper understanding of the training process.

*yaswitha-gujju@g.ecc.u-tokyo.ac.jp
†rongyang.sun@riken.jp
‡t-shirakawa@riken.jp
§yunoki@riken.jp

2 Toric code

The toric code model [8] is characterized by qubits positioned at the bond centers of a square lattice with dimensions $L_x \times L_y$ and a total of N bonds. The Hamiltonian is defined as:

$$H_{TC} = -\sum_s A_s - \sum_p B_p,$$

where $A_s = \prod_{i \in s} \sigma_i^z$ and $B_p = \prod_{i \in p} \sigma_i^x$. The ground state of the above Hamiltonian is a topological quantum spin liquid characterized by a $\mathbb{Z}_2$ topological order [8, 7] with the characteristic that H_{TC} is exactly solvable.

In the representation below, each 'o' represents a qubit located at the bond centers of a square lattice while the lines represent the bonds between them.

```
o---o---o
|   |   |
o---o---o
|   |   |
o---o---o
```

Recently, Satzinger et al. [5] demonstrated the construction of the unique ground state of the toric code model with open boundary conditions (OBCs). Building upon this work, Sun et al. [1] used it as a motivation to develop an efficient ansatz for the Hamiltonian H_{TM}. In addition, they explored the topological quantum phase transition [4, 3], which occurs when the toric code model deviates from its exactly solvable point due to the application of an external magnetic field along the z direction. The corresponding Hamiltonian $H_{TCM}(x)$ is defined as

$$H_{TCM}(x) = (1-x)H_{TC} - x\sum_{i=1}^{N} \sigma_i^z.$$

where the parameter x determines the influence of the magnetic component on the Hamiltonian. Notably, when $x = 1$, the exact ground state of the system is given by $|00\ldots0\rangle$.

3 PLGC ansatz

The groundbreaking research conducted by [5] established a significant milestone in implementing the toric code circuit on current NISQ (Noisy Intermediate-Scale Quantum) devices with remarkable precision. Their work introduced a method to generate the state $|\Psi_0\rangle$ by utilizing the Hadamard gate (H) on a specific qubit associated with a plaquette. Subsequently, CNOT gates were applied to the remaining qubits within the same plaquette, with these designated qubits serving as the control inputs. The circuit construction employed in this approach results in a linear growth in circuit depth with increasing L_y.

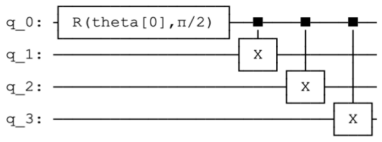


Figure 1: Illustration of the PLGC ansatz for the 1 Plaquette case

The PLGC ansatz replaces the the Hadamard gates with rotation-y gates in the construction of $|\Psi_0\rangle$. This helps in the creation of an imbalanced superposition state, $\cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$.

4 Experiments

In this section, we compare the performance of two different ansatzes, the Parameterized Loop Gas Circuit (PLGC) and the Hardware-efficient ansatz, for lattice structures of sizes 2×1, 3×2, and 3×3 with 4, 7, and 12 qubits, respectively. We employ the Variational Quantum Eigensolver (VQE) approach to optimize the Hamiltonian $H_{TCM}(x)$ for x ranging from 0 to 1 under open boundary conditions. The simulations are performed using the Qiskit framework [11], utilizing both the noise-free statevector simulator and the QASM simulator with finite shots.

For the hardware-efficient ansatz, we utilize the circular entanglement structure with R_y gates and 2 repetitions. The initial parameters for both ansatzes are set to $|00\ldots0\rangle$. We choose this as the initial state to compare the performance of both the ansatz without any bias. We compare the performance across different optimization algorithms such as COBYLA, SPSA, Sequential Least Squares Programming (SLSP), and Limited-memory BFGS Bound.

To evaluate the performance under realistic conditions, we conduct experiments using the QASM simulator with noise models obtained from the IBM Quantum devices *ibmq_belem* and *ibmq_jakarta*. Furthermore, we run the 1 Plaquette case on the actual IBM Quantum device *ibmq_belem*, specifically for the case without magnetic settings (i.e., $x = 0$). In all cases, the circuit optimization level is set to 3. For the experiments on the real device, we apply different error mitigation techniques, such as Zero Noise Extrapolation and Twirled Readout Error Extinction, to the results obtained.

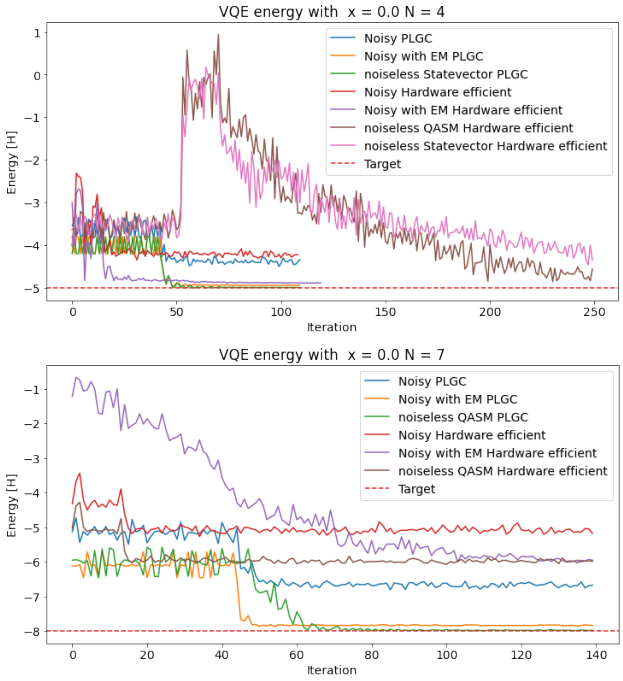


Figure 2: Plot illustrating the energy convergence with the number of iterations in a single plaquette configuration consisting of 4 qubits (top) and two plaquette configuration consisting of 7 qubits (bottom), specifically in the case where x = 0 using the PLGC and Hardware efficient ansatz. The simulations are conducted using the statevector simulator, QASM simulator (both with and without a noise model), and with the inclusion of error mitigation techniques.

5 Conclusion and Discussion

From the energy convergence plots, we see that the PLGC ansatz takes lesser number of iterations compared to the hardware efficient ansatz (Figure 2). The PLGC ansatz demonstrates superior performance when combined with the simultaneous perturbation stochastic approximation (SPSA) optimizer [6] in both the 4 and 7 qubit case, while the hardware-efficient ansatz performs best with SPSA in the 4 qubit case and COBYLA [10] in the 7 qubit case. This behavior is consistent across all the lattices considered. Due to the presence of shot noise in the case of the QASM simulator, gradient based optimizers such as SLSQP and L_BFGS performed worse likely due to the noise.

Another advantage offered by the PLGC ansatz over the Hardware efficient ansatz is the number of parameters that need to be optimized in the PQC. In the case of the Hardware efficient ansatz, the number scales exponentially with the size of the lattice. For example, in the case of 4×4 lattice, the PLGC ansatz needs 9 parameters while the Hardware efficient ansatz needs 72 parameters. Additionally, we compare the performance using error noise models and note that the performance of the PLGC ansatz remains consistent in comparison to the Hardware Efficient ansatz. The results after applying error mitigation also suggest that the PLGC performance remains consistent.

When running the case of $x = 0$ for the 1 Plaquette (4 qubit) case on the actual quantum device with Twirled Readout Error extinction, the obtained expectation value exhibit an average of -4.529 ± 0.3180 (Figure 3) while the expectation value (as obtained on the statevector simulator) is around -5. This outcome is based on the execution of 152 independent VQE trials, utilizing readout mitigation shots calibration set to 8192 and 4000 shots. In contrast, when zero error mitigation is employed, the achieved results yield an expectation of -4.3305 ± 0.0467. These results were obtained from 100 circuits with 4000 shots, employing a linear extrapolator. The difference in the results obtained between the quantum hardware and that of the error mitigated QASM simulator results are more evident.

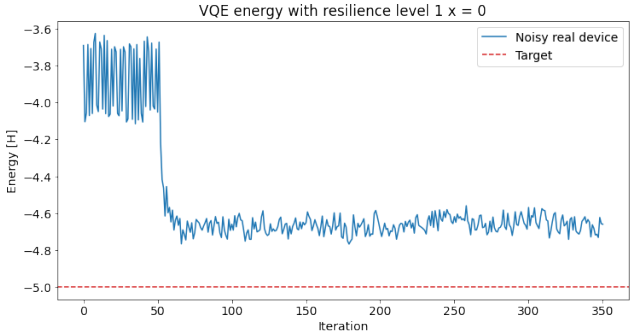


Figure 3: Energy convergence with iterations for VQE using the PLGC ansatz on the real device *ibm_belem* using 4 qubits for the case when $x = 0$ in the 1 Plaquette case using error mitigation.

Examining the scalability of the PLGC ansatz to larger lattice structures becomes crucial due to the feasibility of training given the parameter space. Such an investigation could demonstrate its advantageous potential. Subsequently, the next objective would involve comparing the PLGC ansatz with other approaches, such as the Hamiltonian variational ansatz.

References

[1] Rong-Yang Sun, Tomonori Shirakawa, and Seiji Yunoki. Parametrized quantum circuit for weight-adjustable quantum loop gas. *Physical Review B*, 107(4):L041109, 2023.

[2] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021.

[3] Fengcheng Wu, Youjin Deng, and Nikolay Prokof'ev. Phase diagram of the toric code model in a parallel magnetic field. *Physical Review B*, 85(19):195104, 2012.

[4] Simon Trebst, Philipp Werner, Matthias Troyer, Kirill Shtengel, and Chetan Nayak. Breakdown of a topological phase: Quantum phase transition in a

loop gas model with tension. *Physical review letters*, 98(7):070602, 2007.

[5] KJ Satzinger, Y-J Liu, A Smith, C Knapp, M Newman, C Jones, Z Chen, C Quintana, X Mi, A Dunsworth, et al. Realizing topologically ordered states on a quantum processor. *Science*, 374(6572):1237–1241, 2021.

[6] James C Spall. Multivariate stochastic approximation using a simultaneous perturbation gradient approximation. *IEEE transactions on automatic control*, 37(3):332–341, 1992.

[7] Alexei Kitaev. Anyons in an exactly solved model and beyond. *Annals of Physics*, 321(1):2–111, 2006.

[8] A Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of physics*, 303(1):2–30, 2003.

[9] Xavier Bonet-Monroig, Hao Wang, Diederick Vermetten, Bruno Senjean, Charles Moussa, Thomas Bäck, Vedran Dunjko, and Thomas E O'Brien. Performance comparison of optimization methods on variational quantum algorithms. *Physical Review A*, 107(3):032407, 2023.

[10] Ruben E Perez, Peter W Jansen, and Joaquim RRA Martins. pyopt: a python-based object-oriented framework for nonlinear constrained optimization. *Structural and Multidisciplinary Optimization*, 45:101–118, 2012.

[11] Qiskit contributors. Qiskit: An open-source framework for quantum computing, 2023.

Extended Abstract for Analysis of Higher Order Dynamical Decoupling by Relative Integral Action Method

Changhao Yi[1 2 3 *] Milad Marvian[1 †]

[1] *Center for Quantum Information and Control, Department of Physics and Astronomy, University of New Mexico, NM 87131, USA*

[2] *State Key Laboratory of Surface Physics and Department of Physics, Fudan University, Shanghai 200433, China*

[3] *Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China*

Abstract. In this work we provide rigorous error bounds for different types of dynamical decoupling protocols without resorting to Magnus expansion. Instead, by exploiting and generalizing the relative integral action method, we propose the concept of higher order integral condition and use it as a framework to describe and analyze the higher order protocols. Finally, we show two applications of our results: higher order quantum Zeno dynamics and higher-order symmetry protection Hamiltonian simulation.

Keywords: dynamical decoupling, quantum Zeno dynamics, error suppression

Dynamical decoupling (DD) is a common scheme of suppressing non-Markovian noise [1, 2, 3, 4, 5, 6], it has many applications in quantum information technologies. Using fast-driven periodical pulses, we are able to enforce the system to possess a certain type of symmetry. In DD, the pulses are designed to commute with the system Hamiltonian, while the interaction between the system and the environment is suppressed.

Here is a quick example: when the system Hamiltonian is a Heisenberg model $H_S = -\sum_j (J_x X_j X_{j+1} + J_y Y_j Y_{j+1} + J_z Z_j Z_{j+1})$, we can set the pulses to be the repetitive conjugation of $\{I^{\otimes N}, X^{\otimes N}, Y^{\otimes N}, Z^{\otimes N}\}$. It is easy to verify that $[H_S, P^{\otimes N}] = 0, P \in \{I, X, Y, Z\}$ so the pulse does not influence H_S, and any general single Pauli error σ is eliminated on the average of $\sum_P P^{\otimes N} \sigma P^{\otimes N} = 0$. In this way, we decouple the Pauli error σ from H_S using dynamical controls.

The effect of dynamical decoupling can be strengthened by designing more delicate pulses. Concatenated DD [7, 8] and Uhrig's DD [9, 10, 11, 12] are two famous examples. In concatenated DD, we repetitively apply the same sequence of operator conjugations on the evolution of a single period; in Uhrig's DD, we give freedom to the intervals between pulses in a single period. Furthermore, the two methods can be combined to generate more efficient protocols [10, 12, 13]. We call them *higher order DD* protocols.

A common method to analyze the performance of higher order DD is to use the first few orders of *Magnus expansion* [14]. However, the convergence condition of Magnus expansion causes problems to the rigorous analysis. Recently, the *relative integral action* (RIA) method proposed in [15] (similar to the method in [16]) provides a rigorous way to analyze a list of problems, including the lowest order DD. But one big drawback of the current RIA method is it cannot provide proper upper bounds for higher order DD pulses.

In this work we provide rigorous error bounds for different types of DD protocols without resorting to Magnus expansion. Instead, by exploiting and generalizing the RIA method, we propose a new framework to describe and analyze the higher order protocols.

Here is an intuitive explanation of our method. In the error analysis of DD, we deal with a time-dependent perturbation problem: given a Hamiltonian H_0 and a time-dependent perturbation term $V(t)$ (the noise term in the interaction picture), the purpose is to quantify the distance between the free evolution and the evolution generated by the full Hamiltonian. We find that in DD protocols, all $V(t)$ can be described by the *higher order integral conditions*. If $\exists t_0$ such that

$$V(t) = V(t + t_0),$$
$$\int_0^{t_0} dt_1 \int_0^{t_1} dt_2 \cdots \int_0^{t_{K-1}} dt_K V(t_K) = 0,$$

then we say $V(t)$ satisfies the K-th order integral condition. For instance, the time reflection symmetry $V(t) = V(t_0 - t)$ is a special case of second order integral condition. The larger K is, the more efficient the DD pulses are. Using the special properties of higher order integral conditions, we efficiently incorporate higher order DD with the RIA method. Eventually, the question of quantifying error bounds can be reduced to analyzing different orders of integrals.

Finally, we provide rigorous bounds for several higher order DD protocols using this method. Our new results reveals features of DD that were not emphasized before. For example, in general concatenated DD, there exists an error term that does not decay with the order of concatenation. The application of our analytic tool is not limited to analyzing existing methods. We also show

*yichangh@fudan.edu.cn
†mmarvian@unm.edu

two applications of our results: higher order quantum Zeno dynamics [17] and higher-order symmetry protection Hamiltonian simulation [18]. The idea is similar to higher order DD: using more delicate protocols, we are able to suppress the unwanted part of the Hamiltonian in a more efficient way.

In conclusion, our main contributions in this work include:

- a convenient notation for the higher order DD pulses, which might also be useful in dynamical Hamiltonian engineering [6];
- a generalized version of RIA method;
- rigorous bounds for several different types of DD;
- higher order quantum Zeno dynamic inspired by higher order DD;
- higher order symmetry protected Hamiltonian simulation inspired by higher order DD.

The technical version of this work is written in appendix.

References

[1] Lorenza Viola, Emanuel Knill, and Seth Lloyd. Dynamical decoupling of open quantum systems. *Physical Review Letters*, 82(12):2417, 1999.

[2] Lorenza Viola, Emanuel Knill, and Seth Lloyd. Dynamical generation of noiseless quantum subsystems. *Physical Review Letters*, 85(16):3520, 2000.

[3] Kaveh Khodjasteh and Daniel A Lidar. Rigorous bounds on the performance of a hybrid dynamical-decoupling quantum-computing scheme. *Physical Review A*, 78(1):012355, 2008.

[4] Hui Khoon Ng, Daniel A Lidar, and John Preskill. Combining dynamical decoupling with fault-tolerant quantum computation. *Physical Review A*, 84(1):012305, 2011.

[5] Gregory Quiroz and Daniel A Lidar. High-fidelity adiabatic quantum computation via dynamical decoupling. *Physical Review A*, 86(4):042333, 2012.

[6] Joonhee Choi, Hengyun Zhou, Helena S Knowles, Renate Landig, Soonwon Choi, and Mikhail D Lukin. Robust dynamic hamiltonian engineering of many-body spin systems. *Physical Review X*, 10(3):031002, 2020.

[7] Kaveh Khodjasteh and Daniel A Lidar. Fault-tolerant quantum dynamical decoupling. *Physical review letters*, 95(18):180501, 2005.

[8] Kaveh Khodjasteh and Daniel A Lidar. Performance of deterministic dynamical decoupling schemes: Concatenated and periodic pulse sequences. *Physical Review A*, 75(6):062310, 2007.

[9] Wen Yang and Ren-Bao Liu. Universality of uhrig dynamical decoupling for suppressing qubit pure dephasing and relaxation. *Physical review letters*, 101(18):180403, 2008.

[10] Jacob R West, Bryan H Fong, and Daniel A Lidar. Near-optimal dynamical decoupling of a qubit. *Physical review letters*, 104(13):130501, 2010.

[11] Götz S. Uhrig and Daniel A. Lidar. Rigorous bounds for optimal dynamical decoupling. *Phys. Rev. A*, 82:012301, Jul 2010.

[12] Wan-Jung Kuo, Gregory Quiroz, Gerardo Andres Paz-Silva, and Daniel A Lidar. Universality proof and analysis of generalized nested uhrig dynamical decoupling. *Journal of mathematical physics*, 53(12):122207, 2012.

[13] Zhen-Yu Wang and Ren-Bao Liu. Protection of quantum systems by nested dynamical decoupling. *Phys. Rev. A*, 83:022306, Feb 2011.

[14] Sergio Blanes, Fernando Casas, Jose-Angel Oteo, and José Ros. The magnus expansion and some of its applications. *Physics reports*, 470(5-6):151–238, 2009.

[15] Daniel Burgarth, Paolo Facchi, Giovanni Gramegna, and Kazuya Yuasa. One bound to rule them all: from adiabatic to zeno. *Quantum*, 6:737, 2022.

[16] Milad Marvian and Daniel A Lidar. Error suppression for hamiltonian-based quantum computation using subsystem codes. *Physical review letters*, 118(3):030504, 2017.

[17] Paolo Facchi, Daniel A Lidar, and Saverio Pascazio. Unification of dynamical decoupling and the quantum zeno effect. *Physical Review A*, 69(3):032314, 2004.

[18] Minh C Tran, Yuan Su, Daniel Carney, and Jacob M Taylor. Faster digital quantum simulation by symmetry protection. *PRX Quantum*, 2(1):010323, 2021.

[19] Daniel A Lidar. Review of decoherence free subspaces, noiseless subsystems, and dynamical decoupling. *arXiv preprint arXiv:1208.5791*, 2012.

[20] Daniel A Lidar, Paolo Zanardi, and Kaveh Khodjasteh. Distance bounds on quantum dynamics. *Physical Review A*, 78(1):012308, 2008.

[21] Itai Arad, Tomotaka Kuwahara, and Zeph Landau. Connecting global and local energy distributions in quantum spin models on a lattice. *Journal of Statistical Mechanics: Theory and Experiment*, 2016(3):033301, 2016.

[22] Tomotaka Kuwahara, Takashi Mori, and Keiji Saito. Floquet–magnus theory and generic transient dynamics in periodically driven many-body quantum systems. *Annals of Physics*, 367:96–124, 2016.

[23] Wan-Jung Kuo and Daniel A Lidar. Quadratic dynamical decoupling: Universality proof and error analysis. *Physical Review A*, 84(4):042329, 2011.

[24] Gregory Quiroz and Daniel A Lidar. Quadratic dynamical decoupling with nonuniform error suppression. *Physical Review A*, 84(4):042328, 2011.

[25] Andrew M Childs, Yuan Su, Minh C Tran, Nathan Wiebe, and Shuchen Zhu. Theory of trotter error with commutator scaling. *Physical Review X*, 11(1):011020, 2021.

.

Optimal Qubit Permutation Search for Matrix Product State Encoding with Minimal Loss

Hyeongjun Jeon[1] * Kyungmin Lee[1] † Dongkyu Lee[2] ‡ Bongsang Kim[2] §
Taehyun Kim ¶[1 3 4 5 6]

[1] *Department of Computer Science and Engineering, Seoul National University, Seoul 08826, Republic of Korea*
[2] *Quantum AI Dept, AI Lab, CTO, LG Electronics, Seoul 06772, Republic of Korea*
[3] *Automation and System Research Institute, Seoul National University, Seoul 08826, Republic of Korea*
[4] *Inter-university Semiconductor Research Center, Seoul National University, Seoul 08826, Republic of Korea*
[5] *Institute of Computer Technology, Seoul National University, Seoul 08826, Republic of Korea*
[6] *Institute of Applied Physics, Seoul National University, Seoul 08826, Republic of Korea*

Abstract. Matrix product state (MPS) offers a framework for encoding classical data into quantum states, enabling the efficient utilization of quantum resources for data representation and processing. This research paper investigates techniques to enhance the efficiency and accuracy of MPS representations specifically designed for encoding classical data. Based on the observations that MPS truncation error depends on the pattern of the classical data, we utilized qubit permutations, which reorganize the qubits in the system, thereby improving the efficiency and fidelity of the MPS representation. Furthermore, we also evaluate the performance of the optimized MPS representations in the context of quantum classifiers, demonstrating their enhanced performance compared to the standard MPS.

Keywords: Amplitude Encoding, Matrix Product State, Optimization

1 Introduction

Various quantum algorithms are suggested that can solve computational tasks exponentially faster than their classical counterpart. These algorithms include quantum Fourier transform [1], factoring algorithm [2], solving systems of linear equations [3], quantum support vector machine [4], quantum principal component analysis [5], and quantum convolutional neural network [6]. Among these, except so-called Shor's algorithm which prepares the quantum state using a mathematical relation, those algorithms usually come with an assumption of black boxes for quantum state preparation [7]. In most research, it is assumed that these black boxes have polynomial computational complexity with respect to the number of qubits.

However, it is well-known that preparing arbitrary n-qubit quantum states requires exponential overhead [8]. For example, Araujo *et al.* [9] proposed a quantum circuit for state preparation that requires exponential depth [10] while Zhang *et al.* suggested a polynomial-depth circuit, but only with exponential number of auxiliary qubits. Note these quantum circuits prepare exact quantum states.

On the other hand, real-world data often contain correlations or patterns. In classical information processing, redundancies play a crucial role in the efficient encoding of data, as they are commonly utilized to achieve efficient compression by discarding some of the redundancies, while maintaining the essential features.

In the context of quantum mechanics, matrix product state (MPS) is a mathematical framework used to represent quantum states with local entanglement characterized by low-rank matrices [11]. A parameter called bond dimension χ determines the capability of MPS in representing quantum states. Previous research showed that images such as modified National Institute of Standards and Technology database (MNIST) [12] and Fashion-MNIST [13] can be encoded into MPS with low bond dimensions [14, 15].

Similar to the classical compression, it is conceivable that a method exists to transform quantum data into a more compressed format for encoding purposes. This would involve finding a way to represent the data using a smaller number of quantum gates, without losing crucial information about the original data. This study introduces a novel technique aimed at improving the fidelity of the MPS. Specifically, we propose a method that involves permuting the qubits used by encoding circuits. To verify the effectiveness of the our method, we apply this approach to the encoding of data: the MNIST and Fashion-MNIST datasets. Our approach leads to an improvement in accuracy of state encoding, which also enhances the test accuracy of quantum classifiers, thereby demonstrating the overall utility of the proposed method.

2 Algorithm

For a given quantum state, there exists an efficient algorithm called MPS-SVD[16] that constructs an MPS with the smallest distance in terms of Frobenius norm for a given bond dimension. However, the accuracy of the MPS depends heavily on the entanglement structure of the state being encoded [16]. It is known that MPS with low bond dimension corresponds to states with local entanglement. Therefore, by permuting the order of the qubits to change the entanglement structure to be more

*ijshj10@snu.ac.kr
†anfry15rudals@snu.ac.kr
‡dongkyu44.lee@lge.com
§bongsang.kim@lge.com
¶taehyun@snu.ac.kr

local, we can anticipate a reduction in the truncation error. In this context, the truncation error can be utilized as a cost, and graph search algorithms [17, 18] can be employed to search for the optimal permutation of qubits.

Algorithm 1: MPS-SVD with permutation

Input:
n-qubit quantum state
$\mathbf{a} \leftarrow (a_1, a_2, ..., a_{2^n})$
number of qubits n
bond dimension χ
Output:
Optimal qubit permutation with the lowest truncation error
Initialize:
min-heap ← empty heap
$x \leftarrow \lfloor log_2 x \rfloor$
1: **for** l **in** *combination*(n, x)) **do**
error ← *partial_truncation_error(l)*
min-heap.push((error,l))
2: **end**
3: **loop do**
(error, l) ← min-heap.pop()
if *len(l)* = *n-x* **then**
return l
end
for *index* **in** *not used by l* **do**
l2 ← *copy(l)*
append index to l2
error ← *error* + *truncation_error(l2)*
min-heap.push((error,l2))
end
4: **end**

It can be also shown that there is a mathematical symmetry in the permutation space, which generally leads to a reduction of the search space significantly.

3 Result

A. Image encoding optimization To verify the effectiveness of the our algorithm compared to the standard MPS-SVD algorithm, we applied both algorithms to two types of datasets: the MNIST and Fashion-MNIST. Figure 1 shows the comparison of those two approaches when they are applied to MNIST dataset.

Figure 2 shows the same type of comparison between two MPS representations with Fashion-MNIST dataset where similar performance improvement is observed.

As the results indicate, our proposed algorithm has led to a consistent improvement in both the numerical value of the Frobenius distance and the visual appearance of the output images especially for the low bond dimension.

B. Benchmark with quantum classifiers To assess the effect of input state quality on quantum information processing tasks, we trained two quantum classifiers - a variational quantum circuit (VQC) classifier and an MPS classifier - using both algorithms. Our results showed a

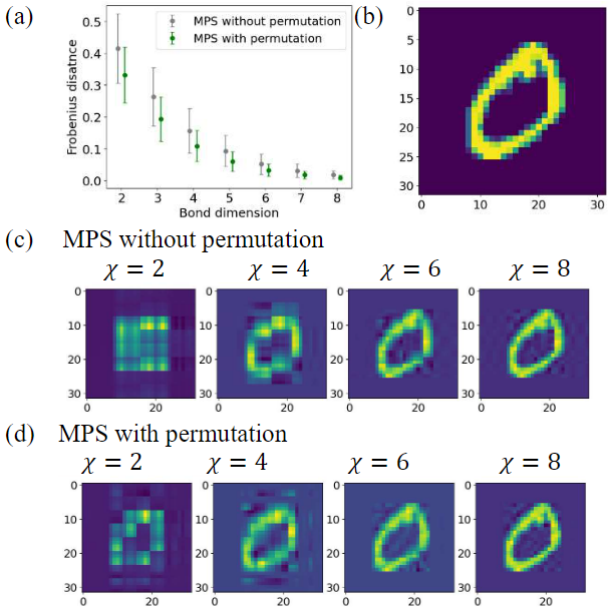


Figure 1: Comparison of the permuted MPS method and the MPS without permutation for MNIST dataset. (a) Plot of Frobenius distance between the input data and MPS representations with and without permutation as a function of bond dimension. (c), (d) Visual comparison of the MPS states for bond dimensions 2, 4, 6, and 8 with and without permutation corresponding to the original MNIST image data shown in (b).

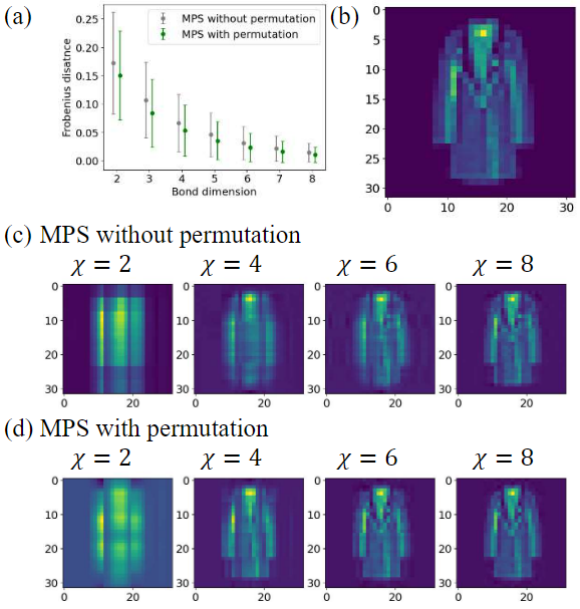


Figure 2: Comparison of the permuted MPS method and the MPS without permutation for Fashion-MNIST dataset.

Table 1: Test accuracies of VQC classifiers trained by quantum states prepared with different encoding schemes.

Train \ Test	MPS w/ perm	MPS w/o perm	Exact
MPS w/ perm	95.8±2.3%	-	94.6±2.6%
MPS w/o perm	-	93.8±9.0%	89.5±11.6%
Exact	-	-	94.6±2.2%

significant increase in the test accuracy of both quantum classifiers when they were trained using our scheme.

For benchmarking with a VQC classifier, we opted to train our models on a binary classification task using the MNIST dataset [19] and attached a quantum convolutional neural network (QCNN) structure [6] to the output of the MPS encoding circuit and the expectation value of measurement is used as a probability. To estimate the maximum achievable test accuracy, in addition to both MPS encoding schemes, we included amplitude-encoded states with exact image data in the comparison summarized in Table 1.

It is worth mentioning that when testing classifiers trained with MPS images, their accuracy surpasses that of classifiers trained with exact input images, but only if the test set is given in MPS form. This suggests that the classifiers trained with the MPS encoded by both algorithms may have overfitted to the corresponding encoding schemes. To avoid over-estimation of the power of MPS encoding scheme, we will only consider amplitude-encoded states with exact image data as the test dataset for the subsequent classifiers.

We also tested a different type of quantum classifiers based on MPS structure with two classification tasks: MNIST and Fashion-MNIST dataset.

Figure 3 shows that the classifiers trained with our scheme outperform the classifiers trained with the standard MPS. The improvement in performance is the maximum at low bond dimension, which is consistent with the large Frobenius distance gap observed in the Fig. 1 and Fig. 2

4 Discussion

Our study suggests that the proposed encoding scheme improved the image fidelity in terms of Frobenius distance as well as the classification accuracy compared to the standard MPS encoding when it is applied to two types of image datasets. The improvement is pronounced at low bond dimensions, which means that the new scheme will be most useful for the noisy intermediate-scale quantum computer [20].

While the permutation search space might seem to appear to grow exponentially with the number of qubits, we reduced the search space significantly by utilizing the

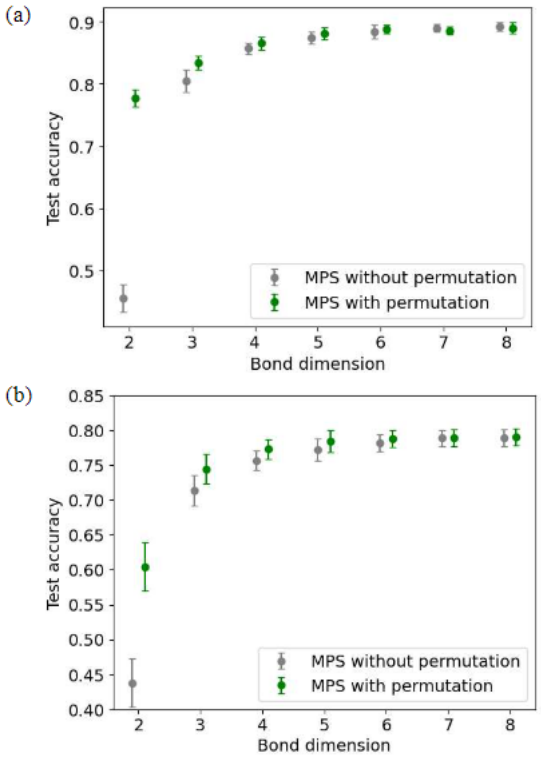


Figure 3: Test accuracies of MPS classifiers with (a) MNIST and (b) Fashion-MNIST

symmetry of the MPS structure under certain permutation, combined with the uniform-cost search. Moreover, our experiments have shown that there exist specific permutations that result in low truncation errors, where only a small portion of the entire permutation space had to be explored while leading to a fast termination.

References

[1] D Coppersmith. An approximate fourier transform useful in quantum factoring. *IBM Research Report*, pages RC–19642, 1994.

[2] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[3] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15):150502, 2009.

[4] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd. Quantum support vector machine for big data classification. *Physical Review Letters*, 113(13):130503, 2014.

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

[6] Iris Cong, Soonwon Choi, and Mikhail D Lukin. Quantum convolutional neural networks. *Nature Physics*, 15(12):1273–1278, 2019.

[7] Ewin Tang. Quantum principal component analysis only achieves an exponential speedup because of its state preparation assumptions. *Physical Review Letters*, 127(6):060503, 2021.

[8] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[9] Israel F Araujo, Daniel K Park, Francesco Petruccione, and Adenilton J da Silva. A divide-and-conquer algorithm for quantum state preparation. *Scientific Reports*, 11(1):1–12, 2021.

[10] Xiao-Ming Zhang, Man-Hong Yung, and Xiao Yuan. Low-depth quantum state preparation. *Physical Review Research*, 3(4):043200, 2021.

[11] David Perez-Garcia, Frank Verstraete, Michael M Wolf, and J Ignacio Cirac. Matrix product state representations. *arXiv preprint quant-ph/0608197*, 2006.

[12] Li Deng. The mnist database of handwritten digit images for machine learning research [best of the web]. *IEEE Signal Processing Magazine*, 29(6):141–142, 2012.

[13] Han Xiao, Kashif Rasul, and Roland Vollgraf. Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms. *arXiv preprint arXiv:1708.07747*, 2017.

[14] R. Dilip, Y. J. Liu, A. Smith, and F. Pollmann. Data compression for quantum machine learning. *Physical Review Research*, 4(4), 2022.

[15] L Wright, F Barratt, J Dborin, V Wimalaweera, B Coyle, and AG Green. Deterministic tensor network classifiers. *arXiv preprint arXiv:2205.09768*, 2022.

[16] Ivan V Oseledets. Tensor-train decomposition. *SIAM Journal on Scientific Computing*, 33(5):2295–2317, 2011.

[17] Edsger W Dijkstra. *A note on two problems in connexion with graphs*, pages 287–290. Springer, 1959.

[18] Stuart J Russell. *Artificial intelligence a modern approach*. Pearson Education, Inc., 2010.

[19] Gerhard Hellstem. Hybrid quantum network for classification of finance and mnist data. In *2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)*, pages 1–4, 2021.

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

Improvement in quantum communication using quantum switch

Arindam Mitra[1 2 *] Himanshu Badhani[1 2 †] Sibasish Ghosh[1 2 ‡]

[1] *Optics and Quantum Information Group, The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India.*

[2] *Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai 400094, India.*

Abstract. It is well known that quantum switch is an example of indefinite causal order. Recently, application of quantum switch on quantum channels, became a hot topic of discussion. It is possible to achieve significant improvement in communication, when a quantum switch is applied on quantum channels. Though above-said improvement is not possible for all quantum channels. For some quantum channels, improvement can be very high. One such example has been discussed in [New J. of Phys. 23, 033039 (2021)] where perfect communication can be achieved. But incidentally that example of channel is unique up to unitary transformations. Therefore, it is important to study the application of quantum switch on other quantum channels where improvement may not be ultimate but significant. Here, we study the application of quantum switch on various quantum channels. In particular we show that if it is not possible to achieve improvement deterministically, it may be possible to achieve improvement probabilistically. It is known that if a quantum channel is useless for some information theoretic task, concatenation of quantum channels generally does not provide any advantage whenever that channel is used. But we show that if a quantum channel is useless even after use of quantum switch, concatenation of quantum channel can make it useful. We also show that quantum switch can help to get quantum advantage in quantum random access code when only useless channels are available for communication. Then we show that quantum switch can be useful to prevent the loss of coherence in a quantum system. We also discuss the fact that if noise is introduced in the switch, then improvement can significantly be decreased.

Keywords: Quantum Channels, Entanglement Breaking channels, Quantum Switch

This submission is for a CONTRIBUTED TALK or POSTER in AQIS 2023 conference. This extended abstract is non-technical and brief. The full technical version can be found here- [Published version- Phys. Scr. 98 045101 (2023) or arXiv pre-print version- arXiv:2108.14001 [quant-ph]].

Extended Abstract

Introduction

Quantum channels (except for identity channel) introduces noise in the quantum state. Practically it very difficult to implement identity channel, since it is difficult to avoid the interaction from the environment. There are some quantum channels which are too bad to transfer some quantum features. For example, entanglement breaking channels can not be used to transfer the entanglement. Recently, it has been proposed that quantum switch can improve the communication through these quantum channels.

Preliminaries

In this section, we discuss the preliminaries.

Entanglement breaking channels: An entanglement breaking channel (EBC), is a quantum channel which provides the output as a separable state while given maximally entangled state as the input [5]. These channels can not transfer the entanglement. in transferring the entanglement. Therefore, as entanglement is a resource in different information theoretic task, these channels are useless in the context of those contexts.

Incompatibility breaking channels: A quantum channel which breaks the incompatibility of any set of arbitrary n observables (a particular $n \in \mathbb{N}$) is known as n-incompatibility breaking channel(n-IBC). If a quantum hannel which breaks the incompatibility of any set of arbitrary n observables for any $n \in \mathbb{N}$) is known as incompatibility breaking channel (IBC). It is well known that $IBC \subseteq ..... \subseteq (n+1) - IBC \subseteq n - IBC \subseteq ..... \subseteq 2 - IBC$. The set of all EBCs is a subset of the set of all IBCs.

Indefinite causal order: Process matrices are the generalisation of density matrices. It has been mentioned in [4] that not all process matrices are causally non-separable i.e., the time ordering between two events are not well defined. This is known as indefinite causal order.

Quantum switch: An example to indefinite causal order is a quantum switch which does not violate the causal inequality. Quantum switch was introduced as a quantum circuit that simulates the indefinite causal order between two different operations. This is done by coupling two operations with two orthogonal quantum states a control qubit and keeping the state of the control qubit in the superposition of those two states.
Let the Krauss operators of channels Λ_A and Λ_B are $\{\mathcal{A}_x\}$ and $\{\mathcal{B}_x\}$ respectively. The Krauss operators for the Switch is given by [1]:

$$\mathsf{S}_{x,y} = \mathcal{A}_x\mathcal{B}_y \otimes |0\rangle\langle 0| + \mathcal{B}_y\mathcal{A}_x \otimes |1\rangle\langle 1| \qquad (1)$$

*arindammitra143@gmail.com
†himanshub@imsc.res.in
‡sibasish@imsc.res.in

Using $|0\rangle\langle 0| = (\sigma_z + I)/2$ and $|1\rangle\langle 1| = (I - \sigma_z)/2$, the above Krauss operators take the following form

$$\mathsf{S}_{x,y} = \frac{1}{2}(\mathcal{A}_x\mathcal{B}_y + \mathcal{B}_y\mathcal{A}_x) \otimes I + \frac{1}{2}(\mathcal{A}_x\mathcal{B}_y - \mathcal{B}_y\mathcal{A}_x) \otimes \sigma_z \quad (2)$$

If we input identical channels into the switch, that is $\Lambda_A = \Lambda_B$, the resultant channel has the following form [1]:

$$\begin{aligned}
&\mathsf{S}_{\Lambda_A,\Lambda_A,\omega}(\rho) \\
&= \frac{1}{4}\sum_{x,y}\Big(\{\mathcal{A}_x, \mathcal{A}_y\}\rho\{\mathcal{A}_x, \mathcal{A}_y\}^\dagger \otimes \omega \\
&+ [\mathcal{A}_x, \mathcal{A}_y]\rho[\mathcal{A}_x, \mathcal{A}_y]^\dagger \otimes \sigma_z\omega\sigma_z\Big) \\
&\equiv C_{+,\Lambda_A,\Lambda_A}(\rho) \otimes \omega + C_{-,\Lambda_A,\Lambda_A}(\rho) \otimes \sigma_z\omega\sigma_z \qquad (3)
\end{aligned}$$

where ω is the initial state of control qubit. Therefore, switch operation creates two branches of CP maps $C_{+,\Lambda_A,\Lambda_A}$ and $C_{-,\Lambda_A,\Lambda_A}$. If original channel is a Pauli channel then both branches are multiple of quantum channels (in that case, we denote these quantum channels as C_+ and C_-).

Perfect communication through zero capacity channels: It has been shown in [1] that using a quantum switch, one can achieve *perfect* communication using the entanglement breaking channel $\Lambda_{perfect}(\rho) = \frac{1}{2}\sigma_x\rho\sigma_x + \frac{1}{2}\sigma_y\rho\sigma_y$. But unfortunately, this example of quantum channel is essentially *unique* upto the unitary equivalence, i.e., there is *no* other quantum channel which provides perfect communication under the action of quantum switch. Therefore, unless this channel is available, the perfect communication is impossible even using quantum switch.

Main results

In this section, we discuss our main result. We want to mention here that throughout the paper we will repeatedly use the term "useless channels" which is context dependent e.g., EBCs are useless in the context of entanglement transfer and IBcs are useless in the context of QRAC or quantum steering (it will be discussed later in the relevant sections). The channels which are not useless depending on the context, are useful. *Subsections under this section are similar to the full manuscript*.

Transfer of entanglement through EBC using quantum switch: In this subsection, we discuss the possibility of deterministic transfer and probabilistic transfer of entanglement. We write the first theorem-
Theorem 1: If Alice is using the channel Λ_A and the quantum switch to send a quantum state ρ, then

(a) If both the branches $C_{+,\Lambda_A,\Lambda_A}(\rho)$ and $C_{-,\Lambda_A,\Lambda_A}(\rho)$ are EB CP maps, there does not exist any quantum measurement based control operation which can make the final channel (after tracing out the control qubit part) a non-EBC.

(b) If both branches (In case of Pauli channels) are the multiples of arbitrary quantum channels $C_+(\rho)$ and $C_-(\rho)$ and both $C_+(\rho)$ and $C_-(\rho)$ are IBC, there does not exist any quantum measurement based controlled operation which can make the final channel (after tracing out the switch part) a non-IBC.
Therefore, if at least one of the branch is non-EBCP, at least probabilistic transfer of entanglement can be done by the selective measurement on the control qubit part. We have studied the case for depolarising channel as an example (*Please check the full manuscript (Sec. III A) on arxiv (for free access) for the graph and details*). Then for the Pauli channels, we have studied whether C_+ or C_- branch become useful under he quantum switch (*Several graphs and details are provided in the full manuscript (Sec. III A) on arxiv*).

Concatenation of quantum channels and the quantum Switch: It is well known that if Λ is EBC (or IBC) then $\Phi \circ \Lambda$ is also EBC (or IBC) for any channel Φ. Therefore, if Λ is unavoidable for communication, concatenation of quantum channels will not help in the transfer entangled states (or steerable states). Below, we show that if one uses quantum switch, concatenation of quantum channels may provide a advantage in quantum communication. We start with our next observation.

Observation 1: There exist quantum channels which do not provide any advantage under the action of quantum switch, but such a channel may become useful under the action of quantum switch if it is concatenated with another quantum channel.

The results of the concatenation are more interesting if Φ is also an EBC as we show in the next observation:

Observation 2: There exist quantum channels which do not provide any advantage under the action of quantum switch, but such a channel may become useful under the action of quantum switch if it is concatenated with another EBC.

Then for Pauli channels and 3-parameter non-unital channels we study the effect of concatenation of useless channels on switch operation (Sec: III B in the full manuscript). We provide some Venn diagram (Please check Sec: III B in the full manuscript) which dictates the possibility that a useless channel (under the action of a quantum switch) will be useful (under the action of a quantum switch) under concatenation. We call the channel completely useless if under both C_+ and C_- it remains useless. The Venn diagrams suggests us to give following conjecture-

Conjecture 1: Concatenation of two completely useless channels is always completely useless.

Advantages in different information theoretic tasks:

1. Advantage in quantum random access code

Let, Alice has n-dits denoted by $\vec{x} = (x_1, ..., x_n)$ at her disposal. She encodes a particular n-dit string in the qudit and then transfers this qudit to Bob. In addition, Bob receives a random number j. Now, Bob's task is to guess the jth dit x_j. He does this by doing a measurement on the qudits sent by Alice. He has n choices of measurements with d outcomes. After obtaining the random number j, he performs the j-th measurement on the qudit sent by Alice. Depending on the outcome of the measurement, Bob guesses the dit. Let, his guess is y. The game will be successful if $y = x_j$. This is

known as $(n, d)-$quantum random access code(QRAC). It has a classical counterpart, known as $(n, d)-$random access code (RAC), where Alice is allowed to send a dit to Bob instead of a qudit. The maximum average success probability of random access code is $P_{rac}^{(2,d),max} = \frac{1}{2}(1 + \frac{1}{d})$. But the maximum average success probability of quantum random access code is $P_{qrac}^{(2,d),max} = \frac{1}{2}(1 + \frac{1}{\sqrt{d}})$. Therefore, $P_{rac}^{(2,d),max} < P_{qrac}^{(2,d),max}$. We will call a particular encoding of Alice and a particular set of measurements performed by Bob to guess the desired qudit as a "useful strategy" if it can achieve quantum advantage in the average success probability i.e., the average success probability $P_{qrac}^{(2,d)} > P_{rac}^{(2,d),max}$.

Now suppose only the noisy channel Λ is available to Alice to transfer the qudit to Bob. In this case the achievable success probability decreases. Depending on Λ, this decrement of probability can be drastic. Noting that we have the following theoremThere exist quantum channels which do not provide any advantage under the action of quantum switch, but such a channel may become useful under the action of quantum switch if it is concatenated with another EBC.-

Theorem 2: If Alice has only $2 - IBC$ channels to transfer the qudit to Bob in a $(2, d) - QRAC$ game, there does not exist any measurement strategy to Bob and any qudit encoding to Alice which can be useful i.e., can get quantum advantage.

Therefore, if Alice has only $2 - IBC$ to communicate with Bob, it will be useless in this context. Then through an example we have shown that if Alice has quantum switch, she can get rid of the situation (even if she has only an IBC to communicate with Bob) and improve the communication (*Please check Sec: III C 1 in the full manuscript*).

2. Advantage in quantum steering

Suppose, Alice and Bob shares a bipartite quantum state $\rho^{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and Alice has a measurement assemblage $\mathcal{M}_A = \{M_x\}$. Each M_x has the outcome set Ω_x. Now state ρ^{AB} is called unsteerable from Alice to Bob i.e., from A to B with $\mathcal{M}_A$ if there exist a probability distribution π_λ, a set of states $\{\sigma_\lambda\}$ and a set of probability distributions $P_A(a_x|x, \lambda)$ for all $a_x \in \Omega_x$ and for all x such that

$$\rho^B_{a_x|x} = \mathrm{Tr}_A[(M_{a_x|x} \otimes \mathbb{I}_B)\rho^{AB}] = \sum_\lambda \pi_\lambda P_A(a_x|x, \lambda)\sigma_\lambda \qquad (4)$$

holds. A state ρ^{AB} is called unsteerable from A to B if it is unsteerable from A to B with any measurement assemblage $\mathcal{M}_A$. A state ρ^{AB} is called unsteerable if it is unsteerable from both A to B and from B to A. Otherwise it is called steerable.

Now suppose, Bob is preparing a bipartite entangled state ρ^{AB} and sending the part A to Alice. This shared bipartite entangled quantum state, they will use in different information theoretic tasks which can be performed with the help of A to B steering. Now, we write the following theorem-

Theorem 3: Suppose Bob is sending A part of a bipartite state ρ^{AB} to Alice (i.e., from B to A) through an n-incompatibility breaking channel Λ then $\rho'^{AB} = (\Lambda \otimes \mathcal{I})(\rho^{AB})$ is not steerable from A to B with any measurement assemblage $\mathcal{M}_A = \{M_x\}_{x=1}^n$ where $\mathcal{I}$ is an identity channel.

Now, we write the following corollary-

Corollary 4: Suppose Bob is sending A part of a bipartite state ρ^{AB} to Alice (i.e., from B to A) through an incompatibility breaking channel Λ then $\rho'^{AB} = (\Lambda \otimes \mathcal{I})(\rho^{AB})$ is not steerable from A to B where $\mathcal{I}$ is a identity channel.

The Corollary 4 is also proved in the Theorem 1 of [7]. A Corollary similar, but not exactly same with the Corollary 4, has been derived using channel state duality in [6].

Therefore, if Alice has only IBC to communicate with Bob, it will be useless in this context. Then through an example we have shown that if Alice has quantum switch, she can get rid of the situation (even if she has only an IBC to communicate with Bob) and improve the communication (*Please check Sec: III C 2 in the full manuscript*).

3. Prevention of the loss of coherence

Suppose Alice is preparing quantum states for Bob who uses the coherence of these states w.r.t. some basis as a resource to get the advantage in different information-theoretic and thermodynamic tasks. But if Alice has only coherence-breaking channels to communicate with Bob, she will be unable to transfer the coherence of the state. Whereas if she has incoherent channels, the coherence of state which Alice sends for Bob, will decrease when the state will reach to Bob.

In these types of cases, if she has a quantum switch, she will be able to perform better communication, as states in the following theorem.

Theorem 5: A coherence breaking qubit channel may be converted to a non-coherence breaking qubit channel with the help of a quantum switch along with a measurement-based controlled incoherent unitary operation..

Therefore, action of quantum switch can prevent the loss of coherence. *For more details on this, please check full manuscript (Sec. III C 3) .*

Communication using noisy quantum switch: Till now, we have discussed only noiseless control qubit state. But in practice due to the interaction of environment in the switch state. We show through an example that if depolarising noise is acted on switch, improvement in communication can be significantly decreased. *For more details on this, please check full manuscript (Sec. III D) .*

Conclusions

We have shown that in case deterministic improvement in communication is not possible using quantum, probabilistic improvement may be possible using it. We discuss the communication improvement for several quantum channels. We show that if a channel is useless even after using quantum switch, concatenation of it with some other channels may provide communication improvement under action of quantum switch. In particular, we have studied the conversion of useful channels into useful channel through concatenation which will be useful in quantum communication technology in future. We have shown that communication improvement due to action of quantum switch helps to get advantage in Quantum Random Access Codes as well as helps to demonstrate quantum steering when only useless channels are available for communication, preventing the loss of coherence

etc. We show that the noise introduced in the switch may hamper the communication improvement. Our research opens up several research avenues. It is open problem to find out necessary sufficient condition for quantum channel which provides improvement under action of quantum switch. Though we have shown that that if a channel is useless even after using quantum switch, concatenation of it with some other channels may provide communication improvement under action of quantum switch, the necessary and sufficient condition for improvement in this case, is not known. It may also be interesting to compare with the effectiveness of noisy quantum switch in achieving improvements in different quantum information processing (or, quantum communication) tasks.

This work may have many practical significances in quantum communication technology and therefore, we think that this work will be interesting for the participants of AQIS 2023.

Note

This paper is already submitted to a journal for review.

References

[1] Giulio Chiribella et al. Indefinite causal order enables perfect quantum communication with zero capacity channels. New J. Phys. **23** 033039 (2021)

[2] Michael Horodecki, Peter W. Shor & Mary Beth Ruskai. General Entanglement Breaking Channels. Rev. Math. Phys **15**, 629–641 (2003)

[3] Lorenzo M. Procopio et al. Communication Enhancement through Quantum Coherent Control of N Channels in an Indefinite Causal-Order Scenario. Entropy 2019, **21**(10), 1012 (2019)

[4] Ognyan Oreshkov, Fabio Costa & Časlav Brukner. Quantum correlations with no causal order. Nature Communications **3**, 1092 (2012)

[5] Giulia Rubino et al. Experimental verification of an indefinite causal order. Sci. Adv. **3**, e1602589 (2017).

[6] J. Kiukas, C. Budroni, R. Uola, Juha-Pekka Pellonpää, Continuous-variable steering and incompatibility via state-channel duality, Phys. Rev. A **96**, 042331 (2017).

[7] H. Y. Ku, J. Kadlec, A. Černoch, M. T. Quintino, W. Zhou, K. Lemr, N. Lambert, A. Miranowicz, S. L. Chen, F. Nori, and Y. N. Chen, Detecting quantum non-breaking channels without entanglement, arXiv:2106.15784v2 [quant-ph].

Analyzing quantum machine learning using tensor network

S. Shin[1] * Y. S. Teo[1] † H. Jeong[1] ‡

[1] *Department of Physics and Astronomy, Seoul National University, 08826 Seoul, South Korea*

Abstract. Our work presents a unified framework using tensor networks (TN) to compare classical and quantum machine learning (QML) models. By representing QML models as TN models, we identify the model as a featured linear model with a constrained coefficient and a computationally efficient feature map. Using this, we can generate classical TN machine learning models having the same feature map as QML models efficiently. By analyzing the coefficient components of the models using matrix product states, we could fairly compare the function classes of the two feature-equivalent models and performances in the context of kernel method.

Keywords: Quantum Machine Learning, Tensor Network, Variational Quantum Algorithm

1 Introduction

Quantum Machine Learning (QML) garners a huge interest among various communities and industries for the past few years as a prominent candidate for practical applications for quantum computers in the NISQ era. Usually, QML uses a variational quantum circuit as a data processor, and the variational parameters in the quantum circuit are optimized with the help of classical optimization algorithms such as gradient descent methods. Variational QML (VQML) aims to achieve a more powerful machine learning model by exploiting the power of a quantum computer. In other words, quantum advantage in the machine learning (ML) area.

While there are theoretical proofs that demonstrate the possibility of achieving a quantum advantage in ML tasks through fully quantum settings [1, 2], arguably the most interesting applications of ML employ classical data. Moreover, if one does not have access to coherent quantum memory and quantum channel, then even if the VQML uses a 'quantum state' as its input, one cannot avoid using classical data to generate the quantum state onto the quantum circuit. Therefore in the near-term quantum era, it is important and worthwhile to investigate the power of using VQML with classical data as input. When dealing with classical data, one cannot avoid comparing VQML and classical ML, which have inherently different structures. Consequently, establishing a fair comparative framework remains a challenge.

In this study, we propose a unified tensor network (TN) formalism to systematically investigate between classical TNML models and given VQML models. This approach is based on the ability to transform a given generally-encoded VQML model into a TN structure, subsequently separating it into two components: the basis part (or the feature map), which formulates the basis functions for the linear model, and the coefficient part, which generates the coefficient on these basis functions. A number of linearly independent basis functions can possibly scale exponentially with the number of encoding gates [3]. However, by utilizing the knowledge of data pre-processing prior to implementing VQML, we can simply observe that the basis part is an easily manageable tensor-product form. A tensor product feature map can generate an exponential number of basis functions utilizing only polynomial calls of pre-processing functions and polynomial memory. This allows us to construct a classical TN model having a computationally efficient classical feature map that produces the same set of basis functions as the provided VQML model, thereby ensuring a cohesive comparative analysis. Setting the two models to be basis-equivalent, we characterize their function classes as constrained-coefficient linear models within the shared function space, so that the comparison can be conducted in the context of coefficient expressivity. To analyze and compare the coefficient components of these models, we utilize a special one-dimensional TN structure, known as the matrix product states (MPS). MPS admits systematic analysis of expressivity and computational efficiency in the context of entanglement. With numerical simulations and use of dimensional arguments of the function spaces, identify conditions under which VQML models can be easily approximated by the classical MPS model.

Finally, we compare the performance of VQML and classical ML models in ML tasks. We do function regressions using the kernel method, which is an important facet of machine learning that finds the optimal function in the linear model within the feature space in terms of the basis kernel functions. There exists a Hilbert space spanned by these kernel functions and the optimal function minimizing the loss function from the given training data resides in that space. This Hilbert space is the Reproducing Kernel Hilbert Space (RKHS). We observe that the efficient classical kernel from the basis-equivalent classical MPS model has an RKHS that covers the RKHS from the quantum kernel. We compare the performance of the classically hard-to-simulate quantum kerenel and classical MPS kernel in ML tasks.

2 Main results

Preparing the VQML For any VQML employing the classical data as input, one cannot avoid using data-encoding circuits. These encoding circuits can contain general multi-qubit gates that depend on the classical

*wookshin@snu.ac.kr
†yong.siah.teo@gmail.com
‡h.jeong37@gmail.com

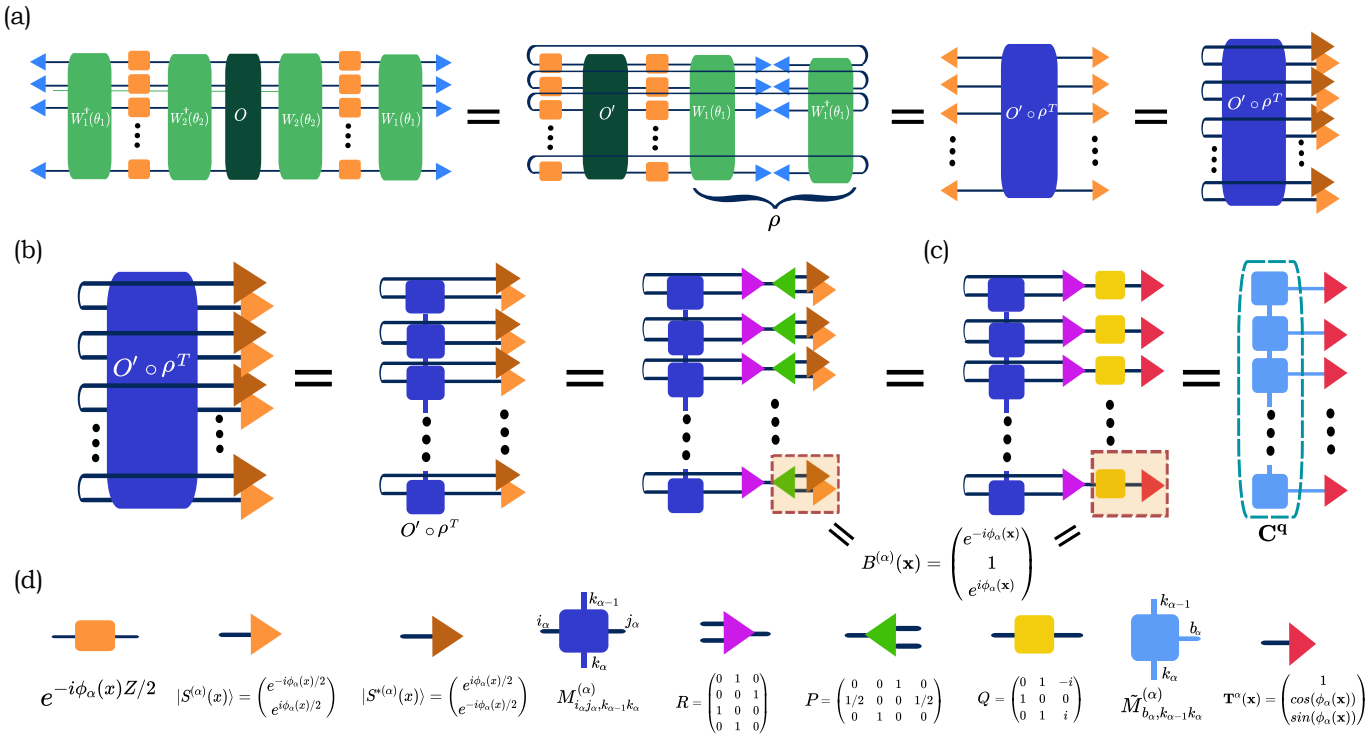


Figure 1: (a) Graphical depiction of the transformation of a simple parallel VQML model, $f_Q(\boldsymbol{x};\boldsymbol{\theta})$, into an FLM form. The $\circ$ denotes the Hadamard product (element-wise product). The dependence on $\boldsymbol{\theta}$ of O' and ρ^T has been omitted for simplicity. (b) The model is then reshaped into an MPS model form that incorporates the feature map $\mathbf{B}$. By transforming $O' \circ \rho^T$ into the MPO, vectorizing the matrix, and applying additional tensors, we achieve the MPS form. (c) The final result is an FLM, where the feature map is the product of N of $\mathbf{T}^{(\alpha)}(\boldsymbol{x})$'s and the coefficient part is the MPS $\mathbf{C^q}(\boldsymbol{\theta}_1, \boldsymbol{\theta}_2)$, which is the contracted form of $(O' \circ \rho^T) \cdot \mathbf{R} \cdot \mathbf{Q}$. All tensors are real-valued. (d) Each block's description is provided. The site index is denoted by α.

data $\boldsymbol{x} \in \mathbb{R}^d$. However, to implement any general encoding strategy in a near-term quantum circuit, one should decompose all the multi-qubit gates into single-qubit gates and non-parametrized 2-qubit gates (such as CNOT gates). This decomposition results in N single-qubit Pauli-Z rotation encoding gates, $\{e^{-i\phi_\alpha(\boldsymbol{x})Z/2}\}_\alpha$ where $\phi_\alpha : \mathbb{R}^d \to \mathbb{R}$ is the pre-processing functions that depend on the encoding strategy.

VQML models as featured linear model We focus on the VQML models with N qubits having all encoding gates positioned parallel between two trainable unitaries $W_1(\boldsymbol{\theta}_1), W_2(\boldsymbol{\theta}_2)$. Any general-structure quantum models can be transformed into this parallel form (See appendix A in [4]), so no generality is loss. This parallel VQML generates the function

$$f_Q(\boldsymbol{x};\boldsymbol{\theta}) = \langle 0| W_1^\dagger(\boldsymbol{\theta}_1)\mathbf{S}^\dagger(\boldsymbol{x})W_2^\dagger(\boldsymbol{\theta}_2)O \cdots W_2(\boldsymbol{\theta}_2)\mathbf{S}(\boldsymbol{x})W_1(\boldsymbol{\theta}_1)|0\rangle, \quad (1)$$

where O is the observable, and $\mathbf{S}(\boldsymbol{x})$ represents the parallel data-encoding circuit composed of Pauli-Z rotations. $f_Q(\boldsymbol{x};\boldsymbol{\theta})$ can be represented as TN, and following the graphical description in the Fig. 1, we can identify the VQML model as a featured linear model (FLM),

$$f_Q(\boldsymbol{x};\boldsymbol{\theta}) = \mathbf{C^q}(\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, O) \cdot \mathbf{T}(\boldsymbol{x}) \quad (2)$$

where the feature map is defined as

$$\mathbf{T} : \boldsymbol{x} \mapsto \bigotimes_{\alpha=1}^{N} \begin{pmatrix} 1 \\ \cos(\phi_\alpha(\boldsymbol{x})) \\ \sin(\phi_\alpha(\boldsymbol{x})) \end{pmatrix}. \quad (3)$$

Here the coefficient part $\mathbf{C^q}(\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, O)$ is constructed by the variational part of the quantum circuit, so it is constrained in general.

Basis-equivalent classical MPS model and approximability of VQML Owing to the fact that the basis component in the VQML model can be expressed as a product of vectors, and by using our knowledge of the pre-processing functions, $\{\phi_\alpha\}_\alpha$ from the preparation stage of VQML, we can construct a basis-equivalent linear model (an equivalent feature map) *efficiently* by utilizing the TN method. We have represented the coefficient part in the VQML model to an MPS form, so we choose a classical MPS, denoted as $\mathbf{C^c}(\boldsymbol{\theta})$, as the structure for the trainable coefficients (see Fig 2). The constructed classical MPS (cMPS) model $f_c(\boldsymbol{x};\boldsymbol{\theta}) = \mathbf{C^c}(\boldsymbol{\theta}) \cdot \mathbf{T}(\boldsymbol{x})$ has a computaional complexity of $O(N\chi^2)$, where N is the length of $\mathbf{T}$ (the number of single-qubit encoding gates) and χ is the maximum bond dimension of $\mathbf{C^c}(\boldsymbol{\theta})$. Therefore, by controlling the bond dimension of $\mathbf{C^c}(\boldsymbol{\theta})$, one can create an efficient cMPS

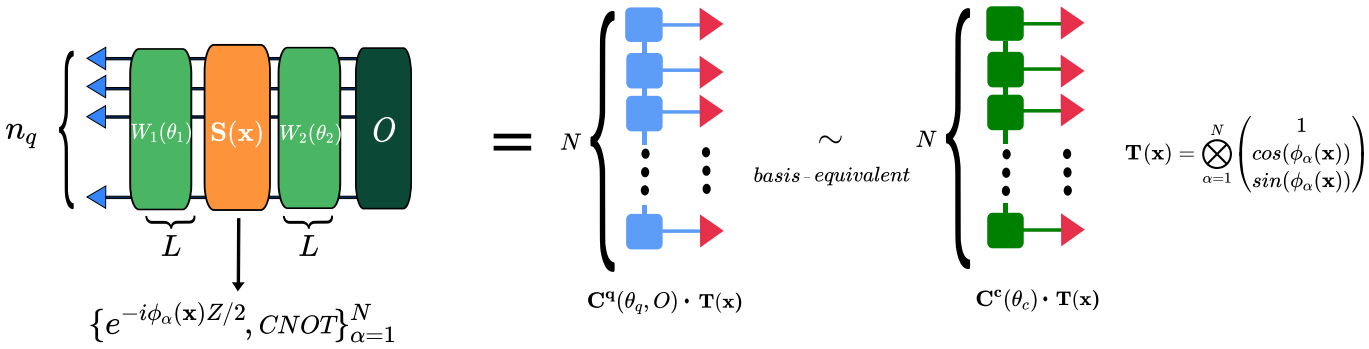


Figure 2: We approximate the given VQML model using the basis-equivalent cMPS model. The coefficients are structured as an MPS, enabling us to employ metrics like bond dimension or entanglement entropy to analyze the inherent properties of the coefficient spaces, including efficiency, expressiveness, and the capacity for approximation. θ_q represents the variable parameters in the quantum circuit, while θ_c represents the parameters in the classical MPS.

model. This efficient model requires only a computational cost that scales polynomially with the number of qubits in the corresponding quantum model, but generates basis functions that are identical to those produced by the VQML model. Since an MPS with small entanglement can be approximated by an MPS with a smaller bond dimension, it is possible for efficient cMPS model to closely approximate quantum models.

We numerically examined the Renyi-2 entropy of $\mathbf{C^q}(\boldsymbol{\theta}, O)$ derived from various VQML models, discovering that noiseless poly-depth circuit VQMLs are difficult to approximate, while noisy and more constrained circuits such as data re-uploading circuits are easier for classical approximation. Additionally, feature spaces of small dimensions render VQML models susceptible to efficient classical approximations. All numerical results can be found in Sec .V and VI of [4]

Kernel method Every feature map in the FLM yields a kernel, which evaluates the inner product between feature-mapped data. Utilizing the kernel method, the optimal function that minimizes empirical risk can be analytically determined. Kernel method posits full and free control over the coefficients in the linear model. Given that all VQML models are the FLM with feature map $\mathbf{T}$ and constrained coefficients, the optimal function derived from the quantum kernel method falls within the function class of the cMPS model with the same feature map. The kernel from the feature map of a basis-equivalent cMPS model is $\mathcal{K}_c(\boldsymbol{x}_i, \boldsymbol{x}_j) = \langle \mathbf{T}(\boldsymbol{x}_i) | \mathbf{T}(\boldsymbol{x}_j) \rangle$, which is efficient to compute (only linearly scaling with the number of encoding gates). $\mathcal{K}_c$ explores the function space beyond the quantum kernel. In this work, we compare the performance of the classically hard-to-simulate quantum kernel [5] with the corresponding basis-equivalent $\mathcal{K}_c$. We discover that $\mathcal{K}_c$ can fit the data as accurately as the quantum kernel, surpassing the performance of any classical method covered in prior research [6]. Nevertheless, its generalizability, a crucial attribute of ML, falls short of the quantum kernel for the small size of the circuit, while becomes comparable when the size increases.

3 Conclusion

We presented a general methodology to explicitly convert any VQML model into an MPS ML model. By leveraging this technique, we identify VQML models as FLMs with an efficient feature map $\mathbf{T}(\boldsymbol{x})$ and constrained coefficient $\mathbf{C^q}(\boldsymbol{\theta}, O)$. This finding illustrates that the fundamental disparity between classical and quantum ML models does not lie in the exponentially large feature space, but rather in the structure of the coefficient they each possess. Through analyzing the coefficient of the VQML model using MPS, we were able to determine the conditions under which VQML models can be approximated by cMPS models and contrast their expressivity within the context of entanglement. Additionally, we identified an efficient kernel capable of generating a function space that encompasses the space from the quantum kernel. Numerically, we demonstrated that this classical kernel is as expressive as its quantum counterpart. This research proposes a unified approach to compare quantum and classical machine learning models, and suggests potent classical ML model that may exhibit comparable performance to the VQML models in certain situations. Our work strengthens the connection among interdisciplinary communities such as quantum machine learning, classical machine learning, and tensor network communities.

References

[1] H.-Y. Huang et al. Quatnum advanrage in learning from experiments. Science 376, 1182 (2022), 2112.00778.

[2] H.-Y. Huang et al. Information-Theoretic Bounds on Quantum Advantage in Machine Learning. Physical Reviews Letters, 126,190505 (2021), 2101.02464.

[3] S. Shin et al. Exponential data encoding for quantum supervised learning. Physical Review A 107, 012422 (2023)

[4] S. Shin et al. Analyzing quantum machine learning using tensor network. (Preprint, attached as appendix)

[5] V. Havlicek et al. Supervised learning with quantum-enhanced feature spaces. Nature 567, 209-212 (2019)

[6] S. Jerbi et al. Information-Theoretic Bounds on Quantum Advantage in Machine Learning. Nature communications 14, 517 (2023).

Graph-theoretical optimization of fusion-based graph state generation

Seok-Hyung Lee[1 2 *] Hyunseok Jeong[1 †]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Republic of Korea*
[2] *Centre for Engineered Quantum Systems, School of Physics, University of Sydney, Sydney, NSW 2006, Australia*

Abstract. Graph states are versatile resources for various quantum information processing tasks, including measurement-based quantum computing. Although fusion gates enable all-optical generation of graph states by combining small graph states, its nondeterministic nature hinders efficient generation of large graph states. Here, we present a graph-theoretical strategy to effectively optimize fusion-based generation of any given graph state. Our strategy comprises three stages: simplifying the target graph state, building a fusion network, and determining the order of fusions. We expect that our strategy and software will assist researchers in developing and assessing experimentally viable schemes that use photonic graph states.

Keywords: Graph state, Photonic quantum computing, Measurement-based quantum computing, Fusion-based quantum computing

1 Introduction

Graph states represent a family of multi-qubit states where qubits are entangled following a specific structure determined by an associated graph. Owing to their highly entangled nature [1], graph states find applications in various quantum information processing domains, such as measurement-based quantum computing (MBQC) [2–5], fusion-based quantum computing (FBQC) [6], quantum error correction [7, 8], quantum secret sharing [9, 10], quantum repeaters [11–14], and quantum metrology [15].

All-optical methods for constructing photonic graph states are commonly processed by merging multiple smaller graph states into a larger one using type-II fusion operations [16]. A severe problem is that fusions are non-deterministic; for example, when employing dual-rail-encoded qubits and restricting the setup to linear-optical devices and photodetectors, the success probability of a fusion is limited to 50% without ancillary resources [17]. Therefore, resource overhead remains a significant challenge for generating large-scale graph states. It is thus essential to carefully design a procedure for generating a desired graph state from basic resource states to minimize resource overhead as much as possible.

In this work, we introduce a graph-theoretical strategy to effectively identify a resource-efficient method for fusion-based generation of any given graph state. Technical description of our work is presented in Ref. [18]. Moreover, our strategy is implemented in an open-source Python package, *OptGraphState*, which is publicly available on Github: `https://github.com/seokhyung-lee/OptGraphState`.

For a given graph G, the corresponding *graph state* $|G\rangle$ can be generated by placing a qubit with the state $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ on each vertex of G and applying a controlled-Z (CZ) gate on each pair of qubits connected by an edge. *Local complementation* with respect to a vertex v is a graph operation that, for every pair of adjacent vertices of v, connect them if they are disconnected and disconnect them if they are connected. It is known that, for a vertex v, Clifford gates $\exp\left[-i(\pi/4)\hat{X}\right]$ on v and $\exp\left[i(\pi/4)\hat{Z}\right]$ on its neighbors transform the graph state $|G\rangle$ by a local complementation with respect to v [19].

The *type-II fusion operation* [16] indicates a destructive measurement of two Pauli operators $\hat{X}\otimes\hat{Z}$ and $\hat{Z}\otimes\hat{X}$ on a pair of qubits. By applying a fusion on an unconnected pair (v_1, v_2) of vertices in a graph state, we can connect (disconnect) every adjacent vertex of v_1 with every adjacent vertex of v_2 up to several Pauli-Z operators if they are unconnected (connected). For single-photon polarization qubits, a fusion can be done with linear optical devices and photodetectors [20], which succeeds with the probability of $p_{\text{succ}}(\eta) = (1-\eta)^2/2$ when each photon suffers loss with probability η and the input state is maximally mixed.

2 Results

2.1 Strategy

Our basic resource state is the three-qubit star graph state $\left|G_*^{(3)}\right\rangle := (|{+}0{+}\rangle + |{-}1{-}\rangle)/\sqrt{2}$. Hence, our goal is to find an efficient way to build a desired graph state $|G\rangle$ by performing fusions on multiple $\left|G_*^{(3)}\right\rangle$ states. The resource efficiency is quantified by the average number Q of $\left|G_*^{(3)}\right\rangle$'s required to successfully generate one $|G\rangle$ state through post-selection.

The strategy is summarized as follows: (i) Simplifying the graph of the desired graph state by *unraveling* subgraphs of specific types. (ii) Constructing a *fusion network* from the simplified graph. (iii) Determining the fusion order with the *min-weight-maximum-matching-first* method. (iv) Iterating the above steps (which contain randomness) a sufficient number of times and select the best one.

2.1.1 Simplification of graph by unraveling

If the graph $G = (V, E)$ of the desired graph state $|G\rangle$ contains specific types of subgraphs, it is posible to generate $|G\rangle$ by applying single-qubit Clifford operations and/or fusions (called external fusions) on the graph

*seokhyung.lee@sydney.edu.au
†jeongh@snu.ac.kr

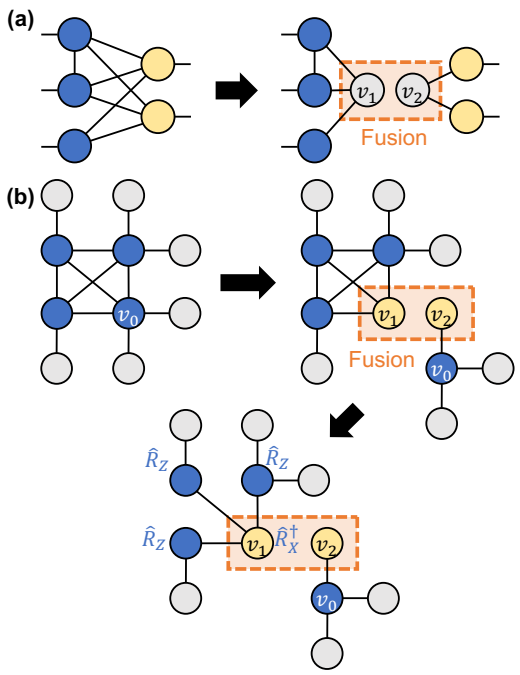


Figure 1: Unraveling processes of **(a)** a bipartitely-complete graph and **(b)** a clique.

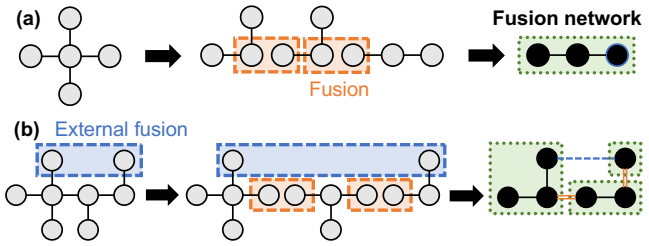


Figure 2: Constructing fusion networks for **(a)** a five-qubit star graph state and **(b)** a general graph state.

state of a simplified graph. Unraveling means the process to build such a simplified graph G_{unrv} (referred to as an *unraveled graph*) and specify the information necessary to recover $|G\rangle$ from $|G_{\mathrm{unrv}}\rangle$. We currently have unraveling schemes for two types of subgraphs: *bipartitely-complete subgraphs* (BCSs) and *cliques*.

A BCS of a graph means a subgraph where the vertices can be grouped into two disjoint subsets such that every vertex in the first subset is connected with every vertex in the other subset. A BCS can be unraveled by adding two vertices and one fusion; see Fig. 1(a) for an example. A clique of a graph, which is a fully-connected subgraph, can be unraveled by adding two vertices that undergo a fusion and applying a local complementation, as shown in Fig. 1(b). In our strategy, we repeat the cycle of finding non-overlapping BCSs and cliques (that do not share any vertices) and unraveling them as above until no new BCSs and cliques are found.

2.1.2 Construction of fusion network

A fusion network is a graph where vertices correspond to individual $\left|G_*^{(3)}\right\rangle$ states and edges indicate fusions between them required to generate the target graph state $|G\rangle$. An m-qubit star graph state can be constructed by conducting fusions on $m-2$ copies of $\left|G_*^{(3)}\right\rangle$, which leads to a linear fusion network with $m-2$ nodes; see Fig. 2(a) for an example. A general graph state can be decomposed into multiple star graph states with fusions as shown in Fig. 2(b), thus its fusion network can be constructed by connecting the fusion networks of these star graphs. Note that the above process contains ambiguity, which needs to be optimized.

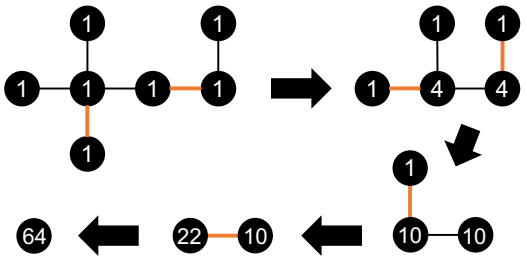


Figure 3: Determining the fusion order with the min-weight-maximum-matching-first method. Each step is an intermediate fusion network after contracting links (orange bold lines) in the previous step. The numbers inside the nodes indicate their weights. We assume $p_{\mathrm{succ}} = 1/2$.

2.1.3 Determination of fusion order

We can regard a fusion network as a weighted graph where each node indicates a group of entangled qubits and each link represents a fusion between these groups that needs to be done. The weight of each node $w(n)$ is defined as the resource overhead of the process of generating the corresponding entangled states. Upon the above setting, the action of a fusion can be treated as the contraction of a link with a suitable update rule of weight values. Hence, if the order of the fusions is given, the resource overhead Q of the entire process can be obtained from the weights of the last remaining nodes after contracting all the edges in the order.

Our strategy to determine the order of fusions is based on the following two intuitions: (i) It is preferred to contract links with small weights first, where the weight of a link l is defined as the weight of the merged vertex when the link is contracted. (ii) Links that do not share endpoints can be contracted simultaneously and it is preferred to contract links as parallelly as possible. Based on these intuitions, we use the *min-weight-maximum-matching-first* method to determine the fusion order, which is done by identifying a maximum matching of the subgraph of each intermediate fusion network induced by the set of links with the smallest weight. We illustrate an example in Fig. 3.

2.2 Numerical results

Figure 4 visualizes the distributions of the obtained resource overheads of random graphs optimized by our strategy for various values of $|V|$ and $|E|$ when $p_{\mathrm{succ}} = 0.5$ or 0.75. To sample random graphs, we use the

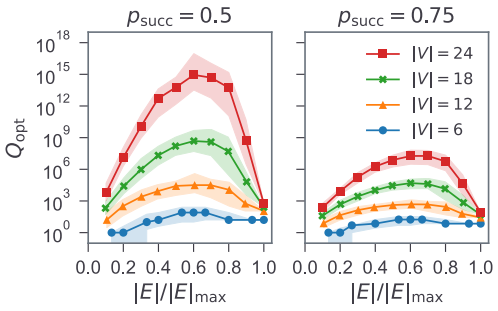


Figure 4: Distribution of the optimized resource overhead Q_{opt} for random graphs sampled with fixed numbers of vertices ($|V|$) and edges ($|E|$) by the Erdős–Rényi model [21]. Two different fusion success rates are considered: $p_{\mathrm{succ}} \in \{0.5, 0.75\}$. $|E|_{\mathrm{max}} = |V|(|V|-1)/2$ is the maximal possible number of edges for the given vertex number. For each combination of $(p_{\mathrm{succ}}, |V|, |E|)$, 100 random graphs are sampled [18]. The median of the distribution is indicated as a dot and its total range is shown as a shaded region.

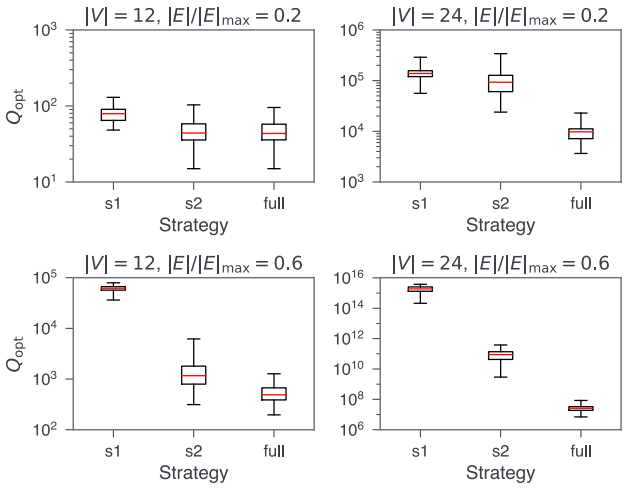


Figure 5: Comparison of the distributions of Q_{opt} for different optimization strategies. Three strategies are considered: the strategy without unraveling (s1), the strategy with random selection of the fusion order (s2), and our full strategy. The distribution of Q_{opt} is visualized as a box plot, where the red line indicates the median, the box extends from the first quartile (Q1) to the third quartile (Q3), and the whisker covers the entire range of the values.

Erdős–Rényi model [21], where all graphs that contain given fixed values of $|V|$ and $|E|$ have an equal probability. Here, we sample 100 random graphs for each combination $(p_{\mathrm{succ}}, |V|, |E|)$ and use the adaptive iteration method of $m_{\mathrm{init}} = 600$ [18]. We note several observations from the results: (i) Q_{opt} increases exponentially (or super-exponentially) as $|V|$ grows when $|E|/|E|_{\mathrm{max}}$ is fixed. (ii) For a fixed value of $|V|$, Q_{opt} is maximal when $|E| \approx 0.6|E|_{\mathrm{max}}$. Q_{opt} is inversely correlated with $|E|$ for large values of $|E|$ since bipartitely-complete subgraphs and cliques are more likely to appear for when $|E|$ is large. (iii) The fusion scheme with $p_{\mathrm{succ}} = 0.75$ may greatly reduce the order of Q_{opt}, compared to the one with $p_{\mathrm{succ}} = 0.5$, especially when $|V|$ is large. Note that, to achieve $p_{\mathrm{succ}} = 0.75$ with linear optics, we require an ancillary two-photon Bell state [22] or four ancillary unentangled photons [23] per fusion and photon-number resolving detectors that can discriminate at least four photons. On the other hand, the scheme with $p_{\mathrm{succ}} = 0.5$ requires only on-off detectors and no ancillary photons.

We now show that our strategy is indeed effective by comparing it with two "deficient" strategies in which a certain stage is missing from the original "full" strategy. In detail, we consider the following two alternative strategies:

(s1) The strategy without the unraveling process, where the original graph is directly used for generating a fusion network. The other steps are the same as the full strategy.

(s2) The strategy where the fusion order is randomly selected without using the min-weight-maximum-matching-first method. The other steps are the same as the full strategy.

In Fig. 5, the distributions of Q_{opt} optimized by these three strategies for random graphs are presented as box plots. Each box extends from the first quartile (Q1) to the third quartile (Q3) and the corresponding whisker covers the entire range of the values. It clearly shows that the full strategy is significantly more powerful than the deficient ones, especially when there exist many vertices and edges. In other words, each step in the full strategy contributes to reducing the resource overhead.

3 Conclusion

In this work, we proposed a graph-theoretical strategy to construct a resource-efficient method for generating an arbitrary graph state with the type-II fusion operation. The strategy is composed of multiple trials to find the optimal one, where each round contains three stages: unraveling the graph, constructing a fusion network, and determining the fusion order. We applied the strategy to random graph states and verified numerically that each step of the strategy is indeed necessary to achieve high resource efficiency.

We anticipate that our strategy and software will aid researchers in designing experimentally feasible approaches utilizing photonic graph states and in evaluating the practicality of their proposed schemes. For example, the basic resource states of MBQC and FBQC can be logically-encoded star or cycle graph states [6, 24]. Employing larger or more complex codes may improve the fault-tolerance of these schemes; however, generating such resource states could become a bottleneck in their implementation. Our strategy can contribute to evaluating such a trade-off relation and identifying the most practical sweet spot.

References

[1] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel. Entanglement in graph states and its applications. In *Quantum Computers, Algorithms and Chaos*, pages 115–218. IOS Press, 2006.

[2] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[3] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, 2003.

[4] R. Raussendorf, J. Harrington, and K. Goyal. A fault-tolerant one-way quantum computer. *Ann. Phys.*, 321(9):2242–2270, 2006. ISSN 0003-4916.

[5] R. Raussendorf, J. Harrington, and K. Goyal. Topological fault-tolerance in cluster state quantum computation. *New J. Phys.*, 9(6):199, 2007.

[6] Sara Bartolucci, Patrick Birchall, Hector Bombin, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, et al. Fusion-based quantum computation. *Nat. Commun.*, 14(1):912, 2023.

[7] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65:012308, 2001.

[8] A. Pirker, J. Wallnöfer, H. J. Briegel, and W. Dür. Construction of optimal resources for concatenated quantum protocols. *Phys. Rev. A*, 95:062332, 2017.

[9] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78: 042309, 2008.

[10] B. A. Bell, Damian Markham, D. A. Herrera-Martí, Anne Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.*, 5: 5480, 2014.

[11] M. Zwerger, W. Dür, and H. J. Briegel. Measurement-based quantum repeaters. *Phys. Rev. A*, 85:062326, 2012.

[12] M. Zwerger, H. J. Briegel, and W. Dür. Universal and optimal error thresholds for measurement-based entanglement purification. *Phys. Rev. Lett.*, 110:260503, 2013.

[13] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nat. Commun.*, 6 (1):6787, 2015.

[14] J. Wallnöfer, M. Zwerger, C. Muschik, N. Sangouard, and W. Dür. Two-dimensional quantum repeaters. *Phys. Rev. A*, 94:052307, 2016.

[15] Nathan Shettell and Damian Markham. Graph states as a resource for quantum metrology. *Phys. Rev. Lett.*, 124:110502, 2020.

[16] Daniel E. Browne and Terry Rudolph. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.*, 95:010501, 2005.

[17] Samuel L. Braunstein and A. Mann. Measurement of the Bell operator and quantum teleportation. *Phys. Rev. A*, 51:R1727–R1730, 1995.

[18] Seok-Hyung Lee and Hyunseok Jeong. Graph-theoretical optimization of fusion-based graph state generation. quant-ph/2304.11988, 2023.

[19] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. Graphical description of the action of local Clifford transformations on graph states. *Phys. Rev. A*, 69:022316, 2004.

[20] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. Bell measurements for teleportation. *Phys. Rev. A*, 59:3295–3300, 1999.

[21] Paul Erdős and Alfréd Rényi. On random graphs I. *Publicationes mathematicae*, 6(1):290–297, 1959.

[22] W. P. Grice. Arbitrarily complete Bell-state measurement using only linear optical elements. *Phys. Rev. A*, 84:042331, 2011.

[23] Fabian Ewert and Peter van Loock. 3/4-efficient Bell measurement with passive linear optics and unentangled ancillae. *Phys. Rev. Lett.*, 113:140403, 2014.

[24] Seok-Hyung Lee, Srikrishna Omkar, Yong Siah Teo, and Hyunseok Jeong. Parity-encoding-based quantum computing with bayesian error tracking. *npj Quantum Inf.*, 9:39, 2023.

Implementation of lattice surgery-based logical operations in a fault-tolerant quantum software framework

Youngchul Kim[1] * Soo-Cheol Oh [1] † Sangmin Lee [1] ‡ Ki-Sung Jin [1] § Gyuil Cha [1] ¶

[1] *Future Computing Research Division, ETRI, Daejeon, Republic of Korea*

Abstract. We present a quantum software framework that supports fault-tolerant quantum computing. Using the lattice surgery technique, this framework encodes logical qubits in surface codes and implements logical Clifford and T gates. By interfacing the QPlayer simulator with the framework, we have configured six two-dimensional logical qubits with a distance of three and have evaluated the lattice surgery-based logical operations, which have been presented theoretically by simulating quantum circuits composed of universal quantum gates. In conclusion, we have shown that the proposed framework can effectively perform Clifford and T gates in fault-tolerant quantum computing based on surface code logical qubits.

Keywords: fault-tolerant quantum computing, quantum software framework, surface code, lattice surgery, quantum simulator

1 Introduction

Developing quantum computers from current noisy quantum devices requires fault tolerance using quantum error correction(QEC)[1]. There is much research on QEC to support fault tolerance with topological codes, especially surface codes[2, 4, 5]. Surface code is considered the most prominent QEC method due to its high error threshold (up to 1%)[2] and simple two-dimensional(2D) structure with only nearest-neighbor(NN) interactions. However, encoding logical qubits with surface codes requires many physical qubits, and it is necessary to scale to larger surface codes to suppress the error rate of logical qubits. Surface code with a distance of three can correct single-qubit or, at most two-qubit errors with the smallest number of qubits. Implementing and performing quantum circuits with surface code logical qubits fault-tolerantly, surface code needs to be encoded with a distance of at least 3.

Surface code performs logical operations by interacting between locally adjacent lattices in a 2D structure. Various techniques, such as transversal gates and teleported gates[3], have been studied to perform logical operations, but they are costly and complex. The lattice surgery(LS)[4, 5, 6, 7, 8] method can alleviate these problems.

In practice, we need to provide a quantum computer that supports universal quantum gates to reap the benefits of quantum computing. To do this end, we have to support Clifford and non-Clifford gates. Clifford gates, generated by *CNOT*, *H*, and *S* gates, can be effectively simulated on a classical computer[9] and implemented via the LS. However, it is not easy to implement non-Clifford gates, typically T gate, which requires magic state distillation[10] that needs many resources and time. Therefore, in previous studies, LS-based logical Clifford+T operations have been theoretically analyzed[4, 5] or experimentally implemented with small surface codes[8].

We have implemented a quantum software framework to support a fault-tolerant universal quantum computer. This framework provides LS-based logical Clifford+T gates. This paper uses QPlayer[11, 12] to simulate quantum circuits composed of Clifford+T gates and verify the computational results. For this purpose, the quantum circuits are translated into LS-based logical operations and converted into physical operations to perform on the simulator.

2 Fault-tolerant quantum software framework

The fault-tolerant quantum software framework has been implemented in a layered architecture[13]. Qubits are accessed at logical, virtual, and physical levels at each layer. A quantum program is written with a quantum programming language, and a quantum compiler translates it into LS-based logical operations defined in Table 1, which are processed in this framework. The fault-tolerant software framework is outlined in Fig. 1, and

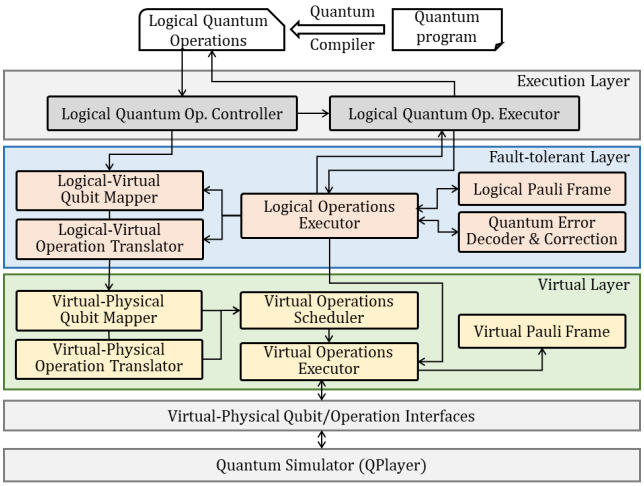


Figure 1: Fault-tolerant quantum software framework.

*kimyc@etri.re.kr
†ponylife@etri.re.kr
‡sanglee@etri.re.kr
§ksjin@etri.re.kr
¶gicha@etri.re.kr

Table 1: LS-based logical operations.

Operation types	Operations
Init. & Pauli	Init_X(Z), X(Z)
Measurement	Measure_X(Z)
Lattice Surgery	Merge_Mxx(Mzz), Split_Mxx(Mzz) CNOT_Post_Mxx(Mzz) Move_Post_Mxx(Mzz) Hadamard, Deform Flip_Expand(Contract, Shift) Inject_Y(A), S(T, T_Dag)_Post

the features of each layer are as follows:

Execution layer performs logical qubit mapping and logical operation translation through the Fault-tolerant layer. After executing the translated logical operations, it does post-logical operations according to the qubit measurement outcomes or returns the qubit measurement outcomes to the quantum program.

Fault-tolerant layer encodes logical qubits in rotated surface code using virtual qubits and arranges a 2D logical qubit architecture into a checkerboard form, as shown in Fig. 2. It maps logical qubits to virtual qubits and converts logical operations to virtual operations. A logical qubit is made up of virtual qubits, and a logical operation is composed of operations on the virtual qubits that make up the logical qubit. It performs logical operations after mapping the qubits and converting the operations. Each time it does, it performs error syndrome measurement(ESM) for the logical qubit. After ESM execution, error detection and correction are performed according to the measurement outcomes. Among the logical operations, Pauli operations are handled in software through the logical Pauli frame[14].

Virtual layer maps virtual qubits to physical qubits and converts virtual operations to the corresponding physical operations. It can perform virtual operations in parallel and schedule according to the physical operation properties provided by the quantum simulator. In this paper, physical qubits and operations are emulated by the QPlayer simulator. The QPlayer simulator processes the virtual operations through the Virtual-Physical qubit/gate interface and returns the execution results. Within the virtual operations, Pauli operations are handled in software through the physical Pauli frame[14].

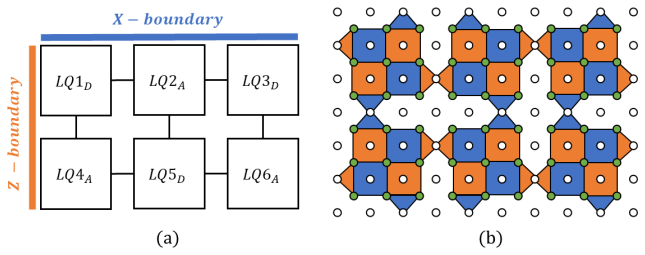


Figure 2: Logical qubit architecture. (a) shows the logical connectivity of the logical qubits. $LQ1_D$, $LQ3_D$, and $LQ5_D$ indicate logical data qubits. $LQ2_A$, $LQ4_A$, and $LQ6_A$ indicate logical ancilla qubits. (b) shows rotated surface codes constructed from physical qubits.

Quantum simulator supports simulations of physical qubit operations. It provides the properties of physical operations and the connectivity between physical qubits. A physical two-qubit operation can only be performed between NN qubits connected to each other. QPlayer is a quantum simulator that provides more qubits and faster quantum operations with smaller memory. It selectively tracks realized quantum states using a reduced quantum state representation scheme instead of loading the entire quantum states into memory.

3 Implementation of LS-based logical operations

The LS is a fault-tolerant protocol that can perform state teleportation or gate teleportation between logical qubits encoded in a surface code. It is performed in two steps: merging and splitting. Merging and splitting perform the logical joint measurements along the X(Z)-boundaries, $M_{ZZ}(M_{XX})$, on which they operate. Fig. 3 shows circuits of logical operations using LS, such as state teleportation, $CNOT$, S, and T. In particular, the logical S and T operations require the magic state that can be prepared with the state injection process. However, since state injection is not fault-tolerant, the injected magic state has low fidelity and needs to be distilled. Magic state distillation procedures are not easy to implement because it costs a lot of resources and time to obtain a higher-fidelity magic state from multiple lower-fidelity states[2, 5, 16]. In this work, we prepare the magic state through the injection process without the magic state distillation and assume it has high fidelity.

We have implemented the Clifford+T gates, such as H, $CNOT$, $S/S^\dagger$, and $T/T^\dagger$ using LS in the rotated surface code. The logical $CNOT$ operation performs a logical joint measurement, $M_{ZZ}(M_{XX})$, along the boundary with the adjacent ancilla qubit according to the logical connectivity of the control and target qubits in the logical qubit architecture. It then performs Pauli corrections on the measurement outcomes. The logical $S/S^\dagger$ operation performs a logical joint measurement on the X-boundary, M_{ZZ}, with the neighboring ancilla qubit injected magic state $|Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$. It then performs a Pauli correction based on the joint measurement outcome and the ancilla qubit measurement outcome. The Pauli correction operation is processed in software using the Pauli frame. The logical $T/T^\dagger$ operation requires the magic state $|A\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{4}}\,|1\rangle)$. It performs a logical joint measurement on the X-boundary, M_{ZZ}, with the neighboring ancilla qubit injected magic state. Then, depending on the joint measurement outcome and the ancilla qubit measurement outcome, Clifford correction, $S/S^\dagger$ operation, is applied, or Pauli correction is performed in software using the Pauli frame. In addition, the $SWAP$ gate, which three consecutive $CNOT$ gates can implement, can be performed using LS-based logical state teleportations.

Table 2: Evaluation of quantum circuits composed of Clifford+T gates.

Original circuits							LS-based circuits					
Circuit	Qubits	X	H	CX	S/S†	T/T†	Qubits$_{L_D}$	Qubits$_{L_A}$	Qubits$_P$	Op.$_L$	Op.$_V$	Op.$_P$
deutsch_n2	2	1	3	1	0	0	2	2	70	26	1894	1608
grover_n2	2	4	10	2	0	0	2	2	70	70	5245	4416
iswap_n2	2	1	4	2	2	0	2	2	70	45	3465	2972
teleportation_n3	3	0	4	2	1	1	3	3	106	50	3817	3307
toffoli_n3	3	0	2	6	1	7	3	3	106	128	10209	8985

We have simulated some quantum circuits in QASMBench[17] and identified the expected results by changing the input states in the quantum circuits. Table 2 shows the count of qubits and gates that make up the benchmark quantum circuits. The table also shows the count of logical data and ancilla qubits when these circuits are translated to LS-based circuits. The physical qubit counts include the physical qubits encoding the distance-3 rotated surface code and the syndrome physical qubits of the stabilizers newly added between the two logical qubits in the merging operation. The operation counts indicate the count of logical, virtual, and physical operations as LS-based circuits are transformed and executed through the layers in our framework. Due to the Pauli frames, the physical operation counts performed in the simulator are less than the virtual operation counts.

The T gate is a typical non-Clifford gate with significant overhead to implement fault-tolerant. For example, Fig. 4 shows a *Toffoli* gate decomposed using H, $CNOT$, T, $T^\dagger$, and S gates. The decomposed circuit of a *Toffoli* gate contains nine Clifford gates and seven non-Clifford gates. Therefore, it requires multiple LS operations and Clifford corrections based on the joint measurement outcomes and ancilla qubit measurement outcomes. We have performed simulations of the LS-based *Toffoli* operation with eight input states, $|000\rangle$, $|001\rangle$, ..., $|111\rangle$, and identified that the measurement outcomes are the same as the truth table of *Toffoli* gate.

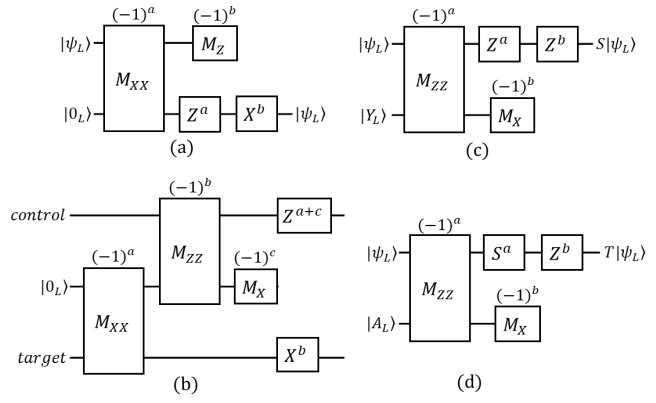


Figure 3: LS-based logical operations. (a) logical state teleportation. (b) logical $CNOT$ operation. (c) logical S operation. (d) logical T operation

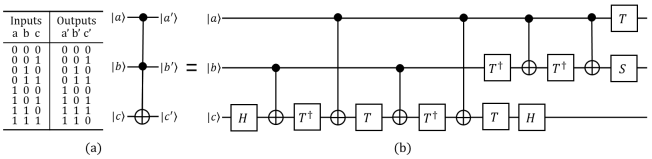


Figure 4: (a) Truth table and quantum circuit of *Toffoli* gate. (b) *Toffoli* gate decomposition using Clifford+T gates.

4 Conclusion

We have presented a quantum software framework for fault-tolerant universal quantum computers. It implements LS-based logical Clifford+T gates using rotated surface code on logical qubit architecture. We have simulated quantum circuits with Clifford+T gates in the framework and evaluated LS-based logical operations. The quantum software framework can be extended to architectures arranged with more logical qubits, and the LS-based logical operations implemented in this work can serve as a primary reference model. As a next step, we will apply various quantum error models to verify the LS-based logical operations.

Acknowledgements

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00014, A Technology Development of Quantum OS for Fault-tolerant Logical Qubit Computing Environment).

References

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2010.

[2] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A.* 86, 2012.

[3] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature.* 402, 1999.

[4] C. Horsman, A. G. Fowler, S. Devitt, and R. V. Meter. Surface code quantum computing by lattice surgery. *New Journal of Physics.* 14, 2012.

[5] D. Herr, F. Nori, and S. J. Devitt. Lattice surgery translation for quantum computation. *New Journal of Physics.* 19, 2017.

[6] L. Lao, B. V. Wee, I. Ashraf, J. V. Someren, N. Khammassi, K. Bertels and C. G. Almudever. Mapping of lattice surgery-based quantum circuits on surface code architectures. *Quantum Sci. Technol.* 4, 015005, 2018.

[7] C. Vuillot, L. Lao, B. Criger, C. G. Almudéver, K. Bertels and B. M. Terhal. Code deformation and lattice surgery are gauge fixing. *New Journal of Physics.* 21, 2019.

[8] A. Erhard, H. P. Nautrup, M. Meth, L. Postler, R. Stricker, M. Stadler, V. Negnevitsky, M. Ringbauer, P. Schindler, H. J. Briegel, R. Blatt, N. Friis and T. Monz. Entangling logical qubits with lattice surgery. *Nature.* 589, 2021.

[9] D. Gottesman. The Heisenberg Representation of Quantum computers. arXiv:quant-ph/9807006, 1998.

[10] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A.* 71, 2005.

[11] K. S. Jin and G. I. Cha. QPlayer: Lightweight, scalable, and fast quantum simulator. *ETRI Journal.* 45 (2023), 304–317.

[12] K. S. Jin and G. I. Cha. Multilayered logical qubits and synthesized quantum bits. *Quantum Science and Technology.* (2023).

[13] N. C. Jones, R. V. Meter, A. G. Fowler, P. L. McMahon, J. S. Kim, T. D. Ladd, and Y. Yamamoto. Layered Architecture for Quantum Computing. *Physical Review X.* 2, 2012.

[14] J. H. On, C. Y. Kim, S. C. Oh, S. M. Lee, and G. I. Cha. A multilayered Pauli tracking architecture for lattice surgery-based logical qubits. *ETRI Journal.* (2022), 1–17, doi:10.4218/etrij.2022-0037.

[15] A. G. Fowler and C. Gidney. Low overhead quantum computation using lattice surgery. arXiv:1808.06709, 2019.

[16] L. Lao and B. Criger. Magic state injection on the rotated surface code. *ACM Int'l Conf. on Computing Frontiers.*, 2022.

[17] A. Li, S. Stein, S. Krishnamoorthy, and J. Ang. QASMBench: A Low-Level Quantum Benchmark Suite for NISQ Evaluation and Simulation. *ACM Trans. on Quantum Computing.*, 2022.

Fault-tolerance analysis of photonic hybrid quantum computation

Nuri Kang[1 2] Jaehak Lee[1 3] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, South Korea*
[2] *Department of Physics, Korea University, Seoul 02841, South Korea*
[3] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, South Korea*

Abstract. To realize practical quantum computation, logical errors should not be increased when accumulating all components of quantum computing architecture. To achieve this, a physical error rate should be achieved to be below a certain threshold called the fault-tolerance threshold. Analyzing the fault-tolerance threshold as well as the resource overhead for a given certain quantum error correction scheme is essential for implementing and designing scalable fault-tolerance quantum computing architectures. Here we develop a tool to simulate fault-tolerance threshold for a given quantum error correction code and error model. We then analyze the fault-tolerance threshold of photonic quantum computing protocols including the hybrid qubit schemes with cat code proposed recently by authors, and show that it outperforms other previous protocols.

Keywords: Photonic hybrid quantum computation, Quantum error correction, Fault-tolerance analysis

1 Introduction

To realize universal quantum computation, the fault-tolerance implies that errors are not accumulated as increasing the size of the system including all the components of quantum computing architecture. For this, a physical error of each component should be below a certain value called the fault-tolerance threshold. In addition, the resource cost to achieve the fault-tolerance is also an important parameter for practical realization of quantum computers. Therefore. analyzing the fault-tolerance threshold and the resource overhead for a given certain quantum error correction scheme and quantum computing platform is essential for designing scalable quantum computing architectures.

Meanwhile, various photonic quantum computation schemes have been proposed so far toward fault-tolerant quantum computation. In linear optical approach, two-qubit gate operation typically require the Bell state measurement (BSM) for gate teleportation instead of direct coupling because of the non-interactive nature of photons. However, the success probability of BSM based on linear optics is at most 1/2 [1], and due to the effect of photon loss, the success probability in practice is even worse. To solve these problems, various BSM schemes using ancillary photons and BSM scheme with discrete-variable (DV) error correction code [2] have been prooseded. Improved BSMs can make the measurement process itself more resistant to photon loss, but the photonic qubits are still vulnerable to photon loss for the full fault-tolerance of photonic quantum computation.

Recently, authors have proposed a scheme for photonic hybrid quantum computation with single photon and cat code [3]. Cat-code is a bosonic error correction code [4, 5] encoding logical qubits against photon loss in even-parity cat states $\{|\mathcal{C}_\alpha^+\rangle, |\mathcal{C}_{i\alpha}^+\rangle\}$. However, nonorthogonality between logical basis states makes it difficult to implement gate operations such as Z gate. We address this problem by introducing hybrid qubits that combine discrete-variable (DV) qubits and continuous-variable (CV) qubits [3]. In previous studies [6], polarization states $\{|D\rangle, |A\rangle\}$ and coherent states have been used as DV and CV qubits, respectively. On the other hand, in this work we incorporate the error correcting feature of cat codes into the CV part of the hybrid qubit, so the logical basis is $\{|0_L\rangle = |D\rangle|\mathcal{C}_\alpha^+\rangle, |1_L\rangle = |A\rangle|\mathcal{C}_{i\alpha}^+\rangle\}$. This allows us to improve the resilience to photon loss, while also making it possible to implement gate operations. Recently, linear optical implementation of cat codes has been developed in Refs.[7] and [8], by which we define a hybrid BSM (HBSM) by incorporating together with the standard polarization qubit BSM [1].

We here develop a tool to simulate fault-tolerance threshold for a given quantum error correction code and error model. Based on this, we analyze the fault-tolerance of photonic quantum computing protocols including the previous [6] and recent hybrid quantum computing scheme [3] and compare their performances. We employ HBSM as a logical BSM to analyze the fault-tolerance and resource overhead of concatenated codes quantum low-depth parity check (qLDPC) codes as an outer logical code. We devise a gate teleportation scheme for universal quantum computation to demonstrate concatenated codes and a measurement-based quantum computation (MBQC) scheme to qLDPC codes. In MBQC, HBSM is used to create a cluster state from unit resource states. A HBSM can achieve an arbitrary high success probability, which allows to perform near-deterministic logical BSM without the need for any other improved BSM techniques. Our results show that the photonic hybrid quantum computation using single photon and cat code outperforms other previous proposals in fault-tolerance analysis.

2 Error model

In optical systems, photon loss is the most common error. Other errors, such as coherent errors and dephasing errors, are much less common. Therefore, we only con-

*swleego@gmail.com

sider photon loss in fault-tolerance analysis. Photon loss affects both the failure probability of HBSM and the logical error rate. We use the result of Ref. [7] to calculate the failure probability of HBSM. Since the photon-photon coupling strength γ is very small, we can assume that the process is Markovian. we calculated the logical errors by solving the Lindblad master equation

$$\frac{d\rho}{dt} = \gamma \left(\hat{a}\rho\hat{a}^\dagger - \frac{1}{2}\{\hat{a}^\dagger\hat{a}, \rho\} \right). \quad (1)$$

The photon loss probability is defined as $\eta = 1 - \exp(-\gamma t)$. The HBSM failure and logical Z error are both functions probability of η and encoding amplitude α. We assumed that each photon has a probability η of being lost between two consecutive HBSMs. Therefore, η s the average photon loss probability per step in both gate teleportation and MBQC. We also assumed that the unit resource states are already prepared by a heralding resource preparation process. This means that the failure of HBSMs and photon loss in this process only affect the resource overhead. In both gate teleportation and MBQC, we estimate the photon loss threshold for each encoding amplitude α using Monte-Carlo method.

3 Fault-tolerance analyses

We first consider the `STEANE` code as an outer logical code and estimate the fault-tolerance with several concatenation levels. Since CSS codes including `STEANE` code only use the Hadamard gate (H_L), the controlled-Z gate (CZ_L), the preparation of the $|+_L\rangle$ state, and the measurement in the X_L basis, we only need to consider these operations. The state preparation and measurement are trivial, but applying H_L and CZ_L requires the gate teleportation. Both gates can be performed using the unit resource state $|\Phi_H\rangle \propto |0_L, 0_L\rangle + |0_L, 1_L\rangle + |1_L, 0_L\rangle - |1_L, 1_L\rangle$ and $|\Phi_{CZ}\rangle \propto |0_L, 0_L, 0_L, 0_L\rangle + |0_L, 0_L, 1_L, 1_L\rangle + |1_L, 1_L, 0_L, 0_L\rangle - |1_L, 1_L, 1_L, 1_L\rangle$, respectively. In the physical level, resource states can be created by combining two types of entangled states: DV entangled pairs and hybrid entangled states. A hybrid entangled state can be generated by a cross-Kerr interaction between a single photon and an even cat state. In logical levels, we prepare the transversal $|\Phi_H\rangle$ and $|\Phi_{CZ}\rangle$ and apply the syndrome projection measurement to prepare the logical states. We use the Knill-type error correction circuit proposed in Ref. [9] for both the physical and logical levels.

In MBQC, we used the surface code, which is the most well-known and widely used qLDPC code. The cluster state used in MBQC scheme for the surface code is the `Raussendorf-Harrington-Goyal` (RHG) lattice graph state [10]. Typically assume that cluster states are prepared off-line using a heralding process. This means that errors caused by photon loss or the failure of a BSM used in off-line process are not considered. This makes the presented schemes more robust to errors, but it also requires exponentially more resources. In this work, we assumed that only unit resource states were prepared. The unit resource states we used are the central micro cluster $|\mathcal{C}_3^C\rangle = \frac{1}{\sqrt{2}}(|0_L0_L0_L\rangle + |1_L1_L1_L\rangle)$ and side micro cluster

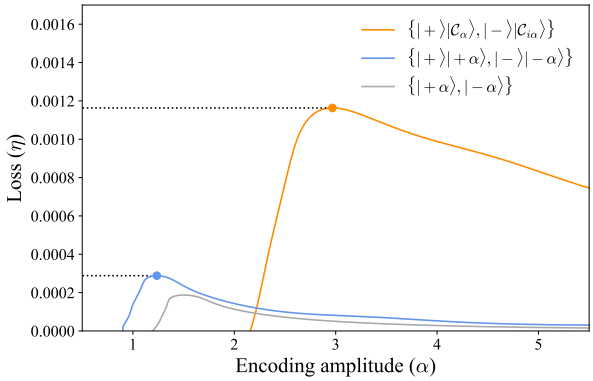


Figure 1: Loss threshold for `STEANE` code. Logical basis for each curve is shown at upper right corner. Circles represent the highest loss threshold with the optimal encoding amplitude.

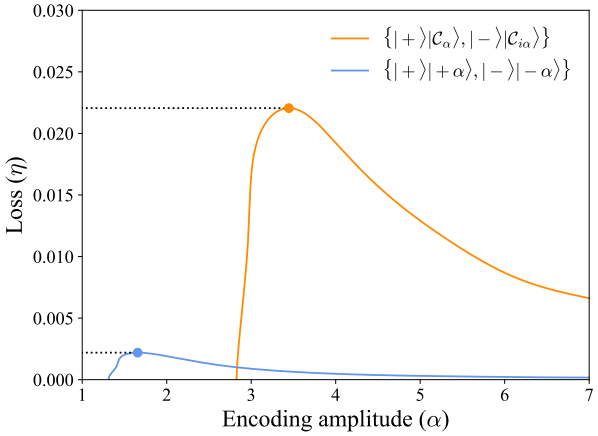


Figure 2: Loss threshold for `RHG` lattice.

$|\mathcal{C}_3^S\rangle = \frac{1}{2}(|0_L0_L0_L\rangle + |1_L1_L0_L\rangle + |0_L0_L1_L\rangle - |1_L1_L1_L\rangle)$. These states can be created in a similar manner with gate teleportation. We first create a star cluster state $|\mathcal{C}^*\rangle$ using HBSM. This state has one central vertex qubit and four side vertex qubits connected to it by edges. Next, we apply the HBSM to the closest side qubits of two neighboring star cluster states. This generates a `RHG` lattice state.

For Monte-Carlo simulation, we used the percolation model for HBSM failure with adaptive measurement scheme [11] and weighted minimum-weight perfect matching decoder via PyMatching package [12].

4 Results

We have evaluated the fault-tolerance threshold for photonic quantum computation schemes using coherent state qubits, hybrid qubits with single photon and coherent states [13], and hybrid qubits with single photon and cat code [3] by changing the encoded amplitude α. Figure 1 and Figure 2 shows the results for the `STEANE` code and `RHG` lattice, respectively. When using the `STEANE`

code error correction, the hybrid qubit with cat code achieves a much higher loss threshold of 0.116% than all the previous proposals, which is about four times greater with a slightly larger amplitude α than the loss threshold of 0.029% achieved by hybrid qubit with coherent states [13].

In the case of the `RHG` lattice, we found that the threshold for the hybrid qubit with cat code is improved by almost an order of magnitude compared to the hybrid qubit with coherent states. The optimal threshold is observed to be 2.21% at $\alpha \approx 3.45$, which is, to the best of our knowledge, the highest threshold for CV encoding of optical qubits [14].

References

[1] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Bell measurements for teleportation, Phys. Rev. A. **59**, 3295 (1999).

[2] Seok-Hyung Lee, Seung-Woo Lee, and Hyunseok Jeong, Loss-tolerant concatenated Bell-state measurement with encoded coherent-state qubits for long-range quantum communication, Phys. Rev. Research. **3**, 043205 (2021).

[3] J. Lee *et al.*, to be submitted (2023).

[4] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, Hardware-Efficient Autonomous Quantum Memory Protection, Phys. Rev. Lett. **111**, 120501 (2013).

[5] M. Bergmann and P. van Loock, Quantum error correction against photon loss using multicomponent cat states, Phys. Rev. A 94, 042332 (2016).

[6] S.-W. Lee and H. Jeong, Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits, Phys. Rev. A **87**, 022326 (2013).

[7] D. Su, I. Dhand, and T. C. Ralph, Universal quantum computation with optical four-component cat qubits, Phys. Rev. A **106**, 042614 (2022).

[8] J. Hastrup and U. L. Andersen, All-optical cat-code quantum error correction, Phys. Rev. Research **4**, 043065 (2022).

[9] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen, Noise thresholds for optical cluster-state quantum computation, Phys. Rev. A. **73**, 052306 (2006)

[10] R. Raussendorf, J. Harrington, and K. Goyal, A fault-tolerant one-way quantum computer, Ann. Phys. **321**, 2242 (2006).

[11] A. C. Whiteside and A. G. Fowler, Upper bound for loss in practical topological-cluster-state quantum computing, Phys. Rev. A **90**, 052316 (2014).

[12] O. Higgott, Pymatching: A python package for decoding quantum codes with minimum-weight perfect matching, ACM Trans. Quantum Comput. 10.1145/3505637 (2021)

[13] S.-W. Lee and H. Jeong, Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits, Phys. Rev. A **87**, 022326 (2013).

[14] N. Kang *et al.* to be submitted (2023).

Nondestructive Bell state discrimination between distant particles

Bohdan Bilash[1 2 *] Youngrong Lim[3] Hyukjoon Kwon[3] Yosep Kim[1]
Hyang-Tag Lim[1 2] Wooyeong Song[1 †] Yong-Su Kim[1 2 ‡]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea*

[2] *Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Republic of Korea*

[3] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Republic of Korea*

Abstract. We propose a scheme to nondestructively discriminate all four Bell states between distant parties. Without pre-shared entanglement, the successful nondestructive discrimination probability is limited to $p = 1/4$ which is equivalent to random guessing. Here, we show that harnessing two pairs of pre-shared entanglement, one can achieve a complete nondestructive Bell state discrimination between distant parties. Using IonQ quantum computer simulation, we also demonstrate that our scheme surpass the classical limit of 1/4 on a present quantum processor.

Keywords: Quantum Entanglement, Discrimination, Non-demolition, Bell state

Quantum state discrimination is crucial for various applications, including quantum key distribution [1, 2]. One of possible methods to share information are Bell states. However, typical Bell state discrimination schemes destroy the quantum state. To preserve the state, ancillary qubits can interact with system qubits, enabling nondestructive discrimination of Bell states [3, 4].

In quantum networks, shared entangled particles among distant parties face security challenges due to potential threats from malicious third parties or insecure quantum channels. Nondestructive verification of shared entanglement is desirable but limited by the implementing interaction with both distant system qubits. Local operation and classical communication (LOCC) is insufficient for discriminating shared entanglement. Recent investigations highlight the importance of entangled ancillary qubits for nondestructive quantum state discrimination [5].

Here, we focus on nondestructive discrimination of all four Bell states between distant parties. Theoretical analysis establishes upper bounds of success probability with LOCC, and a scheme which can nondestructively distinguish all four Bell states using pre-shared ancillary entangled qubits is proposed. Experimental results on an IonQ quantum computer validate the protocol's effectiveness by surpassing the classical limit.

Consider two distant parties, Alice and Bob, aim to determine any of four possible Bell states $|\Psi\rangle_{AB}$ without destroying it. Let probability to succesfully determine given Bell state is P_D and probability that Bell state will not be changed after interaction is P_F. In the case of perfect discrimination (when $P_D = 1$, $P_F = 1$), the overall success probability $P_{\text{cl}} = P_D P_F$ is 1. However, with random guessing without measurement (when $P_D = 1/4$, $P_F = 1$), P_{cl} is 1/4 since there are equal chances to choose randomly one of four possible Bell states.

*bohdan@kist.re.kr
†wysong@kist.re.kr
‡yong-su.kim@kist.re.kr

On the other hand Alice and Bob can employ simple projection measurements to discriminate the Bell state. By measuring their qubits in the Z basis, they can obtain information about the state. If both obtain $|0\rangle$, it indicates the state was either $|\phi^+\rangle$ or $|\phi^-\rangle$ Bell states, resulting in a success probability of $P_D = 1/2$. However, since they are separated, they cannot recover the entangled state. The nondestructive probability P_F (state overlap) with the original state, assuming they prepare $|00\rangle$ based on their outcomes, is 1/2. Hence, the overall success probability of nondestructive quantum state discrimination is $P_{\text{cl}} = 1/4$. This winning probability is actually the classical upper bound without ancillary entanglements [5].

We propose a pre-shared entanglement-assisted scheme for nondestructive discrimination of Bell states between distant parties. With the assistance of pre-shared entanglement, the parties can discriminate the Bell states using local operations and classical communication (LOCC) without the need for additional global operations. The scheme in Figure 1 involves two ancillary entangled states shared between Alice and Bob, along with the system qubits representing the Bell states.

It starts with two ancillary entangled states between Alice and Bob along with the system qubits as follow.

$$|\Psi\rangle_{\text{int}} = |\phi^+\rangle_{a_1 b_1} \otimes |\phi^+\rangle_{a_2 b_2} \otimes |\Psi\rangle_{s_A s_B} \qquad (1)$$

where the system qubits are in one of four possible Bell states, $|\Psi\rangle_{s_A s_B} \in \{|\phi^\pm\rangle, |\psi^\pm\rangle\}$ and two ancillary entangled qubits are prepared in $|\phi^+\rangle$. After state evolution, showed on Figure 1 system qubits will not be changed and ancillary qubits will change depending on which Bell state was prepared. Thus, proposed scheme lets to completely discriminated unknown Bell state.

We repeated experiment 10,000 times for each possible Bell state. Result of experiment is shown on Figure 2. There, TT means that Alice and Bob succesfully determined system state without destroying it; TF means that Alice and Bob succesfully determined system state,

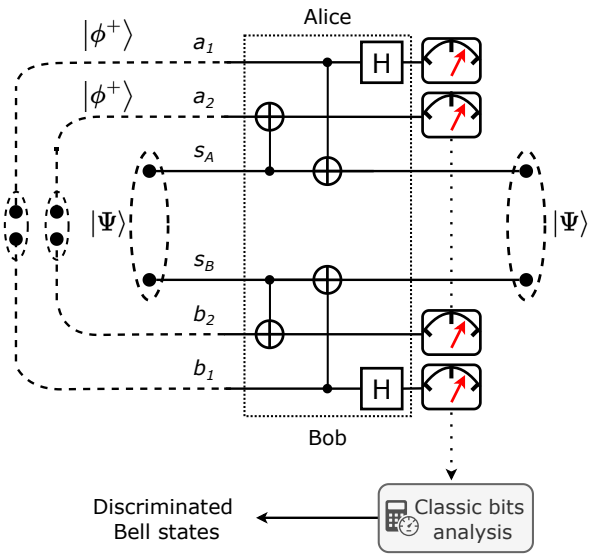


Figure 1: Nondestructive Bell state discrimination between distant parties using two ancillary entangled pairs $|\phi^+\rangle_{a_1b_1}$ and $|\phi^+\rangle_{a_2b_2}$ with system qubits s_A and s_B.

but system qubits were changed; FT means, that Alice and Bob wrongly determined system state, but system state did not destroyed; FF means that Alice and Bob wrongly determined system state and system qubits were changed. For success probability we are interested in TT cases. The average probability of nondestructive quantum state discrimination for all Bell states is average value of all TT cases from Figure 2 and its value is $P_{\text{succ}} = 0.736 \pm 0.012$. Notably, this success probability exceeds the upper bound of $P_{\text{cl}} = 1/4$ for entanglement discrimination without shared entanglement.

We have demonstrated the importance of verifying pre-shared entanglement for nondestructive quantum communication protocols. We showed that nondestructive entanglement discrimination between distant parties cannot be achieved without additional pre-shared entanglement pairs. Our proposed scheme utilizes two ancillary entangled qubit pairs to achieve nondestructive Bell state discrimination. We verified the feasibility of our protocol through a proof-of-principle experiment on an IonQ quantum computer.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossin", Theoretical Computer Science **560**, 7 (2014).

[2] C. H. Bennett, "Secure quantum key distribution with realistic devices", Physical Review Letters **68**, 3121 (1992).

[3] M. Gupta et al., "General circuits for indirecting and distributing measurement in quantum computation", International Journal of Quantum Information **05**, 627 (2007).

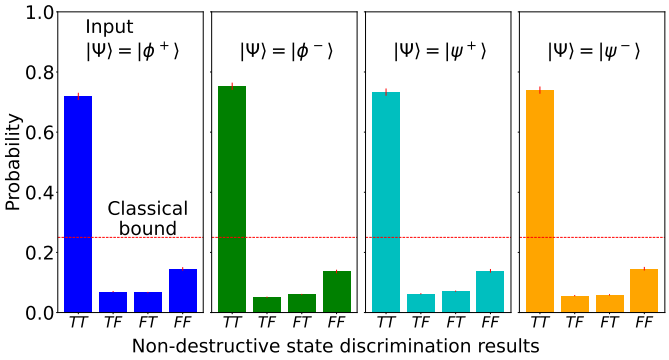


Figure 2: The experimental truth table for nondestructive entanglement discrimination consists of four outcomes: i) successful state discrimination with unchanged system qubits (TT), ii) successful state discrimination but system qubits altered (TF), iii) failed to discriminate the state but system qubits are unchanged (FT), and iv) state discrimination failed and system qubits altered (FF).

[4] M. Sisodia, A. Shukla, and A. Pathak, "Experimental realization of nondestructive discrimination of Bell states using a five-qubit quantum computer", Physics Letters A **381**, 3860 (2017).

[5] A. J. Paige et al., "Quantum Delocalized Interactions", Physical Review Letters **125**, 240406 (2020).

Quantum sequential scattering model for quantum state learning

Mingrui Jing[1] Geng Liu[1] Hongbin Ren[1] Xin Wang[1]

[1] *Institute for Quantum Computing, Baidu Research, Beijing 100193, China*

Abstract. Quantum state learning is central to quantum machine learning as it provides numerous applications and characterizes quantum nature. However, given many copies of an unknown quantum state, how to learn and prepare the state is challenging and the method via quantum neural networks is severely limited due to barren plateaus (BP). In this work, we introduce the quantum sequential scattering model to efficiently and accurately learn and prepare quantum states. The model's effectiveness is demonstrated through theoretical analysis and numerical simulations involving noise. A truncated version is also presented, showing well performances for learning low-entangled states e.g., GHZ and W states. Our method could avoid BP in the cases where the targets carry polynomial-scaled reduced states' ranks and provide at least a square root advantage on gradient magnitude for mitigating BP in the worst case. Our results imply more entanglement between subsystems of the target state leads to more resources required for purification, which brings down the efficiency of QSSM state learning. Note that the technical version is attached.

Keywords: quantum machine learning, quantum neural networks, quantum state learning, barren plateaus

Introduction: Quantum computing is a promising field that has spurred advancements in various disciplines [1, 2, 3, 4]. To establish a near-term quantum advantage, quantum machine learning (QML) has been developed using noisy intermediate-scale quantum (NISQ) devices [5]. Quantum neural networks (QNNs) [6, 7], based on the principles of quantum mechanics, have emerged as a potential solution for classically hard problems. Several QNN models have been studied and demonstrate advantages over classical models [8, 9, 10, 11].

Learning unknown probability distributions is important in classical machine learning [12]. As a quantum analog, learning or preparing an arbitrary quantum state is a fundamental task that impacts quantum algorithm design, data encoding, physical estimations, and Hamiltonian simulation [13, 14, 15, 16]. The task involves constructing an accessible description of a target state with unexplored representations, which can be reimplemented on real near-term devices for further computational tasks.

Many attempts have been made to reproduce the quantum circuit representation of the target state, for example, the efficient decomposition [17, 18] or relying on powerful QML models [19, 20, 21]. However, trainability has become a critical challenge for the practical usage of QNNs. Specifically, training deep QNNs will encounter severe *barren plateaus* (BP) phenomenon [22] as the system scales up. Although there have been several strategies proposed to overcome the problem including clever initialization strategy [23, 24], adaptive algorithms [25, 26, 27, 28], parameterization generalization [29], different cost functions [30, 31] and different circuit structures [32, 33]. Learning quantum states scalably without BP and defining which kind of quantum states can be efficiently learnt remain to be open and challenging problems in quantum machine learning.

Overview of results: In this work, we introduce a quantum neural network model to learn and prepare arbitrary quantum states efficiently on near-term devices. In particular, we establish the following:

(i) We propose the quantum sequential scattering model (QSSM), motivated by the freedom in state purification, which could build up a quantum state from local to global by hierarchically training the scattering layers. We show that QSSM requires a shallower circuit and fewer parameters for each step, making quantum state learning more efficient on near-term quantum devices.

(ii) We prove that the gradient magnitude is proportional to the maximum layer width of QSSM. We show that QSSM could avoid BP with constant- or polynomial-scaled gradient magnitudes for rank-bounded quantum states. It could mitigate BP by providing a square root advantage on gradient magnitude over the global QNN at worst.

(iii) We showcase the efficiency and accuracy of the QSSM in the numerical simulation and noisy simulation of preparing different quantum states. We also confirm its robustness to BP by demonstrating a constant scaling of gradient magnitude in the number of qubits in experiments as shown in Fig. 2.

Quantum sequential scattering model. Our first contribution is proposing a new QNN model that can be efficient in quantum state learning. The fundamental idea of QSSM is to generate local interactions on partial systems and gradually increase the dimensionalities to construct a global quantum state. In contrast, traditional QNNs process from a global viewpoint handling the entire system at a time.

Given a n-qubit quantum state ρ represented by certainly ordered qubits, we can define a **k-th partition** of ρ ($1 \leq k \leq n$) separating the state into subsystems $\mathcal{A}_k$ and $\bar{\mathcal{A}}_k$ covering the first k qubits and the remaining, respectively. For $k = n$, $\bar{\mathcal{A}}_k = \emptyset$ and $\mathcal{A}_k = \mathcal{H}^{\otimes n}$. We denote ρ_k as the partial state on system $\mathcal{A}_k$, i.e., $\rho_k = \mathrm{tr}_{\bar{\mathcal{A}}_k}[\rho]$ and

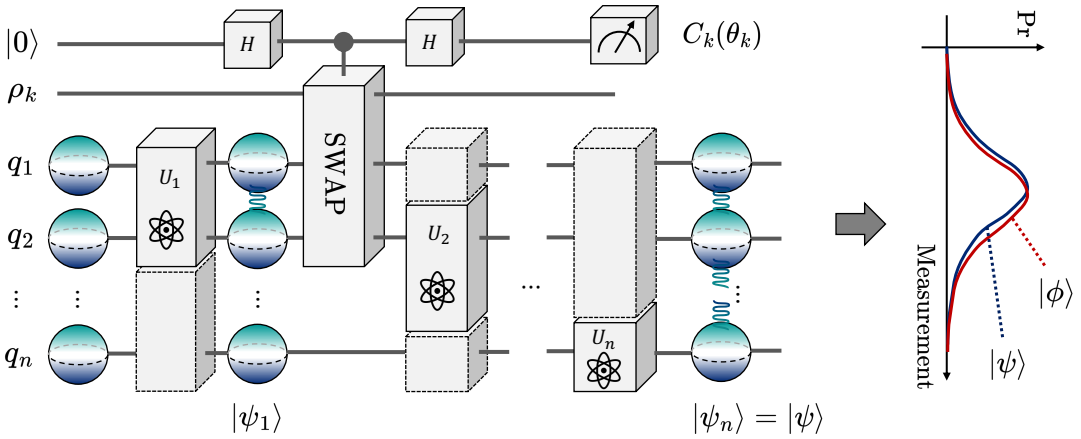


Figure 1: A conceptual diagram of QSSM state learning. Starting with a fully tensor product state (e.g., $|0\rangle^{\otimes n}$) initially, each QSSM layer U_k produces a purification $|\psi_k\rangle$ of the reduced density ρ_k of $|\phi\rangle$. At each step, the cost $C_k(\boldsymbol{\theta}_k)$ can be estimated via *swap-test* [34] shown in the diagram. After all n training steps, the entire trained model produces a complete circuit representation $|\psi\rangle$ approximating the target $|\phi\rangle$. The state $|\psi\rangle$, therefore carries almost the same stochastic behaviors as $|\phi\rangle$ and can be used conveniently for further computational assignments.

define a (Schmidt) rank sequence $\mathcal{R}_\rho$ of ρ as,

$$\mathcal{R}_\rho = \{r_1, r_2, \cdots, r_{n-1}, r_n\} \tag{1}$$

where r_k indicates the rank of ρ_k. Our QSSM could find a set of local unitary $\{U_k\}$ which generate purification of ρ_k based on previous learning steps. Each layer acts on w_k qubits, called the layer width, and is trained by optimizing an adaptive k-th step cost function as,

$$C_k(\boldsymbol{\theta_k}) = \mathrm{tr}[(\sigma_k(\boldsymbol{\theta_k}) - \rho_k)(\sigma_k(\boldsymbol{\theta_k}) - \rho_k)^\dagger] \tag{2}$$

where σ_k indicates the k-th partition of the layer output state $|\psi_k\rangle$.

Algorithm 1 QSSM for state learning

Require: Copies of the n-qubit target state $\rho = |\phi\rangle\langle\phi|$, layer depth D.
Ensure: Input a state $|0\rangle^{\otimes n}$ with qubit labels $q_1, q_2, \cdots, q_n$.
1: Initialize step index $k \leftarrow 1$.
2: Pre-determine a set of widths $\{w_k\}_{k=1}^n$.
3: **while** $k \leq n$ **do**
4: Random initialize $U_k(\boldsymbol{\theta}_k)$ acting on qubits $q_k \sim q_{k+w_k-1}$.
5: Minimize $C_k(\boldsymbol{\theta}_k)$ via classical optimizations.
6: $k \leftarrow k + 1$.
7: **end while**
8: Store all $\boldsymbol{\theta}_1, \cdots, \boldsymbol{\theta}_n$ in the classical memory.
9: Prepare the target $|\psi\rangle = U_n \cdots U_1 |0\rangle^{\otimes n} \approx |\phi\rangle$.

The state learning algorithm is summarized in Algorithm 1 driven via both gradient-free and -based optimizers. The model also applies to the mixed target state by considering its purification. The layer width w_k can be pre-determined according to the rank r_k of ρ_k. We usually set $w_k = k + 1$ or $n - k + 1$ to cover any state of $r_k = 2^{\min\{k, n-k\}}$ based on Uhlmann's theorem and freedom in purification. It is also worth noting that we can restrict the maximum width w_{max} to get a truncated version of QSSM, which can gain advantages in efficiency and use fewer parameters while maintaining relatively high performance in learning some low-entangled state.

We choose the cost (2) involving terms of $\mathrm{tr}[\rho^2]$ and $\mathrm{tr}[\rho\sigma]$, which can be efficiently estimated via *swap-test* [34]. Besides, the parameter shift rule [35, 36] applies to our QSSM for obtaining analytic gradient as we employ hardware-efficient ansatz [37] for scattering layers.

Trainability of QSSM Our second contribution is to show that QSSM will not exhibit BP for a large class of quantum states by establishing an explicit relation between the trainability of QSSM and its rank sequence. The rigorous analysis of the variance of the cost gradient $\partial_\mu C_k$ of QSSM is given in the following Proposition 1.

Proposition 1 *For a n-qubit target state ρ with fixed-order representation, we suppose its rank sequence is $\mathcal{R}_\rho = \{r_1, r_2, \cdots r_{n-1}, r_n\}$. Then for learning the target state ρ with QSSM, if the circuit used for each step is sufficiently random that forms a local 4-design, the expectation of the k-th step $\mathbb{E}[\partial_\mu C_k] = 0$ and the variance of the cost gradient scales with r_k as,*

$$\mathrm{Var}[\partial_\mu C_k] \in \mathcal{O}(\frac{1}{r_k}). \tag{3}$$

Remark 1 *For a class of states whose all the Schmidt ranks in their rank sequence are smaller than a constant C that is not scaling with the number of qubits, for example, $\mathcal{R}_\rho = \{r_k | r_k \leq C,\ \forall k\}$, the gradient magnitude for learning them scales as*

$$\mathrm{Var}[\partial_\mu C_k] \in \mathcal{O}(\frac{1}{r_k}) = \mathcal{O}(1), \tag{4}$$

which means they can be learned without BP via QSSM. More specifically, for learning GHZ state and W state, we can choose C being 2, thus there is no BP learning GHZ state and W state.

(a)

	Global QNN	QSSM		
Maximum layer widths	–	2	5	7
Physical States				
XXX model ground state (GS)	0.533	0.523	**0.956**	**0.926**
XXZ model GS	0.523	0.750	**0.952**	**0.948**
LiH molecule GS	0.531	**0.978**	**0.978**	**0.973**
Algorithmic States				
GHZ state	0.535	**0.994**	**0.989**	**0.971**
W state	0.527	**0.990**	**0.985**	**0.958**
Gaussian distribution	0.561	**0.969**	**0.981**	**0.978**
MNIST data encoding	0.330	0.517	**0.903**	0.867
Random state	0.317	0.318	0.871	0.834

(b)

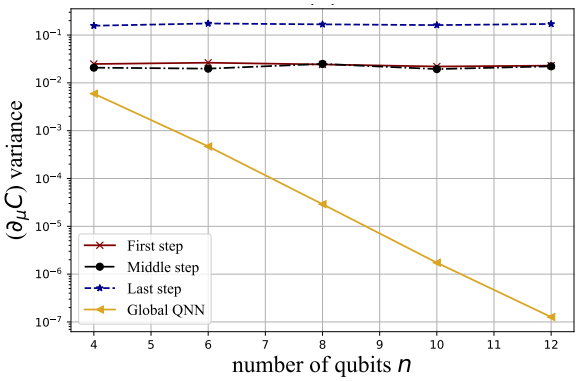


Figure 2: **Comparison of the fidelity performance and gradient magnitude between QSSM and global QNN.** Panel (a) correspond to the experiment results of learning different quantum states via QSSM and global QNN. Maximum layer widths denote the max width w_{max} applied in each step of QSSM. For $n = 12$ states, $w_{\max} = 7$ is equivalent to the worst case of doubling the dimensionality. Panel (b) illustrates the comparison of gradient magnitude between different steps in QSSM and global QNN of learning GHZ state. The red, black and blue lines represent the gradient magnitude of the first step, $\frac{n}{2}$-th step and the last step respectively. The yellow line represents the gradient magnitude of using the randomly initialized global circuit.

This proposition notably implies that the gradient magnitude is greatly determined by the largest Schmidt rank in the rank sequence. In other words, the gradient magnitude scales with the width of each scattering layer as $\mathcal{O}(2^{-w_k})$, which accords with our knowledge of BP. In the worst case, if the rank sequence of the target state is $\mathcal{R}_\rho = \{2^1, 2^2, \cdots 2^{\lfloor n/2 \rfloor}, \cdots, 2, 1\}$, the gradient magnitudes are at least $\mathcal{O}(2^{-\lfloor n/2 \rfloor})$. It is worth noting that even though the gradient magnitude experiences an exponential decay concerning w_k, the vanishing speed of the gradient is quadratically lower than it is of the traditional global case, leading to a square root advantage compared with the global QNN.

In fact, the maximum width $w_{\max}$ does not need to reach $\lceil (n+1)/2 \rceil$ as the total number of qubits increases in most cases. For some particular states, like GHZ state and W state, the maximum width w_k can have a constant upper bound, making gradients magnitude also constant. Moreover, for many other low-entangled states such as the *slightly entangled state* introduced by Vidal [38], we can learn them via QSSM with limited width, leading to the constant or polynomially scaling of gradient magnitude. In fact, slightly entangled states only take a small portion of quantum states that will not experience barren plateau using QSSM. Instead, all the quantum states that have at most polynomially growing Schmidt ranks in any one of its rank sequences $\mathcal{R}$ with possible ordered representations will not exhibit barren plateaus in the learning procedure using QSSM.

Experimental demonstration. Our third contribution is to investigate the efficiency and trainability of QSSM state learning via ideal and noisy numerical simulations, as shown in Fig. 2. We choose both physical and algorithmic meaningful 12-qubit target quantum states and perform learning procedures using QSSM and traditional global QNN with results recorded in Fig. (2a). The advantages in state learning performance from noise-free experiments are clear when comparing QSSM to the global QNN. Unlike global QNN whose training is blocked due to BP, QSSM could achieve high fidelity in preparing these quantum states. Besides, in most cases, $w_{\max}$ need not approach the worst $\lceil (n+1)/2 \rceil$ to obtain > 0.9 fidelity. We particularly perform noisy simulation for QSSM to learn a 4-qubit GHZ state and achieve a final fidelity of 0.91.

Trainability is demonstrated by gradient-test simulations on different scattering layers as shown in Fig. (2b). Specifically, we show the gradient magnitude of learning the GHZ states with different numbers of qubits. The global QNN derives an exponential vanishing gradient by the yellow line. Our QSSM demonstrates a constant scaling of gradient magnitude instead, being consistent with Proposition 1. Above all, experiments have showcased QSSM's superior performance in state learning compared to conventional QNNs, and in some cases, training of QSSM could indeed avoid BP.

Concluding remark We propose QSSM, for the quantum state learning task. With the freedom in purification, our algorithm adopts a sequential learning strategy for preparing quantum states by splitting this challenging task into easier sub-tasks. Moreover, the truncated version of QSSM by fixing the max layer width, together with its ability to avoid the barren plateaus for a large class of quantum states, makes QSSM a practical strategy for near-term quantum devices. Our algorithm provides a reliable and efficient way to learn circuit representations of unknown quantum states, promoting further research and development progress on quantum states. Our study also reveals an underline relationship between state entanglement and learning hardness deserving detailed discussions.

References

[1] Dave Wecker, Matthew B. Hastings, and Matthias Troyer. Progress towards practical quantum variational algorithms. *Physical Review A*, 92(4):042303, oct 2015. ISSN 1050-2947. doi: 10.1103/PhysRevA.92.042303. URL https://link.aps.org/doi/10.1103/PhysRevA.92.042303.

[2] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C Benjamin, and Xiao Yuan. Quantum computational chemistry. *Reviews of Modern Physics*, 92(1):015003, 2020.

[3] Daniel J. Egger, Claudio Gambella, Jakub Marecek, Scott McFaddin, Martin Mevissen, Rudy Raymond, Andrea Simonetto, Stefan Woerner, and Elena Yndurain. Quantum Computing for Finance: State-of-the-Art and Future Prospects. *IEEE Transactions on Quantum Engineering*, 1:1–24, 2020. ISSN 2689-1808. doi: 10.1109/TQE.2020.3030314. URL https://ieeexplore.ieee.org/document/9222275/.

[4] Lloyd CL Hollenberg. Fast quantum search algorithms in protein sequence comparisons: Quantum bioinformatics. *Physical Review E*, 62(5):7532, 2000.

[5] John Preskill. Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79, aug 2018. ISSN 2521-327X. doi: 10.22331/q-2018-08-06-79. URL https://quantum-journal.org/papers/q-2018-08-06-79/.

[6] Subhash C. Kak. Quantum neural computing. volume 94 of *Advances in Imaging and Electron Physics*, pages 259–313. Elsevier, 1995. doi: https://doi.org/10.1016/S1076-5670(08)70147-2. URL https://www.sciencedirect.com/science/article/pii/S1076567008701472.

[7] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. The quest for a quantum neural network. *Quantum Information Processing*, 13(11):2567–2586, 2014.

[8] Patrick Rebentrost, Thomas R Bromley, Christian Weedbrook, and Seth Lloyd. Quantum hopfield neural network. *Physical Review A*, 98(4):042308, 2018.

[9] Jian Zhao, Yuan-Hang Zhang, Chang-Peng Shao, Yu-Chun Wu, Guang-Can Guo, and Guo-Ping Guo. Building quantum neural networks based on a swap test. *Physical Review A*, 100(1):012334, 2019.

[10] Iris Cong, Soonwon Choi, and Mikhail D Lukin. Quantum convolutional neural networks. *Nature Physics*, 15(12):1273–1278, 2019.

[11] Nathan Killoran, Thomas R Bromley, Juan Miguel Arrazola, Maria Schuld, Nicolás Quesada, and Seth Lloyd. Continuous-variable quantum neural networks. *Physical Review Research*, 1(3):033063, 2019.

[12] Michael I Jordan and Tom M Mitchell. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245):255–260, 2015.

[13] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature Physics*, 10(9):631–633, jul 2014. doi: 10.1038/nphys3029. URL https://doi.org/10.1038%2Fnphys3029.

[14] Ryan LaRose and Brian Coyle. Robust data encodings for quantum classifiers. *Physical Review A*, 102(3):032420, sep 2020. ISSN 2469-9926. doi: 10.1103/PhysRevA.102.032420. URL https://link.aps.org/doi/10.1103/PhysRevA.102.032420.

[15] Almudena Carrera Vazquez and Stefan Woerner. Efficient state preparation for quantum amplitude estimation. *Physical Review Applied*, 15(3):034027, 2021.

[16] Guang Hao Low and Isaac L. Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, jul 2019. doi: 10.22331/q-2019-07-12-163. URL https://doi.org/10.22331%2Fq-2019-07-12-163.

[17] Bryan T Gard, Linghua Zhu, George S Barron, Nicholas J Mayhall, Sophia E Economou, and Edwin Barnes. Efficient symmetry-preserving state preparation circuits for the variational quantum eigensolver algorithm. *npj Quantum Information*, 6(1):1–9, 2020.

[18] Xiao-Ming Zhang, Tongyang Li, and Xiao Yuan. Quantum state preparation with optimal circuit depth: Implementations and applications. *Phys. Rev. Lett.*, 129:230504, Nov 2022. doi: 10.1103/PhysRevLett.129.230504. URL https://link.aps.org/doi/10.1103/PhysRevLett.129.230504.

[19] M Cerezo, Kunal Sharma, Andrew Arrasmith, and Patrick J Coles. Variational quantum state eigensolver. *npj Quantum Information*, 8(1):1–11, 2022.

[20] Sanjib Ghosh, Tomasz Paterek, and Timothy CH Liew. Quantum neuromorphic platform for quantum state preparation. *Physical Review Letters*, 123(26):260404, 2019.

[21] Youle Wang, Guangxi Li, and Xin Wang. Variational Quantum Gibbs State Preparation with a Truncated Taylor Series. *Physical Review Applied*, 16(5):054035, nov 2021. ISSN 2331-7019. doi: 10.1103/PhysRevApplied.16.054035. URL https://link.aps.org/doi/10.1103/PhysRevApplied.16.054035.

[22] Jarrod R. McClean, Sergio Boixo, Vadim N. Smelyanskiy, Ryan Babbush, and Hartmut Neven. Barren plateaus in quantum neural network training landscapes. *Nature Communications*, 9(1):1–7, mar 2018. ISSN 20411723. doi: 10.1038/s41467-018-07090-4.

URL http://arxiv.org/abs/1803.11173http://dx.doi.org/10.1038/s41467-018-07090-4.

[23] Edward Grant, Leonard Wossnig, Mateusz Ostaszewski, and Marcello Benedetti. An initialization strategy for addressing barren plateaus in parametrized quantum circuits. *Quantum*, 3, mar 2019. ISSN 2521327X. doi: 10.22331/q-2019-12-09-214. URL http://arxiv.org/abs/1903.05076http://dx.doi.org/10.22331/q-2019-12-09-214.

[24] Ankit Kulshrestha and Ilya Safro. Beinit: Avoiding barren plateaus in variational quantum algorithms. *arXiv preprint arXiv:2204.13751*, 2022.

[25] Harper R. Grimsley, Sophia E. Economou, Edwin Barnes, and Nicholas J. Mayhall. An adaptive variational algorithm for exact molecular simulations on a quantum computer. *Nature Communications*, 10(1):3007, dec 2019. ISSN 2041-1723. doi: 10.1038/s41467-019-10988-2. URL http://www.nature.com/articles/s41467-019-10988-2.

[26] Feng Zhang, Niladri Gomes, Yongxin Yao, Peter P. Orth, and Thomas Iadecola. Adaptive variational quantum eigensolvers for highly excited states. *Physical Review B*, 104(7):1–10, apr 2021. ISSN 24699969. doi: 10.1103/PhysRevB.104.075159. URL http://arxiv.org/abs/2104.12636http://dx.doi.org/10.1103/PhysRevB.104.075159.

[27] Andrea Skolik, Jarrod R. McClean, Masoud Mohseni, Patrick van der Smagt, and Martin Leib. Layerwise learning for quantum neural networks. *Quantum Machine Intelligence*, 3(1):5, jun 2021. ISSN 2524-4906. doi: 10.1007/s42484-020-00036-4. URL http://arxiv.org/abs/2006.14904https://link.springer.com/10.1007/s42484-020-00036-4.

[28] Harper R. Grimsley, George S. Barron, Edwin Barnes, Sophia E. Economou, and Nicholas J. Mayhall. ADAPT-VQE is insensitive to rough parameter landscapes and barren plateaus. *npj Quantum Information*, 2022. URL http://arxiv.org/abs/2204.07179.

[29] Tyler Volkoff and Patrick J Coles. Large gradients via correlation in random parameterized quantum circuits. *Quantum Science and Technology*, 6(2):025008, 2021.

[30] M. Cerezo, Akira Sone, Tyler Volkoff, Lukasz Cincio, and Patrick J. Coles. Cost function dependent barren plateaus in shallow parametrized quantum circuits. *Nature Communications*, 12(1):1791, dec 2021. ISSN 2041-1723. doi: 10.1038/s41467-021-21728-w. URL http://arxiv.org/abs/2001.00550http://dx.doi.org/10.1038/s41467-021-21728-whttp://www.nature.com/articles/s41467-021-21728-w.

[31] Maria Kieferova, Ortiz Marrero Carlos, and Nathan Wiebe. Quantum Generative Training Using Rényi Divergences. jun 2021. URL http://arxiv.org/abs/2106.09567.

[32] Arthur Pesah, M Cerezo, Samson Wang, Tyler Volkoff, Andrew T Sornborger, and Patrick J Coles. Absence of Barren Plateaus in Quantum Convolutional Neural Networks. *Physical Review X*, 11(4):041011, oct 2021. ISSN 21603308. doi: 10.1103/PhysRevX.11.041011. URL https://doi.org/10.1103/PhysRevX.11.041011https://link.aps.org/doi/10.1103/PhysRevX.11.041011.

[33] Xia Liu, Geng Liu, Jiaxin Huang, and Xin Wang. Mitigating barren plateaus of variational quantum eigensolvers. may 2022. URL http://arxiv.org/abs/2205.13539.

[34] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, 1997.

[35] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii. Quantum circuit learning. *Physical Review A*, 98(3), sep 2018. doi: 10.1103/physreva.98.032309. URL https://doi.org/10.1103%2Fphysreva.98.032309.

[36] Maria Schuld, Ville Bergholm, Christian Gogolin, Josh Izaac, and Nathan Killoran. Evaluating analytic gradients on quantum hardware. *Physical Review A*, 99(3):032331, nov 2018. ISSN 2469-9926. doi: 10.1103/PhysRevA.99.032331. URL https://link.aps.org/doi/10.1103/PhysRevA.99.032331http://arxiv.org/abs/1811.11184.

[37] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M Chow, and Jay M Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature*, 549(7671):242–246, 2017.

[38] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91:147902, Oct 2003. doi: 10.1103/PhysRevLett.91.147902. URL https://link.aps.org/doi/10.1103/PhysRevLett.91.147902.

The first-order Trotter decomposition in the dynamical-invariant basis

Takuya Hatomura[1] *

[1] *NTT Basic Research Laboratories & NTT Research Center for Theoretical Quantum Physics, NTT Corporation, Kanagawa 243-0198, Japan*

Abstract. The Trotter decomposition is a basic approach to Hamiltonian simulation (digital quantum simulation). The first-order Trotter decomposition is the simplest one, whose deviations from target dynamics are of the first order of a small coefficient in terms of the infidelity. In this paper, we consider the first-order Trotter decomposition in the dynamical-invariant basis. By using a state-dependent inequality, we point out that deviations of this decomposition are of the second order of a small coefficient. Moreover, we also show that this decomposition includes a useful example, i.e., digital implementation of shortcuts to adiabaticity by counterdiabatic driving.

Keywords: Hamiltonian simulation, Trotter decomposition, dynamical invariant

1 Introduction

Quantum simulation, which is also referred as Hamiltonian simulation, is one of the most promising quantum technologies. In quantum simulation (Hamiltonian simulation), we simulate (Hamiltonians of) target quantum systems by using other programable quantum systems [1]. Since degrees of freedom in quantum systems increase in an exponential way as their components increase, quantum simulation has clear advantage against classical simulation.

The Trotter formulae [2,3] are often used to decompose time-evolution operators of target quantum systems into sequences of simulatable unitary operators [4]. The high-order Trotter formulae [3] give precise simulation, but the depth of quantum circuits tend to be deep. Other approaches to Hamiltonian simulation, e.g., the Taylor series expansion and the linear combination of unitaries [5], quantum signal processing [6], etc., have also been proposed for realizing precise simulation with relatively shallow quantum circuits.

In this paper, we revisit the simplest matrix exponential formula, i.e., the fist-order Trotter decomposition [2]. First, as a preliminary, we introduce the dynamical invariant and the Lewis-Riesenfeld theory [7]. Next, we introduce a state-depdendent inequality which enables us to precisely evaluate digitization errors [8]. Then, we consider the first-order Trotter decomposition in the dynamical-invariant basis. We will find that dominant errors vanish in this decomposition and the scaling of digitization errors is better than the conventional one which arises from the first-order Trotter decomposition [4]. Finally, we show that this specific decomposition includes a useful example, i.e., digitized counterdiabatic driving [9–12].

*takuya.hatomura@ntt.com

2 Preliminary

Suppose that a given quantum system is governed by the Schrödinger equation

$$i\hbar\frac{\partial}{\partial t}|\Psi(t)\rangle = \hat{H}(t)|\Psi(t)\rangle, \tag{1}$$

where $|\Psi(t)\rangle$ is its dynamics and $\hat{H}(t)$ is its Hamiltonian.

Dynamical invariant. A dynamical invariant $\hat{F}(t)$ is an Hermitian operator which satisfies the von Neumann equation

$$i\hbar\frac{\partial}{\partial t}\hat{F}(t) - [\hat{H}(t), \hat{F}(t)] = 0. \tag{2}$$

Note that the density operator is a trivial example, but there are infinite dynamical invariants. We can easily confirm that eigenvalues of dynamical invariants are independent of time, i.e., their time-dependence comes from their eigenvectors.

In the dynamical-invariant basis $\{|\phi_n(t)\rangle\}$, which is the set of the eigenvectors of a dynamical invariant, off-diagonal elements of the Hamiltonian is given by

$$\langle\phi_m(t)|\hat{H}(t)|\phi_n(t)\rangle = i\hbar\langle\phi_m(t)|\partial_t\phi_n(t)\rangle, \quad \text{for } m \neq n, \tag{3}$$

where $|\partial_t\phi_n(t)\rangle = (\partial/\partial t)|\phi_n(t)\rangle$ [7]. Then, the Hamiltonian can be expressed as

$$\begin{aligned}\hat{H}(t) =& \sum_n \langle\phi_n(t)|\hat{H}(t)|\phi_n(t)\rangle|\phi_n(t)\rangle\langle\phi_n(t)| \\ &+ i\hbar\sum_{\substack{m,n \\ (m\neq n)}} |\phi_m(t)\rangle\langle\phi_m(t)|\partial_t\phi_n(t)\rangle\langle\phi_n(t)|,\end{aligned} \tag{4}$$

where the first term is diagonal and the second term is off-diagonal in the dynamical-invariant basis [13,14].

Lewis-Riesenfeld theory [7]. By using the dynamical-invariant basis, the solution of the Schrödinger equation (1) is given by

$$\begin{aligned}|\Psi(t)\rangle &= \sum_n c_n(0)e^{i\kappa_n(t)}|\phi_n(t)\rangle, \\ \kappa_n(t) &= \frac{1}{\hbar}\int_0^t dt'\langle\phi_n(t')|\left(i\hbar\frac{\partial}{\partial t'} - \hat{H}(t')\right)|\phi_n(t')\rangle,\end{aligned} \tag{5}$$

where the coefficient $c_n(0)$ determines the initial state and $\kappa_n(t)$ is the Lewis-Riesenfeld phase. We can easily confirm this fact by considering the time derivative of the state (5) and by using Eq. (3).

3 Results

3.1 State-dependent inequality for Hamiltonian simulation

In this section, we introduce a state-dependent inequality for precisely evaluating digitization errors [8]. For this purpose, we introduce the Fubini-Study angle.

Fubini-Study angle. For given two quantum states, $|\psi\rangle$ and $|\phi\rangle$, the Fubini-Study angle (see, e.g., Ref. [15]) is defined by

$$\mathcal{L}(|\psi\rangle, |\phi\rangle) = \arccos |\langle\psi|\phi\rangle|. \tag{6}$$

The Fubini-Study angle is distance, i.e., it satisfies (i) the identity of indiscernibles, $\mathcal{L}(|\psi\rangle, |\phi\rangle) = 0 \Leftrightarrow |\psi\rangle = |\phi\rangle$ except for a grobal phase factor; (ii) symmetry, $\mathcal{L}(|\psi\rangle, |\phi\rangle) = \mathcal{L}(|\phi\rangle, |\psi\rangle)$; and (iii) subadditivity, $\mathcal{L}(|\psi\rangle, |\phi\rangle) \leq \mathcal{L}(|\psi\rangle, |\chi\rangle) + \mathcal{L}(|\chi\rangle, |\phi\rangle)$ for any quantum state $|\chi\rangle$. It also satisfies (iv) unitary invariance, $\mathcal{L}(|\psi\rangle, |\phi\rangle) = \mathcal{L}(\hat{U}|\psi\rangle, \hat{U}|\phi\rangle)$ for any unitary operator $\hat{U}$.

Now, we consider the dynamics $|\Psi(t)\rangle$ governed by the Schrödinger equation and its digitized dynamics $|\Psi_d(mT/M)\rangle$, where T is the final time, M is the number of time steps, and m is an integer, $m = 0, 1, 2, \ldots, M$, and discuss the overlap between these two dynamics at the final time, $|\langle\Psi(T)|\Psi_d(T)\rangle|$.

State-dependent error bound [8]. By using the unitary invariance and the subadditivity of the Fubini-Study angle, we find the following inequality

$$|\langle\Psi(T)|\Psi_d(T)\rangle| \geq \cos\left(\sum_{n=1}^{M} \mathcal{L}_n\right), \quad \text{for } \sum_{n=1}^{M} \mathcal{L}_n \leq \frac{\pi}{2}, \tag{7}$$

where

$$\mathcal{L}_n = \arccos|\langle\Psi(nT/M)|\hat{U}_d(nT/M, (n-1)T/M) \times [\hat{U}(nT/M, (n-1)T/M)]^\dagger|\Psi(nT/M)\rangle|. \tag{8}$$

Here, $\hat{U}(nT/M, (n-1)T/M)$ and $\hat{U}_d(nT/M, (n-1)T/M)$ are time-evolution operators which transform $|\Psi((n-1)T/M)\rangle$ and $|\Psi_d((n-1)T/M)\rangle$ into $|\Psi(nT/M)\rangle$ and $|\Psi_d(nT/M)\rangle$, respectively. Note that the identical initial states, $|\Psi(0)\rangle = |\Psi_d(0)\rangle$, are assumed.

Now we assume that the Hamiltonian is given by $\hat{H}(t) = \sum_k \hat{H}_k(t)$ and consider the first-order Trotter decomposition for digitization. That is, the time-evolution operator for the digitized dynamics is given by $\hat{U}_d(nT/M, (n-1)T/M) = \prod_k \exp(-\frac{i}{\hbar}\frac{T}{M}\hat{H}_k(nT/M))$.

Dominant errors [8]. When $T/M \ll 1$ holds, we can apply the Taylor expansion to Eq. (8) and it gives

$$\mathcal{L}_n \approx \frac{T^2}{2\hbar^2 M^2}|\langle\Psi(nT/M)|\hat{A}(nT/M)|\Psi(nT/M)\rangle|, \quad \hat{A}(nT/M) = \sum_{k,l}[\hat{H}_k(nT/M), \hat{H}_l(nT/M)]. \tag{9}$$

Here, we assume $\hat{H}(nT/M) \approx \hat{H}((n-1)T/M)$ and discretize the time-evolution operator for the reference dynamics.

Infidelity. The state-dependent inequality for the overlap (7) gives inequality for the infidelity

$$\sqrt{1 - |\langle\Psi(T)|\Psi_d(T)\rangle|^2} \leq \sqrt{1 - \cos^2\left(\sum_{n=1}^{M}\mathcal{L}_n\right)} \approx \sum_{n=1}^{M}\mathcal{L}_n, \quad \text{for small } \sum_{n=1}^{M}\mathcal{L}_n. \tag{10}$$

Since each $\mathcal{L}_n$ is $\mathcal{O}(M^{-2})$ as one can find in Eq. (9), the infidelity is $\mathcal{O}(M^{-1})$. Note that this scaling of the digitization errors is identical with the well-known result [4], but this inequality can reveal true scaling for specific decomposition as discussed below.

3.2 Trotter decomposition in the dynamical-invariant basis

Now we consider dynamics described by the single eigenvector of the dynamical invariant, $|\Psi(t)\rangle = e^{i\kappa_k(t)}|\phi_k(t)\rangle$, and the first-order Trotter decomposition which devide the Hamiltonian into the diagonal part and the off-diagonal part in the dynamical-invariant basis, i.e., we devide the Hamiltonian into the first term and the second term in Eq. (4). Then, we find that the dominant errors (9) vanish because $\hat{A}(nT/M)$ is off-diagonal in the dynamical-invariant basis and the state is given by the single eigenvector of the dynamical invariant $|\Psi(t)\rangle = e^{i\kappa_k(t)}|\phi_k(t)\rangle$.

Dominant errors. By considering higher-order expansion, we find that dominant errors of the first-order Trotter decomposition in the dynamical-invariant basis are given by

$$\mathcal{L}_n \approx \frac{T^3}{6\hbar^3 M^3}|\langle\phi_k(nT/M)|\hat{B}(nT/M)|\phi_k(nT/M)\rangle|, \quad \hat{B}(nT/M) = [\hat{H}_{\rm nd}(nT/M), [\hat{H}_{\rm nd}(nT/M), \hat{H}_{\rm d}(nT/M)]], \tag{11}$$

where $\hat{H}_{\rm d}(nT/M)$ and $\hat{H}_{\rm nd}(nT/M)$ are the diagonal part and the off-diagonal part of the Hamiltonian, i.e., the first term and the second term in Eq. (4), respectively. That is, the infidelity scales as $\mathcal{O}(M^{-2})$ which is better than the conventional prediction $\mathcal{O}(M^{-1})$. Note that this result is a generalization of the result in Ref. [12].

3.3 Application to digitized counterdiabatic driving

Finally, we show a useful example, i.e., digitized counterdiabatic driving [9–12].

Counterdiabatic driving. In shortcuts to adiabaticity by counterdiabatic driving [16, 17], we consider the following Hamiltonian

$$\begin{aligned}\hat{H}(t) &= \hat{H}_{\rm ref}(t) + \hat{H}_{\rm cd}(t),\\ \hat{H}_{\rm ref}(t) &= \sum_n E_n(t)|n(t)\rangle\langle n(t)|,\\ \hat{H}_{\rm cd}(t) &= i\hbar \sum_{\substack{m,n\\(m\neq n)}} |m(t)\rangle\langle m(t)|\partial_t n(t)\rangle\langle n(t)|,\end{aligned} \tag{12}$$

where $\hat{H}_{\rm ref}(t)$ is the reference Hamiltonian and $\hat{H}_{\rm cd}(t)$ is the counterdiabatic Hamiltonian. The counterdiabatic Hamiltonian cancels out diabatic changes and we can realize adiabatic time evolution of the reference Hamiltonian within arbitrary time. It is obvious from the derivation [16, 17], but we can also confirm this fact as follows.

Dynamical invariant in counterdiabatic driving. For the Hamiltonian (12), the following Hermitian operator

$$\hat{F}(t) = \sum_n f_n |n(t)\rangle\langle n(t)|, \tag{13}$$

is the dynamical invariant, where f_n is an arbitrary constant. That is, the set of eigenvectors of the reference Hamiltonian $\{|n(t)\rangle\}$ is that of the dynamical invariant in this system. Then, Eq. (5) gives the adiabatic state of the reference Hamiltonian, i.e.,

$$|\Psi_{\rm ad}(t)\rangle = \sum_n c_n(0) e^{-\frac{i}{\hbar}\int_0^t dt' E_n(t')} e^{-\int_0^t dt' \langle n(t')|\partial_{t'} n(t')\rangle} |n(t)\rangle. \tag{14}$$

Digitized counterdiabatic driving. In digitized counterdiabatic driving [9–12], we devide the time-evolution operator with the Hamiltonian (12) into that of the reference Hamiltonian and that of the counterdiabatic Hamiltonian by using the first-order Trotter decomposition. Since the reference Hamiltonian and the counterdiabatic Hamiltonian are the diagonal part and the off-diagonal part of the total Hamiltonian (12), the dominant errors of this decomposition is given by Eq. (11). It means that the scaling of digitization errors is $\mathcal{O}(M^{-2})$ in terms of the infidelity.

4 Summary

In this paper, we considered the first-order Trotter decomposition in the dynamical-invariant basis. By using the state-depdendent inequality [8], we found that the infidelity scales as $\mathcal{O}(M^{-2})$, whereas conventional approaches predict $\mathcal{O}(M^{-1})$. We also pointed out that this decomposition includes digitized counterdiabatic driving [9–12].

In addition to digitized counterdiabatic driving, there are other possible applications. For example, there is a quantum computation approach based on the Lewis-Riesenfeld theory [18]. Moreover, there is another method of shortcuts to adiabaticity based on the Lewis-Riesenfeld theory, i.e., invariant-based inverse engineering [19]. The present result also gives digital implementation of these applications with the infidelity $\mathcal{O}(M^{-2})$.

References

[1] R. P. Feynman. *Simulating physics with computers.* Int. J. Theor. Phys. **21**, 467 (1982).

[2] H. F. Trotter. *On the Product of Semi-Groups of Operators.* Proc. Am. Math. Soc. **10**, 545 (1959).

[3] M. Suzuki. *Generalized Trotter's formula and systematic approximants of exponential operators and inner derivations with applications to many-body problems.* Commun. Math. Phys. **51**, 183 (1976).

[4] S. Lloyd. *Universal Quantum Simulators.* Science **273**, 1073 (1996).

[5] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma. *Simulating Hamiltonian Dynamics with a Truncated Taylor Series.* Phys. Rev. Lett. **114**, 090502 (2015).

[6] G. H. Low and I. L. Chuang. *Optimal Hamiltonian Simulation by Quantum Signal Processing.* Phys. Rev. Lett. **118**, 010501 (2017).

[7] H. Lewis and W. Riesenfeld. *An Exact Quantum Theory of the Time-Dependent Harmonic Oscillator and of a Charged Particle in a Time-Dependent Electromagnetic Field.* J. Math. Phys. **10**, 1458 (1969).

[8] T. Hatomura. *State-dependent error bound for digital quantum simulation of driven systems.* Phys. Rev. A **105**, L050601 (2022).

[9] N. N. Hegade, K. Paul, Y. Ding, M. Sanz, F. Albarrán-Arriagada, E. Solano, and X. Chen. *Shortcuts to Adiabaticity in Digitized Adiabatic Quantum Computing.* Phys. Rev. Appl. **15**, 034038 (2021).

[10] P. Chandarana, N. N. Hegade, K. Paul, F. Albarrán-Arriagada, E. Solano, A. del Campo, and X. Chen. *Digitized-counterdiabatic quantum approximate optimization argorithm.* Phys. Rev. Res. **4**, 013141 (2022).

[11] N. N. Hegade, X. Chen, and E. Solano. *Digitized counterdiabatic quantum optimization.* Phys. Rev. Res. **4**, L042030 (2022).

[12] T. Hatomura. *Scaling of errors in digitized counterdiabatic driving.* arXiv:2303.04235.

[13] X. Chen, E. Torrontegui, and J. G. Muga. *Lewis-Riesenfeld invariants and transitionless quantum driving.* Phys. Rev. A **83**, 062116 (2011).

[14] K. Takahashi. *Shortcuts to adiabaticity applied to nonequilibrium entropy production: an information geometry viewpoint*. New J. Phys. **19**, 115007 (2017).

[15] W. K. Wootters. *Statistical distance and Hilbert space*. Phys. Rev. D **23**, 357 (1981).

[16] M. Demirplak and S. A. Rice. *Adiabatic Population Transfer with Control Fields*. J. Phys. Chem. A **107**, 9937 (2003).

[17] M. V. Berry. *Transitionless quantum driving*. J. Phys. A: Math. Theor. **42**, 365303 (2009).

[18] M. S. Sarandy, E. I. Duzzioni, and R. M. Serra. *Quantum computation in continuous time using dynamical invariants*. Phys. Lett. A **375**, 3343 (2011).

[19] X. Chen, A. Ruschhaupt, S. Schmidt, A. del Campo, D. Guéry-Odelin, and J. G. Muga. *Fast Optimal Frictionless Atom Cooling in Harmonic Traps: Shortcut to Adiabaticity*. Phys. Rev. Lett. **104**, 063002 (2010).

The work associated with quantum information processing driven by the assistance of a controller

Shintaro Minagawa[1] * Kenta Sakai[1 2] † Kohtaro Kato[1] ‡ Francesco Buscemi[1] §

[1] *Graduate School of Informatics, Nagoya University, Furo-cho, Chikusa-Ku, Nagoya 464-8601, Japan*
[2] *TOYOTA INDUSTRIES IT SOLUTIONS Inc., Albax Tower Kariya Ekimae Akariya Building 1-72-1 Minami-Sakuramachi, Kariya 448-0841, Japan*

Abstract. We deal with quantum information processing driven by a controller and derive formulas about the work needed for the controller and net extractable work from the system and controller. We apply these formulas to quantum feedback control and erasure protocol considered by Sagawa and Ueda as a model of Maxwell's demon. We show that among several assumptions they imposed, one that the demon's measurement is projective is sufficient to derive an inequality, what they call the second law of thermodynamics, that bounds the net extractable work from the system and demon by the decrease in the system's free energy.

Keywords: Information thermodynamics, Maxwell's demon, Quantum feedback control

1 Introduction

The resource theory of quantum thermodynamics (see, e.g., [12]) has revealed the existence of the second law of thermodynamics in quantum information processing [16, 8, 1]. However, concerning information processing driven by the assistance of another system called the controller, thermodynamics of information processing becomes more complicated as represented by the problem of Maxwell's demon [9]. It is a device that can decrease the system's entropy, which has been the focus of many works exploring the relationship between the second law and information processing for example, Refs. [17, 3, 2, 7].

Sagawa and Ueda showed that the amount of extractable work from the system can be beyond the second law by quantum feedback control [13]. The work needed for the measurement and erasure process of the demon compensates for the excess so that the extractable work from both the system and the demon has the free energy decreasing of the system as an upper bound, what they say, the second law [14]. However, this result is based on several assumptions about the demon's measurement process.

We deal with the process where the system and controller evolve by interacting with each other adiabatically and after that, only the controller interacts with the thermal bath. We provide the formulas for the work required by the controller and the extractable work from both the system and controller.

Sagawa–Ueda's quantum feedback control and erasure protocol [14] is a special case of our general formalism by regarding the controller as a demon. Therefore, by applying the to Sagawa–Ueda's protocol, we immediately derive the work needed by the demon and the extractable work from both the system and the demon. Furthermore, we show that the assumption that the demon performs projection measurements is sufficient to derive the second law, even though the protocol is more general in that it does not satisfy all the assumptions imposed by the Sagawa–Ueda protocol.

2 Notations

Consider a quantum system A with a finite-dimensional Hilbert space $\mathscr{H}^A$, the states correspond to a positive semidefinite operator ρ^A with $\mathrm{Tr}\,\rho^A = 1$. The formula of *von Neumann entropy* [19] of a state ρ^A is $H(A)_\rho := -\mathrm{Tr}[\rho^A \ln \rho^A]$. For a composite system $A+B$, *quantum mutual information* of a bipartite states ρ^{AB} is defined by $I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho$.

Given a Hamiltonian $\mathcal{H}^A$ and an inverse temperature β, the corresponding *thermal state* or *Gibbs state* is defined as $\gamma^A := {Z_A}^{-1} e^{-\beta\mathcal{H}^A}$, where $Z_A := \mathrm{Tr}[e^{-\beta\mathcal{H}^A}]$ is the partition function. The *nonequilibrium free energy* [4] of a quantum state ρ^A is defined as $F(\rho^A;\mathcal{H}^A) := F_{\mathrm{eq}}(\mathcal{H}^A) + \beta^{-1}D(\rho^A\|\gamma^A)$, where $F_{\mathrm{eq}}(\mathcal{H}^A) := -\beta^{-1}\ln Z_A$ is the equilibrium free energy and $D(\rho\|\gamma) := \mathrm{Tr}[\rho\ln\rho - \rho\ln\gamma]$ is the *Umegaki quantum relative entropy* between ρ and γ [18]. We frequently use the following relationship [4]:

$$F(\rho^A;\mathcal{H}_A) = E(\rho^A;\mathcal{H}_A) - \beta^{-1}H(A)_\rho \qquad (1)$$

*minagawa.shintaro@nagoya-u.jp
†sakai.kenta_32@nagoya-u.jp
‡kokato@i.nagoya-u.ac.jp
§buscemi@i.nagoya-u.ac.jp

where $E(\rho^A;\mathcal{H}^A) := \mathrm{Tr}[\rho^A\mathcal{H}^A]$ is the expectation value energy of system A. In the following, we omit Hamiltonians in the energy and nonequilibrium free energy in principle.

3 The setup

Suppose that a quantum system S and C, which we call the system and controller, respectively, are initialized in state ρ_0^S and σ_0^C. The Hamiltonian on the system is $\mathcal{H}_0^S$ at time $t = t_0$. The controller's Hamiltonian $\mathcal{H}^C$ is invariant throughout time. Also, we have a thermal bath B with inverse temperature β and the invariant Hamiltonian $\mathcal{H}^B$ and we call such a bath $(\mathcal{H}^B, \beta)$-bath.

First, the system S and controller C, initially in a product state $\rho_0^S \otimes \sigma_0^C$, interact with each other and evolve in time following a CPTP map $\mathcal{D}$ becoming τ_1^{SC} at $t = t_1$. The Hamiltonian of the system becomes $\mathcal{H}_1^S$ at $t = t_1$, which is not necessarily the same as the Hamiltonian $\mathcal{H}_0^S$ at $t = t_0$. The assumption that the process $\mathcal{D}$ happens without any exchange of heat means that the average work we can extract from this transition exactly matches $-\Delta E_{\mathcal{D}}^{SC}$, that is, the energy decrease in S and C caused by $\mathcal{D}$ where $\Delta E_{\mathcal{D}}^{SC} := E(\rho_0^S \otimes \sigma_0^C) - E(\tau_1^{SC})$.

After that, only C interacts with B by unitary interaction $\mathcal{W} := W(\cdot)W^\dagger$ and we obtain the final state ω_2^{SCB} at $t = t_2$. We assume that at $t = t_2$, the system's Hamiltonian $\mathcal{H}_2^S$ is equal to $\mathcal{H}_1^S$. Also, we assume that there is no interaction Hamiltonian at $t = t_0, t_1$, and t_2. As shown in Ref. [8], any unitary interaction between the system and the bath can be realized with a work cost equal to $\Delta E_{\mathcal{W}}^{CB} := E(\omega_2^{CB}) - E(\tau_1^C \otimes \gamma_1^B)$.

In this setup, the work cost for the controller is $W_{\mathrm{in}}^C := \Delta E_{\mathcal{D}}^C + \Delta E_{\mathcal{W}}^{CB}$ where $\Delta E_{\mathcal{D}}^C := E(\tau_1^C) - E(\sigma_0^C)$. Let $\mathcal{E}$ denote the CPTP map corresponding to overall process of S, C and B from $t = t_0$ to $t = t_2$ (Fig. 1). The total average work extracted from S and C during the overall process $\mathcal{E}$ is $W_{\mathrm{ext}}^{SC} := -\Delta E_{\mathcal{D}}^{SC} - \Delta E_{\mathcal{W}}^{CB} = -\Delta E^{SCB}$ where $\Delta E^{SCB} := E(\omega_2^{SCB}) - E(\rho_0^S \otimes \sigma_0^C \otimes \gamma_0^B)$.

4 Main results

The extractable work from the system is $W_{\mathrm{ext}}^S := -\Delta E_{\mathcal{D}}^S$ where $\Delta E_{\mathcal{D}}^S := E(\tau_1^S) - E(\rho_0^S)$. By using Eq.(1), one can easily verify

$$W_{\mathrm{ext}}^S = -\Delta F_{\mathcal{D}}^S - \beta^{-1}\Delta H_{\mathcal{D}}^S \tag{2}$$

where $\Delta F_{\mathcal{D}}^S := F(\tau_1^S) - F(\rho_0^S)$ and $\Delta H_{\mathcal{D}}^S := H(S)_{\tau_1} - H(S)_{\rho_0}$.

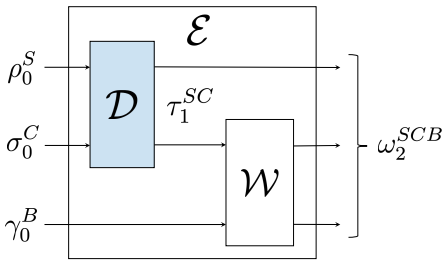


Figure 1: A CPTP map $\mathcal{E}$ consists of an adiabatic process $\mathcal{D}$ of the system S and controller C, and a subsequent unitary interaction $\mathcal{W}$ between the controller C and bath B.

Now we derive the general formula of the work cost of the controller W_{in}^{SC} and net extractable work from both the system and controller W_{ext}^{SC} (for the proof is in Appendix A):

Theorem 1 *The work cost for the controller is*

$$W_{\mathrm{in}}^C = \Delta F^C + \beta^{-1}[\Delta H_{\mathcal{D}}^C + I(C:B)_{\omega_2} + D(\omega_2^B\|\gamma_2^B)] \tag{3}$$

where $\Delta F^C := F(\omega_2^C) - F(\sigma_0^C)$ *and* $\Delta H_{\mathcal{D}}^C := H(C)_{\tau_1} - H(C)_{\sigma_0}$. *The net extractable work from both the system and controller is equal to*

$$\begin{aligned} W_{\mathrm{ext}}^{SC} = &-\Delta F_{\mathcal{D}}^S - \Delta F^C - \beta^{-1}[\Delta H_{\mathcal{D}}^S + \Delta H_{\mathcal{D}}^C \\ &+ I(C:B)_{\omega_2} + D(\omega_2^B||\gamma_2^B)] \,. \end{aligned} \tag{4}$$

5 An application to quantum feedback control and erasure protocols

We analyze the *quantum feedback control and erasure protocol* (Fig. 2) considered in Ref. [13] based on our framework given in the previous section.

First, we prepare the initial state of the system S, memory M, classical register K and bath B at the time t_0 as $\rho_0^S \otimes \rho_0^M \otimes |0\rangle\langle 0|_0^K \otimes \gamma_0^B$ where ρ_0^S and ρ_0^M are arbitrary states on $\mathscr{H}^S$ and $\mathscr{H}^M$.

Considering the role of M and K, which will be explained below, we refer to them collectively as a demon. The system and demon's process from $t = t_0$ to $t = t_2$ is the measurement process and their state becomes $\sum_k p_k \rho_{2(k)}^{SM} \otimes |k\rangle\langle k|_2^K$ where k is the measurement outcome, p_k is the probability of obtaining the outcome k, and $\rho_{2(k)}^{SM}$ is the post-measurement state corresponding the outcome k, and $|k\rangle\langle k|_2^K$ means that the classical register K records the outcome k.

After the measurement, feedback control as controlled unitary based on the measurement outcome acts on the system from $t = t_2$ to $t = t_3$. Then the system and demon's state becomes $\sum_k p_k \rho_{3(k)}^{SM} \otimes$

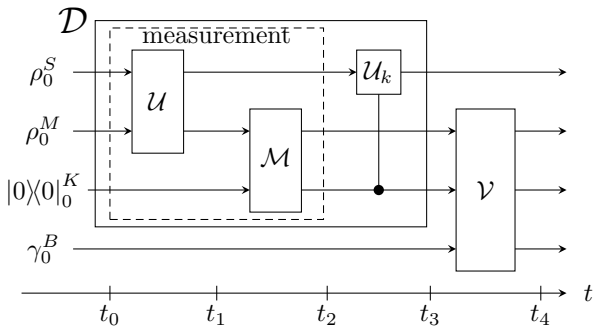


Figure 2: The quantum feedback and erasure protocol. **Interaction stage** ($t_0 \to t_1$): system S and demon's memory M interact according to a unitary $\mathcal{U}$. **Probe stage** ($t_1 \to t_2$): a measurement $\mathcal{M}$ is done on M and the outcome k is written on the classical register K. **Feedback control stage** ($t_2 \to t_3$): a controlled unitary $\mathcal{U}_k$ is applied on S depending on the outcome k. **Erasure stage** ($t_3 \to t_4$): a unitary $\mathcal{V}$ between M, K, and the bath B erase the information of the demon's memory and register.

$|k\rangle\langle k|_3^K$. Let $\mathcal{D}$ denote the system and demon's process from $t = t_0$ to $t = t_3$ as a CPTP linear map.

The erasure process is a unitary $\mathcal{V} := V(\cdot)V^\dagger$ between the demon and the $(\mathcal{H}_B, \beta)$-bath B such that $(\mathrm{id}^S \otimes \mathcal{V})(\sum_k p_k \rho_{3(k)}^{SM} \otimes |k\rangle\langle k|_3^K \otimes \gamma_3^B) = \rho_4^{SMB} \otimes |0\rangle\langle 0|_4^K$ where $\rho_4^M = \rho_0^M$, which means that the unitary $\mathcal{V}$ erases the memory. Here we assume the existence of such a unitary process.

For any time step t_j ($j = 0, 1, 2, 3, 4$), we assume that the Hamiltonian of the demon and bath are invariant and denote those Hamiltonian by $\mathcal{H}_{MK}$, and $\mathcal{H}_B$, respectively. We denote the system's Hamiltonian as $\mathcal{H}_j^S$ ($j = 0, 1, 2, 3, 4$) and assume $\mathcal{H}_3^S = \mathcal{H}_4^S$. Also, we assume that for any time step, the interaction Hamiltonians between S, M, K, and B are zero.

We introduce *Groenewold-Ozawa information gain* [5, 11] defined as $I_{\mathrm{GO}}(S;K) := H(S)_{\rho_0} - H(S|K)_{\rho_3}$ where $H(S|K)_{\rho_3} := \sum_k p_k H(S|k)_{\rho_3}$ is the conditional quantum entropy. Here we use the notation $H(S|k)_{\rho_3} := -\mathrm{Tr}\{\rho_{3(k)}^S \ln \rho_{3(k)}^S\}$.

Now we derive the work associated with the quantum feedback control and erasure protocol. From the concavity of von Neumann entropy (e.g., [20]) and Eq. (2), one can obtain $W_{\mathrm{ext}}^S = -\Delta F_{\mathcal{D}}^S - \beta^{-1}\Delta H_{\mathcal{D}}^S \leqslant -\Delta F_{\mathcal{D}}^S + \beta^{-1} I_{\mathrm{GO}}(S;K)$ [1].

By replacing C in Eq.(3) and (4) with MK and setting $\Delta F^{MK} = 0$ because of the erasure, we have the following theorem (for the proof, see Appendix B):

Theorem 2 *The work cost of the demon's measurement and erasure process W_{in}^{MK} is equal to*

$$W_{\mathrm{in}}^{MK} = \beta^{-1}[\Delta H_{\mathcal{D}}^{MK} + I(MK:B)_{\rho_4} + D(\rho_4^B \| \gamma_4^B)]. \tag{5}$$

The extractable work from both the system and demon W_{ext}^{SMK} is equal to

$$\begin{aligned} W_{\mathrm{ext}}^{SMK} = &-\Delta F_{\mathcal{D}}^S - \beta^{-1}[\Delta H_{\mathcal{D}}^S + \Delta H_{\mathcal{D}}^{MK} \\ &+ I(MK:B)_{\rho_4} + D(\rho_4^B || \gamma_4^B)]. \end{aligned} \tag{6}$$

If the entropy change during the measurement process $\Delta H_{\mathrm{meas}}^{SMK} := H(SMK)_{\rho_2} - H(SMK)_{\rho_0}$ is non-negative, we have $W_{\mathrm{ext}}^{SMK} \leqslant -\Delta F_{\mathcal{D}}^S$.

Sagawa–Ueda [14] showed $W_{\mathrm{ext}}^{SMK} = W_{\mathrm{ext}}^S - W_{\mathrm{in}}^{MK} \leqslant -\Delta F_{\mathrm{eq}}^S$ they call the second law by showing $W_{\mathrm{in}}^{MK} \geqslant \beta^{-1} I$ based on the several assumptions listed in Appendix C. However, as a matter of fact,

Assumption 1 (A1). The measurement process of the demon is projective and the post-measurement states $\rho_{2(k)}^M$ and $\rho_{2(k')}^M$ are mutually orthogonal when $k \neq k'$.

is sufficient in obtaining $W_{\mathrm{ext}}^{SMK} \leqslant -\Delta F_{\mathcal{D}}^S$ and this immediately leads to an inequality $W_{\mathrm{in}}^{MK} \geqslant -\beta^{-1}\Delta H_{\mathcal{D}}^S$. By imposing

Assumption 2 (A2). At $t = t_2$, the system and demon's state is a product state, i.e., $\rho_{2(k)}^S \otimes \rho_{2(k)}^M$ for each outcome k.

in addition to A1, we obtain a more refined inequality of W_{in}^{MK} given in the following proposition (for the proof, see Appendix D):

Proposition 3 *Assume A1. We have $W_{\mathrm{ext}}^{SMK} \leqslant -\Delta F_{\mathcal{D}}^S$ and $W_{\mathrm{in}}^{MK} \geqslant -\beta^{-1}\Delta H_{\mathcal{D}}^S$. Assume A1 and A2. We have $W_{\mathrm{in}}^{MK} \geqslant \beta^{-1}[I_{\mathrm{GO}}(S;K) + I(MK:B)_{\rho_4} + D(\rho_4^B \| \gamma_4^B)]$.*

6 Summary

We consider the general information processing driven by the assistance of the controller as depicted in Fig.1. Then we derive general formulas of the work cost for the controller Eq.(3), the extractable work from the system Eq.(2), and the extractable work both from the system and controller Eq.(4).

We adapt these formulas to Sagawa–Ueda's quantum feedback control and erasure protocol [13, 14] and show that $W_{\mathrm{ext}}^{SMK} \leqslant -\Delta F_{\mathcal{D}}^S$ holds even for more general protocols than those they analyzed, e.g., without A2, as long as it satisfies A1.

[1] This inequality implies Sagawa–Ueda's inequality $W_{\mathrm{ext}}^S \leqslant -\Delta F_{\mathrm{eq}}^S + \beta^{-1} I$ [13]. Here ΔF_{eq}^S is the equilibrium free energy change of the system and I is equal to $I_{\mathrm{GO}}(S;K)$ in their setting. Note that $\Delta F_{\mathcal{D}}^S \geqslant \Delta F_{\mathrm{eq}}^S$ holds.

Acknowledgments

The authors would like to thank Arshag Danageozian, Takahiro Sagawa, and Yosuke Mitsuhashi for their helpful comments and fruitful discussions. S. M. would like to take this opportunity to thank the "Nagoya University Interdisciplinary Frontier Fellowship" supported by Nagoya University and JST, the establishment of university fellowships towards the creation of science technology innovation, Grant Number JPMJFS2120. F.B. acknowledges support from MEXT Quantum Leap Flagship Program (MEXT QLEAP) Grant No. JPMXS0120319794, from MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe" No. 21H05183, and from JSPS KAKENHI, Grants No. 20K03746 and No. 23K03230. K. K. acknowledges support from JSPS Grant-in-Aid for Early-Career Scientists, No. 22K13972; from MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe", No. 22H05254.

References

[1] A. M. Alhambra, L. Masanes, J. Oppenheim, and C. Perry. Fluctuating work: From quantum thermodynamical identities to a second law equality. *Phys. Rev. X*, 6:041017, Oct 2016.

[2] C. H. Bennett. Logical reversibility of computation. *IBM journal of Research and Development*, 17(6):525–532, 1973.

[3] L. Brillouin. Maxwell's demon cannot operate: Information and entropy. i. *Journal of Applied Physics*, 22(3):334–337, 1951.

[4] M. Esposito and C. Van den Broeck. Second law and landauer principle far from equilibrium. *EPL (Europhysics Letters)*, 95(4):40004, 2011.

[5] H. J. Groenewold. A problem of information gain by quantal measurements. *International Journal of Theoretical Physics*, 4(5):327–338, 1971.

[6] O. Klein. Zur quantenmechanischen begründung des zweiten hauptsatzes der wärmelehre. *Zeitschrift für Physik*, 72(2158):767–7775, 1931.

[7] R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5:183–191, 1961.

[8] A. S. Malabarba, A. J. Short, and P. Kammerlander. Clock-driven quantum thermal engines. *New Journal of Physics*, 17(4):045027, 2015.

[9] J. C. Maxwell. *Theory of heat*. Appleton, London, 1871.

[10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[11] M. Ozawa. On information gain by quantum measurements of continuous observables. *Journal of Mathematical Physics*, 27:759–763, 1986.

[12] T. Sagawa. *Entropy, Divergence, and Majorization in Classical and Quantum Thermodynamics*, volume 16 of *SpringerBriefs in Mathematical Physics*. Springer Singapore, 2022.

[13] T. Sagawa and M. Ueda. Second law of thermodynamics with discrete quantum feedback control. *Phys. Rev. Lett.*, 100:080403, Feb 2008.

[14] T. Sagawa and M. Ueda. Minimal energy cost for thermodynamic information processing: Measurement and information erasure. *Phys. Rev. Lett.*, 102:250602, Jun 2009.

[15] T. Sagawa and M. Ueda. Erratum: Minimal energy cost for thermodynamic information processing: Measurement and information erasure [phys. rev. lett. 102, 250602 (2009)]. *Phys. Rev. Lett.*, 106:189901, May 2011.

[16] P. Skrzypczyk, A. J. Short, and S. Popescu. Work extraction and thermodynamics for individual quantum systems. *Nature communications*, 5(1):1–8, 2014.

[17] L. Szilard. über die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen. *Zeitschrift für Physik*, 53:840–856, 1929.

[18] H. Umegaki. On information in operator algebras. *Proc. Japan Acad.*, 37(8):459–461, 1961.

[19] J. von Neumann. *Mathematical foundations of quantum mechanics*. Princeton University Press, 1955.

[20] M. M. Wilde. *Quantum Information Theory, 2nd edition*. Cambridge University Press, 2017.

Quantum Bayesian Inference in Quasiprobability Representations

Clive Cenxin Aw[1] * Kelvin Onggadinata[1] † Dagomir Kaszlikowski[1 2] ‡
Valerio Scarani[1 2] §

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Abstract. Bayesian inference plays a crucial role in information and physical sciences alike. Classical Bayesian inversion is expressed naturally as stochastic matrix acting on probability vectors. Meanwhile the quantum informational Baye's rule, the Petz Recovery channel, has been formulated in the context of Hilbert spaces. In this paper, we derive the expression of the Petz channel within quasiprobability representations. By putting quantum Bayesian inference in the same formal context as its classical counterpart, in (quasi-)stochastic matrices acting on (quasi-)stochastic vector, the core differences between the two regimes is found in the processing of reference priors rather than channel representation.

Keywords: bayesian inference, foundations, reversibility, quasiprobabilistic representations

This extended abstract for the IPS Meeting 2023 covers key points found in [1].

1 The Task

Inference is a logical necessity in every science. This fundamentality is particularly overt in notions of process reversibility and state recovery. Here, the most empirically applied and canonical approach is Bayes' rule:

$$\tilde{\mathcal{E}}_\gamma(a|a') = \mathcal{E}(a'|a)\frac{\gamma(a)}{\tilde{\gamma}(a')}. \tag{1}$$

This relation gives us a recipe for obtaining various probability-theoretic objects [2, 3, 4, 5]. Of particular note, we may use it to obtain the "reverse" transition $\tilde{\mathcal{E}}_\gamma$ for any given (i) the forward process or *transformation* $\mathcal{E}$, and (ii) the reference *prior* γ on the input of said process. The *posterior*, $\tilde{\gamma}(a') = \sum_a \mathcal{E}(a'|a)\gamma(a)$, emerges from these two objects.

Now, moving to the quantum regime, the channel which has garnered a reputation for being the "quantum Bayes' rule" [6, 7] , is the *Petz recovery map* [8, 9, 10]:

$$\hat{\mathcal{E}}_\gamma[\bullet] = \sqrt{\gamma}\,\mathcal{E}^\dagger\left[\frac{1}{\sqrt{\mathcal{E}[\gamma]}}\bullet\frac{1}{\sqrt{\mathcal{E}[\gamma]}}\right]\sqrt{\gamma}, \tag{2}$$

This recovery channel is defined for any CPTP map $\mathcal{E}$ and a reference density operator γ. Notably, when reference priors, input states and the channel share the same eigenbases, the Petz map reduces to the classical Bayes rule [10, 11, 12, 13]. It also appears naturally in the definition of fluctuation theorems in thermodynamics [14, 15, 16] and has vindicated its reputation recently through some axiomatic approaches [7, 13].

Now the Petz map has thus far only been understood in terms of CPTP maps and density operators, living in a Hilbert space. Meanwhile, the classical Bayes rule exists as a stochastic matrix mapping stochastic vectors, living in a real vector space. Thus a formal comparison, between these two kinds of Bayesian inference, is difficult due to this difference in mathematical habitat.

2 The Approach

Thus, we seek to close this gap by formalizing the Petz map in *quasiprobability representations* (QPRs) [17, 18]. These provide a theoretically isomorphic description of quantum theories while sharing the familiar mathematical equipment found in classical probability theory: channels $\mathcal{E}$ map to matrices $S^{\mathcal{E}}$ and density operators ρ map to vectors v^ρ. Details captured in Table 1. The distinction is that *quasiprobabilities* (that is, negativities) are generally necessary in the quantum case [19].

Object	**Quasiprobability Formalism**
Density Operator, ρ	$v^\rho \;:\; v^\rho_a = \mathrm{Tr}[\rho\, F_a]$
POVM, E_m	$\bar{v}^m \;:\; \bar{v}^m_{a'} = \mathrm{Tr}[E_m\, G_{a'}]$
Unitary, $\mathcal{U}$	$S^{\mathcal{U}} : S^{\mathcal{U}}_{a'a} = \mathrm{Tr}\left[F_{a'} U G_a U^\dagger\right]$
CP Maps, $\mathcal{E}[\bullet]$	$S^{\mathcal{E}} :\; S^{\mathcal{E}}_{a'a} = \mathrm{Tr}[F_{a'}\mathcal{E}[G_a]]$
Born Rule, $\mathrm{Tr}[\rho E_m]$	$v^\rho \cdot \bar{v}^m \in [0,1]$
Dimensionality, d	$\mathtt{dim}[\mathbb{R}^d \otimes \mathbb{R}^d] = d^2$

Table 1: Dictionary of relationships between the Hilbert space and quasiprobability formalisms. $v^p_a = p(a)$ indicates the a-th entry in a p-distribution. $S^{\mathcal{E}}_{a'a} = \mathcal{E}(a'|a)$ indicates the entry on the a'-column and a-row of a matrix $S^{\mathcal{E}}$. Thus, $S^{\mathcal{E}} v^\rho = v^{\mathcal{E}[\rho]}$ etc.

Every QPR is defined by choices of frame and dual operators F_i, G_j, which must adhere to some formal condi-

*e0006371@u.nus.edu
†e0546277@u.nus.edu
‡phykd@nus.edu.sg
§physv@nus.edu.sg

tions and features. We simply note in passing that there are two key canonical choices of QPRs in the literature: "normal QPRs" (in particular, the "discrete Wigner representation") and "SIC-POVM representations" (as in symmetric, informationally complete positive operator-valued measures). For the technical details of these and other generalities, we refer the reader to the fuller treatment [1].

The crucial point is that QPRs give us the avenue to situate the Petz map in the same formal habitat as its classical counterpart and in an expression comparable to it. Importantly, we want to do this in such a way that requires nothing but formal equipment in QPR. That is, for some forward, quasistochastic transformation $S^{\mathcal{E}}$ (corresponding to a quantum channel) and a quasistochastic reference prior v^{γ} (corresponding to a quantum state) *only*, how does one construct $S^{\hat{\mathcal{E}}_\gamma}_{\mathbf{QM}}$, the relevant Bayesian inversion? See Figure 1.

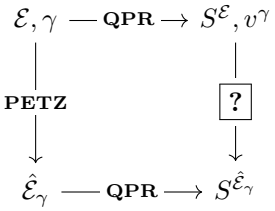


Figure 1: A commutativity diagram illustrating the main task of this work: the protocol "**?**", that is to be executable solely within the QPR framework.

From there we discuss similarities, differences and interpretations wherever appropriate. This makes a formal step in understanding the essential distinctions between classical and quantum inference.

3 Results

3.1 Quantum Bayesian Inference in QPR

We skip over the proof (see [1] for details) and go to our result right away:

Main Result The Petz map in any QPR reads

$$S^{\hat{\mathcal{E}}_\gamma}_{\mathbf{QM}} = M_\gamma^{1/2} \left(S^{\mathcal{E}^\dagger}\right) M_{\mathcal{E}[\gamma]}^{-1/2}, \tag{3}$$

where

$$\begin{aligned} (M_\gamma)_{a'a} &= \sum_{xy} v_x^\gamma v_y^\gamma \, \xi_{a'xay}, \\ \left(M_{\mathcal{E}[\gamma]}\right)_{a'a} &= \sum_{xy} (S^{\mathcal{E}} v^\gamma)_x (S^{\mathcal{E}} v^\gamma)_y \, \xi_{a'xay}. \end{aligned}$$

and $\xi_{pqrs} = \mathrm{Tr}[F_p G_q G_r G_s]$ are structure coefficients determined by the specific QPR via the frames and duals it is defined by. Everything is expressed exclusively in the quasiprobabilistic formalism: no knowledge of Hilbert space renditions of the quantum channel or reference state is required.

For the two canonical choices of QPR mentioned above, we also proved in [1] that

$$\textbf{NORMAL QPR} : S^{\mathcal{E}^\dagger}_{\mathbf{NQ}} = (S^{\mathcal{E}})^{\mathrm{T}}, \tag{4}$$

$$\textbf{SIC-POVM QPR} : S^{\mathcal{E}^\dagger}_{\mathbf{SP}} = (S^{\mathcal{E}})^{\mathrm{T}} + J_{\mathcal{E}}, \tag{5}$$

where $(J_{\mathcal{E}})_{ij} = \frac{1}{d}(\sum_a \mathcal{E}(j|a) - 1)$; whence explicitly

$$S^{\hat{\mathcal{E}}_\gamma}_{\mathbf{NQ}} = M_\gamma^{1/2} (S^{\mathcal{E}})^{\mathrm{T}} M_{\mathcal{E}[\gamma]}^{-1/2}, \tag{6}$$

$$S^{\hat{\mathcal{E}}_\gamma}_{\mathbf{SP}} = M_\gamma^{1/2} \left[(S^{\mathcal{E}})^{\mathrm{T}} + J_{\mathcal{E}}\right] M_{\mathcal{E}[\gamma]}^{-1/2}. \tag{7}$$

3.2 Comparing Inference Across Regimes

We discuss similarities and differences between classical and quantum Bayesian inference, captured by (1) and (3) respectively. See Table 2 for a summary.

3.2.1 Similarities

Firstly, we note that while (1) gives individual transitions $a \to a'$, the mapping of entire distributions is best expressed by writing Bayes' rule as a stochastic matrix:

$$S^{\tilde{\mathcal{E}}_\gamma}_{\mathbf{CL}} = D_\gamma (S^{\mathcal{E}})^{\mathrm{T}} D^{-1}_{\mathcal{E}[\gamma]}. \tag{8}$$

Here, $S^{\mathcal{E}}$ is a stochastic matrix for which the entry on the a'-column and a-row of a matrix $S^{\mathcal{E}}_{a'a}$ is $\mathcal{E}(a'|a)$, and D_p is a diagonal matrix with entries corresponding to some distribution p. Now, this can be rewritten as:

$$S^{\tilde{\mathcal{E}}_\gamma}_{\mathbf{CL}} = (D^2_\gamma)^{1/2} \left(S^{\mathcal{E}^\dagger}\right) (D^2_{\mathcal{E}[\gamma]})^{-1/2} \tag{9}$$

because $(S^{\mathcal{E}})^{\mathrm{T}} = S^{\mathcal{E}^\dagger}$ for classical channels (see [1] for details) and $(D_\gamma)_{ij} = v_i^\gamma \delta_{ij}$. In other words, classical Bayesian inference hides the fact *that the central matrix is an adjoint, and that the left and right matrices should be seen as square roots of more fundamental matrices* X_γ *and* $X_{\mathcal{E}[\gamma]}$. This is the *common form* of classical and quantum Bayesian inference via QPRs.

3.2.2 Differences

Let us now study the *differences* between the two theories. Crucially, the formal differences between the matrices X_γ (D^2_γ for classical, M_γ for quantum). Both can be written

$$(X_\gamma)_{ij} = \sum_{x,y=1}^{d^2} v_x^\gamma v_y^\gamma \xi_{ixjy}\,; \tag{10}$$

but while the M_γ of quantum theory has $\xi_{ixjy} = \mathrm{Tr}[F_i G_x G_j G_y]$, the D^2_γ of classical theory is such that $(D^2_\gamma)_{ij} = (v_i^\gamma)^2 \delta_{ij}$ i.e.

$$\xi_{ixjy} = \delta_{ix}\delta_{jy}\delta_{ij} \qquad [\text{Classical}]\,. \tag{11}$$

This comparison is summarized in Table 2. In these structure coefficients, lie the fundamental difference between quantum and classical Bayesian inference. On this, we make some remarks before concluding.

Bayesian Inference in Theory $\mathcal{T}$

$$S_{\mathcal{T}}^{\bar{\mathcal{E}}_\gamma} = X_\gamma^{1/2}\big(S^{\mathcal{E}^\dagger}\big)X_{\mathcal{E}[\gamma]}^{-1/2}$$

$$(X_\gamma)_j = \textstyle\sum_{xy} v_x^\gamma v_y^\gamma \xi_{ixjy}$$

Object	$\mathcal{T}$**: Quantum**	$\mathcal{T}$**: Classical**
$S^{\mathcal{E}^\dagger}$	**NQ** : $(S^{\mathcal{E}})^{\mathrm{T}}$ **SP** : $(S^{\mathcal{E}})^{\mathrm{T}} + J_{\mathcal{E}}$	$(S^{\mathcal{E}})^{\mathrm{T}}$
ξ_{ixjy}	$\mathrm{Tr}[F_i G_x G_j G_y]$	$\delta_{ix}\delta_{jy}\delta_{ij}$

Table 2: Retrodiction maps for classical probabilities [$S_{\mathcal{T}}^{\bar{\mathcal{E}}_\gamma} \to S_{\mathbf{CL}}^{\hat{\mathcal{E}}_\gamma}$, Eq. (8) or (9)] and quantum quasiprobabilities [$S_{\mathcal{T}}^{\bar{\mathcal{E}}_\gamma} \to S_{\mathbf{QM}}^{\hat{\mathcal{E}}_\gamma}$, Eq. (3)].

4 Discussion & Conclusion

The difference between the structure coefficients highlights features in quantum theory that are simply not present in classical probability theory.

Bayesian inference in both theories involve a similar structure (see $S_{\mathcal{T}}^{\bar{\mathcal{E}}_\gamma}$ in Table 2). Given that the transpose of a classical channel is also its adjoint, the key difference between $S_{\mathbf{CL}}^{\bar{\mathcal{E}}_\gamma}$ and $S_{\mathbf{QM}}^{\hat{\mathcal{E}}_\gamma}$ lies not in the central matrix $S^{\mathcal{E}^\dagger}$, but in the right and left matrices $X_{\mathcal{E}[\gamma]}, X_\gamma$ that capture the description of the priors. This affirms the fact that what separates quantum theory from classical theory is not so much in its dynamics (which is in many ways conceptually similar), but in the description of states.

Mathematically, the difference is captured by the form of the structure coefficients ξ_{ixjy}. In classical theory, the structure coefficients render the matrices diagonal. By contrast, in a QPR of quantum theory, the structure coefficients introduce weighted products $v_x^\alpha v_y^\alpha$ of every pair of entries of the distribution v^α. This is fundamentally due to complementarity, which is being embedded in the frames of the QPR.

Finally, we note how if we set $F_i = G_i = |i\rangle\langle i|$ for all i, then $\mathrm{Tr}[F_i G_x G_j G_y]$ and $\delta_{ix}\delta_{jy}\delta_{ij}$ become equivalent. To do this, however, renders the representation invalid as QPR. Such a frame fails to meet the criteria for a valid QPR framework for quantum theory. Indeed, it can be proven that no frame exists for which this equivalence holds (see [1]). These observations about inference capture a larger point: any attempt to formalize quantum theory as a classical probability framework ultimately loses tomographic completeness, rendering it inconsistent and invalid.

References

[1] C. C. Aw, K. Onggadinata, D. Kaszlikowski, and V. Scarani, "Quantum bayesian inference in quasiprobability representations," *arXiv preprint arXiv:2301.01952*, 2023.

[2] S. Watanabe, "Conditional probabilities in physics," *Progr. Theor. Phys. Suppl.*, vol. E65, pp. 135–160, Jan 1965.

[3] S. Watanabe, "Symmetry of physical laws. part iii. prediction and retrodiction," *Rev. Mod. Phys.*, vol. 27, pp. 179–186, Apr 1955.

[4] R. Jeffrey, *The logic of decision*. McGraw-Hill, 1965.

[5] E. T. Jaynes, *Probability Theory: The Logic of Science*. Cambridge University Press, 2003.

[6] M. S. Leifer and R. W. Spekkens, "Towards a formulation of quantum theory as a causally neutral theory of bayesian inference," *Phys. Rev. A*, vol. 88, p. 052130, Nov 2013.

[7] A. J. Parzygnat and F. Buscemi, "Axioms for retrodiction: achieving time-reversal symmetry with a prior," *arXiv preprint arXiv:2210.13531*, 2022.

[8] D. Petz, "Sufficient subalgebras and the relative entropy of states of a von neumann algebra," *Comm. Math. Phys.*, vol. 105, pp. 123–131, 1986.

[9] D. Petz, "Sufficiency of channels over von Neumann algebras," *The Quarterly Journal of Mathematics*, vol. 39, pp. 97–108, 03 1988.

[10] M. Wilde, "Recoverability in quantum information theory," *Proceedings of the Royal Society A*, vol. 471, p. 20150338, 2015.

[11] M. M. Wilde, "From classical to quantum shannon theory," *arXiv preprint arXiv:1106.1445*, 2011.

[12] K. Li and A. Winter, "Squashed entanglement, k-extendibility, quantum markov chains, and recovery maps," *Found. Phys.*, vol. 48, pp. 910–924, 2018.

[13] A. J. Parzygnat and J. Fullwood, "From time-reversal symmetry to quantum bayes' rules," 2022.

[14] H. Kwon and M. S. Kim, "Fluctuation theorems for a quantum channel," *Phys. Rev. X*, vol. 9, p. 031029, Aug 2019.

[15] F. Buscemi and V. Scarani, "Fluctuation theorems from bayesian retrodiction," *Phys. Rev. E*, vol. 103, p. 052111, May 2021.

[16] C. C. Aw, F. Buscemi, and V. Scarani, "Fluctuation theorems with retrodiction rather than reverse processes," *AVS Quantum Science*, vol. 3, no. 4, p. 045601, 2021.

[17] C. Ferrie and J. Emerson, "Framed hilbert space: hanging the quasi-probability pictures of quantum theory," *New Journal of Physics*, vol. 11, no. 6, p. 063040, 2009.

[18] C. Ferrie, "Quasi-probability representations of quantum theory with applications to quantum information science," *Reports on Progress in Physics*, vol. 74, no. 11, p. 116001, 2011.

[19] C. Ferrie and J. Emerson, "Frame representations of quantum mechanics and the necessity of negativity in quasi-probability representations," *Journal of Physics A: Mathematical and Theoretical*, vol. 41, no. 35, p. 352001, 2008.

Robustness measures for quantifying nonlocality

Kyunghyun Baek[1 2] Junghee Ryu[2] Jinhyoung Lee[3 *]

[1] *Electronics and Telecommunications Research Institute, Daejeon 34129, Republic of Korea*
[2] *Division of National Supercomputing, Korea Institute of Science and Technology Information, Daejeon, 34141, Korea*
[3] *Department of Physics, Hanyang University, Seoul, 04763, Republic of Korea*

Abstract. In this work, we suggest general robustness for quantifying nonlocality and investigate all types of robustness measures, i.e., white-noise, standard, and general robustness measures. As a result, we show that white-noise robustness does not fulfill monotonicity under local operation and shared randomness, while others obey it. To compare monotones, we introduce the concept of inequivalence, indicating a behavior in which the order relationship is reversed according to the choice of monotones. From the operational point of view, the inequivalence of monotones for quantum objects implies no existence of free operations connecting them. By applying this concept, we find that standard and general robustness measures are inequivalent between even and odd dimensional systems up to eight when we share the maximally entangled state and randomly perform the optimal, so-called CGLMP measurement settings.

Keywords: AQIS, template

1 Introduction

Robustness measures have been used to quantify nonlocality by the minimal noises that nonlocal correlations can withstand before becoming local. According to the type of noises, robustness measures are classified into so-called white-noise and standard [1] robustness measures that quantify the tolerance to the addition of white and local noises, respectively. These robustness measures provide operational meanings, i.e., how long the nonlocal correlations withstand in realistic noises such as detector efficiencies.

In this work, we suggest general robustness that quantifies the tolerance to adding no-signaling noises, and we investigate all types of robustness measures, i.e., white-noise, standard, and general robustness measures, for quantifying nonlocality from the resource-theoretical point of view. The standard and the general robustness measures fulfill the monotonicity, which is a required property such that a quantifier monotonically decreases under free operations. However, we show that the white-noise robustness does not fulfill the monotonicity by presenting counter-examples in which it increases under local operations and shared randomness. This behavior occurs due to the dependence of the white-noise model on the dimension because LOSRs allow increasing the number of outcomes in post-processing.

We also introduce the concept of inequivalence to compare the standard and general robustness measures systematically. We define inequivalence as a behavior such that two monotones provide different order relations when we compare two quantum objects by them. Namely, one of two monotones tells us that a quantum object has larger resources than another, while another one tells us that another quantum object is larger than the one. Additionally, we show that an inequivalent behavior implies no existence of free operations connecting quantum objects. This concept can provide a systematic method to numerically investigate different behaviors of monotones, while monotones have been studied from the axiomatic point of view. Applying it to our framework, we find that the standard and the general robustness measures are inequivalent for cases where sharing the maximally entangled state and randomly performing the optimal CGLMP measurement settings up to dimension 8. We further extensively investigate inequivalent behaviors for 2- and 3-dimensional cases for arbitrary states.

*hyoung@hanyang.ac.kr

2 Robustness measures

2.1 Previous robustness measures

Various robustness measures were adopted to investigate nonlocal correlations affected by specific noises from an operational point of view. First of all, *white-noise robustness* was introduced to investigate the effects of dephasing noises, defined as the minimal white-noise that nonlocal correlations disappea. It can be formulated as follows,

$$R_{wn}(\vec{p}) = \min\Big\{ r \geq 0 \Big| \frac{\vec{p} + r_{wn}\vec{p}_{wn}}{1 + r_{wn}} \in \mathcal{L} \quad \text{for } \vec{p}_{wn} = \left(\frac{1}{m_A m_B}, ..., \frac{1}{m_A m_B} \right)^T \Big\},$$

where m_A (m_B) is the number of outcomes for Alice's (Bob's) measurement settings. The uniform vector $\vec{p}_{wn}$ is a $4m_Am_B$-dimensional vector corresponding to a joint probability distribution such that possible outcomes are measured with equal probability because of the white-noise effect.

More strictly, another robustness is defined as the minimal addition of local noises that vanish nonlocal correlations [1]. This type of robustness can be understood as a *standard robustness* in the framework of the general resource theory [2], which is defined as a minimal addition of free (local) objects to a resourceful (nonlocal) object before vanishing its resource (nonlocality). It is

formulated as

$$R_S(\vec{p}) = \min\left\{ r_s \geq 0 \middle| \frac{\vec{p} + r_s \vec{p}_l}{1 + r_s} \in \mathcal{L} \text{ for } \vec{p}_l \in \mathcal{L} \right\}.$$

The minimal value r_s is related to the maximal possible violation $\nu = 2r + 1$ by $\vec{p}$ of a Bell inequality, defined as

$$\nu = \max_{\vec{s}} \frac{|\vec{s} \cdot \vec{p}|}{\max_{\vec{q} \in \mathcal{L}} |\vec{s} \cdot \vec{q}|}.$$

This relationship corresponds to the one found in general convex resource theories in which the standard robustness has an operational meaning as the exact quantifier of maximum advantage in discrimination tasks [2].

2.2 General robustness

Together with the standard robustness, *general robustness* is widely used in resource theoretical frameworks, defined as the minimal addition of general objects to a resourceful object. Applying it to the resource theory of nonlocality, we define the general robustness in the following way,

$$R_G(\vec{p}) = \min\left\{ r_g \geq 0 \middle| \frac{\vec{p} + r_g \vec{p}_{ns}}{1 + r_g} \in \mathcal{L} \text{ for } \vec{p}_{ns} \in \mathcal{NS} \right\}.$$

These robustness measures are selectively adopted according to their properties in specific resource theories. For instance, in the resource theory of entanglement, standard robustness was suggested first and then extended to general robustness. On the other hand, in the resource theory of coherence, the general robustness is only studied intensively because the standard robustness always gives infinite values for resourceful (coherent) states [2].

We reformulate all robustness measures mentioned above to canonical form of linear programming.

3 Non-monotonicity of white-noise robustness

From the resource theoretical point of view, a quantifier should satisfy (i) faithfulness, i.e., a quantifier should vanish if and only if the object is free, and (ii) monotonicity, i.e., a quantifier should monotonically decrease under any free operations (LOSRs in our framework). By definition, it is straightforward to see that all robustness measures hold the faithfulness. Furthermore, it was shown that standard and general robustness measures fulfill the monotonicity in any convex resource theories. [2] However, the monotonicity of white-noise robustness is not guaranteed in general.

To examine the monotonicity of R_{wn}, we find counterexamples that exhibit the increase of R_{wn} under LOSRs. Let us consider so-called output operations as a class of LOSRs that allow one to artificially merge or enlarge possible measurement outcomes as described in [3]. Output operations cannot generate a nonlocal correlation from a correlation admitting LHV model. As a particular case, we assume that $\mathcal{E}_k$ is an output operation that adds k more outcomes to each measurement setting and assigns zero probability to added outcomes, such that

$$p_k(a_x, b_y|x, y) = \begin{cases} p(a_x, b_y|x, y) & \text{for } a_x \leq m_A \text{ and } b_y \leq m_B \\ 0 & \text{for } k \geq a_x > m_A \text{ or } k \geq b_y > m_B \end{cases}$$

where $p_k(a_x, b_y|x, y)$ is the joint probability consisting of $\mathcal{E}_k(\vec{p})$.

In this case, the uniform vector $\vec{p}_{wn}$ should be modified accordingly because the white-noise is assumed to affect all possible outcomes uniformly. Namely, the white-noise effect can be broadened to enlarged outcomes, and as a result, nonlocal correlations can be more robust against white-noise. For instance, let us apply the above operations to $\vec{p}_{max}^{CHSH}$ giving the maximal violation of the CHSH inequality for $m_A = m_B = 2$. Then, applying $\mathcal{E}_k$ to it, we find out that the white-noise robustness strictly increases according to the number of added possible outcomes k. In contrast, the standard and general robustness measures are invariant, as shown in Fig. 1.

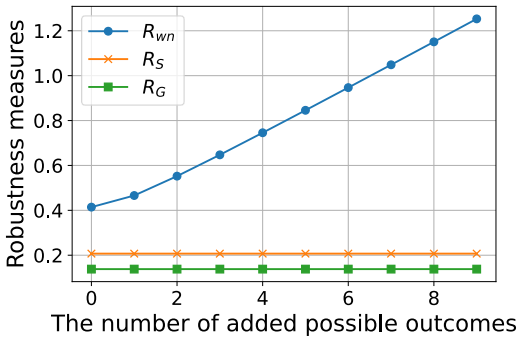


Figure 1: Non-monotonicity of white-noise robustness under LOSRs.

4 Inequivalence of robustness measures

In this section, we will define the inequivalence of monotones and provide extensive numerical investigations for inequivalence between the standard and general robustness measures.

4.1 Inequivalence of monotones

One of the main reasons we quantify resources is to investigate and compare the amount of resources quantitatively. However, even if quantifiers satisfy both faithfulness and monotonicity, they can show different behaviors when we compare the resourcefulness of objects.

Definition 1 (Inequivalence) *Quantifiers Q_1 and Q_2 are said to be inequivalent for objects o_1 and o_2, if there exists some objects o_1 and o_2 showing $Q_1(o_1) > Q_1(o_2)$ and $Q_2(o_1) < Q_1(o_2)$.*

Quantifiers satisfying the faithfulness and monotonicity are called *monotones* that decrease monotonically under free operations. This fact implies the following theorem.

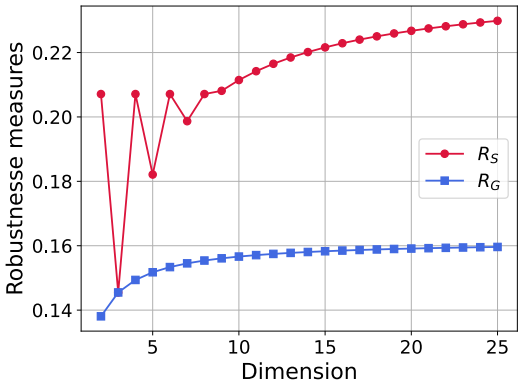


Figure 2: Standard and general robustness measures for sharing maximally entangled states and performing the optimal measurement setting for dimensions from $D = 2$ to 25. Inequivalence between standard and general robustness measures is observed between even and odd dimensions up to $D = 8$.

Theorem 2 *If some monotone Q_1 and Q_2 are inequivalent for objects o_1 and o_2, then no free operation can transform one into another.*

Proof. Any monotones are equivalent for objects that can be transformed by free operations from one to another. That is because if one can generate an object o_1 from o_2 via a free operation $\mathcal{F}$, i.e., $o_1 = \mathcal{F}(o_2)$, then any monotones Q should provide equivalent relations such that $Q(o_1) \geq Q(o_2)$ according to the monotonicity. As we take the contraposition of the statement, the theorem is proved. □ In general, it is not straightforward to prove whether it is possible to transform an object into another by a free operation. According to the theorem, however, the inequivalence of two objects allows one to confirm no existence of free operations connecting given objects. In our framework, if monotones such as the standard and general robustness measures are inequivalent for vectors $\vec{p}_1$ and $\vec{p}_2$, then there is no LOSR $\mathcal{E}$ satisfying $\mathcal{E}(\vec{p}_1) = \vec{p}_2$ or $\mathcal{E}(\vec{p}_2) = \vec{p}_1$. However, we note that equivalence for $\vec{p}_1$ and $\vec{p}_2$ does not imply the existence of a LOSR connecting them.

To examine the inequivalence of monotones Q_1 and Q_2 for many objects simultaneously, one can plot Q_1 against Q_2. Then, on the basis of the interested object o_0, any objects located on the upper right- and lower left-hand corners are equivalent, while objects located on the upper left- and lower right-hand corners are inequivalent. We will apply this method to investigate the inequivalence of standard and general robustness measures in the following.

4.2 Inequivalence of robustness measures

We would like to explore the difference between robustness measures R_S, R_G as investigating their inequivalence in specific examples. Let us assume that Alice and Bob share a maximally entangled state

$$|\Psi_d\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=,0,\ldots,d-1} |ii\rangle_{AB}.$$

Then Alice and Bob randomly perform measurements A_x for $x = 1, 2$ and B_y for $y = 1, 2$ having the nondegenerate eigenstates in D-dimensional Hilbert space, respectively,

$$|k\rangle_{A,x} = \tag{1}$$
$$\begin{cases} \frac{1}{\sqrt{d_{\text{eff}}}} \sum_{j=0}^{d_{\text{eff}}-1} \exp\left(i\frac{2\pi}{d_{\text{eff}}} j(k+\alpha_x)\right) |j\rangle_A & \text{for } k < d_{\text{eff}} \\ |k\rangle_A & \text{for } d_{\text{eff}} \leq k < D \end{cases}$$
$$|l\rangle_{B,y} =$$
$$\begin{cases} \frac{1}{\sqrt{d_{\text{eff}}}} \sum_{j=0}^{d_{\text{eff}}-1} \exp\left(i\frac{2\pi}{d_{\text{eff}}} j(-l+\beta_y)\right) |j\rangle_B & \text{for } l < d_{\text{eff}} \\ |l\rangle_B & \text{for } d_{\text{eff}} \leq l < D \end{cases}$$

with effective dimension d_{eff}, where $\alpha_1 = 0, \alpha_2 = 1/2$, $\beta_1 = 1/4$, and $\beta_2 = -1/4$. The above measurement settings for $d_{\text{eff}} = D$ are used in as optimal measurements for the maximal Bell violation obtained from numerical investigations. We introduce the effective dimension to consider more general cases such that the optimal measurements are performed on the partial space while eigenstates in another partial space are the same.

In the above settings, d and d_{eff} correspond to the amount of entanglement of $|\Psi_d\rangle_{AB}$ and incompatibility of measurement settings, respectively. Intuitively, one can expect that higher entanglement and incompatibility may lead to more nonlocality due to this scenario. The general robustness increases monotonically for $d = d_{\text{eff}} = D$ from 2 to 25. However, the standard robustness is invariant at 0.207107 for even dimensions up to $D = 8$, while it increases for odd dimensions from 0.145489 to 0.198678 up to $D = 7$ as shown in Fig. 2. Thus, they show inequivalence with the increase of dimensions up to eight. As a result, one can confirm that no LOSR operation transforms probability vectors from odd to even dimensional cases and vice versa. This result is a counter-intuitive behavior, compared to the case that entangled state can be transformed from $|\Psi_d\rangle$ to $|\Psi_{d'}\rangle$ for $d > d'$ via local operations and classical communications.

References

[1] M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, and M. M. Wolf, Phys. Rev. Lett. 104, 170405 (2010)

[2] R. Takagi and B. Regula, Phys. Rev. X 9, 031053 (2019)

[3] J. I. de Vicente, Journal of Physics A: Mathematical and Theoretical 47, 424017 (2014)

Chracterizing genuine nonlocality in the square network

Jeonghyeon Shin[1 2] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Korea*
[2] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 02447, Korea*

Abstract. Bell nonlocality is a fundamental concept in quantum mechanics, highlighting the distinction between the classical and quantum worlds. While the standard Bell scenario assumes a single source to distribute particles to multiple parties, the network nonlocality considers independent multiple sources based on the network configuration. The correlations in such network scenarios fundamentally differ from the standard Bell scenario. Without relying on the standard Bell scenario, a quantum distribution that does not admit the trilocal model can be shown to exist in the triangle network. Based on the token-counting strategy, such distribution can be extended to a larger class of networks beyond the triangle network. In this work, we investigate the distribution in the square network by the token counting strategy and compare its characteristics with the triangle distribution in network.

Keywords: Network nonlocality, Square network

1 Introduction

Bell nonlocality is one of the most fundamental discovery in quantum mechanics [1], which reveals a separation between the classical and quantum world. The nonlocal correlation violates a Bell inequality formulated under the local hidden variable model. In the standard Bell experiment, a single source is assumed to distribute particles to multiple parties and then each party measures the respective system of the particle independently depending on their inputs. It is known that the set of correlations compatible with local hidden variable model becomes convex set and can be characterized in terms of a polytope structure [2]. Consequently, in the standard Bell scenario, we can bound local correlations using linear inequalities, commonly known as Bell inequalities.

However, in practical applications of quantum nonlocal correlations in network, more than one source are normally necessary to distribute the correlation over long distance, e.g., by using entanglement swapping [3]. This inspires the study of totally different concept of nonlocal correlation in network scenario with more than one independent source. Unlike standard Bell scenario, the correlations in a network compatible with local hidden variable model does not correspond to a convex set, so it is difficult to characterize the correlation generated in the network scenario.

Various attempts have been made on simple quantum network where there are three parties. An one of the interesting networks is triangle network where all three parties are connected by three independent sources. While an early study on the nonlocality in the triangle network turned out to be fundamentally compatible with standard Bell nonlocality, a recent work by Renou *et al.* demonstrated the genuine triangle network nonlocality [4]. In this scenario, three parties performs fixed measurements without inputs, to yield a fundamentally different form of nonlocality from the standard Bell scenarios. The nonlocality in the trangle network was proved without tracing back to the standard Bell inequality violation.

In this work, we will review several methods to investigate the genuine nonlocality in the triangle network, and employ them to extend the genuine nonlocality to the square network. Especially, we will investigate the distribution in the square network by the token counting strategy and compare its characteristics with the triangle distribution in network for further generalization.

2 Genuine quantum nonlocality in the triangle network

We first review the method to demonstrate the genuine network nonlocality in the triangle scenario in Ref. [4]. In the triangle network, three separate parties are connected by three independent bipartite sources in pairwise yielding outputs a, b and c without inputs. Since there are no inputs, the distribution is given by the joint probability distribution $P(a, b, c)$. We call the distribution as trilocal correlation if it admits the form

$$P(a,b,c) = \int d\alpha d\beta d\gamma P_A(a|\beta,\gamma) P_B(b|\gamma,\alpha) P_C(c|\alpha,\beta), \tag{1}$$

where $\alpha \in X, \beta \in Y$ and $z \in Z$ are the three local variables distributed by each source and P_A, P_B, P_C represent probability distribution from each party conditioned on their suitable choice of local variables.

The family of distributions analyzed in Ref. [4] can be obtained by the following quantum protocol. Each independent source distributes maximally entangled Bell state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle))$ between two parties. Each party then performs a projective measurement on their own system in the same basis yielding possible four outcomes, labled by $\{\uparrow, \downarrow, \chi_0, \chi_1\}$. The basis is given by

$$\begin{aligned} |\downarrow\rangle = |00\rangle\,, \quad |\uparrow\rangle = |11\rangle\,, \\ |\chi_0\rangle = u_0\,|01\rangle + v_0\,|10\rangle\,, \quad |\chi_1\rangle = u_1\,|01\rangle + v_1\,|10\rangle \end{aligned} \tag{2}$$

with real number $\cos\theta = u_0 = -v_1$, $\sin\theta = u_1 = v_0$. For symmetry reason, θ is in the range $(0, \frac{\pi}{4}]$ without loss of generality.

*swleego@gmail.com

The idea of distribution can be generally understood as the token counting strategies as the state $|01\rangle$ represents a token being sent to right and the state $|10\rangle$ represents a token being sent to be left. Thus, the outcome $\downarrow, \uparrow$ and $\chi = \{\chi_0, \chi_1\}$ can be interpreted that a party receives no token, one token and two tokens respectively. It is known that the classical token counting strategies in the triangle is rigid, meaning that there is essentially a unique classical strategy to simulate classical token counting strategies. Based on this, it was proved that the resulting quantum distribution does not admit trilocal model for $0.8860 \lessapprox \cos\theta < 1$ in Ref. [4].

More recently, it was shown in Ref. [5] that the distribution does not admit the trilocal model in an additional range, $0.7504 \leq \cos\theta \leq 0.81001$, extending the abovementioned result. Their approach consists of finding equivalent condition for four outcome distribution in the triangle network to admit trilocal model and then apply inflation technique [6], which is state-of-the-art method in network nonlocality field.

3 Token counting distribution in square network

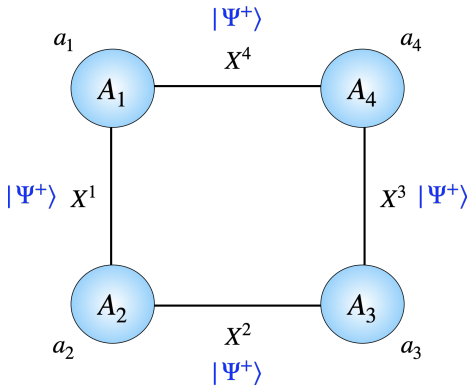


Figure 1: Setting of the square network. A_i denotes the four parties and $a_i \in \{\uparrow, \downarrow, \chi_0, \chi_1\}$ is outcome of each party. The set X_i denotes the local hidden variable source set connecting two parties as in the figure. For token counting distribution, we exploit four independent Bell states $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

The token counting strategy also holds in generic networks [7, 8]. One of the main results in Ref. [7] states that for no-double-common-source network, any classical strategy that simulates a token counting distribution in the given network is essentially a token counting strategy. In essence, they proved the existence of nonlocal distribution in the square network, token counting distributions, via the rigidity of the token counting strategy.

This motivates us to characterize the family of network nonlocal quantum distributions in the square scenario without violation of standard Bell inequality. We generate our token-counting distribution in the square network as described in Figure 1. Basically, the square scenario is an extension of the triangle scenario, where an additional person and one source are connected in a square structure.

The token counting distribution in square network is obtained as follows. First, four independent sources $|\psi^+\rangle$ distribute each system to the connected parties. Then the global state is

$$|\psi_{A_1,A_2,A_3,A_4}\rangle = \frac{1}{2^4}(|01\rangle + |10\rangle)^{\otimes 4} \ .$$

Next, each party performs the same projective measurement in Eq. (2) to their own systems. We denote the result joint distribution as $P_Q(a_1, a_2, a_3, a_4)$ and there are several properties that the distribution $P_Q(a_1, a_2, a_3, a_4)$ satisfies. Our goal is to find the range of the measurement parameter θ that makes the corresponding probability distribution $P_Q(a_1, a_2, a_3, a_4)$ is network nonlocal in the square scenario. To do so, we characterize the constraints for the 4-local correlation to satisfy the properties of the $P_Q(a_1, a_2, a_3, a_4)$.

4 4-local model in the square network

The 4-local model in the square network can be defined in a similar manner to the trilocal model. The 4-local model in the square network takes the form

$$P(a_1, a_2, a_3, a_4) = \int d\alpha^1 \cdots \int d\alpha^4 \times P_{A_1}(a_1|\alpha^4, \alpha^1) \cdots P_{A_4}(a_4|\alpha^3, \alpha^4) \ . \tag{3}$$

where $\alpha^i \in X^i$, $i = 1, \ldots, 4$ denote the four local variables distributed by each source and $P_{A_1}(a_1|\alpha^4, \alpha^1)$, $P_{A_2}(a_2|\alpha^1, \alpha^2)$, $P_{A_3}(a_3|\alpha^2, \alpha^3)$ and $P_{A_4}(a_4|\alpha^3, \alpha^4)$ represent arbitrary deterministic output functions from A_1, A_2, A_3 and A_4 respectively.

If we consider the coarse graining output set $\{\uparrow, \downarrow, \chi = \{\chi_0, \chi_1\}\}$, we observe the following lemma for the 4-local model compatible with $P_Q(a_1, a_2, a_3, a_4)$.

Lemma 1 *We consider the coarse graining of the output set $\{\uparrow, \downarrow, \chi = \{\chi_0, \chi_1\}\}$. The sources sets can be partitioned in two subsets of equal weight*

$$X^1 = X^1_0 \uplus X^1_1, \tag{4}$$

such that the sets from which the local variable α_1 is taken determine all outputs. More precisely, the followings hold.

$$\begin{cases} a_1 = \uparrow & \Leftrightarrow \quad , \alpha^4 \in X^4_0 \quad \alpha^1 \in X^1_1 \\ a_1 = \downarrow & \Leftrightarrow \quad \alpha^4 \in X^4_1, \quad \alpha^1 \in X^1_0 \\ a_1 = \chi & \quad \textit{otherwise.} \end{cases} \tag{5}$$

Similarly, the same holds for other remained parties with a direct orientation of the cycle.

From this fact, we can obtain the necessary condition for the $P_Q(a_1, a_2, a_3, a_4)$ admits the 4-local model. In detail, we obtain 5 parties distribution with binary outcome satisfying several conditions from θ depended probability distribution that admits 4-local model.

Lemma 2 *Let us introduce*

$$q(i_1, i_2, i_3, i_4, t) := 2^3 \times \quad (6)$$
$$p(a_k = \chi_{i_k},\ (\alpha^1, \ldots, \alpha^4) \in (X_t^1 \times \cdots \times X_t^4)).$$

If 4-local model simulates the $P_Q(a_1, \ldots, a_4)$, then $q(i_1, i_2, i_3, i_4, t)$ is a probability distribution. Moreover, the following marginal distributions of $q(i_1, i_2, i_3, i_4, t)$ satisfy:

$$\begin{aligned} q(i_1, i_2, i_3, i_4) &= \sum_t q(i_1, i_2, i_3, i_4, t) \\ &= \frac{(u_{i_1} u_{i_2} u_{i_3} u_{i_4} + v_{i_1} v_{i_2} v_{i_3} v_{i_4})^2}{2}, \end{aligned} \quad (7)$$

$$\begin{aligned} q(i_k, i_{k+1}, t = 0) &= \frac{(u_{i_k} u_{i_{k+1}})^2}{2}, \\ q(i_k, i_{k+1}, t = 1) &= \frac{(v_{i_k} v_{i_{k+1}})^2}{2}. \end{aligned} \quad (8)$$

Thus, our problem can be reduced to check when the $q(i_1, i_2, i_3, i_4, t)$ is not well defined. The well-definedness of the distribution q that is compatible with the 4-local model distribution p_Q imposes several constraints. The remaining part is to calculate the range of the parameter θ not satisfying such constraints. We present an approach that utilizes the inflation technique as a possible method.

References

[1] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195–200, 1964.

[2] A. Fine. Hidden Variables, Joint Probability, and the Bell Inequalities. *Phys. Rev. Lett.*, 48(5):291–295, 1982.

[3] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71(26):4287–4290, 1993.

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

[5] A. Pozas-Kerstjens, N. Gisin, and M.-O. Renou. Proofs of Network Quantum Nonlocality in Continuous Families of Distributions. *Phys. Rev. Lett.*, 130(9):090201, 2023.

[6] E. Wolfe, R. Spekkens, and T. Fritz. The Inflation Technique for Causal Inference with Latent Variables. *Causal Inference*, 7(2):20170020, 2017.

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

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

Building a certifiable source device independent quantum random number generator

Kaiwei Qiu[1] Yu Cai[1] * Nelly Ng[1] Jing Yan Haw[2]

[1] *School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore*
[2] *Centre for Quantum Technologies, National University of Singapore*

Abstract. Randomness, in particular trusted private randomness is an important resource for applications in cryptography. Quantum physics provides some natural ways to generate genuine randomness, however, the generation of certifiable randomness still meets various theoretical and technical challenges. Here, we experimentally implement a certifiable quantum random number generator, built with off-the-shelf optical and electronic components. The resulting device is compact and portable. Furthermore, its security makes no assumptions about the input light source, while its performance is constantly monitored by an integrated certification test.

1 Introduction

While physicists aim to predict the evolution of physical systems, quantum physics does not allow us to do so with infinite precision, due to the uncertainty principle. This unpredictability – randomness – lies at the core of quantum physics. Randomness is not something we always avoid, as it has its value in applications such as Monte Carlo simulation and cryptography. While pseudo randomness is sufficient for simulation purposes, it is not desirable in cryptography as it is generated in a deterministic manner. To achieve stronger security for such applications, we need to consider *true* randomness generators (TRNGs). In particular, studies [1, 2] have been devoted to the development of quantum random number generators (QRNGs), where the randomness is derived from quantum origin.

One advantage of QRNG is that it is certifiably private and secure, i.e. upon passing certain tests, one can be assured that the generated randomness is close to being uniformly random and independent from other systems. Depending on the assumptions based on which the security is derived, QRNGs can be categorised as device independent (DI) or device dependent (DD). The security of DI-QRNG [3, 4, 5, 6] is shown with minimum assumptions, nonetheless it requires more sophisticated (and therefore often costly), while achieving significantly lower key rates compared to device dependent ones. On the other hand, the fully DD regime relies on the ability to be sure that one maintains a high stability of the full experimental setup, which is also unwished-for. A way to overcome these challenges is to consider the intermediate regime of semi-DI, where one limits the amount of assumptions on the device. This often enables the usage of a simpler setup, while maintaining high key rates [7, 8, 9, 10, 11, 12, 13, 14], conditioned on the device passing the certification tests.

Semi-DI protocols often limit their device-dependencies either on the light source, or on the measurement setup. Recently, a notable source device independent (SDI) scheme was proposed in [15], where the measurement apparatus is fully trusted and no assumption about the incoming light source is made. In our work, following the scheme of [15], we built an optical SDI-QRNG with off-the-shelf components, and extended the security analysis to account for a more general setting of using unbalanced beamsplitters. We first present the detailed scheme with the main security claim in Section 2. Then Section 3 will cover the experimental setup and its performance. Finally, we conclude in Section 4.

*yu.cai@ntu.edu.sg

2 Theory of certifiable randomness generation

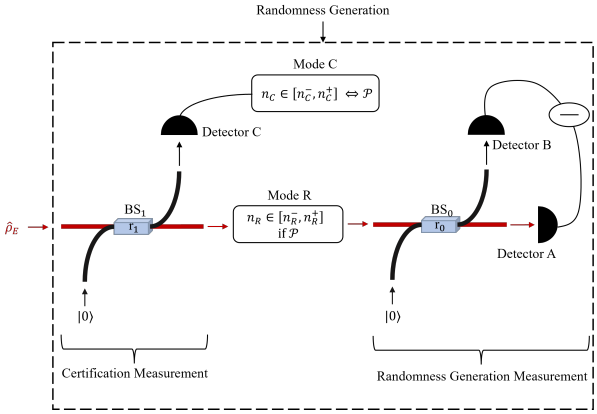


Figure 1: A schematic of the optical SDI-QRNG setup.

The source device independent quantum random number generator (SDI-QRNG) that we study and implement consists of two stages: a quantum randomness generation stage, and a classical randomness extraction stage. The randomness generation has three components: an input source, a certification measurement and a randomness measurement. Fig. 1 shows a schematic drawing of the setup, which can be described as follows [15]:

1. Light is emitted from an untrusted light source, enters mode E. This light is fully untrusted, hence in

principle, Eve has full control over how she would engineer the input state ρ_E such that she obtains as much information as possible about the final randomness generation.

2. The light reflected by BS_1 in mode C is subjected to the certification measurement. It passes if the photon number detected falls in a predetermined range $n_c \in [n_c^-, n_c^+]$.

3. The transmitted light in mode R is then subjected to the difference measurement at detector A and B. The difference $x = n_A - n_B$ is converted to a raw binary string X and sent for post-processing.

4. A final binary string is extracted from the raw string X, if the certification test is passed.

The generated randomness is quantified by the conditional min-entropy $H_{\min}(X|E)$ [16], which is the amount of private randomness present the string X given any external agent Eve's information:

$$H_{\min}(X|E) = -\log\left(\max_{\{\hat{E}_x\}_x} \sum_x p_x \operatorname{tr}\left(\hat{E}_x \hat{\rho}_E^x\right)\right) \quad (1)$$

Now we are ready to state the definition of a randomness generation protocol:
Definition 1: An $(m, \kappa, \epsilon_{\text{fail,m}}, \epsilon_C)$-certified randomness generation protocol produces an output X made of m measurement results such that

- Security: Either the certification test $\mathcal{P}$ fails, or

$$H_{\min}(X \mid E) \geq \kappa,$$

except with probability $\epsilon_{\text{fail,m}} \leq m\epsilon_{\text{fail}}$.

- Completeness: There exists an honest implementation such that the test will be passed with probability $1 - \epsilon_C$.

where ϵ_{fail} is the upper bound probability over all possible input state $\hat{\rho}_E$ such that the photons in mode R falls outside the range $[n_R^-, n_R^+]$ given that the photons in mode C passed the certification test $\mathcal{P}$ with probability $1 - \epsilon_C$.

By modelling the photodetectors as number measurement converting to voltage, smearing with noise, finite dynamic range and finite bin size, a realistic and practical source-independent protocol can be defined, requiring only an optical setup consisting of

- Two trusted vacuum modes,
- Two beamsplitters of reflectivity r_0 and r_1,
- Two noisy photodetectors used to make a difference measurement, and
- A third noisy photodetector used to make a certification measurement which passes the test $\mathcal{P}$ if v_i falls in a chosen range $\left[v_{i_-}^-, v_{i_+}^+\right]$.

These optical elements can be used as a certified $(m, \kappa, \epsilon_{\text{fail,m}}, \epsilon_C)$-randomness generation protocol as per the Definition 1 without making any assumptions about the input source. The analysis of Ref. [15] shows how one may derive the lower bound on min-entropy, κ, as a function of the reflectivity r_0, and parameters n_R^-, n_R^+. The parameters n_R^-, n_R^+ are intricately tied to various intermediate parameters, ultimately giving rise to bounds on the total completeness and security error. These technical details are omitted from this extended abstract. We extend the lower bound on κ derived from Ref. [15] to the case where r_0 in Fig. 1, i.e. the reflectivity of the beamsplitter used in the difference measurement is also unbalanced in general.

3 The experiment and results

3.1 Experimental Implementation

In our setup, a Koheron LPD100 board consists of a laser source (Koheron LD101), operating at $\lambda = 1550$nm, and a balanced photodetector (Koheron PD100B-AC), which used for the randomness generation measurement (detector A & B in Fig. 1). At the certification measurement, Detector C is a single photodetector that is DC coupled (Koheron PD100). The reflectivity for the certification and the randomness generation measurement are $r_1 = 0.109$ (89.1:10.9) and $r_0 = 0.51$ (51:49) respectively. Note that as compared to [15], we have considered a case of non-perfect 50:50 beamsplitter, i.e. $r_0 \neq 0.5$, which is a realistic and practical scenario. Signals from the detectors are acquired and processed by a compact software defined instrument, RedPitaya (STEMlab 125-14).

An honest implementation using coherent light passes the certification test with probability $1 - \epsilon_C = 99.5\%$, with the voltage thresholds v_i chosen accordingly. To achieve a string of random numbers with a security parameter $\epsilon = 5 \times 10^{-10}$, the relevant parameters, such as block size and hashing failure probability, have to be carefully chosen by considering the experimental realisation, for instance the sampling speed and FPGA memory size. This results in a certified min-entropy of $\kappa/m = 1.41$ bits per sample.

In our proof-of-concept implementation, 11.41Mb of certified raw random bits was acquired in $\approx$ 49.8 seconds, translating to an experimental randomness generation rate of $\approx$ 229kb/s. We further tested the randomness extraction over the RedPitaya board, whereby a total of $\approx$ 875.6kb certified random bits were extracted at a rate of 1.21kb/s. We remark that this is due to the limitations and not utilising the FPGA feature, since the hashing was performed by Python programming, which is left as the future work. The resulting random numbers successfully passed the NIST tests as demonstrated in Table 1.

3.2 Using untrusted light

To test if our implementation fulfills its intended purpose, we further execute the protocol by changing the input to a different, untrusted light source, with the same optical power as input and keeping the rest of the setting as before. The protocol is executed successfully, where

Table 1: NIST statistical test suite results

NIST Test		
Test Name	p-value	Result
Freq. Test (Monobit)	0.56225	Random
Freq. Test within a Block	0.09076	Random
Run Test	0.80878	Random
Longest Run of 1's in a Block	0.57095	Random
DFT (Spectral) Test	0.26461	Random
Cummul. Sums (Forward) Test	0.69203	Random
Cummul. Sums (Reverse) Test	0.45584	Random

the collected samples passed the test $\mathcal{P}$ with a probability of 99.4%. By running the protocol with real-time extraction, a total of 874.8 kb of certified real-time random numbers are extracted at a rate of 1.20 kb/s. These random numbers also successfully passed the NIST tests in Table 1.

3.3 Light injection attack

To verify the robustness of the protocol under an eavesdropper attack, we also implemented the situation where the SDI-QRNG is under attack by Eve, who tampers with the original light source, $\hat{\rho}_H$ by injecting an additional light source, $\hat{\rho}_E$ alongside the original incoming beam. This is similar to the injection attack of QKD devices [19]. With a beamsplitter BS_E with reflectivity $r_E = 0.0097$, $\hat{\rho}_H$ and $\hat{\rho}_E$ were mixed at $\approx 99:1$ and sent into mode E as the input to the QRNG.

As shown in Fig. 2, when Eve's optical power (that governs $\hat{\rho}_E$) increases, we observe that the certification responds to the attack by showing a decrease in the length of the random bits extracted. This decrease in response starts slowly, but becomes rapid when Eve's input is around 0.0050mW, and the number of extracted bits reaches zero after 0.0125mW of optical power from Eve's attack. This shows that the protocol responds well to such light injection attacks, by producing lesser certified random numbers as the malicious party increasingly tampers with the light source.

4 Discussion and Outlook

In this work, we showed that a full SDI-QRNG device, consisting of the light source, measurement devices and real-time extraction, can be built solely from cost-effective, off-the-shelves components. Remarkably, the protocol does not require any trust on the light source and certifiable, thus allowing for easy integration as a subsystem in an (optical) quantum technological platforms. This source-agnostic feature is well verified and demonstrated concretely in our experiments, where a direct swap of the light source and an explicit attack via light injection are carried out. A further optimization of our implementation would pave the way in creating a cost-effective, high-bitrate, portable SDI-QRNG, serving e.g. as a local randomness beacon for purposes of cryptography and quantum communication protocols.

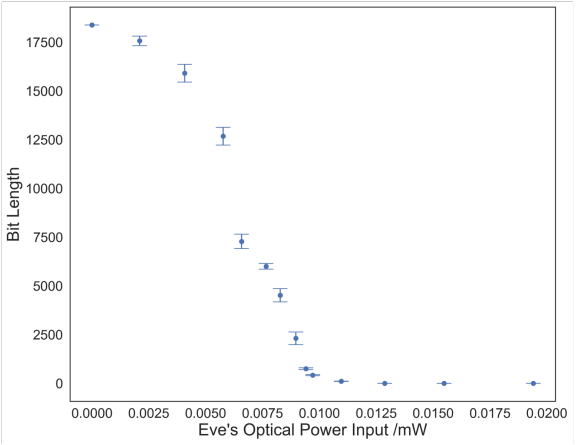


Figure 2: SDI protocol with externally injected, untrusted light source.

Acknowledgments

The authors would like to thank Nathan Walk for useful discussions. This research is supported by the National Research Foundation, Singapore and A*STAR under its Quantum Engineering Programme (NRF2021-QEP2-04-P01), and by the start-up grant for Nanyang Assistant Professorship of Nanyang Technological University, Singapore.

References

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum Random Number Generation, npj Quantum Inf. 2, 16021, 2016.

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum Random Number Generators, Rev. Mod. Phys. 89, 015004, 2017.

[3] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning et al., Random Numbers Certified by Bell's Theorem, Nature (London) 464, 1021, 2010.

[4] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, . Christensen, S. W. Nam et al., Experimentally Generated Randomness Certified by the Impossibility of Superluminal Signals, Nature (London) 556, 223, 2018.

[5] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Yu.-H. Li, L.-K. Chen, H. Li et al., High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole, Phys. Rev. Lett. 120, 010503, 2018.

[6] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan et al., DeviceIndependent Quantum Random-Number Generation, Nature (London) 562, 548, 2018.

[7] Z. Cao, H. Zhou, and X. Ma, Loss-Tolerant MeasurementDevice-Independent Quantum Random Number Generation, New J. Phys. 17, 125011, 2015.

[8] A. Chaturvedi and M. Banik, Measurement-Device–Independent Randomness from Local Entangled States, Europhys. Lett. 112, 30003, 2015.

[9] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Experimental Measurement-DeviceIndependent Quantum Random-Number Generation, Phys. Rev. A 94, 060301(R), 2016.

[10] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, Phys. Rev. X 6, 011020, 2016.

[11] M. Pawłowski and N. Brunner, Semi-Device-Independent Security of One-Way Quantum Key Distribution, Phys. Rev. A 84, 010302(R), 2011.

[12] T. Lunghi, J. Bohr Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, SelfTesting Quantum Random Number Generator, Phys. Rev. Lett. 114, 150501, 2015.

[13] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-Device-Independent Framework Based on Natural Physical Assumptions, Quantum 1, 33, 2017.

[14] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Applied 7, 054018, 2017.

[15] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified Quantum Random Numbers from Untrusted Light, Phys. Rev. X, 10, 041048, 2020

[16] R. Konig, R. Renner, and C. Schaffner. “The operational meaning of min-and max-entropy”. In: IEEE Transactions on Information theory 55.9, pp. 4337–4347, 2009.

[17] K. Marton and A. Suciu. “On the interpretation of results from the NIST statistical test suite”. In: Science and Technology 18.1, pp. 18–32, 2015.

[18] Lijiong Shen et al. “Randomness extraction from bell violation with continuous parametric down-conversion”. In: Physical review letters 121.15, p. 150402, 2018.

[19] Pang, Xiao-Ling et al. ”Hacking quantum key distribution via injection locking”. In: Physical review applied 13, 3, 034008, 2020.

Optimizing Quantum Integer Factorization Performance: A Scalable Evaluation Approach with Parameter Pre-Selection Method

Junseo Lee[1] * Kibum Bae[1] Chang-Nyoung Song[1] Hyunchul Jung[1]

[1] *Norma Inc.*

Abstract. As quantum technologies continue to advance, the performance of quantum computing simulators has reached a mature stage. However, the potential threat posed by quantum computing to cybersecurity necessitates a thorough assessment of its practical implications. This research presents a scalable evaluation approach for measuring the time required for integer factorization using Shor's algorithm [1] in a gate-based quantum computing simulator called simulator_mps. Furthermore, the study investigates the impact of parameter pre-selection in Shor's algorithm. Specifically, the pre-selection technique ensures a higher success rate of integer factorization with a reduced number of iterations, enabling efficient performance measurement under fixed conditions. A comparative analysis against random parameter selection demonstrates that the pre-selection of parameters enables scalable evaluation of integer factorization with improved efficiency.

Keywords: Quantum technologies, Quantum computing simulators, Integer factorization, Shor's algorithm, Parameter pre-selection

1 Introduction

Advancements in quantum computing have sparked interest in quantum information theory and the potential for solving complex problems. However, there are concerns about the impact of quantum technologies on cybersecurity, as traditional cryptographic algorithms are vulnerable to attacks using quantum algorithms like Shor's algorithm for factorization. Previous research has focused on evaluating quantum algorithms in specific scenarios using simulations, limiting the understanding of the threat posed by quantum computing. This study addresses these limitations by evaluating Shor's algorithm in a gate-based quantum computing environment, using an IBM platform and a pre-selection technique for random parameters. This scalable evaluation approach provides insights into the performance of the algorithm across a wide range of input values, contributing to the development of quantum information science and enhancing our understanding of quantum phenomena.

Overall, this research aims to assess the practical implications of quantum computing on cybersecurity and explores the potential of gate-based quantum computing systems. By evaluating the performance of Shor's algorithm for factorization and considering the scalability of the evaluations, this study contributes to the advancement of quantum information science and enables reliable simulations of large-scale quantum systems.

2 Integer Factorization using Selected Parameter

2.1 Simulator Selection

The IBM quantum computing simulators are software tools that allow users to simulate the behavior of quantum computers on classical computers. These simulators are designed to provide accurate and efficient simulations of quantum circuits, enabling researchers and developers to test and refine their algorithms before running them on real quantum hardware. Table 1 summarizes the currently supported IBM simulators and the number of qubits they can handle, along with the theoretically breakable bits in the RSA scheme using Shor's algorithm.

IBM Simulator Type	Q	β
simulator_statevector	32	7
simulator_stabilizer	5000	1249
simulator_extended_stabilizer	63	15
simulator_mps	100	24
ibmq_qasm_simulator	32	7

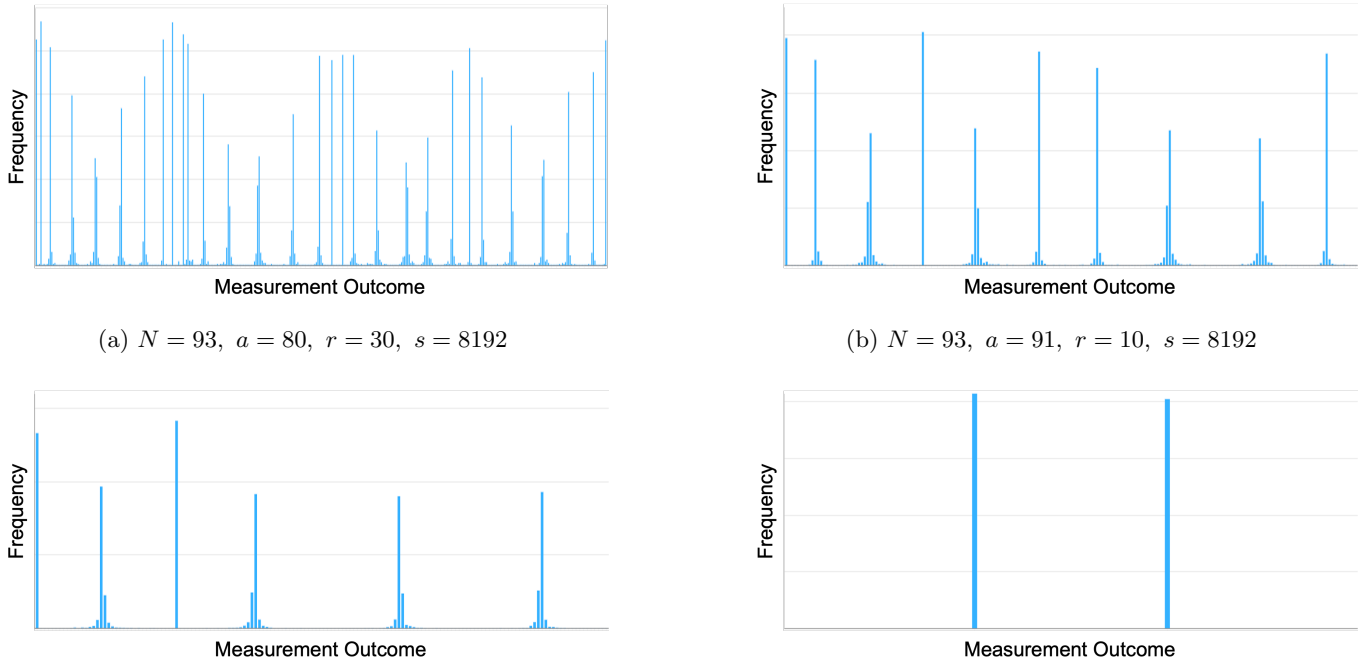
Table 1: Types of IBM simulators and theoretically breakable bits β depending on their supported qubits Q

This study specifically utilized the Matrix Product State (MPS) simulator provided by IBM for simulating quantum circuits. The MPS simulator represents quantum states using matrix products, enabling efficient simulation of circuits with a small number of qubits but many gates. With support for up to 100 qubits, it facilitated the evaluation of Shor's algorithm for integer factorization of numbers up to 24 bits. Notably, the simulator_mps tool also allowed for simulating noise and errors in quantum circuits, enabling analysis of their impact and the development of error mitigation strategies. In comparison, the simulator_stabilizer, which supports the most qubits, was limited to simulating Clifford gates and lacked support for non-Clifford gates essential to implementing Shor's algorithm effectively. Consequently, the simulator_mps proved to be the most suitable choice for the study's objectives.

2.2 Pre-selection of Parameters in Shor's Algorithm

The selection of random parameters plays a crucial role in the success of Shor's algorithm. Specifically, the choice

*js_lee@norma.co.kr



(a) $N = 93,\ a = 80,\ r = 30,\ s = 8192$

(b) $N = 93,\ a = 91,\ r = 10,\ s = 8192$

(c) $N = 93,\ a = 88,\ r = 6,\ s = 8192$

(d) $N = 93,\ a = 32,\ r = 2,\ s = 8192$

Figure 1: Simulation results of the quantum period-finding subroutine in Shor's algorithm when varying N, a, r

of a random parameter a in step 1 is of utmost importance for the algorithm to work efficiently. If we happen to select a random number that shares a common factor with the number N we want to factorize, then the greatest common divisor (GCD) computed in step 2 will be greater than 1. In this case, we can directly obtain a nontrivial factor of N. On the other hand, if we choose a random number that is coprime to N, the GCD will be 1, and we will rely on the quantum period-finding subroutine to determine the period r of the function $f(x) = a^x \bmod N$. Therefore, the success of the algorithm depends on the random selection of parameters and the probabilistic nature of quantum measurement.

The results obtained from the quantum period-finding subroutine in Shor's algorithm are represented as probability distributions based on measurement outcomes. Figure 1 illustrates these distributions. In an ideal noiseless quantum computer, the number of bars in the histogram would precisely correspond to the value of r. However, when using a noisy quantum simulator or quantum computer, errors are introduced, as depicted in the figures. Interpreting the experimental results can be challenging if an insufficient number of iterations is employed. It can be anticipated that larger values of r will require more iterations. For instance, when $r = 2$, the histogram will consist of only two bars, making it feasible to obtain the result of the quantum period-finding subroutine with a small number of iterations. Figures 1a to 1d demonstrate the factoring results of the value $N = 93$, with chosen values of a (80, 91, 88, and 32) that yield values of r equal to 30, 10, 6, and 2, respectively. Here, s represents the number of iterations, also referred to as the number of shots for the quantum circuit.

To facilitate scalable testing of Shor's algorithm, we pre-select a value of a that yields the minimum possible value of r ($r = 2$) instead of randomly choosing a. This approach helps maintain consistency in the testing process. To compare the time required for factorization using a quantum simulator as N increases while restricting a to the same value of r, Table 2 provides several values of a that result in $r = 2$ for actual semiprime N values. In order to measure the performance of the simulator under standardized conditions, the (N, a) pairs listed in the table are executed together instead of selecting a random a.

N	15	129	335	687	7617	9997
a	4	44	66	230	2540	768

Table 2: Examples values of a where $r = 2$.

3 Performance of Shor's Algorithm at Scale

In this section, we present the time required for integer factorization using Shor's algorithm on the IBM quantum computing simulator under two scenarios: preselection of parameter a and random selection of parameter a. The factorization times mentioned refer specifically to the time taken by the quantum period-finding subroutine.

3.1 Pre-selection of Parameter

Figure 2 illustrates the performance of Shor's algorithm in terms of the time required for integer factorization for various input values of N, when the parameter a is pre-selected. The graph shows a linear trend on

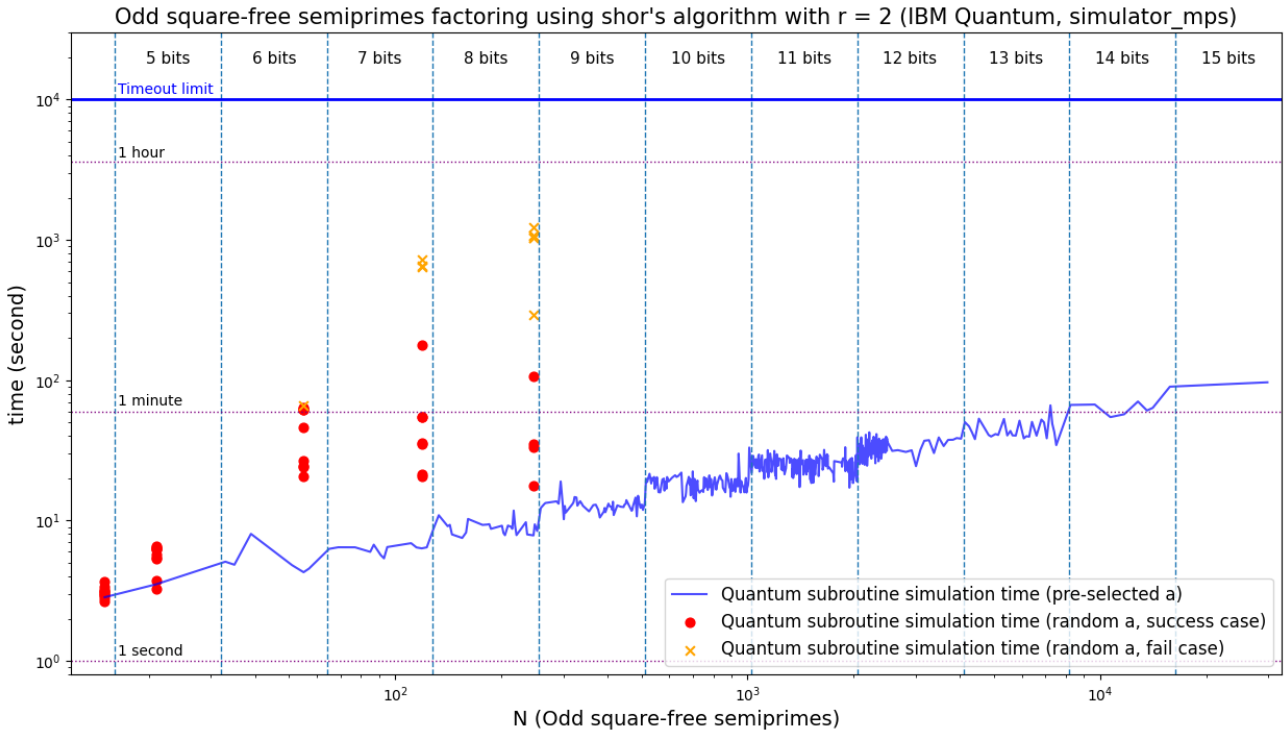


Figure 2: The result of quantum period-finding subroutine time of N using Shor's algorithm using IBM simulator. We successfully factorized all N values up to 15 bits when parameter a is pre-selected and depicted in line. In case of a is randomly selected, we partially succeed to factorize N up to 8 bits.

a log-log scale, indicating that the integer factorization time increases exponentially with the value of N. Although Shor's algorithm is theoretically expected to have a polynomial time complexity with respect to $\log N$, the simulation results on a quantum computer deviate from this prediction. However, the pattern remains consistent within the same number of bits, and a significant increase in the required time is observed as the number of bits increases. Figure 2 summarizes the results of our experimental findings.

One notable feature of the graph is that the performance measurement of integer factorization is scalable with respect to N. This means that the measurements were not limited to specific numbers but are applicable to all possible values of N, enabling the prediction of the time required for integer factorization for any given N. This scalability is highly significant as it allows for the assessment of the feasibility and time requirements of integer factorization for all possible values of N. Additionally, it is worth mentioning that all experimental results were obtained with a fixed number of shots (8 shots). When a is pre-selected with a minimum period of $r = 2$, 8 shots were sufficient to factorize all the given input numbers.

3.1.1 Random Selection of Parameter

When parameters are randomly chosen, the results show that the value of r (the period of the function) varies and may not always be sufficient for successful factorization. Even when successful, it often requires more iterations in the continued fraction algorithm. As a result, the performance of integer factorization varies across experiments. In contrast, when a is pre-selected, all N values were successfully factorized without any failures and with consistent performance.

3.1.2 Main Takeaway

Based on the comparative evaluation of integer factorization performance between pre-selection and random selection of parameters, it is concluded that pre-selecting a facilitates the measurement of quantum computing performance at scale. The choice of a significantly impacts the performance of Shor's algorithm as it determines the period of the function being evaluated. Therefore, careful selection of a is crucial, especially for input numbers with a large number of bits, where the function's period can be very large and the classical computation part becomes computationally expensive.

Acknowledgments

This work was partly supported by the National Research Foundation of Korea (NRF) through a grant funded by the Ministry of Science and ICT (NRF-2022M3H3A1098237).

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

Quantum target detection under single-mode Gaussian channel

Su-Yong Lee[1 2 *] Dong Hwan Kim[1] Yonggi Jo[1] Zaeill Kim[1] Duk Y. Kim[1]

[1] *Team Quantum, Agency for Defense Development, Daejeon 34186, South Korea*
[2] *Weapon Systems Engineering, ADD School, University of Science and Technology, Daejeon 34060, South Korea*

Abstract. Quantum target detection using entangled states is on the purpose of taking quantum advantage over the classical counterparts. When the target reflectivity is extremely smaller than 1, it is interesting to figure out if there exists the target or not. In a laboratory, a low-reflectivity target is simply replaced by a low-reflectivity beam splitter. Since environmental noise is unavoidable in the target detection protocol, it makes sense to consider vacuum noise in optical wave range and thermal noise in microwave range, together with loss. Here we investigate how single-mode Gaussian channel affects the performance of quantum target detection.

Keywords: Single-mode Gaussian channel, Quantum target detection, Quantum advantage

1 Introduction

Target detection is to shed a light on a spot and detect if a target exists or not. Quantum target detection was proposed with input entangled light, while beating the performance of input un-entangled light [1]. Since we are interested in figuring out if the target exists or not in a fixed range, it is quite similar to other quantum information topics, such as quantum channel discrimination and quantum state discrimination. They utilize the same performance evaluation methods as quantum Chernoff bound (QCB) and Helstrom bound. In a sense of figuring out a small difference of a physical parameter, it is close to quantum parameter sensing whose performance limit is given by quantum Cramer Rao bound using quantum Fisher information.

According to a target range, it is better to emit optical waves in a short range and microwaves in a long range. It is known that optical waves are dominantly affected by photon loss and microwaves are dominantly affected by thermal noise. At room temperature, there is about 10^{-7} of the mean photon number of thermal noise in the infrared regime(e.g.,400THz) and 600 of the mean photon number of thermal noise in the micrwave regime(e.g.,10GHz). In particular, due to thermal noise, there is no entanglement in the output state after interacting an input entangled state with the target. However the output states contain quantum correlation that includes quantum discord and beats classical correlation.

2 Results and Method

We consider single-mode Gaussian channels on signal and idler modes in quantum target detection, as shown in Fig. 1. The single-mode Gaussian channel consists of displacement and single-mode squeezing operations as well as loss and thermal noise. Since a two-mode squeezed vacuum (TMSV) state is a nearly optimal input state in the quantum target detection, we apply the Gaussian channels to the TMSV state.

First, we obtain that displacement operation provides better performance than single-mode squeezing operation in signal mode, irrespective of the signal mean photon number of the TMSV state and thermal noise [2]. For the idler mode, we ignore displacement and single-mode squeezing operations that are included in measurement step. The displacement operation is useful to boost the performance when we cannot increase a two-mode squeezing parameter in the initial TMSV state.

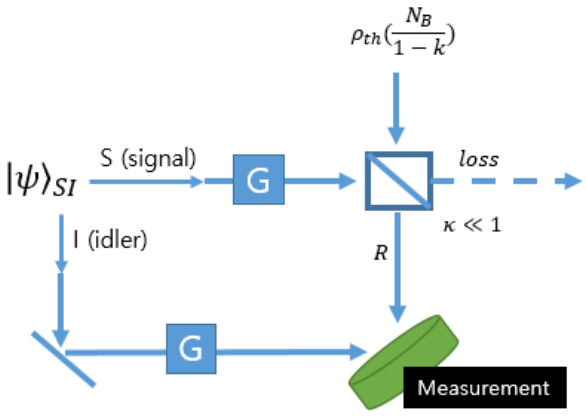


Figure 1: Quantum target detection with single-mode Gaussian channels on both modes. G represents a Gaussian channel, and κ is a target reflectivity. We assume that the mean photon number of thermal noise is much larger than one, i.e., $N_B \gg 1$. All the processes are in Gaussian regime.

Second, we obtain that single-mode squeezing operation on the idler mode can be useful to compensate loss and thermal noise in the ldler mode. However the overall performance is worse than the performance of the classical counterpart, i.e., coherent state. The result is independent of displacement operation before the loss and noise channels in the idler mode. Thus, it is the best to keep the idler mode without loss and noise.

Third, given a TMSV state as an input, we find the limit of an idler memory that takes quantum advantage over the coherent state. Let us assume that the idler memory consists of loss and thermal noise channels. Ac-

*suyong2@add.re.kr

cording to the mean photon number of thermal noise in the idler mode, we obtain the minimum transmittivity of the idler memory to observe quantum advantage. In a low signal mean photon number regime, it is allowed for more range in the transmittivity of the idler memory to have quantum advantage.

The performance is quantified with the detection error probability that is a sum of miss detection probability $P(\text{off}|\text{on})$ and false alarm probability $P(\text{on}|\text{off})$. Given a positive operator valued measure, we obtain the upper bound of the minimum error probability by QCB. A coherent state attains its QCB by homodyne detection, and a classically correlated (thermal) state attains its QCB [3] by photon number difference measurement after a 50 : 50 beam splitting operation. Both states achieve the bounds by local measurement. However a TMSV state approaches its QCB asymptotically by collective measurements [4]. Based on the QCB, quantum target detection using the TMSV state improves the error probability exponent by a factor of 4 over the classical counterparts [5]. Our results are based on the exponent of the QCB that represents the decay constant. We also develop that the decay constant is analytically calculated by using the covariance matric components and the first-order moments [2].

Acknowledgments - This work was supported by a grant to Defense-Specialized Project funded by Defense Acquisition Program Administration and Agency for Defense Development.

References

[1] S. Lloyd, Science **321**, 1463 (2008).

[2] D.H. Kim et al., arXiv:2302.07498.

[3] S.-Y. Lee et al., Phys. Rev. A **105**, 042412 (2022).

[4] Q. Zhuang, Z. Zhang, and J.H. Shapiro, Phys. Rev. Letts. **118**, 040801 (2017).

[5] S.H. Tan et al., Phys. Rev. Letts. **101**, 253601 (2008).

Asymmetric Quantum Secure Multi-Party Computation With Weak Clients Against Dishonest Majority

Theodoros Kapourniotis[1] * Elham Kashefi[2 3] † Dominik Leichtle[3] ‡ Luka Music[4] §
Harold Ollivier[5] ¶

[1] *Department of Physics, University of Warwick, Coventry CV4 7AL, United Kingdom*
[2] *School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[3] *Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, 4 Place Jussieu, 75005 Paris, France*
[4] *Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France*
[5] *DI-ENS, Ecole Normale Supérieure, PSL University, CNRS, INRIA, 45 rue d'Ulm, 75005 Paris, France*

Abstract. Secure multi-party computation (SMPC) protocols allow several parties that distrust each other to collectively compute a function on their inputs. In this paper, we introduce a protocol that lifts classical SMPC to quantum SMPC in a composably and statistically secure way, even for a single honest party. Unlike previous quantum SMPC protocols, our proposal only requires very limited quantum resources from all but one party; it suffices that the weak parties, i.e. the *clients*, are able to prepare single-qubit states in the $X - Y$ plane.

The novel quantum SMPC protocol is constructed in a naturally modular way, and relies on a new technique for quantum verification that is of independent interest. This verification technique requires the remote preparation of states only in a single plane of the Bloch sphere. In the course of proving the security of the new verification protocol, we also uncover a fundamental invariance that is inherent to measurement-based quantum computing.

Keywords: Quantum Verification, Delegated Computation, Secure Multi-Party Computation, Distributed Quantum Computing.

1 Motivation

Secure Multi-Party Computation (SMPC) protocols allow several parties who do not trust one another to collectively compute a function on their inputs. This question was first considered by Yao [36] and has been developed extensively in various settings (see [6] and references therein). Several security guarantees can be provided by such protocols depending on the setting: all parties can be on an equal footing, doing each their share of the computation, or one can handle the brunt of the computation while all others provide the data. In the first case, the security goal is to maximise the privacy of the data, while in the latter it extends to the privacy of the computation which is delegated to the server.

Practical computationally-secure protocols have been developed and implemented in commercial solutions for protecting classical multi-party computations. In the quantum case, several concrete protocols have been proposed (see § 2). In the circuit model, the state-of-the-art protocol [9] provides an information theoretic upgrade of classical SMPC that can withstand a dishonest majority. In the measurement-based model, where weakly quantum clients delegate their computation to a powerful server, the best protocol [25] does not provide verification of the computation and settles instead for blindness (i.e. privacy) of the data when there is no client-server collusion.

In this work, we show that this difference is not due to the asymmetry of the clients-server setting. We introduce for this specific situation a statistically secure lift of a classical SMPC protocol to a quantum one that provides blindness and verification for BQP computations. It remains secure so long as a single client is honest, thus withstanding possible collusions between dishonest clients and the server. Building on the techniques introduced in [22], its security is proved in the Abstract Cryptography (AC) framework. The protocol is highly modular and can tolerate a fixed amount of global noise during the quantum computation without aborting nor compromising statistical security. Additionally, it has no space overhead compared to an unprotected delegated computation, thereby allowing clients to use the server's full power to perform their desired computation, while security comes only at the price of a polynomial number of repetitions.

2 Related Work

Quantum SMPC is a long standing research topic in quantum cryptography, with several directions being explored in the past two decades. The first one started with [7]. Along with the introduction of the concept itself, it provided a concrete protocol for performing such computations in the quantum circuit model. This work has been later extended in [4], lowering the minimum number of honest players required for security to a strict majority.

The second focuses on the interesting edge case of two-party quantum computations. Several constructive results have been proposed in the circuit model. In [12], a protocol was introduced and proven secure for quantum honest-but-curious adversaries. This restriction on the

*t.kapourniotis@warwick.ac.uk
†ekashefi@inf.ed.ac.uk
‡dominik.leichtle@lip6.fr
§luka.music@quandela.com
¶harold.ollivier@inria.fr

adversaries was removed in [13] which proved security in the fully malicious setting and with negligible security bounds. The measurement-based model of quantum computation has also been considered for constructing secure two-party quantum computations as it provides a different set of tools than the circuit model. Verifiable Blind Quantum Computation (VBQC) first was introduced in [16] in this model, followed by optimised protocols [27, 21]. In [26] a protocol was proposed in this setting and proven secure against honest-but-curious adversaries. In [24] this result was extended to fully malicious adversaries with inverse-polynomial security using the Quantum Cut-and-Choose technique. More recently, a round-optimal protocol was given in [3] based on Oblivious Transfer and LWE, showing that two-party quantum computation tasks can be performed in as little as three rounds in the CRS model, and two if quantum pre-processing is allowed.

A third set of results focuses on the composability of such protocols, as earlier results didn't satisfy this property. Bit commitment was shown to be complete in the Quantum Universal Composability framework of [35], meaning that it is sufficient for constructing quantum or classical SMPC if parties have access to quantum channels and operations. This result was later extended in [14, 11].

More recently, building on these previous works, new concrete protocols have been proposed to decrease the restrictions on adversaries while also providing composable security. In the circuit model, a composably-secure protocol has been introduced in [9]. It is an extension of [13] that is able to cope with a dishonest majority, but which relies on a complete graph for quantum communication and on a large number of quantum communication rounds together with powerful quantum participants. In the MBQC model, [25] describes a protocol that is composable, can tolerate a dishonest majority and allows the clients to delegate the quantum computation to a powerful server. Its security is an information-theoretic upgrade of the classical SMPC primitive used for constructing the protocol. It is however limited by the absence of verifiability of outputs and the impossibility to tolerate client-server collusions. Other protocols have been proposed in alternative models or with different trust assumptions such as [20, 29]. Finally, recent protocols for secure delegated quantum computations can be run even by purely classical clients. These have been lifted to a multi-client setting in [2] while at the same time optimising the number of classical rounds of communication. This is however at the cost of a larger computation space on the server's device, which needs to be able to perform QFHE computations of functions large enough to be computationally-secure.

A subset of the authors proposed an earlier protocol for QSMPC [23] which comprised a blind pre-computation step meant to produce a resource state that could then be used to perform VBQC. This pre-computation turned out to be vulnerable to an attack that can be applied blindly by the server while having an effect only on some specific types of qubits thereby compromising security of the whole protocol. While the present work is a complete redesign of the protocol that shows improved performance, we include in § C of the full paper an in-depth analysis of the shortcommings of the previous construction. This might be a useful tool to revisit earlier work where a similar blind pre-computation step is used.

3 Overview of the Protocol and Results

In this paper, we consider the setting where several weakly quantum clients want to securely delegate their quantum computation to a powerful server. The proposed construction turns a single-client MBQC-based protocol into a multi-party one. More precisely, we use single-client Secure Delegated Quantum Computing (SDQC) protocols obtained through the techniques presented in [22]. Such protocols interleave several computation rounds and test rounds, the latter of which correspond to stabiliser measurements of the MBQC resource graph-state used to perform the computations. In such a protocol, the client must perform two different tasks. First, it has to prepare encrypted single-qubit states and send them to the server. This prevents the server from distinguishing computation and test rounds and also hides the client's data. Then, the client uses the classical encryption key as well as the measurement outcomes reported by the server to classically drive the computations and tests performed by the server on these encrypted qubits. Hence, turning this protocol into a multi-party one amounts to finding (i) an appropriate single-client SDQC protocol that will (ii) be composed with a secure collaborative remote state preparation for the single qubit encrypted states and that will (iii) be driven collaboratively to perform and verify the desired computation.

In § 2 of the full paper, we describe a single-client SDQC Protocol using only $|+_\theta\rangle = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$ states, based on the generic single-client SDQC Protocol of [22]. This was an open question in the field as all previous SDQC protocols in the MBQC framework with a formal security analysis use computational basis states (called dummies) to isolate single qubits in the computation graph. These remain unchanged if the server is honest and can be used as traps to detect deviations. To overcome this restriction, we must ideally find a generating set of stabilisers of the graph state for the client's computation that can be written with I, X and Y Paulis only. However, while it is possible to construct $N-1$ independent stabilisers of this form – where N denotes the number of vertices of the graph – it seems that the stabiliser which consists of Z operators on odd-degree vertices of the graph cannot be generated. This therefore corresponds to a server's deviation which cannot be caught by our tests on graphs containing odd degree nodes. If this attack would corrupt the client's computation, the whole protocol would be insecure. Fortunately, this is not the case for classical input/output computations. Indeed, we prove that this deviation corresponds to a server which has chosen a different orientation of the

Z axis compared to the client. Because inputs are prepared in the $X-Y$ plane and outputs are projected onto it, we show that this has no effect on the outcome of the computation. As a consequence, it is not necessary to detect this specific deviation by the server to verify the computation. This proves that the generic single-client SDQC Protocol of [22] can be used to produce secure dummyless protocols.[1]

Theorem 1 (Informal) *For any graph G, there exists a single-client statistically secure SDQC protocol in the Abstract Cryptography framework that requires the client to only prepare states in the $X-Y$ plane.*

We then focus on turning this new single-client protocol into a multi-party one. In § 3 of the full paper, we introduce a Collaborative Remote State Preparation (CRSP) protocol. We show that this gadget (Protocol 2) securely implements Remote State Preparation (Resource 2), which allows a classical party request any $|+_\theta\rangle$ state to be prepared on the server's device with the help of clients preparing single qubit states in the $X-Y$ plane.

Theorem 2 (Informal) *The CRSP gadget is a statistically secure implementation of the Remote State Preparation Resource in the Abstract Cryptography framework.*

The second set of tasks in the single-client protocol, i.e. choosing the measurement angles of the various computation and test rounds according to the states prepared using CRSP, only involve classical computations. These can be performed using a composably secure classical SMPC.[2]

In § 4 of the full paper, we compose the CRSP gadget, classical SMPC, and the dummyless SDQC protocol into a complete quantum SMPC protocol (Protocol 3). Its outline is:

1. The clients use the CRSP gadget to prepare $|+_\theta\rangle$ states on the server's side.
2. They use the classical SMPC together to drive and verify the single-client SDQC protocol.
3. Upon acceptance, the results and decryption keys are sent by the classical SMPC to each client.

The security proof relies on the composable security of all three ingredients. Because the CRSP gadget and the dummyless protocol are statistically secure, this is a direct upgrade of classical to quantum SMPC.

Theorem 3 (Informal) *Composable classical SMPC can be lifted to perform robust quantum SMPC for* BQP *computations in a statistically secure way, such that all parties but one are restricted to singe-qubit preparations.*

We note that this protocol requires no additional resources in terms of hardware or quantum communication from the client's side compared to the single-client protocol. The server only needs to be able to perform the CRSP gadget in addition to the operations required by the single-client protocol.

4 Discussion

In the course of constructing our protocol, we have built two new ingredients that we believe are of independent interest.

The first one is the Collaborative Remote State Preparation gadget. Its main feature is to provide some privacy amplification for the classical-quantum correlations that clients share with the server. Interestingly, we give evidence that it is hard to construct a generic gadget that would have similar features for correlations outside of a single plane of the Bloch sphere, while retaining its usefulness for cryptographic purposes. We leave it as an open question to prove a full no-go theorem in the Abstract Cryptography framework to further explore what seems to be a deep difference between classical and quantum input-output computations. Note also that this work supersedes a previous effort to construct a quantum SMPC protocol in the clients-server setting with quantum input and outputs. The proposed construction was similar in spirit with a collaborative remote state preparation gadget that allowed to prepare encrypted $X-Y$ plane states but also dummies. However, we give an attack on multiple approaches which were explored to perform this task, further strengthening the belief that such cryptographic protocols are hard if not impossible to construct.

The second new ingredient of our proof is the first dummyless SDQC protocol. Outside of the specific purpose of quantum SMPC, it exemplifies the usefulness of the general tests that were introduced in [22]. By reducing the requirements on the client side, it also possibly decreases a source of errors in physical implementations as it is not uncommon that rotations around one specific axis of the Bloch sphere are notably easier to perform than others. We also strongly believe that similar approaches, where traps are tailored to specific settings, will find applications in the future. Additionally, we show that while dummyless tests were not enough to detect all deviations, it is possible to nonetheless verify computations thanks to an as of now unknown invariance in MBQC. This raises the question of whether it is possible to do this on purpose, and engineer an invariance in order to lighten the constraints on the error-detection scheme that the traps implement.

Finally, note that because all SDQC protocols constructed from the generic protocol of [22] are robust to a fixed amount of global noise, so is our new multi-party protocol. While not being enough to scale to large quantum computations, it opens the possibility to implement experimental proof-of-concepts without resorting to error correction on near term devices.

[1] Note that here has been a previous protocol for dummyless verification [15], whose security analysis didn't take into account the above deviation. Our proof of invariance of MBQC to this specific error shows that this deviation does not constitute a security threat to the protocol in [15].

[2] The Abstract Cryptography framework used in this work is equivalent to the Quantum Universal Composability (Q-UC) Model of [35] if a single Adversary controls all corrupted parties – which is the case here. Therefore any Classical SMPC protocol which is secure in the Q-UC model can be used to instantiate this functionality.

References

[1] Alon, B., Chung, H., Chung, K.M., Huang, M.Y., Lee, Y., Shen, Y.C.: Round efficient secure multiparty quantum computation with identifiable abort (Nov 2020), https://eprint.iacr.org/2020.1464

[2] Bartusek, J.: Secure quantum computation with classical communication. In: Nissim, K., Waters, B. (eds.) Theory of Cryptography. pp. 1–30. Springer International Publishing, Cham (2021)

[3] Bartusek, J., Coladangelo, A., Khurana, D., Ma, F.: On the round complexity of secure quantum computation. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2021. pp. 406–435. Springer International Publishing, Cham (2021)

[4] Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science. pp. 249–260. FOCS '06, IEEE Computer Society, Washington, DC, USA (2006). https://doi.org/10.1109/FOCS.2006.68, http://dx.doi.org/10.1109/FOCS.2006.68

[5] Broadbent, A., Fitzsimons, J., Kashefi, E.: Universal blind quantum computation. In: IEEE (ed.) 50th Annual IEEE Symposium on Foundations of Computer Science (2009)

[6] Cramer, R., Damgrd, I.B., Nielsen, J.B.: Secure Multiparty Computation and Secret Sharing. Cambridge University Press, USA, 1st edn. (2015), https://dl.acm.org/doi/book/10.5555/2846411

[7] Crépeau, C., Gottesman, D., Smith, A.: Secure multi-party quantum computation. In: Proceedings of the Thiry-fourth Annual ACM Symp. on Theory of Computing. p. 643. STOC '02, ACM, New York, NY, USA (2002). https://doi.org/10.1145/509907.510000, http://doi.acm.org/10.1145/509907.510000

[8] Danos, V., Kashefi, E.: Determinism in the one-way model. Phys. Rev. A **74**, 052310 (Nov 2006). https://doi.org/10.1103/PhysRevA.74.052310, http://link.aps.org/doi/10.1103/PhysRevA.74.052310

[9] Dulek, Y., Grilo, A.B., Jeffery, S., Majenz, C., Schaffner, C.: Secure multi-party quantum computation with a dishonest majority. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 729–758. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_25

[10] Dunjko, V., Fitzsimons, J.F., Portmann, C., Renner, R.: Composable security of delegated quantum computation. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology – ASIACRYPT 2014. pp. 406–425. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)

[11] Dupuis, F., Fehr, S., Lamontagne, P., Salvail, L.: Adaptive versus non-adaptive strategies in the quantum setting with applications. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016. pp. 33–59. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)

[12] Dupuis, F., Nielsen, J.B., Salvail, L.: Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_37, http://dx.doi.org/10.1007/978-3-642-14623-7_37

[13] Dupuis, F., Nielsen, J.B., Salvail, L.: Actively secure two-party evaluation of any quantum operation. In: Advances in Cryptology–CRYPTO 2012, pp. 794–811. Springer (2012)

[14] Fehr, S., Katz, J., Song, F., Zhou, H.S., Zikas, V.: Feasibility and completeness of cryptographic tasks in the quantum world. In: Sahai, A. (ed.) Theory of Cryptography. pp. 281–296. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)

[15] Ferracin, S., Kapourniotis, T., Datta, A.: Reducing resources for verification of quantum computations. Physical Review A **98**(2), 022323 (2018)

[16] Fitzsimons, J.F., Kashefi, E.: Unconditionally verifiable blind quantum computation. Phys. Rev. A **96**, 012303 (Jul 2017). https://doi.org/10.1103/PhysRevA.96.012303, https://link.aps.org/doi/10.1103/PhysRevA.96.012303

[17] Gheorghiu, A., Kapourniotis, T., Kashefi, E.: Verification of quantum computation: An overview of existing approaches. Theory of Computing Systems **63**(4), 715–808 (May 2019). https://doi.org/10.1007/s00224-018-9872-3, https://doi.org/10.1007/s00224-018-9872-3

[18] Hallgren, S., Smith, A., Song, F.: Classical cryptographic protocols in a quantum world. International Journal of Quantum Information **13**(04), 1550028 (2015). https://doi.org/10.1142/S0219749915500288, https://www.worldscientific.com/doi/abs/10.1142/S0219749915500288

[19] Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states (2003)

[20] Houshmand, M., Houshmand, M., Tan, S.H., Fitzsimons, J.: Composable secure multi-client

delegated quantum computation. arXiv preprint arXiv:1811.11929 (2018)

[21] Kapourniotis, T., Dunjko, V., Kashefi, E.: On optimising quantum communication in verifiable quantum computing (2015), presented at AQIS'15 conference

[22] Kapourniotis, T., Kashefi, E., Leichtle, D., Music, L., Ollivier, H.: Unifying quantum verification and error-detection: Theory and tools for optimisations. arxiv:2206.00631 (2022)

[23] Kapourniotis, T., Kashefi, E., Music, L., Ollivier, H.: Delegating multi-party quantum computations vs. dishonest majority in two quantum rounds (2021)

[24] Kashefi, E., Music, L., Wallden, P.: The quantum cut-and-choose technique and quantum two-party computation (2017)

[25] Kashefi, E., Pappa, A.: Multiparty delegated quantum computing. Cryptography **1**(2), 1–20 (7 2017). https://doi.org/10.3390/cryptography1020012

[26] Kashefi, E., Wallden, P.: Garbled quantum computation. Cryptography **1**(1), 6 (2017)

[27] Kashefi, E., Wallden, P.: Optimised resource construction for verifiable quantum computation. Journal of Physics A: Mathematical and Theoretical; preprint arXiv:1510.07408 (2017), http://iopscience.iop.org/10.1088/1751-8121/aa5dac

[28] Leichtle, D., Music, L., Kashefi, E., Ollivier, H.: Verifying bqp computations on noisy devices with minimal overhead. Phys. Rev. X Quantum **2**(040302) (2021)

[29] Lipinska, V., Ribeiro, J., Wehner, S.: Secure multiparty quantum computation with few qubits. arXiv e-prints arXiv:2004.10486 (Apr 2020)

[30] Ma, Y., Kashefi, E., Arapinis, M., Chakraborty, K., Kaplan, M.: QEnclave – a practical solution for secure quantum cloud computing. npj Quantum Information **8**(1), 128 (2022)

[31] Maurer, U.: Constructive cryptography – a new paradigm for security definitions and proofs. In: Mödersheim, S., Palamidessi, C. (eds.) Theory of Security and Applications. pp. 33–56. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)

[32] Maurer, U., Renner, R.: Abstract cryptography. In: Innovations in Computer Science. pp. 1 – 21. Tsinghua University Press (jan 2011), https://conference.iiis.tsinghua.edu.cn/ICS2011/content/papers/14.html

[33] Rains, E.M.: Nonbinary quantum codes. IEEE Transactions on Information Theory **45**(6), 1827–1832 (1999). https://doi.org/10.1109/18.782103

[34] Raussendorf, R., Briegel, H.J.: A one-way quantum computer. Phys. Rev. Lett. **86**, 5188–5191 (May 2001). https://doi.org/10.1103/PhysRevLett.86.5188, http://link.aps.org/doi/10.1103/PhysRevLett.86.5188

[35] Unruh, D.: Universally composable quantum multiparty computation. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. pp. 486–505. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)

[36] Yao, A.: How to generate and exchange secrets. In: Foundations of Computer Science, 1986., 27th Annual Symposium on. pp. 162–167. IEEE (1986)

Fully quantum observational entropy

Ge Bai[1] * Dominik Šafránek[2] Joseph Schindler[3] Francesco Buscemi[4]
Valerio Scarani[1 5]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *Center for Theoretical Physics of Complex Systems, Institute for Basic Science (IBS), Daejeon 34126, Republic of Korea*
[3] *Física Teòrica: Informació i Fenòmens Quàntics, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain*
[4] *Department of Mathematical Informatics, Nagoya University, Furo-cho, Chikusa-ku 464-8601 Japan*
[5] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Abstract. We observe that the difference between the quantum observational entropy and von Neumann entropy can be interpreted as, and quantitatively equal to, the expected entropy production of the measurement process. Based on this observation, we provide a generalization of quantum observational entropy that includes a reference prior state that need not commute with the measured state. Such generalization is justified by its agreement with the quantum generalization of entropy production, which is related to the quantum generalization of the Bayesian retrodiction defined with the Petz recovery map.

Keywords: Observational entropy, entropy production, relative entropy, Bayesian inference, Petz recovery map

Originally defined by von Neumann, *observational entropy* has been the object of renewed interest [1, 2, 3, 4, 5, 6]. The original definition reads

$$S_{\mathbb{M}}(\rho) \quad = \quad -\sum_i r_i \ln \frac{r_i}{V_i} \tag{1}$$

where $\mathbb{M} = \{\Pi_i\}$ is a POVM, $r_i = \mathrm{Tr}[\rho\Pi_i]$ and $V_i = \mathrm{Tr}[\Pi_i]$. The observational entropy interpolates between the von Neumann entropy $S(\rho) \equiv -\mathrm{Tr}[\rho \ln \rho]$ and the Boltzmann entropy $S_B(i) \equiv \ln V_i$, where V_i is interpreted as the number of microstates compatible with outcome i. At one extreme, if $V_i = 1$ for all i, $S_{\mathbb{M}}(\rho) = -\sum_i r_i \ln r_i$ is a Shannon entropy, which coincides with $S(\rho)$ if the measurement is projective in the eigenstates of ρ. At the other extreme, if one of the Π_i is the identity on the support of ρ, $S_{\mathbb{M}}(\rho) = \ln V_i$ is of the Boltzmann type.

In general, $S(\rho)$ is a lower bound of $S_{\mathbb{M}}(\rho)$ [2] and it is natural to interpret their difference

$$\Delta_{\mathbb{M}}(\rho) \equiv S_{\mathbb{M}}(\rho) - S(\rho) \tag{2}$$

as *observational entropy generation*, since it quantifies the entropy generated by the measurement. This aligns with the intuition that a "precise" measurement in the eigenstates of ρ produces no additional uncertainty other than the internal uncertainty of ρ, while a "weak" measurement such as Π_i being identity is more uncertain.

The observational entropy generation turns out to be related to the entropy production arising in classical stochastic thermodynamics. There, the physical ("forward") process is described by the joint probability distribution $P_F(x, y)$ of the input $x \in X$ and the output $y \in Y$. The entropy production by the transition $x \to y$ is $s(x, y) = \ln \frac{P_F(x,y)}{P_R^\gamma(x,y)}$, where $P_R^\gamma(x, y)$ is the so-called reverse process, whose definition generically requires a reference prior distribution $\gamma(x)$ [7, 8]. This reverse process describes the retrodiction of the initial state based on the observations on the final state. With this definition, the expectation of entropy production in the physical process is captured by the relative entropy (a.k.a. Kullback-Leibler pseudodistance) between the forward and the reverse probability distributions:

$$\langle s \rangle_F = \sum_{x,y} P_F(x, y) s(x, y) \quad \equiv \quad D(P_F||P_R^\gamma) \,. \tag{3}$$

The observational entropy generation and the entropy production turn out to be different stories about the same quantity – their values are equal for a classical process. Let $\rho = \sum_x \lambda_x |x\rangle\langle x|$ be the eigendecomposition of ρ, and define $P_F(x, y)$ as the distribution of measurement outcomes of each eigenstate weighted by their eigenvalues

$$P_F(x, y) \equiv \lambda_x \langle x| \Pi_y |x\rangle \,. \tag{4}$$

We observe that

$$D(P_F||P_R^u) = S_{\mathbb{M}}(\rho) - S(\rho) = \Delta_{\mathbb{M}}(\rho), \tag{5}$$

where P_R^u is the reverse process with reference prior being the uniform prior distribution u, and $\Delta_{\mathbb{M}}(\rho)$ is the observational entropy generation (2).

Eq. (5) indicates a retrodictive interpretation of observational entropy – it measures the entropy production of the observer's measurement with a uniform prior, which is the relative entropy between the forward and reverse processes related by Bayesian retrodiction. It is then natural to generalize it to a non-uniform prior γ as in the case of retrodiction. Furthermore, we show that, with proper generalization of the relative entropy, the input ρ and the reference prior γ are allowed to be non-commuting operators, achieving a quantumization of Eq. (5) for quantum measurements with the forward and reverse processes related by the Petz map [6, 9, 10].

*baige@nus.edu.sg

To show this, we propose a *fully quantum definition of observational entropy production* $\Delta^{\gamma}_{\mathbb{M}}(\rho)$, that takes count in a reference state γ, defined as following:

$$\Delta^{\gamma}_{\mathbb{M}}(\rho) \equiv D_{\mathrm{BS}}(\rho\|\gamma) - D_{\mathbb{M}}(\rho\|\gamma) \tag{6}$$

where D_{BS} is the Belavkin-Staszewski relative entropy [11], defined as

$$D_{\mathrm{BS}}(\rho\|\sigma) \equiv \mathrm{Tr}[\rho \ln \rho\sigma^{-1}], \tag{7}$$

and $D_{\mathbb{M}}$ is the measured relative entropy, defined as

$$D_{\mathbb{M}}(\rho\|\gamma) \equiv D(\mathbb{M}(\rho)\|\mathbb{M}(\gamma)) = \sum_y \mathrm{Tr}[\rho\Pi_y] \ln \frac{\mathrm{Tr}[\rho\Pi_y]}{\mathrm{Tr}[\gamma\Pi_y]} \tag{8}$$

where $\mathbb{M}(\rho)(y) \equiv \mathrm{Tr}[\rho\Pi_y]$ and $\mathbb{M}(\gamma)(y) \equiv \mathrm{Tr}[\gamma\Pi_y]$ are the outcome probability distributions of the measurement $\mathbb{M}$ on ρ and γ, respectively.

We justify this definition of $\Delta^{\gamma}_{\mathbb{M}}(\rho)$ by showing that it satisfies the following properties:

1. The definition recovers the original definition of observational entropy when the prior γ is equal to the uniform distribution $u \equiv \mathbb{1}/d$:

$$\Delta^{u}_{\mathbb{M}}(\rho) = S_{\mathbb{M}}(\rho) - S(\rho) = \Delta_{\mathbb{M}}(\rho)\,. \tag{9}$$

2. If ρ and γ commute, for any $\mathbb{M}$, the entropy generated by the measurement can be directly matched to the entropy production of classical stochastic thermodynamics. Namely, for $[\rho, \gamma] = 0$,

$$\Delta^{\gamma}_{\mathbb{M}}(\rho) = D(P_F\|P^{\gamma}_R) \tag{10}$$

where the classical process P_F is constructed as

$$P_F(x, y) \equiv \lambda_x \langle x|\,\Pi_y\,|x\rangle \tag{11}$$

where $\rho = \sum_x \lambda_x |x\rangle\langle x|$ is the eigendecomposition of ρ, and P^{γ}_R is the reverse process of P_F with reference γ.

3. In the general case where ρ and γ may not commute, our definition is new. We arrived at it by requesting that the logical form of classical entropy production (5) is preserved: a statistical comparison between the process and its reverse. Indeed, one can express our observational entropy generation as the quantum relative entropy

$$\Delta^{\gamma}_{\mathbb{M}}(\rho) = D_{\mathrm{BS}}\left(Q^{\dagger}_F Q_F \middle\| (Q^{\gamma}_R)^{\dagger} Q^{\gamma}_R\right), \tag{12}$$

where Q^{γ}_R is related to Q_F by the Petz recovery map. More specifically, Q_F and Q^{γ}_R are so defined that they resemble the joint distributions P_F and P^{γ}_R in the sense that the marginal operators of $Q_F Q^{\dagger}_F$ and $Q^{\gamma}_R (Q^{\gamma}_R)^{\dagger}$ produce the inputs and outputs of the forward and reverse processes.

References

[1] Dominik Šafránek, J. M. Deutsch, and Anthony Aguirre. Quantum coarse-grained entropy and thermodynamics. *Phys. Rev. A*, 99(1):010101, January 2019.

[2] Dominik Šafránek, J. M. Deutsch, and Anthony Aguirre. Quantum coarse-grained entropy and thermalization in closed systems. *Phys. Rev. A*, 99(1):012103, January 2019.

[3] Dominik Šafránek, Anthony Aguirre, Joseph Schindler, and J. M. Deutsch. A Brief Introduction to Observational Entropy. *Foundations of Physics*, 51(5):101, October 2021.

[4] Philipp Strasberg and Andreas Winter. First and second law of quantum thermodynamics: A consistent derivation based on a microscopic definition of entropy. *PRX Quantum*, 2:030202, Aug 2021.

[5] Dominik Šafránek and Juzar Thingna. Quantifying Information Extraction using Generalized Quantum Measurements. *arXiv e-prints*, page arXiv:2007.07246, July 2020.

[6] Francesco Buscemi, Joseph Schindler, and Dominik Šafránek. Observational entropy, coarse quantum states, and Petz recovery: information-theoretic properties and bounds. *arXiv e-prints*, page arXiv:2209.03803, September 2022.

[7] Francesco Buscemi and Valerio Scarani. Fluctuation theorems from bayesian retrodiction. *Phys. Rev. E*, 103:052111, May 2021.

[8] Clive Cenxin Aw, Francesco Buscemi, and Valerio Scarani. Fluctuation theorems with retrodiction rather than reverse processes. *AVS Quantum Science*, 3(4):045601, 2021.

[9] Denes Petz. Sufficient subalgebras and the relative entropy of states of a von neumann algebra. *Comm. Math. Phys.*, 105:123–131, 1986.

[10] Denes Petz. Sufficiency of channels over von Neumann algebras. *The Quarterly Journal of Mathematics*, 39(1):97–108, 03 1988.

[11] Viacheslav P Belavkin and P Staszewski. C^*-algebraic generalization of relative entropy and entropy. In *Annales de l'IHP Physique théorique*, volume 37, pages 51–58, 1982.

Plug-and-play QKD architecture with self-optical pulse train generator

Min ki Woo[1], Chang Hoon Park[1], Sang-Wook Han[1, 2, *]

[1]*Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea*
[2]*Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Republic of Korea*
[1] *swhan@kist.re.kr,

Abstract. The Commercializing Quantum Key Distribution (QKD) for secure communication in the quantum computer era has garnered interest. Plug-and-play (PnP) QKD is a stable system, but to avoid backscatter noise generated in the round-trip structure, it has evolved into a structure with a storage line (SL) that is tens of kilometers long to transmit and store signals for a specific time (pulse train). did. This results in slow key distribution and also challenges the miniaturization of the system. In this study, we propose a method using an optical pulse train generator (OPTG) structure to remove SL. It is expected that this method can overcome the miniaturization limitation of PnP QKD and the slow security key speed.

Keywords: PnP QKD, self-optical pulse train generator

1 Introduction

Quantum key distribution (QKD) allows two distant users (Alice and Bob) to share a secure key. QKD guarantees unconditional security via the laws of quantum physics [1]. Since its first proposal in 1984 [2], it has become the most rapidly developed quantum technology, as its first commercial products appeared in the 2000s [3]. For expanding a market, the technologies have been consistently developed such as QKD network, long distance, higher secure key rate, miniaturization, long term stable operation, and so on [4-8]. Furthermore, verifications via several testbeds have been conducted [9-14].

Among the various structures of QKD, plug-and-play (PnP) QKD is stable and innovative enough to enable the development of commercial products with a control system that can be minimized [15]. However, there are some structural drawbacks. The presence of a storage line (SL) in the reciprocal signal structure, designed to prevent backscattering noise, leads to slower encryption key generation compared to one-way QKD systems, and the bulky SL hinders miniaturization. In this study, we propose and experimentally demonstrate a novel structure using an optical pulse train generator (OPTG) to overcome these limitations. With OPTG, Alice duplicates Bob's seed pulse, eliminating the need for an SL, and Bob doesn't have to send multiple pulse trains, enabling miniaturization and faster cryptographic key generation.

2 Theorems and Proofs

The main cause of the disadvantages of PnP QKD is the storage line (SL) used for removing backscattering noise. This not only slows down key generation but also hinders miniaturization. In response, we have implemented an optical pulse train generator (OPTG) to replace the SL. Figure 1 illustrates the overall QKD system implementing this OPTG in Alice.

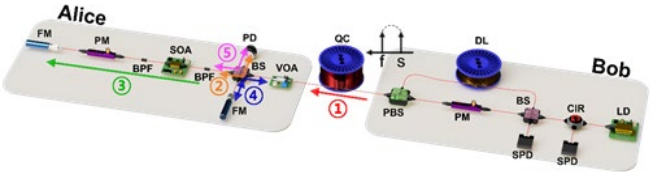


Fig. 1 PnP QKD system where Alice's SL is substituted by an OPTG. (FM: Faraday mirror, PM: phase modulator, BPF: Bandpass filter, SOA: semiconductor optical amplifier, BS: beam splitter, PD: photodiode, VOA: variable optical attenuator, QC: quantum channel, PBS: polarization beam splitter, DL: delay line, CIR: circulator, SPD: single photon detector, LD: laser diode)

The proposed OPTG is based on a reciprocating optical cavity consisting of two Faraday mirrors (FM). A beam splitter (BS) is inserted between these components to facilitate signal input and output. When a seed signal enters the BS, it reflects off the optical cavity, completes a round trip, and a portion of it is then outputted. Within this setup, a solid-state optical amplifier (SOA) is positioned to amplify the signal and compensate for losses caused by output, optics, and other factors. Additionally, a polarization modulator (PM) is placed in the middle to perform polarization modulation for the BB84 protocol.

When using the implemented OPTG to generate signals, the signal transmission with the pulse train and SL is depicted in Figure 2. By employing OPTG, the signal transmission efficiency is higher compared to conventional PnP QKD, as there is no time delay associated with passing through the SL. Ideally, assuming the operation time of OPTG approaches infinity, the signal transmission efficiency becomes equivalent to that of conventional one-way QKD. With OPTG implemented, Alice also has the potential for miniaturization. The advantage of miniaturization arises from the absence of the previously used SL, which typically spanned tens of kilometers. Additionally, it is anticipated that the design

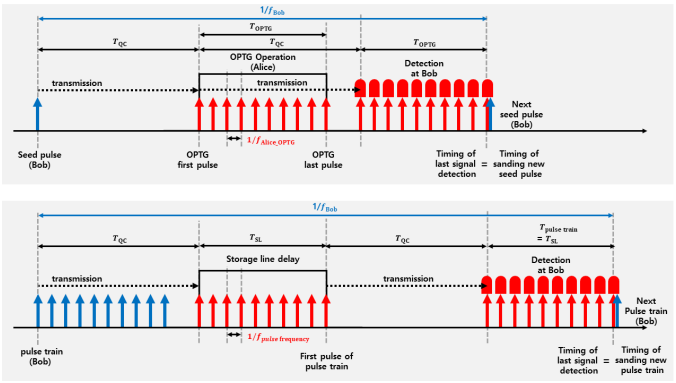


Fig. 2 Signal flow over time (top: when utilizing the proposed OPTG method, bottom: when using the conventional SL). The absence of a SL in Alice leads to a faster repetition sequence of the pulse train.

could be integrated into a chip due to the presence of standard components.

We successfully implemented this structure in practice, generating 10 pulses using a single seed pulse. Furthermore, by interfering these 10 pulses, we observed the interference results as shown in Figure 3. When measured using phase modulation (0, π/2, π, 3π/2) employed in the BB84 protocol, the error rate in each case did not exceed 5%. This demonstrates the feasibility of implementing PnP QKD using the proposed method.

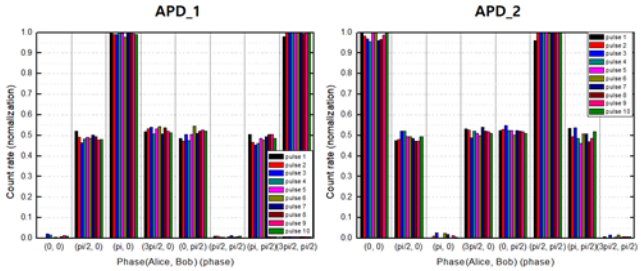


Fig. 3 The interference results of 10 signals generated by OPTG. Alice's PM was controlled at 0, π/2, π, and 3π/2, while Bob's PM was controlled at 0 and π/2 for measuring the interference results. The interference measurements according to each phase modulation showed that the error rate did not exceed 5%.

3 Theorems and Proofs

Our research proposes an optical pulse train generator (OPTG) as a substitute for the storage line (SL), which serves as the biggest obstacle in miniaturizing existing PnP QKD systems due to its physical volume limitation. We experimentally validate the new PnP QKD architecture utilizing OPTG. With OPTG, Alice can replicate Bob's seed pulse to generate pulse trains, enabling system implementation without the need for a storage line. Experimental results demonstrate that Alice generates 10 signals using OPTG and applies phase modulation (0, π/2, π, 3π/2) for the BB84 protocol. This showcases the successful integration of our proposed architecture into practical PnP QKD systems, enabling normal operation. Furthermore, these results demonstrate the potential for miniaturizing PnP QKD systems without the requirement of a storage line, and if implemented on a chip, it can further increase the pulse generation rate, leading to a higher secure key generation rate.

References

[1] N. Gisin, G. Ribordy, W. Tittel & H. Zbinden, "Quantum cryptography," Reviews of Modern Physics 74(1), 145-195 (2002).

[2] C. H. Bennett & G. Brassard Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of the IEEE International conference on Computers, Systems and Signal Processing, 175-179 (1984).

[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar & V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics 4(10), 686-689 (2010).

[4] B. Frohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan & A. J. Shields, "A quantum access network," Nature 501(7465), 69-72 (2013).

[5] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang & J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," Nature Photonics 15(8), 570-575 (2021).

[6] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe & A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Applied Physics Letters 92(20) (2008).

[7] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien & M. G. Thompson, "Chip-based quantum key distribution," Nature Communications 8(1), 13984 (2017).

[8] B. K. Park, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S. Moon & S.-W. Han, "User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1 × N quantum key distribution network system," Photonics Research 8(3), 296-302 (2020).

[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J. B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev & A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt Express 19(11), 10387-10409 (2011).

[10] S. Wang, W. Chen, Z. Q. Yin, Y. Zhang, T. Zhang, H. W. Li, F. X. Xu, Z. Zhou, Y. Yang, D. J. Huang, L. J. Zhang, F. Y. Li, D. Liu, Y. G. Wang, G. C. Guo & Z. F. Han, "Field test of wavelength-saving quantum key distribution network," Opt. Lett. 35(14), 2454-2456 (2010).

[11] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han & G. Guo, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," Chinese Science Bulletin 54(17), 2991-2997 (2009).

[12] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer & H. Yeh Current status of the DARPA quantum network. Proc. SPIE 5815, 138-149 (2005).

[13] C. Elliott, "Building the quantum network*," New J. Phys. 4, 46 (2002).

[14] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen & J.-W. Pan, "Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network," Physical Review X 6(1), 011024 (2016).

[15] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden & N. Gisin, ""Plug and play" systems for quantum cryptography," Applied Physics Letters 70(7), 793-795 (1997).

Strategies to Mitigate Decoherence in Superconducting Qubits

Abstract

A key advantage of using a superconducting circuit as a qubit is the flexibility in engineering its dynamics. In particular, the flexibility to design the circuit and its environment to make the qubit become resilient against environmental noise has led to significant improvements in the coherence time of the qubit over the years. In this work, we present experimental implementations of some of the current techniques and characterization of the qubit performance. We also theoretically explore the dynamics of a two-mode circuit, which belongs in the family of more recently proposed multi-mode circuit designs that may offer simultaneous protection against depolarization and dephasing. These designs currently face challenges in being experimentally realized, often due to their stringent fabrication requirements. By systematically exploring few-mode circuit designs such as the one presented in this work, we anticipate a better understanding on the required conditions for noise-protected qubit designs that are within fabrication feasibility.

Extended Abstract

Introduction

Since the first realization of superconducting qubit as a single-Cooper-pair box [1], the lifetime of the qubit has gone through significant improvements over the years [2]. There have been two main types of breakthroughs that have resulted in dramatic leaps: (1) improvements in circuit topology or parameters, and (2) embedding of qubit in a 3D cavity. In the former, the lifetime of the qubit is improved by engineering the circuits to be insensitive to various mechanisms that contribute to decoherence. The latter technique improves the coherence time by placing the superconducting qubit chip in a 3D microwave cavity with a high quality factor.

In this work, we present experimental implementations of these techniques and characterization of the qubit performance. We also analyze the limitations of the current approach and propose a direction to further improve the performance of the device.

Transmon in 3D Cavity

We fabricate the transmon qubit by depositing on a high resistivity silicon wafer an $Al/AlO_x/Al$ Josephson junction between aluminium capacitor pads. The qubit chip is then embedded in a 3D aluminium cavity which has input and ouput coaxial ports.

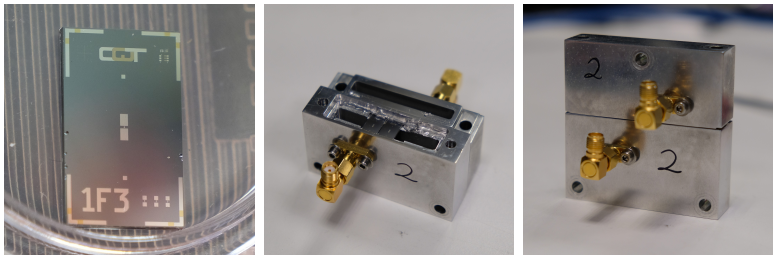


Figure 1: A transmon qubit (left) and a 3D cavity containing the chip (center and right).

The transmon qubit couples to the electromagnetic field of the cavity, such that we can control the qubit states by sending microwave pulses into the cavity and readout the states by measuring the transmission through the cavity.

The coherence performance of the qubit is typically charaterized by two figures of merit: (1) T_1 which characterizes the rate of depolarization, and (2) T_2 which characterizes a combination of depolarization and dephasing rates.

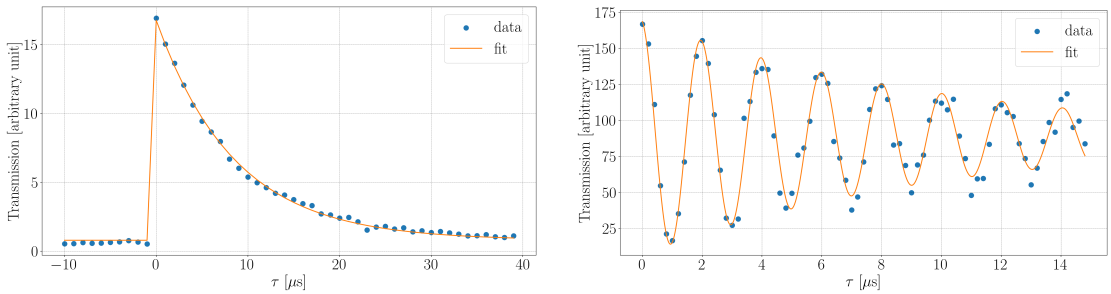


Figure 2: Measurements of qubit coherence time, T_1 (left) and T_2^R (right).

In the experiments, T_1 denotes the time constant in the decay of the $|1\rangle$ state to the $|0\rangle$ state, while T_2^R and T_2^E denote the decay time constants in Ramsey spectroscopy and spin echo

experiment respectively. The median values of the coherence times across our qubit samples in 3D cavity were measured to be $T_1 = (8.8 \pm 0.4)$ μs, $T_2^R = (9.1 \pm 0.7)$ μs, and $T_2^E = (15 \pm 2)$ μs.

Transmons on a 2D Chip

While the 3D cavity architecture provides a conducive environment for high qubit coherence times, feasibility to scale up the system to large numbers of qubits is not yet clear. In order to increase the number of qubits and thus the processing power of the quantum processing unit, we design a 2D chip that accommodates more qubits. Our design contains four transmons, each of which is coupled to a charge drive line for qubit control and a coplanar waveguide resonator for readout.

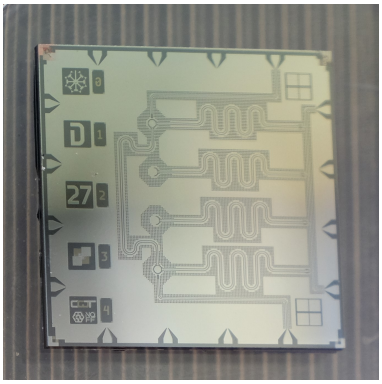


Figure 3: A 2D chip design with four transmon qubits.

The median values of the coherence times across our qubit samples were measured to be $T_1 = (14 \pm 2)$ μs and $T_2^R = (15 \pm 3)$ μs.

Moving Beyond Transmon

Two of the notable examples of innovations in circuit design are transmon [3] and fluxonium [4]. Transmon is designed to be protected against dephasing, by rendering the qubit energy dispersion to become small with respect to charge noise. Fluxonium on the other hand is designed to be protected against depolarization, by localizing the qubit wavefunctions in distinct regions of the potential.

A limitation in these designs however is that they are single-mode qubits, and are intrinsically unable to attain simultaneous protection against both depolarization and dephasing noises [5]. More recent studies have proposed circuit designs that offer such simultaneous protection, by designing multi-mode circuits [6] [7] [8] [9]. The main challenge in experimentally implementing these designs is the stringent requirements on the circuit parameters.

Here, we explore the dynamics and noise-protection properties of a two-mode circuit. Our circuit has the transmon-type and fluxonium-type parts joined by a superinductor. The circuit topology creates two inductive loops, through which external fluxes Φ_0 and Φ_2 thread. The dynamics of this circuit is specified with the Lagrangian $\mathcal{L} = T - V$, where

$$\begin{aligned} T &= \frac{E_{C1}}{2}\dot{\phi}_1^2 + \frac{E_{C2}}{2}\dot{\phi}_2^2 + \frac{E_{C0}}{2}(\dot{\phi}_1 - \dot{\phi}_2)^2 \\ V &= -E_{J1}\cos\phi_1 - E_{J2}\cos\phi_2 + \frac{E_{L0}}{2}(\Phi_0 + \phi_2 - \phi_1)^2 + \frac{E_{L2}}{2}(\Phi_2 - \phi_2)^2 \end{aligned} \tag{1}$$

in terms of the phase variables of the two ungrounded nodes, ϕ_1 and ϕ_2.

In order to protect the qubit against depolarization, the wavefunctions of the computational states need to be localized in distinct regions in their domains, spanned by ϕ_1 and ϕ_2. However,

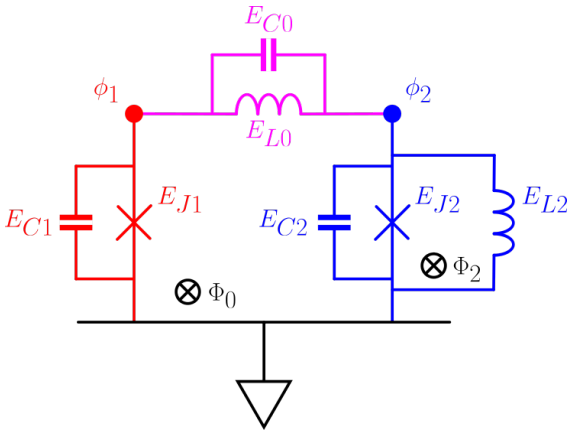


Figure 4: Lumped element model of our two-mode superconducting qubit. the circuit consists of a transmon-type sub-circuit (red part), and a fluxonium-type sub-circuit (blue part), which are joined together by a superinductor (magenta part).

the wavefunctions need to be delocalized in the directions to which the external fluxes couple, in order to be protected against dephasing. Because the two external fluxes couple to two linearly independent directions, $(\phi_2 - \phi_1)$ and ϕ_2 respectively, in the two-dimensional space, this circuit design is insufficient to achieve exponential protection against both depolarization and dephasing simultaneously. Nevertheless, it may be possible to achieve partial protection against both, by delocalizing the wavefunctions in the $A(\phi_2 - \phi_1) + B(\phi_2)$ direction for positive A and B, while localizing them in the orthogonal direction. The circuit parameters can then be chosen to tune between offering more protection toward either decoherence mechanism. Furthermore, this circuit has the advantage of absent spurious modes which are present in some of the other multi-mode circuits such as 0-π qubit [9].

References

[1] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-Cooper-pair box. Nature **398**, 786 (1999).

[2] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver. Superconducting qubits: Current state of play. Annu. Rev. Condens. Matter Phys. **11**, 369 (2020).

[3] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Charge-insensitive qubit design derived from the Cooper pair box. Phys. Rev. A **76**, 042319 (2007).

[4] V. E. Manucharyan, J. Koch, L. I. Glazman, and M. H. Devoret. Fluxonium: Single Cooper-Pair Circuit Free of Charge Offsets. Science **326**, 113 (2009).

[5] A. Gyenis, A. Di Paolo, J. Koch, A. Blais, A. A. Houck, and D. I. Schuster. Moving beyond the Transmon: Noise-Protected Superconducting Quantum Circuits. Phys. Rev. X **2**, 030101 (2021).

[6] A. Kou, W. C. Smith, U. Vool, R. T. Brierley, H. Meier, L. Frunzio, S. M. Girvin, L. I. Glazman, and M. H. Devoret, Fluxonium-Based Artificial Molecule with a Tunable Magnetic Moment, Phys. Rev. X 7, 031037 (2017).

[7] W. Smith, M. Villiers, A. Marquet, J. Palomo, M. Delbecq, T. Kontos, P. Campagne-Ibarcq, B. Douçot, and Z. Leghtas, Magnifying quantum phase fluctuations with cooper-pair pairing, arXiv:2010.15488 (2020).

[8] W. C. Smith, A. Kou, X. Xiao, U. Vool, and M. H. Devoret, Superconducting circuit protected by two-Cooper-pair tunneling, npj Quantum Inf. 6, 8 (2020).

[9] A. Gyenis, P. S. Mundada, A. Di Paolo, T. M. Hazard, X. You, D. I. Schuster, J. Koch, A. Blais, and A. A. Houck. Experimental realization of a protected superconducting circuit derived from the 0-π qubit. PRX Quantum **2**, 010339 (2021).

Estimation of fidelity with unknown observables with simpler Clifford circuit structure.

Guedong Park[1] * Yong Siah Teo[1] † Hyunseok Jeong[1] ‡

[1] *Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*

Abstract. Using equatorial stabilizer POVM(esPOVM), we introduce classes of n-qubit randomized shadow tomography algorithms that require only at most $[\frac{n}{2} + \mathcal{O}(log(n))]$-depth Clifford bases and Pauli measurements. Also, with only neighboring gates, we can achieve this algorithm with $2n$-depth which enables us to have a circuit with a more affordable error threshold and simpler structure than previously known ones. Furthermore, we introduce an even smaller subset of esPOVM that performs shadow tomography on real observables. Polynomial sampling-copy numbers are preserved with these low-depth algorithms.

Keywords: Quantum tomography, Shadow tomography, Clifford gates, Stabilizer states, Equatorial stabilizer states (*esPOVM*), Informationally completeness.

1 Introduction

Quantum algorithms, which are algorithms based on quantum mechanical principles, have been shown to outperform the classical algorithms for many computational tasks [1, 2]. To implement such algorithms, including quantum state preparation and quantum communication, certifying the structure of a given quantum state is an important task. Quantum tomography is a representative method to search the all matrix elements of an unknown n-qubit quantum state ρ. However, as the n increases, we need exponentially many samples of ρ for an accurate reconstruction.

On the other hand, if we are to estimate the physical properties of unknown states within additive ϵ-error, *shadow tomography* [3] enables us to require only a poly-sized number of samples depending on the structure of observables. Furthermore, Ref.[4] proposes two algorithms. The first is *randomized Pauli tomography*, which is useful for estimating the expectation of Hamiltonian with low locality. This algorithm has a very simple circuit structure because we do not need an intermediate quantum operation but just randomized Pauli measurements. The second algorithm, *randomized Clifford tomography* is better for estimating fidelity between unknown input and target states. However, this algorithm includes long-ranged Clifford gates with depth $n+\mathcal{O}(log(n))$ [5, 6], and for large n, it is very hard to implement experimentally since operations with long depth accumulate physical errors so large.

Therefore, reducing the depth of randomized circuits while preserving the efficiency of fidelity estimation is crucial for practical implementations. General measurements [7, 8, 9] over the Pauli measurements will optimize the depth but these are believed to be hard to implement fault tolerantly. Ref.[10] shows that for observables that are matrix product state(MPS) with low bond dimension, and MPS input states, efficient fidelity estimation is possible with only two-qubit neighboring Clifford gates of $\mathcal{O}(log(n))$-depth. However, for arbitrary input and target states, we need general Clifford operations and hence $5n$ depth neighboring Clifford gates [6, 11] and the most optimal depth bound of this problem is still not known.

In this paper, we propose new schemes of randomized Clifford tomography for fidelity estimation which employ shallower depth. The main point is that it is not necessary to utilize the whole *stabilizer POVM (sPOVM)* [12] comprising all Clifford-rotated bases. Instead, our schemes employ a smaller stabilizer subset, *equatorial stabilizer POVM (esPOVM)* [13] together with the computational basis. Additionally, we give a more specific subset *real equatorial stabilizer POVM (resPOVM)*, which still gives a tomography scheme for the target state with real coefficient with respect to computational basis. Next, we give a theoretical upper bound for the estimation variance, which is directly related to the *shadow norm* [4]. Both esPOVM and resPOVM tomography require at most Clifford bases of depth $\frac{n}{2} + \mathcal{O}(log(n))$. Moreover, if we have only neighboring Clifford bases, we can achieve the same algorithms with depth $2n$. Our algorithms need a larger sample overhead than Ref.[4]. However, we highlight that these are, to the best of our knowledge, the most depth-optimized tomography with Clifford gates, and both variances have the same scaling with the shadow norms of Ref.[4] for the fidelity estimation.

2 Main results

First, we define two classes of states which will be used throughout this paper.

Definition 1. *For the n qubit system,*

$$|\phi_A^{\text{eq}}\rangle \equiv \frac{1}{\sqrt{2^n}} \sum_{x\in\mathbb{Z}_2^n} i^{xAx^T} |x\rangle\,, \tag{1}$$

$$|\phi_A^{\text{req}}\rangle \equiv \frac{1}{\sqrt{2^n}} \sum_{x\in\mathbb{Z}_2^n} (-1)^{xAx^T} |x\rangle\,, \tag{2}$$

where in Eq. (1), $A = (a_{ij})_{i,j\in[n]}$, $a_{ij} \in \{0,1,2,3\}$ if $i = j$, and $a_{ij} = a_{ji} \in \{0,1\}$ if $i \neq j$.

*rbeh7336@snu.ac.kr
†yong.siah.teo@gmail.com
‡jeongh@snu.ac.kr

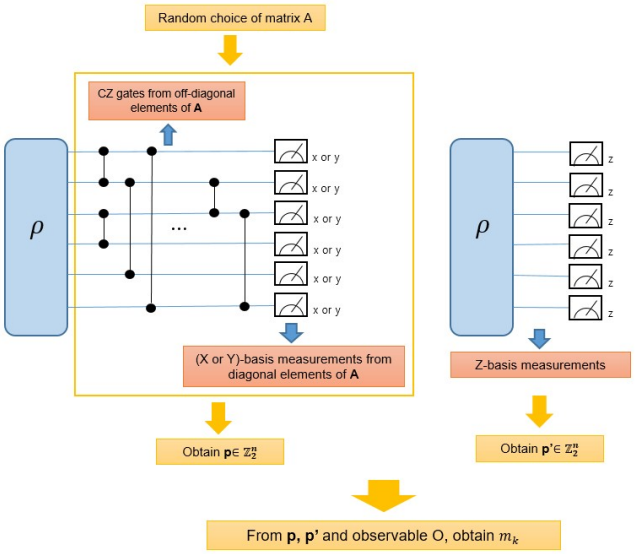


Figure 1: Diagrammatic blueprint of 6-qubit esPOVM tomography. The unknown state is ρ and the target observable is O. The task is to estimate $\mathrm{Tr}(O\rho)$. Detailed expression of the algorithm is written in the main text.

Also in Eq. (2), $A = (a_{ij})_{i,j\in[n]}$, $a_{ij} \in \{0,1\}$ if $i \leq j, a_{ij} = 0$ if $i > j$. x is a binary row vector. Equation (1) is called *equatorial stabilizer* [13] and Eq. (2) is called *real equatorial stabilizer* We define *(real resp.)equatorial stabilizer set* $\mathcal{S}_n^{(\mathrm{r})\mathrm{eq}}$ as the set of n qubit (real)equatorial stabilizers. We note that both sets are proper subsets of stabilizer set $\mathcal{S}_n$. Now, we offer our important lemma.

Lemma 1. *For unknown n qubit quantum state ρ and hermitian operator O,*

$$(i) \sum_{|\phi_A^{\mathrm{eq}}\rangle\in\mathcal{S}_n^{\mathrm{eq}}} \frac{2^{2n}}{|\mathcal{S}_n^{\mathrm{eq}}|} \langle\phi_A^{\mathrm{eq}}|\rho|\phi_A^{\mathrm{eq}}\rangle \langle\phi_A^{\mathrm{eq}}|O|\phi_A^{\mathrm{eq}}\rangle + \sum_{x\in\mathbb{Z}_2^n} \langle x|\rho|x\rangle \langle x|O|x\rangle - \mathrm{tr}(O) = \mathrm{tr}(O\rho). \quad (3)$$

Now, if O is a real matrix with respect to computational basis,

$$(ii) \sum_{|\phi_A^{\mathrm{req}}\rangle\in\mathcal{S}_N^{\mathrm{req}}} \frac{2^{2n-1}}{|\mathcal{S}_n^{\mathrm{req}}|} \langle\phi_A^{\mathrm{req}}|\rho|\phi_A^{\mathrm{req}}\rangle \langle\phi_A^{\mathrm{req}}|O|\phi_A^{\mathrm{req}}\rangle + \sum_{x\in\mathbb{Z}_2^N} \langle x|\rho|x\rangle \langle x|O|x\rangle - \frac{1}{2}\mathrm{tr}(O) = \mathrm{tr}(O\rho). \quad (4)$$

We can write an algorithm for new quantum tomography with an equatorial stabilizer set from this. We only show esPOVM tomography based on Eq, (3) for convenience. Given the unknown n qubit quantum state ρ and hermitian operator O, the task is to estimate $\mathrm{Tr}(O\rho)$. We fix the *sampling-copy number* $N \in \mathbb{N}$.

esPOVM tomography algorithm
For $k \in [N]$, do,

1. Prepare the state ρ as an input. Uniformly randomly choose $|\phi_A^{\mathrm{eq}}\rangle$ in $\mathcal{S}_n^{\mathrm{eq}}$. This is possible by randomly choosing the matrix $A = (a_{ij})$ of $|\phi_A^{\mathrm{eq}}\rangle$.
2. For $i, j \in [n]$ satisfying $i \neq j$ and $i < j$, $a_{i,j} = 1$, act $CZ_{i,j}$ to ρ.
3. For $i \in [n]$, if $a_{ii} = 0\ (mod\ 2)$, then measure the i-th qubit with a Pauli X measurement. Otherwise, do a Pauli Y measurement. After the measurement, obtain the outcome $\mathbf{p} \in \mathbb{Z}_2^n$.
4. Take the measured *stabilizer*, $|\phi_{A'}^{\mathrm{eq}}\rangle$ where $A' = (a'_{ij})$ satisfies that $a'_{ij} = a_{ij}$ for $i \neq j$ but $a'_{ii} = a_{ii} + 2p_i\ (mod\ 4)$.
5. Prepare another fresh state ρ as an input. Measure in Pauli Z-basis to get an outcome $\mathbf{p}' \in \mathbb{Z}_2^n$.
6. Calculate $m_k = 2^n \langle\phi_{A'}^{\mathrm{eq}}|O|\phi_{A'}^{\mathrm{eq}}\rangle + \langle\mathbf{p}'|O|\mathbf{p}'\rangle - \mathrm{tr}(O)$.

Finally, desired estimation is $m = \frac{1}{N}\sum_{k=1}^{N} m_k$.

Figure 1 briefly describes the above algorithm. We note that we need one another Z-basis measurement step and hence two fresh inputs for a single trial. The reason is that esPOVM solely does not make Informationally Complete(IC) POVM which is a necessary property for tomography [15]. With the aid of a computational basis, it becomes truly IC. We note that the above algorithm only requires CZ gates and Pauli measurements in the last section. Even in the resPOVM case where O is real, circuit architecture does not change but we only do X and Z-basis measurements.

We summarize these as a theorem.

Theorem 1. *In the n-qubit system, suppose we are capable of efficiently initializing n-qubit state ρ. Implementation of n-qubit esPOVM tomography to ρ requires at most CZ gates of depth $n+1$, and n number of single qubit Pauli(X,Y,Z) measurements. For resPOVM, the Y basis is not needed.*

The depth bound of CZ gates can be obtained by Vizing's theorem [16]. With the aid of other Clifford basis, we can reduce the depth to $\frac{n}{2} + \mathcal{O}(log(n))$ [5]. Furthermore, we can implement CZ gates followed by measurements with only two-qubit neighboring gates with depth $2n$ [11].

Now we want to make our objective more sharper. We want to make sure that our estimation is accurate such that additive error is lower than $\epsilon > 0$. How many are samples needed to achieve this accuracy? This can be solved by inspecting the variance of the estimator.

We define, $\hat{O}_A^{(\mathrm{r})\mathrm{eq}} \equiv 2^{n(-1 \text{ for req})} \langle\phi_A^{(\mathrm{r})\mathrm{eq}}|O|\phi_A^{(\mathrm{r})\mathrm{eq}}\rangle$ and $\hat{O}_x^{\mathrm{bin}} \equiv \langle x|O|x\rangle$. These are estimators of each circuit board. The estimation variance $Var(O)$ is,

$$Var(O) = Var(\hat{O}_A^{(\mathrm{r})\mathrm{eq}}) + Var(\hat{O}_x^{\mathrm{bin}}). \quad (5)$$

Each variance term on the right side is equivalent with *shadow norm* [4] of esPOVM measurement and Z-basis measurement respectively. Now, we introduce our second main result.

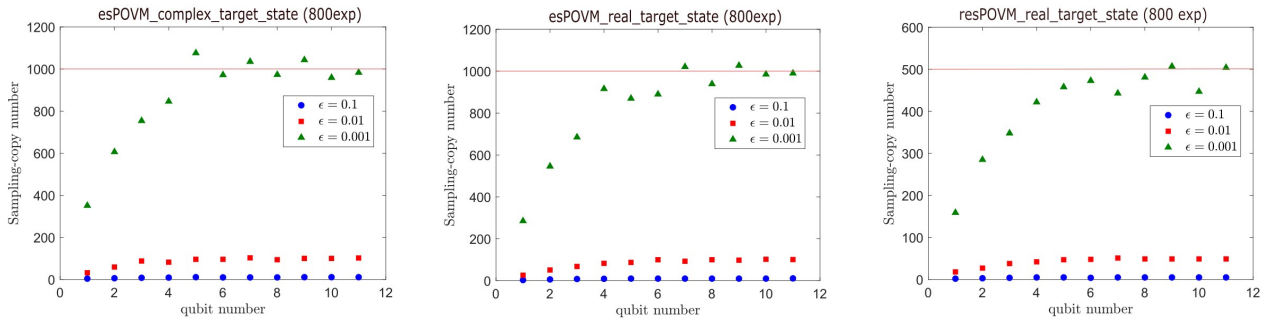


Figure 2: Sampling-copy number N to achieve the Mean Squared Error(MSE) ϵ. For each number of qubits from 1 to 11, we increased N from 1 to 2000, and take the N at which the average value of squared errors (between true value and estimation) from 800 experiments hit 0.1, 0.01, and 0.001. For graph (a), we used uniformly randomly chosen complex input states and target states. For (b) and (c), we uniformly randomly chose the complex input state and real target states. Red lines are theoretical asymptotic values of MSE = 0.001. (a): Result for esPOVM tomography for complex target states. (b): Results for esPOVM tomography for real target states. (c) Results for resPOVM tomography for real target states.

Theorem 2. *Suppose an unknown quantum state ρ and we have the ability to prepare ρ as input as much as possible. Also, suppose we are given an observable O(for $\mathcal{S}_N^{\mathrm{req}}$, take O as real). With (r)esPOVM tomography scheme, we can estimate* $\mathrm{tr}(O\rho)$ *within additive ϵ-error with $1-\delta$ success probability if we repeat that scheme over $\mathcal{O}(\frac{Var(O)}{\epsilon^2} log(\frac{1}{\delta}))$, where*

$$Var(O) \leq 76(19 \text{ for } \mathcal{S}_N^{\mathrm{req}}) max \left\{ \left|(tr(O))^2\right|, \left|tr(O^2)\right|, \right. \\ \left. |tr(O)| \, \|O\|_\infty, \|OO^T\|_\infty, \|O^T O\|_\infty \right\}, \tag{6}$$

where $\|O\|_\infty \equiv \max_{|\psi\rangle} |\langle\psi| O |\psi\rangle|$.

Our second main theorem shows that for many cases, estimation variance is very reasonable so that the sampling-copy number is not exponentially large by increasing n. For example, if O is also a state σ, then the right side of Eq. (6) becomes constant hence required sampling-copy number is independent of the number of qubits. This $Var(O)$ has a very rough bound, which means the exact value is far less than this bound.

Furthermore, we can see that variance of resPOVM has a much lower bound. It means that for real observables, using the resPOVM tomography is better than esPOVM.

3 Numerical results

In this section, we numerically show the accuracy of our tomography algorithms and reasonable sampling-copy numbers. See Figure 2. Throughout this section, we consider the target is the state, hence the main task is to estimate fidelity between input and target. We examined three cases. The first one is esPOVM for uniformly randomly chosen input states and target states. The second is for uniformly randomly chosen input states and real target states. The last one is resPOVM, random choice was done in the same manner as the second one. For each experiment, with the number of qubits from 1 to 11, we record the sampling-copy number at which Mean Squared Error (MSE) over 800 experiments reaches the designated value, 0.1,0.01, and 0.001.

From the above graphs, we observed that averaged sampling-copy number is proportional with $\frac{1}{\epsilon}$ (Here, ϵ is not exactly an error, but the target MSE). This is a natural phenomenon from Hoeffding's inequality. The important point is that sampling-copy numbers are bounded by a constant, which is much lower than bound in Eq. (6). These overheads are not increasing by the number of qubits. Also, the deviation of these values will be bounded because as in the Theorem 2, estimation variance is bounded by a constant when the target is a quantum state. Even though we recorded up to 11 qubits, we expect the tendency will be continued over 11 qubits. Another interesting point is that from Figure 2 (b) and (c), the saturated value of resPOVM is twice less than esPOVM. Surprisingly, we can analytically prove that averaged values of estimation variances of two cases asymptotically differ by factor 2.

For large n, for efficient estimation, we must assume that we can efficiently calculate the trace between the arbitrary equatorial stabilizer and a given observable. From this perspective, we believe that our algorithms will encompass a larger region of target states than previous Clifford tomography [4] because esPOVM and resPOVM are much smaller subsets of sPOVM.

References

[1] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review 41, 303, 1999.

[2] D. Deutsch, R. Jozsa. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences 439, 553, 1992.

[3] Scott Aaronson. Shadow tomography of quantum states. Proceedings of the 50th annual ACM SIGACT symposium on theory of computing, pages 325–338, 2018.

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

[5] Dmitri Maslov, Ben Zindorf Depth Optimization of CZ, CNOT, and Clifford Circuits. IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-8, 2022.

[6] Sergey Bravyi and Dmitri Maslov. Hadamard-free circuits expose the structure of the Clifford group. IEEE Transactions on Information Theory, 67(7):4546–4563, 2021.

[7] Daniel Grier, Hakop Pashayan, and Luke Schaeffer. Sample-optimal classical shadows for pure states. 10.48550/ARXIV.2211.11810, 2022.

[8] Atithi Acharya, Siddhartha Saha, and Anirvan M Sengupta. Shadow tomography based on informationally complete positive operator-valued measure. Physical Review A, 104(5):052418, 2021.

[9] H. Chau Nguyen, Jan Lennart Bonsel, Jonathan Steinberg, and Otfried Guhne. Optimizing Shadow Tomography with Generalized Measurements. Phys. Rev. Lett., 129:220502, Nov 2022.

[10] Christian Bertoni, Jonas Haferkamp, Marcel Hinsche, Marios Ioannou, Jens Eisert, and Hakop Pashayan. Shallow shadows: Expectation estimation using low-depth random clifford circuits. 10.48550/ARXIV.2209.12924, 2022.

[11] Dmitri Maslov and Willers Yang. CNOT circuits need little help to implement arbitrary Hadamard-free Clifford transformations they generate. arXiv:2210.16195, 2023

[12] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. Physical Review A 70, 052328, 2004

[13] Sergey Bravyi, David Gosset. Simulation of quantum circuits by low-rank stabilizer decompositions. Quantum, 3:181, 2019.

[14] J. I. Cirac and P. Zoller Quantum Computations with Cold Trapped Ions Phys. Rev. Lett. 74, 4091, 1995

[15] G M D'Ariano, P Perinotti and M F Sacchi. Journal of Optics B: Quantum and Semiclassical Optics Informationally complete measurements and group representation. Journal of Optics B: Quantum and Semiclassical Optics 6 S487, 2004.

[16] Claude Berge and Jean Claude Fournier. short proof for a generalization of vizing's theorem. ournal of graph theory, 15(3):333–336, 1991.

Tripartite entanglement measures based on three-party teleportation capability

Minjin Choi[1] * Eunok Bae[2] † Soojoon Lee[2 3] ‡

[1] *Division of National Supercomputing, Korea Institute of Science and Technology Information, Daejeon 34141, Korea*

[2] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*

[3] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 02447, Korea*

Abstract. To use entanglement as a resource, we need an entanglement measure that can compare the usefulness of quantum states in some quantum information processing. We here define new tripartite entanglement measures based on the capability of three-qubit teleportation, and hence we can explain the relationship between the teleportation capability and tripartite entanglement through our measures. Our measures distinguish between biseparable and genuinely multipartite entangled states and do not increase under local operations and classical communications, which are essential requirements for quantifying entanglement.

Keywords: genuine multipartite entanglement, multipartite entanglement measure, multi-party teleportation capability

1 Three-qubit teleportation capability

Three-qubit teleportation proceeds as follows. Suppose that three parties, Alice, Bob, and Charlie, share a three-qubit state. After one performs an orthogonal measurement on his/her system, the rest carry out the standard teleportation over the resulting state with the measurement outcome.

Let F_{ij} be the maximal fidelity of teleportation over the resulting state in the systems i and j after measuring the system k, where i, j, and k are distinct systems in $\{A, B, C\}$. Then we have [1];

$$F_{ij} = \frac{2f_{ij}+1}{3}, \tag{1}$$

where

$$f_{ij} = \max_{U_k} \sum_{t=0}^{1} \langle t| U_k \rho_k {U_k}^\dagger |t\rangle \, f\left(\rho_{ij}^{U_k,t}\right). \tag{2}$$

Here, U_k is a unitary operator, that is, ${U_k}^\dagger |0\rangle\langle 0| U_k - {U_k}^\dagger |1\rangle\langle 1| U_k$ describes a one-qubit orthogonal measurement on the system k, $\rho_{ij}^{U_k,t}$ is the resulting state with the outcome t, and f is the fully entangled fraction, which is given by

$$f(\rho) = \max \langle e| \rho |e\rangle, \tag{3}$$

where the maximum is over all maximally entangled states $|e\rangle$ of two qubits. We say that a given state is useful for three-qubit teleportation if and only if $\min\{F_{AB}, F_{BC}, F_{CA}\} > 2/3$.

We note that the maximal fidelity F_{ij} on pure states can be written as a combination of other entanglement measures. For three-qubit pure states, it has been shown that the following equation holds [1]:

$$F_{ij} = \frac{\sqrt{\tau + C_{ij}^2} + 2}{3}, \tag{4}$$

where τ is the three-tangle [2] and C_{ij} is the concurrence [3, 4] for the reduced density operator ρ_{ij}.

By using Eq. (4), we have the following lemmas.

Lemma 1 *Let $|\phi\rangle_{ABC}$ be a three-qubit pure state. Then for any distinct i, j, and k in $\{A, B, C\}$, $F_{ij} = \frac{2}{3}$ if and only if $|\phi\rangle_{ABC} \in SEP(i:jk)$ or $|\phi\rangle_{ABC} \in SEP(j:ik)$. Moreover, if $F_{ij} > \frac{2}{3}$ and $F_{ik} > \frac{2}{3}$, then $F_{jk} > \frac{2}{3}$.*

Lemma 2 *The fidelities F_{AB}, F_{BC}, and F_{CA} do not increase on average under local operations and classical communication.*

2 Entanglement measures based on three-qubit teleportation capability

Note that minimal conditions for being a good entanglement measure have been suggested as follows [5]:

(i) $E(\rho) > 0$ if and only if ρ is a nonbiseparable state.

(ii) E is invariant under local unitary transformations.

(iii) E is not increasing on average under LOCC. That is, if we have states $\{\rho_k\}$ with probabilities $\{p_k\}$ after applying a LOCC transformation to ρ, then $\sum_k p_k E(\rho_k) \leq E(\rho)$.

(iv) E fulfills convexity.

If a multipartite entanglement measure satisfies these conditions, then we call it a genuine multipartite entanglement (GME) measure.

Let us now define entanglement measures based on the three-qubit teleportation capability.

Definition 3 *Let $\mathcal{T}_{ij} = 3F_{ij} - 2$, where F_{ij} is the fidelity in Eq. (1). For three-qubit pure states, we define multipartite entanglement measures $\mathcal{T}_{min}$ and $\mathcal{T}_{GM}$ as*

$$\begin{aligned} \mathcal{T}_{min} &\equiv \min\{\mathcal{T}_{AB}, \mathcal{T}_{BC}, \mathcal{T}_{CA}\}, \\ \mathcal{T}_{GM} &\equiv \sqrt[3]{\mathcal{T}_{AB}\mathcal{T}_{BC}\mathcal{T}_{CA}}, \end{aligned} \tag{5}$$

*mathcmj89@gmail.com
†eobae84@gmail.com
‡level@khu.ac.kr

respectively. For three-qubit mixed states, we generalize them via the convex roof extension

$$E(\rho) = \min_{\{p_l, \psi_l\}} \sum_l p_l E\left(|\psi_l\rangle\right), \tag{6}$$

where the minimum is over all possible decompositions $\rho = \sum_l p_l |\psi_l\rangle \langle\psi_l|$.

It directly follows from Lemma 1 that $\mathcal{T}_{min}$ and $\mathcal{T}_{GM}$ distinguish biseparable and genuinely multipartite entangled states. We know that they are invariant under local transformations from the definition of F_{ij}. From Lemma 2, we can also prove that they do not increase under local operations and classical communication. The convexity is guaranteed by the convex roof extension. Therefore, we have the following theorem.

Theorem 4 *Entanglement measures* $\mathcal{T}_{min}$ *and* $\mathcal{T}_{GM}$ *are GME measures.*

In Lemma 1, we also showed that for any distinct i, j, and k in $\{A, B, C\}$, if $F_{ij} > \frac{2}{3}$ and $F_{ik} > \frac{2}{3}$, then $F_{jk} > \frac{2}{3}$. Therefore, only two quantities $\mathcal{T}_{ij}$ and $\mathcal{T}_{ik}$ are enough to define a GME measure.

Definition 5 *For any distinct* i, j, *and* k *in* $\{A, B, C\}$, *we define multipartite entanglement measures* $\mathcal{T}^{(i)}_{min}$ *and* $\mathcal{T}^{(i)}_{GM}$ *as*

$$\begin{aligned} \mathcal{T}^{(i)}_{min} &\equiv \min\{\mathcal{T}_{ij}, \mathcal{T}_{ik}\}, \\ \mathcal{T}^{(i)}_{GM} &\equiv \sqrt{\mathcal{T}_{ij}\mathcal{T}_{ik}} \end{aligned} \tag{7}$$

on three-qubit pure states. For three-qubit mixed states, we generalize them through the convex roof extension.

By applying the same proof method in Theorem 4, we have the following theorem.

Theorem 6 *Entanglement measures* $\mathcal{T}^{(i)}_{min}$ *and* $\mathcal{T}^{(i)}_{GM}$ *are GME measures for* $i \in \{A, B, C\}$.

3 Example

The following example shows that our GME measures are more suitable to capture the usefulness of a given state for three-qubit teleportation. We note that GME measure C_{min} is given by

$$C_{min} \equiv \min\{C_{A(BC)}, C_{B(CA)}, C_{C(AB)}\}$$

on three-qubit pure states [5].

For $0 \le r \le 1$, let

$$\begin{aligned} |\psi(r)\rangle_{ABC} &= r\,|000\rangle_{ABC} + \frac{\sqrt{1-r^2}}{2}\,|101\rangle_{ABC} \\ &+ \frac{\sqrt{1-r^2}}{\sqrt{2}}\,|110\rangle_{ABC} + \frac{\sqrt{1-r^2}}{2}\,|111\rangle_{ABC}, \end{aligned} \tag{8}$$

$$|\xi(r)\rangle = \frac{\sqrt{1-r^2}}{\sqrt{2}}\,|001\rangle + \frac{\sqrt{1-r^2}}{\sqrt{2}}\,|010\rangle + r\,|100\rangle. \tag{9}$$

Then we can see that for $0.7 < r < 0.9$,

$$\begin{aligned} C_{min}\left(\xi(r)\right) &> C_{\min}\left(\psi(r)\right), \\ \mathcal{T}_{min}\left(\xi(r)\right) &< \mathcal{T}_{min}\left(\psi(r)\right). \end{aligned} \tag{10}$$

The GME measure $\mathcal{T}_{min}$ is defined based on three-qubit teleportation capability. Thus, we can say that if $|\psi\rangle$ is more entangled than $|\xi\rangle$ with respect to $\mathcal{T}_{min}$, then $|\psi\rangle$ is more useful than $|\xi\rangle$ in three-qubit teleportation. In other words, although $|\psi(r)\rangle$ is more valuable for three-qubit teleportation than $|\xi(r)\rangle$ in this case, C_{min} does not catch this fact. Similar examples can be readily found for other GME measures as well.

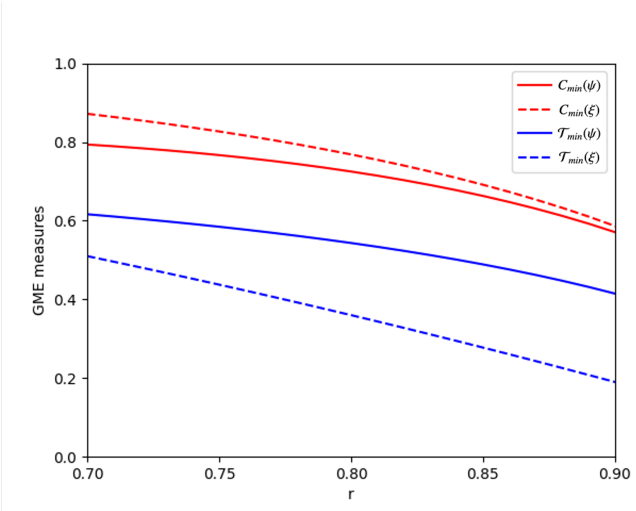


Figure 1: If we calculate GME measures C_{min} and $\mathcal{T}_{min}$ for the states $|\psi(r)\rangle$ in Eq. (8) and $|\xi(r)\rangle$ in Eq. (9), then $C_{min}\left(\xi(r)\right) > C_{\min}\left(\psi(r)\right)$ but $\mathcal{T}_{min}\left(\xi(r)\right) < \mathcal{T}_{min}\left(\psi(r)\right)$ for $0.7 \le r \le 0.9$. Hence, we can say that C_{min} is not appropriate for comparing teleportation capabilites.

References

[1] S. Lee, J. Joo, and J. Kim, Entanglement of three-qubit pure states in terms of teleportation capability. *Phys. Rev. A* **72**, 024302 (2005).

[2] V. Coffman, J. Kundu, and W. K. Wootters, Distributed entanglement. *Phys. Rev. A* **61**, 052306 (2000).

[3] S. A. Hill and W. K. Wootters, Entanglement of a pair of quantum bits. *Phys. Rev. Lett* **78**, 5022 (1997).

[4] W. K. Wootters, Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett* **80**, 2245 (1998).

[5] Z.-H. Ma *et al.*, Measure of genuine multipartite entanglement with computable lower bounds. *Phys. Rev. A* **83**, 062325 (2011).

Parallel-in-time quantum simulation via Page and Wootters quantum time

N. L. Diaz[1 2 *] Paolo Braccia[1] Martin Larocca[1] J.M. Matera[2] R. Rossignoli[2]
M. Cerezo[1 †]

[1] *Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[2] *National University of La Plata, La Plata 1900, Argentina*

Abstract. We present quantum algorithms for parallel-in-time simulations inspired by the Page and Wooters formalism. By introducing clock qubits entangled with system qubits, our algorithms can use only $\log_2(N)$ "clocks" to compute averages over N different times of quantities such as the dynamical structure factors, and Loschmidt echos. In addition, we prove that the entanglement created between the system qubits and the clock qubits has operational meaning, as it encodes valuable information about the system's dynamics. The latter indicates that our algorithms does not only achieve an exponential trade-off between time and spatial complexities, but also enable a new dimension for studying temporal properties.

Keywords: Quantum algorithm, Dynamical-in-time properties, Quantum Simulations

1 Introduction

Quantum foundations studies the fundamental principles of quantum theory, such as the nature of quantum states, the interpretation of measurements and the emergence of classicallity [1, 2, 3, 4]. Recently, the incorporation of time in a fully quantum framework has also raised much attention within this field. Notably, several proposals have appeared in the literature to "extend" quantum mechanics in order to treat time in symmetry with other observables [5, 6, 7, 8, 9, 10], some of which take into account the relativistic regime [11, 12, 10] and quantum information aspects [13, 14].

Another interesting and not very explored feature of these proposals is their use for finding new algorithms involving time-related quantities. For instance, in the so-called Page and Wooters (PaW) formalism [5, 6, 15, 16, 13, 14, 17, 11, 12] one assumes a stationary "universe" composed by a quantum system of interest plus an ancillary "clock" (see Fig. 1(a-b)). This framework is particularly interesting from the quantum computational perspective as the conventional unitary evolution of the system emerges from its entanglement with the clock and is recovered by measuring and conditioning over the latter. This suggests quantum algorithms in which part of the qubits have the role of "clock qubits".

In this work, we will borrow inspiration from the PaW mechanism to develop quantum algorithms for studying temporal averages of several dynamical properties of a quantum system (see Fig. 1(c)). Specifically, given a time-independent Hamiltonian H acting on n-qubits, and its associated time evolution operator $U(t) = e^{-iHt}$, we consider the problem of estimating general quantities of the form

$$\begin{aligned}\overline{F}(O_1, O_2, \omega) &= \lim_{T\to\infty} \int_0^T \frac{dt}{T} e^{-i\omega t} \langle O_1(t) O_2 \rangle_\rho \\ &= \lim_{T\to\infty} \int_0^T \frac{dt}{T} e^{-i\omega t} \mathrm{Tr}[\rho O_1(t) O_2] \,,\end{aligned} \tag{1}$$

where $O_1(t) = U^\dagger(t) O_1 U(t)$. Here, ρ is an n-qubit state acting on the d-dimensional Hilbert space $\mathcal{H}_S$ (with $d = 2^n$), O_1 and O_2 are two operators, and $\omega \in \mathbb{R}$. $\overline{F}(O_1, O_2, \omega)$ contains as a special case infinite temporal average of an observable, infinite-time averages of Loschmidt echos, two-point correlation, as well as their Fourier transforms [18, 19, 20, 21].

While the importance of Eq. (1) is clear, its computation might not be straightforward (as it involves an infinite time limit). As such, one often times wants to compute the discrete-time approximation

$$\widetilde{F}(O_1, O_2, \omega) = \frac{1}{N} \sum_{t=0}^{N-1} e^{-i\omega\varepsilon t} \langle O_1(\varepsilon t) O_2 \rangle_\rho \,, \tag{2}$$

where we have $\varepsilon = T/N$ (for simplicity, we will henceforth assume that N is a power of 2). That is, for a given (finite) time window T, we are computing the average over N points separated by a spacing ε.

*nldiaz@iflp.edu.ar
†cerezo@lanl.gov

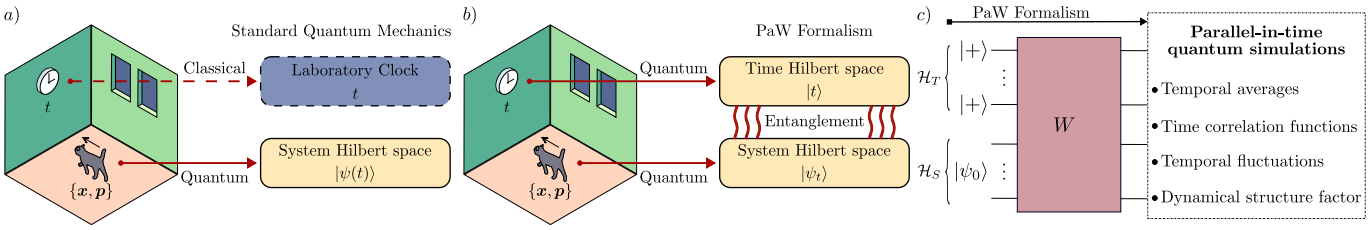


Figure 1: In Hamiltonian classical mechanics, dynamical variables are functions of the phase space coordinates position $\boldsymbol{x}$ and momentum $\boldsymbol{p}$. a) In standard quantum mechanics, one promotes $\boldsymbol{x}$ and $\boldsymbol{p}$ to quantum operators, but the time variable t is treated as a classical parameter that is external to the quantum system being studied. This creates an asymmetry between position (a fully quantum variable), and time (a classical variable). b) In the PaW formalism, time is treated as a quantum variable, with its own associated Hilbert space. c) In this work we borrow inspiration from the PaW framework to develop algorithms for parallel-in-time-simulations.

2 Main results

When considering the task of evaluating Eq. (2), one can readily find an algorithm where each expectation value $\langle O_1(\varepsilon t)O_2\rangle_\rho$ is *sequentially* evaluated and the measurement outcomes are combined with classical post-processing. Evidently, here we have:

Proposition 1 *There exists an algorithm for sequential-in-time simulations that requires $(n+1)$-qubits, and estimates the quantity $\widetilde{F}(O_1, O_2, \omega)$ up to δ accuracy with $\mathcal{O}(N/\delta^2)$ experiments.*

In our work, we aim to improve on the experiment complexity in Proposition 1. For this purpose, we leverage the basic ingredient of the PaW formalism: The so-called "history" states, defined as

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{t=0}^{N-1} |t\rangle|\psi(\varepsilon t)\rangle\,. \tag{3}$$

Here, $|\psi(\varepsilon t)\rangle = U(\varepsilon t)|\psi_0\rangle$. Notably, $|\Psi\rangle$ can be prepared with $\log_2(N)$ ancillary qubits, and one can see it is an equal superposition of the (discrete) time evolution of a quantum system for all times $t = 0, \ldots, N$. From here, we can prove our first main result.

Theorem 1 *The circuit in Fig. 2, which requires $(n+\log_2(N)+1)$-qubits, can be used to estimate the quantity $\widetilde{F}(O_1, O_2, \omega)$ of Eq. (2) up to δ accuracy with $\mathcal{O}(1/\delta^2)$ experiments.*

This theorem shows that using the history state allows us to push the complexity of running multiple experiments onto ancillary clock-qubit requirements. More importantly, we show that the entanglement present between the time and system qubits in the history state has operational meaning and

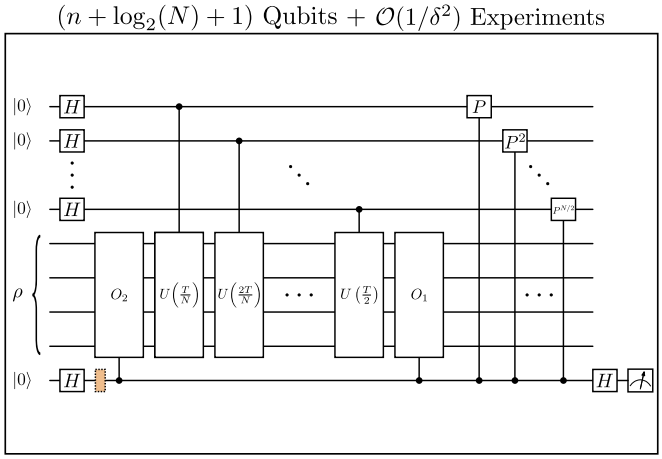


Figure 2: Algorithm for parallel-in-time estimation of the quantity $\widetilde{F}(O_1, O_2, \omega)$ up to precision δ. In the figure, P denotes a $\omega\varepsilon$ phase gate. This algorithm contains as a sub-routine the circuit for preparing the history state. The colored dashed gate is replaced with an identity (an $S^\dagger$ gate) to compute the real (imaginary) part of $\widetilde{F}(O_1, O_2, \omega)$.

contains information that we can use to learn about the system's dynamics.

Let us study the special case when $\widetilde{F}(O_1, O_2, \omega)$ and $\widetilde{F}(O_1, O_2, \omega)$ respectively corresponds to the infinite-time average Loschmidt's echo $\bar{\mathcal{L}}(\psi_0)$, and its discrete time approximation $\widetilde{\mathcal{L}}(\psi_0)$ (i.e., $\bar{\mathcal{L}}(\psi_0) \equiv \overline{F}(|\psi_0\rangle\langle\psi_0|, \mathbb{I}, 0)$). We prove that

Theorem 2 *Let $|\Psi\rangle$ be the discrete history-state in Eq. (3), and let E_2 be the linear entropy of the system-time partition. Then, for any T and N we have*

$$E_2 \leq (1 - \bar{\mathcal{L}}(\psi_0))\,. \tag{4}$$

Theorem 2 has several important implications. First, it bounds the amount of entanglement be-

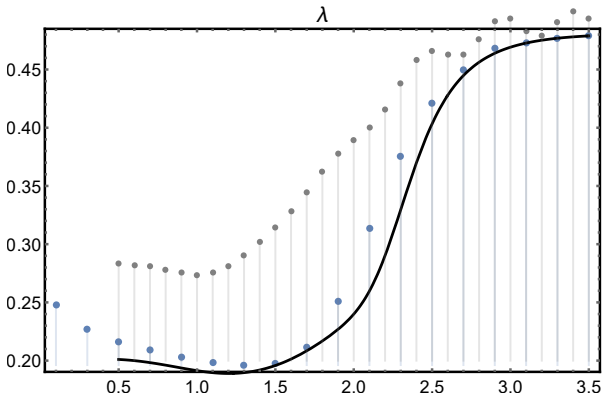


Figure 3: We show for different values of λ in the XX Hamiltonian the infinite-time Loschmidt echo, $\bar{\mathcal{L}}(\psi_0)$ (black curve), as well as its discrete time approximation $\widetilde{\mathcal{L}}(\psi_0)$ (grey dotted curve), and the linear entropy (blue dotted curve). We see than the entropy curve approximates $\bar{\mathcal{L}}(\psi_0)$ better than $\widetilde{\mathcal{L}}(\psi_0)$. Results are for $N = 64$ and a chain of $n = 14$ spins.

tween the system and the clock qubits. In particular, it shows that the system-time entanglement can only be large if the infinite time average of the Loschmidt echo value is small. Conversely, if $\bar{\mathcal{L}}(\psi_0)$ is large, E_2 has to be small. Second, let us remark that Eq. (4) is valid for all values of T, but most notably, also for all values of N. For large N and T the equality is reached asymptotically, and we have that Eq. (4) becomes $\mathrm{Tr}[\rho_T^2] \equiv \bar{\mathcal{L}}(\psi_0)$ (with ρ_T the reduced state of the $|\Psi\rangle$ on the clock qubits). More surprisingly, as shown in Fig. 3, we numerically find that that E_2 is a better approximation of $\bar{\mathcal{L}}(\psi_0)$ than $\widetilde{\mathcal{L}}(\psi_0)$. Since E_2 is easy to compute (see for instance Fig. 4), we can readily use the History state to study the infinite-time Loschmidt echo. Moreover, we can extend Theorem 2 to show that E_2 also bounds the temporal fluctuations of observables.

Corollary 1 *Let O be an observable, and let ΔO^2 denote its temporal variance. The system-clock entanglement provides bound on temporal fluctuations as $\Delta \bar{O}^2 \leq ||O||^2 (1 - E_2)$.*

It is clear that implementing the circuit in Fig. 2 might require prohibitively deep circuits due to the need of controlling the $\log_2 N$ gates $U(2^{j-1}\varepsilon) = U(\varepsilon)^{2^{j-1}}$ (for $j = 1, \ldots, \log_2 N$). Hence, to make our algorithm more near-term we present in our work a near-term version of this circuit where one achieves depth-reduction via variational Hamiltonian diagonalization [22, 23] and Cartan decomposition [24, 25, 26]. As an explicit test of these ideas, we also develop a numerical analysis of the XX Hamiltonian

$$H = \frac{J}{4} \sum_j (X_j X_{j+1} + Y_j Y_{j+1}) + \frac{\lambda}{4} \sum_j \cos(2\pi\alpha j)(Z_j + 2)\,,$$

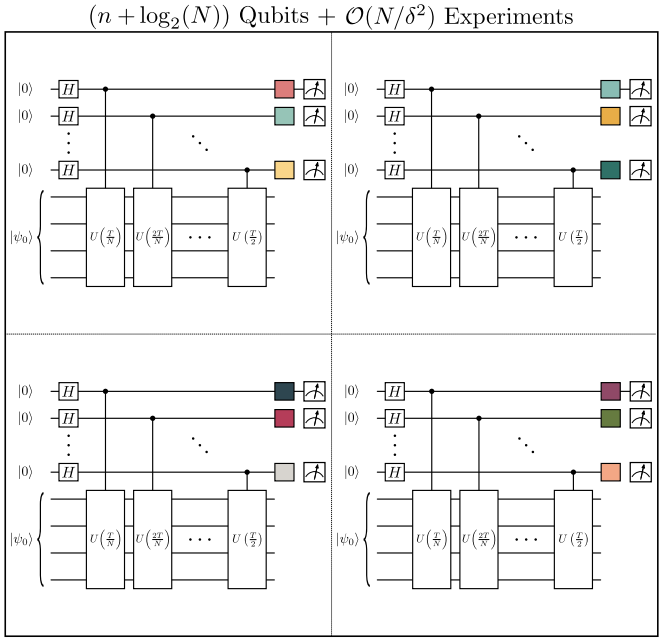


Figure 4: In this circuit, we leverage classical shadows [28] to estimate $\mathrm{Tr}[\rho_T^2]$ up to δ precision with a quantum device with $(n + \log_2(N))$-qubits and $\mathcal{O}(N/\delta^2)$ different experiments.

where X_j, Y_j and Z_j respectively denote the Pauli gates acting on the j-th qubits. This model exhibits an Anderson localization-delocalization transition [27], which we can be detect through the use of the system-time entanglement entropy and/or by time-discrete approximations of the Loshmidt echo (computable with the previous circuit). In this case, we can reduce the depth of the circuit as follows.

Theorem 2 *Let H be an XY Hamiltonian, we can implement the circuits used in Theorem 1 with circuit depths in $\mathcal{O}(\log_2(N)n)$.*

3 Conclusions and Outlook

We present algorithms that can compute averages over N different times by only using $\log_2(N)$ clock qubits. As such, we achieve an exponential trade-off between time and spatial complexities. In addition, we rigorously prove that the entanglement created between the n system qubits and the $\log_2(N)$ clock qubits has operational meaning, as it encodes valuable information about the system's dynamics.

Since our algorithms were inspired by the PaW formalism, we envision that our work will inspire others to borrow tools from foundations of quantum mechanics (an often-times untapped source of inspiration) to develop novel quantum algorithms.

References

[1] G. Auletta and G. Parisi, *Foundations and Interpretation of Quantum Mechanics: In the Light of a Critical-Historical Analysis of the Problems and of a Synthesis of the Results* (World Scientific, 2001).

[2] W. H. Zurek, Reviews of modern physics **75**, 715 (2003).

[3] M. Schlosshauer, Reviews of Modern physics **76**, 1267 (2005).

[4] J. A. Wheeler and W. H. Zurek, *Quantum theory and measurement*, Vol. 53 (Princeton University Press, 2014).

[5] D. N. Page and W. K. Wootters, Physical Review D **27**, 2885 (1983).

[6] W. K. Wootters, International journal of theoretical physics **23**, 701 (1984).

[7] A. Connes and C. Rovelli, Classical and Quantum Gravity **11**, 2899 (1994).

[8] C. J. Isham, Journal of Mathematical Physics **35**, 2157 (1994).

[9] J. F. Fitzsimons, J. A. Jones, and V. Vedral, Scientific reports **5**, 18281 (2015).

[10] N. L. Diaz, J. M. Matera, and R. Rossignoli, Physical Review D **103**, 065011 (2021).

[11] N. L. Diaz, J. M. Matera, and R. Rossignoli, Physical Review D **100**, 125020 (2019).

[12] N. L. Diaz and R. Rossignoli, Physical Review D **99**, 045008 (2019).

[13] A. Boette, R. Rossignoli, N. Gigena, and M. Cerezo, Physical Review A **93**, 062127 (2016).

[14] A. Boette and R. Rossignoli, Physical Review A **98**, 032108 (2018).

[15] V. Giovannetti, S. Lloyd, and L. Maccone, Physical Review D **92**, 045033 (2015).

[16] S. Massar, P. Spindel, A. F. Varón, and C. Wunderlich, Physical Review A **92**, 030102 (2015).

[17] D. Pabón, L. Rebón, S. Bordakevich, N. Gigena, A. Boette, C. Iemmi, R. Rossignoli, and S. Ledesma, Physical Review A **99**, 062333 (2019).

[18] G. Rickayzen, *Green's functions and condensed matter* (Courier Corporation, 2013).

[19] E. Khatami, G. Pupillo, M. Srednicki, and M. Rigol, Physical review letters **111**, 050403 (2013).

[20] J. Pedernales, R. Di Candia, I. Egusquiza, J. Casanova, and E. Solano, Physical Review Letters **113**, 020505 (2014).

[21] M. L. Baez, M. Goihl, J. Haferkamp, J. Bermejo-Vega, M. Gluza, and J. Eisert, Proceedings of the National Academy of Sciences **117**, 26123 (2020).

[22] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles, Nature Reviews Physics **3**, 625–644 (2021).

[23] B. Commeau, M. Cerezo, Z. Holmes, L. Cincio, P. J. Coles, and A. Sornborger, arXiv preprint arXiv:2009.02559 (2020).

[24] E. Kökcü, T. Steckmann, Y. Wang, J. Freericks, E. F. Dumitrescu, and A. F. Kemper, Physical Review Letters **129**, 070501 (2022).

[25] D. Camps, E. Kökcü, L. Bassman Oftelie, W. A. De Jong, A. F. Kemper, and R. Van Beeumen, SIAM Journal on Matrix Analysis and Applications **43**, 1084 (2022).

[26] E. Kökcü, D. Camps, L. B. Oftelie, J. K. Freericks, W. A. de Jong, R. Van Beeumen, and A. F. Kemper, Physical Review A **105**, 032420 (2022).

[27] Ann. Israel Phys. Soc. **3**, 133 (1980).

[28] H.-Y. Huang, R. Kueng, and J. Preskill, Nature Physics **16**, 1050 (2020).

Efficient MZM Bias Control Method for Quantum Key Distribution Systems

Chang-Hoon Park[1 2 *] Min-Ki Woo[2 †] Byung-Kwon Park[1 ‡] Seung-Woo Jeon[1 §]
Hojoong Jung[1 ¶] Sangin Kim[2 ‖] Sang-Wook Han[1 3 **]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea*
[2] *Department of Electrical and Computer Engineering, Ajou University, Suwon 16499, Republic of Korea*
[3] *Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Republic of Korea*

Abstract. We propose a new method for controlling the bias of a Mach-Zehnder modulator (MZM) in a quantum key distribution (QKD) system using N diagnostic pulses. The method does not require additional hardware and does not significantly reduce the key rate. The proposed method was experimentally demonstrated in a field-deployed QKD network, showing that it can maintain the MZM extinction ratio stably over 20 dB with a bit error rate of $\leq 1\%$.

Keywords: quantum key distribution, Mach-Zehnder modulator, auto-bias control

1 Introduction

Quantum cryptography has gained significant attention due to the development of quantum computing technology. Quantum key distribution (QKD) systems are of particular interest as they allow secure key sharing between distant parties [1]. However, practical QKD systems are sensitive to environmental noise, which has led to efforts [2, 3] to design noise-tolerant optical architecture and stabilize optical devices such as lasers, detectors, and modulators. Nevertheless, a Mach-Zehnder modulator (MZM) bias control method for QKD systems has not been developed yet, which is critical for implementing a decoy-state protocol to prevent photon number splitting attacks. Previous MZM bias control methods utilizing optical power monitoring or dither signals are not suitable for QKD systems due to optical crosstalk noise and additional optical devices.

In this study, we propose an MZM bias control method [4] based on a software modification that adds diagnostic pulses to estimate bias drift, allowing efficient MZM bias control without additional devices. The proposed method has advantages in terms of system miniaturization, key rate maintenance, parallel implementation, and faster convergence rate compared to conventional PID control. We experimentally demonstrate the feasibility of the proposed method in a field test, showing its potential for QKD network systems.

2 Method

The proposed method for the MZM bias control is as follows (Figure 1). Here, the transmitter and receiver are indicated as Alice and Bob, respectively, similar to conventional QKD systems.

1. During the conventional QKD protocol, Alice transmits N (≥ 2) types of diagnostic pulses modulated [5] by $\theta^i_{\mathrm{mod}} = \frac{2\pi}{N}(i-1)$ for $i = \{1, \ldots, N\}$ as substitutes for some decoy pulses.

2. Bob measures the incoming pulses and publicly announces the time indexes. Then, Alice and Bob perform the rest of the protocol.

3. Simultaneously, Alice accumulates the click results of the diagnostic pulses unless no significant phase drift occurs inside the MZM.

4. Then, Alice calculates $p_i = \frac{N}{2} \times \frac{C_i}{\sum C_i}$ and $\mathrm{Err}(\theta^T_{\mathrm{drift}}) = \sum[p_i - p_{T_i}(\theta^T_{\mathrm{drift}})]^2$, where C_i is the count for the i-th diagnostic pulse, and $p_{T_i}(\theta^T_{\mathrm{drift}})$ is the theoretical detection probability for the i-th diagnostic pulse with the theoretical phase drift $\theta^T_{\mathrm{drift}} = [0°, 360°)$.

5. Alice finds $\theta^T_{\mathrm{drift}}$ minimizing $\mathrm{Err}(\theta^T_{\mathrm{drift}})$ and estimates the found value as the practical phase drift θ_{drift}.

6. Alice compensates for the phase drift by applying $\theta_{\mathrm{mod}} = \theta_{\mathrm{mod}} - \theta_{\mathrm{drift}}$.

Alice repeats the above calibration steps at specific intervals or when a phase drift higher than a predefined threshold is detected.

3 Experimental Results

The control method was tested on a 1×3 QKD network system [6, 7] installed in a secure communication system of a smart factory in South Korea (Figure 2). The control system was implemented using a personal computer and an FPGA board equipped with multiple

*originalpch@kist.re.kr
†025160@kist.re.kr
‡pbk2324@naver.com
§sw_jeon@kist.re.kr
¶hojoong.jung@kist.re.kr
‖sangin@ajou.ac.kr
**swhan@kist.re.kr

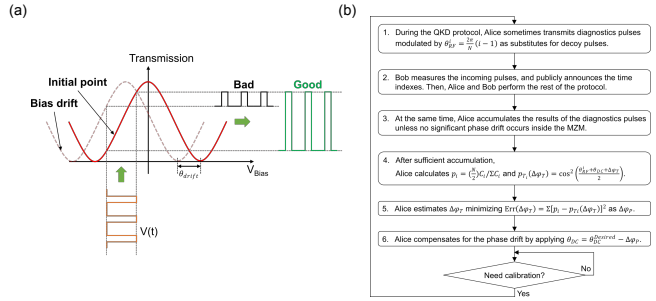


Figure 1: (a) Transfer function of the MZM (b) Block diagram of the proposed method.

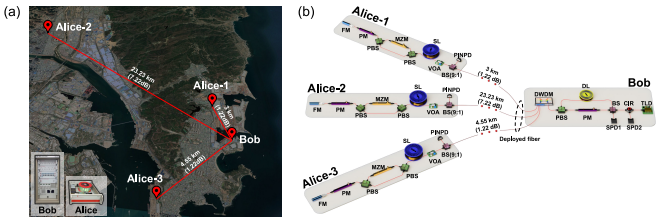


Figure 2: (a) Field deployment and (b) experimental setup of the 1×3 quantum key distribution (QKD) network system. Map data: Google, © 2021 Maxar Technologies, TerraMetrics.

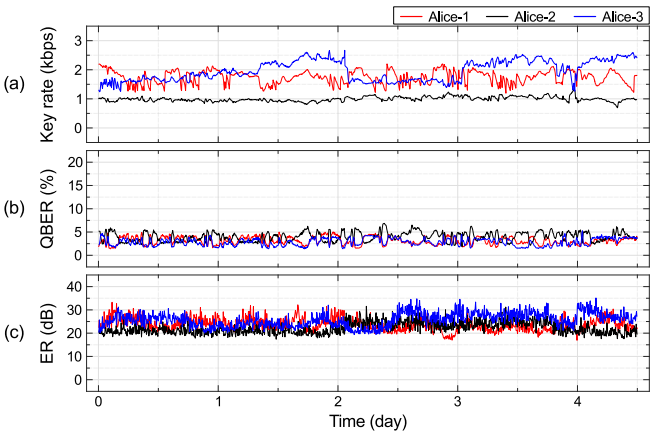


Figure 3: Experimental results of the field test: (a) Sifted key rates; (b) Quantum bit error rates (QBERs); (c) Extinction ratios (ERs) of the MZMs. The red, black, and blue solid lines are the results of Alice 1–3, respectively.

16-bit digital-to-analog converters, and each transmitter had an individual control system.

The field test was conducted over a 4-5 day period, during which the extinction ratios (ERs) of the MZMs and QKD performance parameters were measured. The results (Figure 3) showed that all the ERs were maintained over 20 dB, and satisfactory QKD performances were achieved, indicating that the proposed method could maintain MZM stability in an actual network environment.

4 Conclusion

In this study, we proposed and experimentally demonstrated an efficient MZM bias control method for QKD systems. Our experimental results showed that the proposed method can handle temperature changes and maintain the ERs over 20 dB (bit error rate $\leq 1\%$) for several days in a 1×3 QKD network testbed installed in the security facility of a smart factory in South Korea. These results demonstrate the potential of the proposed method as a cost-effective and efficient way to implement MZM bias control in QKD systems.

In future work, we plan to further improve the control performance through parameter optimization and develop an advanced method for multiple MZMs.

5 Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) under grants 2021M1A2A2043892 and 2022M3K4A1097119, the Institute for Information and Communications Technology Promotion (IITP) under grant 2020-0-00890, the Commercializations Promotion Agency for R&D Outcomes under grant 2022SCPO_B_0210, the KREONET Advanced Research Program Grant from KISTI, and the KIST research program under grants 2E31531 and 2E32801.

References

[1] Bennett, C. H. & Brassard, G., "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 175-179 (1984).

[2] Park, B. K. *et al.*, "QKD system with fast active optical path length compensation." Sci. China Phys. Mech. Astron. **60**, 060311 (2017).

[3] Wang, D. *et al.*, "Real-Time Phase Tracking Scheme With Mismatched-Basis Data for Phase-Coding Quantum Key Distribution." IEEE Photonics Journal **12**, 1-7 (2020).

[4] Park, C.-H. *et al.*, "Experimental Demonstration of an Efficient Mach-Zehnder Modulator Bias Control for Quantum Key Distribution Systems." Electronics **11** (2022).

[5] Hofer, L. R. *et al.*, "Bias Voltage Control in Pulsed Applications for Mach-Zehnder Electrooptic Intensity Modulators." IEEE Trans. Control Syst. Technol. **25**, 1890-1895 (2017).

[6] Park, B. K. *et al.*, "User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1xN quantum key distribution network system." Photonics Res. **8**, 296-302 (2020).

[7] Woo, M. K. *et al.*, "One to Many QKD Network System Using Polarization-Wavelength Division Multiplexing." IEEE Access **8**, 194007-194014 (2020).

Universal quantum optical classifier on a silicon chip

Wojciech Roga[1] * Takafumi Ono[2 3] † Baptiste Chevalier[1 4] ‡ Masahiro Takeoka[1] §

[1] *Department of Electronics and Electrical Engineering, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa, 223-8522 Japan*

[2] *Program in Advanced Materials Science Faculty of Engineering and Design, Kagawa University, 2217-20 Hayashi-cho, Takamatsu, Kagawa 761-0396, Japan*

[3] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama 332-0012, Japan*

[4] *Sorbonne Université, CNRS, LIP6, 4 place Jussieu, F-75005 Paris, France*

Abstract. The idea of data re-uploading in a qubit circuit was proposed in [1] to show that even a single qubit system can compute complicated functions of parameters of the circuit. The universality of such quantum classifier was proven. In the presented research [2] we extend these ideas to bosonic systems with even a single photon. Moreover, we experimentally demonstrate the classification using integrated photonics silicon chip. The technique applied a supervised machine learning with hybrid quantum-classical training. For training we use a novel sequential minimum optimization technique. We also discuss a fully quantum version with quantum algorithms used for training.

Keywords: Quantum Classifier, Quantum Machine Learning, Integrated Photonics

1 Context and motivation

(This submission is mostly based on arXiv:2207.06614 [2].)

In the modern data driven society data classification is a fundamental task involving the most advanced technology with big impact on everyday life and on the economy. It is predicted that the data classification market value will reach globally 5,197.92 million USD by 2028 with predicted growth by 24.29% every year [3]. Among the challenges there are the volumes of unstructured data produced today, privacy and security, as well as risks related to wrong decisions based on imprecise or false classifications by automated algorithms. Therefore, the research in the field of machine learning based classifiers is intense today. The researchers also explore possibilities offered by nowadays and future quantum technology hoping that quantum features such as: exponential scaling of the dimensionality of quantum states with the number of elementary systems, parallelism of quantum superposition, non-classical correlations provided by quantum entanglement, computational speed-up offered by quantum algorithms, and hardware developed on many platforms today, can appear useful for data handling [4]. Indeed the volume of research papers on the "quantum classifier" topic as well as the number of citations sharply increases [5] within the last ten years, see figure 1, with no sign of saturation yet. For a review see, e.g., [6].

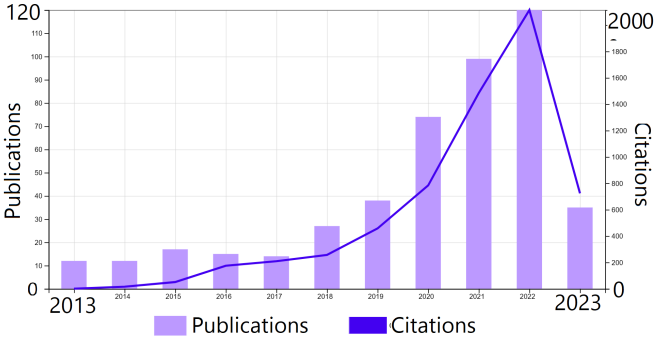


Figure 1: Clarivate Web of Science Citation Report chart for the number of publications and citations related to "quantum classifier" from 2013, as for May 2023. It shows strong interest of the community in the topic.

2 Quantum classifier with data re-uploading

One of the challenges of quantum technology applied to machine learning tasks including classifiers is the intrinsic linearity of quantum physics. The non-linearity which is used in machine learning, for example, in activation functions of neural networks, here can be introduced by measurements, many copies of data dependent quanutm states input to the system, or other tricks.

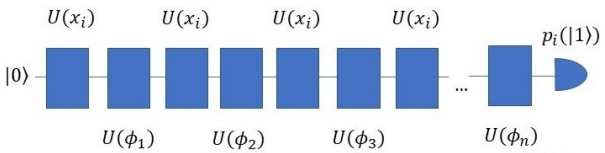


Figure 2: Scheme of deta re-uploading circuit. Training data x_i is introduced many times as a parameter of unitary transformations. Other unitary transformations contain tunable parameters used for training. The classification is based on the value of the probability $p_i(|1\rangle)$.

In [1] the authors proposed to use the so-called data re-uploading technique to introduce nonlinearites of parameters of a signle-qubit circuit. The classical data is encoded in a classically tuned parameters of gates of the

*wojciech.roga@keio.jp
†ono.takafumi@kagawa-u.ac.jp
‡baptiste.chevalier@etu.sorbonne-universite.fr
§takeoka@elec.keio.ac.jp

circuit, see figure 2. The nonlinearity of data is obtained when the values characterising a data point are introduced several times in different parts of the circuit (re-uploaded). The circuit contains also free parameters that allow for training the circuit such that the finally measured probability of a chosen state can be used as an indicator of a classification task. The probability is used to construct an appropriate cost function which is minimized during training. In this solution the training is classical that makes the setup a hybrid quantum-classical classifier.

The authors of [1] provided the arguments of the universality of such classifier, i.e., an analogue of the universal approximation theory in a single layer neural network. This demonstrates that even a single qubit system can compute complicated functions of parameters of the circuit if it is long enough and is appropriately trained.

In the present research we extend these ideas to bosonic systems with even a single photon as is shown in figure 3. Moreover, we experimentally demonstrate a classification using integrated photonics silicon chip.

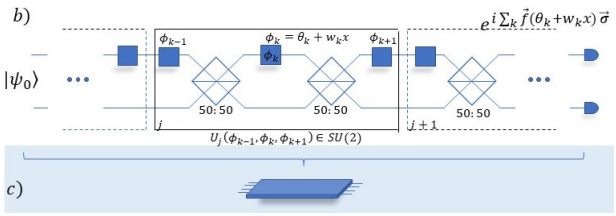


Figure 3: Two mode circuit scheme of a bosonic classifier with data re-uploading. Two 50:50 beamsplitters and three phase shifters realize an arbitrary SU(2) unitary transformation of the modes creation operators. The concatenation of such elements can realize a universal function of data x to be classified which is repeatedly uploaded together with appropriate weights w and biases θ in the arguments of the specific phase shifters.

To experimentally demonstrate the performance of the classifier we have used a chip of integrated silicon wires with total 220 photonic elements which can realize arbitrary unitary 4 mode circuit and operates in the room temperature [2]. The optical quantum circuits were fabricated using lithographic techniques on standard SOI wafers using a commercially available Multi Project Wafer service. In our proof of principle experiments, we have used two modes of this circuit to demonstrate computational abilities of even small systems when the data re-uploading method is applied similarly to the single qubit classifier of [1]. An input state in our case was a data independent two photon state. The value of features of points to be classified were input in the phases of a few phase shifters at once together with appropriate tunable weights and biases in each phase shifter. That allows us to obtain a classifier with universality feature [1, 2] schematically shown in figure 3.

3 Training

During training of the classifier in our experiment, we have used a novel method of adjusting tunable parameters. It is called Sequential Minimal Optimization method. It was proposed in [7] and was further adapted to a bosonic classifier by us [2] and adapted to estimators based on small number of measurements also by us [8]. In this method we sequentially fix all but one parameter, find the cost function as a function of this parameter, where the coefficients of the function are measured in the same circuit, and update the parameter with the value in which the cost function directly achieves the minimum. This approach offers several advantages including fast convergence to the global minimum of the cost function and robustness against the impact of barren plateaus. The condition for the method to work is that one has an easy access to exact functional dependence of the cost function on a chosen parameter while other parameters are fixed. This assumption is naturally satisfied in our system with phase shifters as the only elements with tunable parameters.

The classifying problem we considered was to correctly recognize two classes of points on the 2D surface separated by a curved line based on training data chosen randomly, figure 4 (a). In our proof of principle experiment involving 6 tunable parameters we achieved 94% accuracy of classification of points separated by an elliptical curve, figure 4 (b). The universality argument implies that more complicated problems can be solved if longer circuits are applied, which can be further tested on our circuit. We can also involve the other modes of our chip to study the influence of more complex quantum states on the classification process.

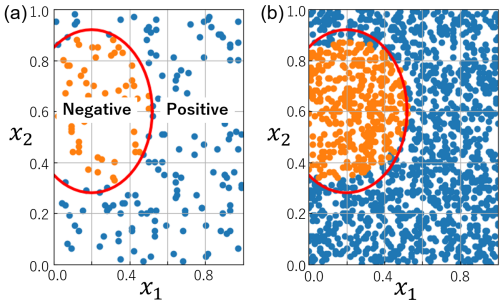


Figure 4: (a) Training point and the area to be classified by the optical quantum circuit. Red line denotes the boundary of two classes. (b) Classification results by our experiment.

As the silicon photonics systems are relatively easily extendable we conclude that this is natural and promising platform for quantum machine learning tasks. Our experiment is the first quantum optical realization of the data re-uploading based quantum classifier.

The preprint with the results discussed above is published in [2].

Although the goal of this work was to experimentally demonstrate that low dimensional quantum optical system can achieve the universal features such as classical

neural network and we did not intend to show any quantum advantage, in the next section we provide some arguments that shows that some quantum advantage is possible for example in the parallelised version of the data re-uploading classifier.

4 Quantum Training

As the number of parameters in the classifier considered by us can quickly grow the training of the circuit becomes challenging. We explored the possibility of a parallel version of the qubit based classifier in which we introduce the dependence of the tunable parameters which we assume now to be binary on additional qubits, figure 5. This trick allows us to create a quantum superposition with the amplitudes related to different values of a specifically chosen cost function. We propose to perform the quantum maximization algorithms [9] and nonlinear transformations of quantum amplitudes [10] to maximize the cost function and train the classifier. We analyzed the complexity of this scenario and observe that under specific conditions the fully quantum training can be advantageous with respect to classical maximum search algorithms achieving at most quadratic speed up.

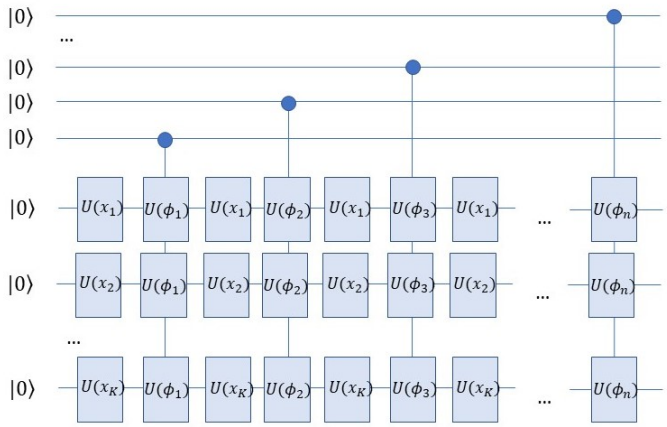


Figure 5: A parallelised version of the qubit based quantum classifier with data re-uploading in which quantum search algorithms can be used for training. Parameters x denote training data, parameters ϕ adjustable parameters which we assume here to be binary.

At the moment of the abstract submission this scenario has not been published yet.

References

[1] [2] A. Perez-Salinas, A. Cervera-Lierta, E. Gil-Fuster, and J. I. Latorre, Data re uploading for a universal quantum classifier, Quantum **4**, 226 (2020).

[2] [1] T. Ono, W. Roga, K. Wakui, M. Fujiwara, S. Miki, H. Terai, and M. Takeoka, Demonstration of a bosonic quantum classifier with data re uploading, arXiv:2207.06614 (2022).

[3] Data Bridge Market Research Report, Global Data Classification Market – Industry Trends and Forecast to 2028, *www.databridgemarketresearch.com/reports/global−data − classification − market* (2021).

[4] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, Challenges and opportunities in quantum machine learning, Nat. Comput. Sci. **2**, 567–576 (2022).

[5] Clarivate Web of Science Citation Report chart for the number of publications and citations relate to "quantum classifier" as for May 2023.

[6] W. Li, D.-L. Deng, Recent advances for quantum classifiers. Sci. China Phys. Mech. Astron. **65**, 220301 (2022).

[7] K. M. Nakanishi, K. Fujii, and S. Todo, Sequential minimal optimization for quantum classical hybrid algorithms, Phys. Rev. Research **2**, 043158 (2020).

[8] W.Roga, T. Ono, M. Takeoka, Sequential minimum optimization algorithm with small sample size estimators, arXiv:2303.00992 (2023).

[9] C. Dürr, P. Høyer. A quantum algorithm for finding the minimum, arXiv:9607014 (1996).

[10] N. Guo, K. Mitarai, K. Fujii, Nonlinear transformation of complex amplitudes via quantum singular value transformation, arXiv:2107.10764 (2021).

Self-Testing Graph States Permitting Bounded Classical Communication

Uta Isabella Meyer[1] * Ivan Šupić[1] † Frédéric Grosshans[1] ‡ Damian Markham[1] §

[1] *Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, F-75005 Paris, France*

Abstract. In this work, we give a procedure to robustly convert any inflated graph state to a state locally isomorphic to the original graph state using correlations only the inflated graph state can achieve up to unitary operations on the chain vertices. We measure the correlations with local quantum devices even permitting them to communicate classically with each other up to some restricted distance along the graph's edges. Thus, we provide a self-test for connected graph states when allowing for bounded classical communication. We also provide a self-test for any graph state, but the graph states from an underlying triangle graph or a pair of vertices, inflated or not.

Keywords: non-locality, graph states, self-testing

Self-testing involves the utilization of non-local correlations to validate multi-partite states using local devices whose precise actions are unknown or untrusted. In the research by McKague in [1], a robust self-testing approach is presented for any connected graph state, where the local units correspond to the vertices of the graph. This method assumes no communication between the local quantum devices employed to measure the correlations.

In the paper by Barrett et al. discussed in [2], correlations within a graph state are presented, which cannot be reproduced by any local hidden variable (LHV) model, even with the assistance of restricted classical communication. This result has implications in various areas such as distributed computation [4], randomness extraction [5], and establishing a depth complexity separation between classical and quantum circuits [7], [3]. This prompts the question of extending the concept of self-testing to graph states that allow communication between the quantum devices, relaxing the previous assumption.

In [6], we further extend the findings of Barrett et al. [2] to encompass any graph state by introducing a notion called "inflated graph states." For any connected graph $G = (V, E)$, an inflated graph $G' = (V', E')$ is formed by replacing each initial edge with a chain of $2d$ vertices (see Fig.1 for an example). We refer to the additional vertices as chain vertices and to the ones originating from the old graph as main vertices. The inflated graph states then exhibit correlations that no distance-d-communication-assisted LHV model can achieve.

Our work outlines a robust procedure to convert any inflated graph state into a state that is locally isomorphic to the original graph state, using correlations exclusive to the inflated graph state, up to unitary operations on the chain vertices. The correlations are archive by measurements with local quantum devices, with the provision of limited classical communication between them,

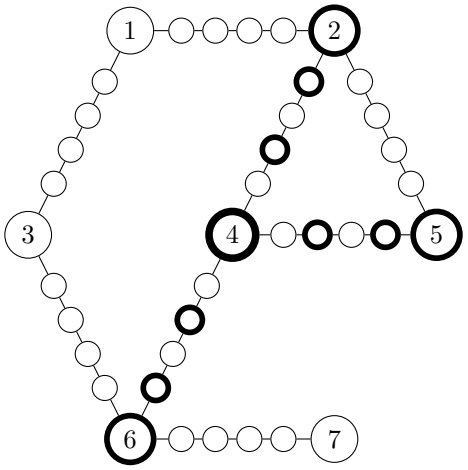


Figure 1: Example of an inflated graph for $d = 2$ from a graph with 7 (large) vertices with two induced odd cycles (vertices $1, 2, 4, 6, 3$ and vertices $2, 5, 4$). The thickened circles highlight the vertices that measure a non-trivial operator when measuring the inflated vertex stabilizer element for the main vertex 4. Main vertex 4 and all highlighted chain vertices measure Pauli operator σ^x while the power vertices $2, 5, 6$ measure Pauli operator σ^z.

*uta-isabella.meyer@lip6.fr
†ivan.supic@lip6.fr
‡frederic.grosshans@lip6.fr
§damian.markham@lip6.fr

up to a restricted distance along the edges of the graph. Consequently, we establish a self-testing mechanism for connected graph states that allows for bounded classical communication. Additionally, we present a self-test for any graph state containing a line with three vertices (excluding the triangle), regardless of inflation, thus adding to the work of [1].

Our methodologies draw inspiration from the techniques employed in [1]. In that work, McKague presents two reference experiments, which consist of measurement settings and a state representing the expected behavior of the devices. By ensuring that the reference experiments possess the same number of measurement settings as the actual quantum devices, one can certify the devices' action and the given state if the measurement outcomes align with the predictions of the reference experiment.

The first reference experiment can be applied to a graph that contains an induced odd cycle, represented by a subgraph specified by a subset of vertices, including the subset of edges formed by tuples of the subset of vertices (see Fig. 1 for an example). The measurement settings contain all vertex stabilizer elements, generators of the graph states' stabilizer group,

$$g_u^{(\prime)}|G^{(\prime)}\rangle = |G^{(\prime)}\rangle\,, \qquad \forall u \in V^{(\prime)}\,, \tag{1}$$

with $g_u^{(\prime)} = \sigma_u^x \bigotimes_{(u,v)\in E^{(\prime)}} \sigma_v^z$ and the Pauli operators $\sigma^{x,z}$. Using both reference experiments, and assuming that the devices' measurement outcomes match those of the reference experiments, [1] deduce two anti-commuting variables on each vertex of the respective subgraphs based on the measurement settings. By measuring the vertex stabilizer elements on the remaining vertices, they extend the existence of two anti-commuting variables to all vertices of the connected graph. These anti-commuting variables correspond to SWAP gates on each vertex, establishing a local isometry [10] that maps the given state to the reference graph state.

In our work, we introduce three reference experiments with the measurement settings incorporate what we term *inflated vertex stabilizer elements* on the inflated graph state,

$$f'_u = g'_u \prod_{\substack{|u-v|\%2=0\,,\\ |u-v|\%2\leq 2d}} g'_v = \sigma_u^x \bigotimes_{\substack{|u-v|\%2=0\,,\\ |u-v|\%2\leq 2d}} \sigma_v^x \bigotimes_{|u-w|=2d+1} \sigma_w^z\,, \tag{2}$$

where g'_u are vertex stabilizer elements of the inflated graph state $g'_u|G'\rangle = |G'\rangle$ for all $u \in V'$ and $|u-v|$ measures the distance of vertices u, v along the graph's edges. Consequently, the f'_u represent stabilizer elements on the inflated graph state for every main vertex $u \in V$, emulating the vertex stabilizer elements of the original graph state on the main vertices (see Fig. 1 for an example). It is worth noting that the chain vertices either perform no measurement or measure in the Pauli σ^x basis.

The first reference experiment considers an induced odd cycle subgraph. Apart from the inflated vertex stabilizer element, we include the product of all inflated vertex stabilizer elements in the list of measurement settings. Additionally, we add two more stabilizer elements from the d-inflated graph state for every vertex in the induced odd cycle to protect the non-local correlations against distance-d classical communication along the edges of the inflated graph.

The second reference experiment self-tests a (inflated) graph state with an induced (inflated) star graph, which consists of a central vertex and at least two adjacent vertices that share no edges amongst themselves. The measurement settings for this experiment comprise all (inflated) vertex stabilizer elements, including the stabilizer element obtained by multiplying all (inflated) vertex stabilizer elements on the induced (inflated) star graph.

When an inflated graph state from a pair of vertices, we resort to Clifford measurements for the third reference experiment. Clifford operators can be decomposed into products of Pauli operators, which are either stabilizer elements or not. Therefore, the constituent stabilizer elements of the Clifford operators are products of inflated vertex stabilizer elements.

We demonstrate that for all three reference experiments, the measurement settings on all chain vertices commute. As a result, we establish the same anti-commutation relations for the two variables on each main vertex, similar to the approach in [1] applied to the original graph's vertices. By utilizing SWAP gates on every main vertex, we construct a local isometry that maps the given state to the original graph state, up to unitary operators in the Pauli σ^x basis on the chain vertices. By measuring the chain vertices in the Pauli σ^x basis, the unitary operators are eliminated, thereby completing the procedure. To gain intuition regarding the procedure, [8] describe the effects of a Pauli σ^x measurement on a vertex of a graph with two nearest neighbors. After the measurement, the resulting state is locally isomorphic to a graph state with the vertex removed and the nearest neighbors sharing a new edge. By solely considering the chain vertices in the Pauli σ^x basis, one can perceive our procedure as "inflating" a graph by a factor of d in order to self-test it using local devices that can communicate up to a distance of d, while simultaneously "deflating" the inflated graph to a state isomorphic to the original graph state.

To ensure robust self-testing, we bound the anti-commutation relations and the distance between the isomorphism of the given state and the reference state by the maximal deviation ϵ of the measurement outcomes. Our tools and dependencies on ϵ are akin to those used in [1], although our bounds are slightly looser due to the additional measurement settings in the reference experiments. On the other hand, our second reference experiment for (non-inflated) graph states from graph containing an induced star subgraph allows for a more robust self-test.

References

[1] M. McKague. Self-testing graph states. In *Conf. on Quantum Computation, Communication, and Cryptography*, pages 104–120, 2011.

[2] J. Barrett. C. M. Caves. B. Eastin. M. B. Elliott. S. Pironio. Modeling Pauli measurements on graph states with nearest-neighbor classical communication. Physical Review A, 2007.

[3] S. Bravyi. D. Gosset. R. König. Quantum advantage with shallow circuits. Science 362, 2018.

[4] F. Le Gall. H. Nishimura. A. Rosmanis. Quantum Advantage for the LOCAL Model in Distributed Computing. 36th International Symposium on Theoretical Aspects of Computer Science (STACS), 49:1–49:14, 2019.

[5] M. Coudron. J. Stark.T. Vidick. Trading locality for time: certifiable randomness from low-depth circuits. Communications in mathematical physics, 2021.

[6] U. I. Meyer. F. Grosshans. D. Markham. Inflated Graph states Refute Communication Assisted LHV model. arXiv:2210.07068, 2022.

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

[8] M. Hein. J. Eisert. H. J. Briegel. Multiparty entanglement in graph states. Physical Review A, 2004.

[9] D. M. Greenberger. M. A. Horne. A. Shimony. A. Zeilinger. Bell's theorem without inequalities. American Journal of Physics, 1990.

[10] D. Mayers. A. Yao Self testing quantum apparatus. Quantum Information & Computation, 2004.

Implementation of multiparty reference-frame-independent QKD using N-qubit GHZ state

Donghwa Lee[1 2 *] Kyujin Shin[1 3 †] Yosep Kim[1 ‡] Hyang-Tag Lim[1 2 §]
Yong-Su Kim[1 2 ¶]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea*
[2] *Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Republic of Korea*
[3] *Materials Research & Engineering Center, R&D Division, Hyundai Motor Company, Uiwang 16082, Republic of Korea*

Abstract. We report that the RFI-QKD protocol can be extended to the multiparty systems using Greenberger-Horne-Zeilinger (GHZ) state. We derive the asymptotic key rate and perform proof-of-principle experiments to verify the feasibility of a secure quantum network.

Keywords: Quantum key distribution, Quantum network

1 Introduction

Entanglement provides a way to share the security of random keys between remote parties, such as quantum key distribution (QKD) [1]. In the near future, larger scale entanglement will provide us quantum networks enabling secure communication between multimode. As the number of nodes in a quantum network increases, the complexity and requirements for constructing the system also increase. One significant issue is a reference-frame mismatch among multiple parties. In typical two-party quantum key distribution (QKD) protocols, e.g., BB84 protocol, the correlation between measurement results is used to check the existence of Eve, so secure key generation fails due to this misalignment. To address this problem in two-parties QKD protocol, Reference-Frame-Independent QKD (RFI-QKD) utilizes frame rotation invariant parameter to ensure the security of quantum channel [2]. This presentation proposes a multiparty RFI-QKD protocol using N-qubit GHZ state.

2 Theory

Figure 1 shows the schematic diagram of multiparty RFI-QKD using GHZ state. To construct N-parties QKD protocol, N-qubit GHZ state is transmitted into N participants $(P_1, P_2, \cdots, P_{N-1}, P_N)$ via quantum channels. Then, all participants randomly perform projective measurement on a given single qubit on a Pauli basis and announce some

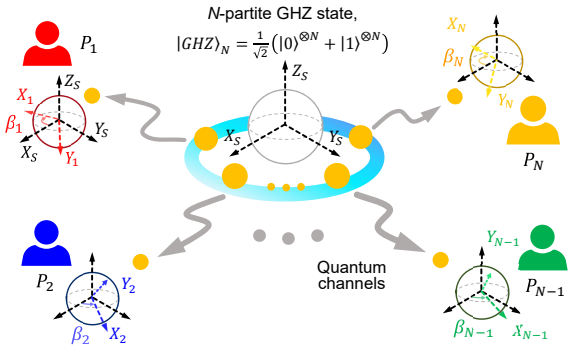


Figure 1: The schematic diagram of RFI-QKD using N-qubit GHZ state. Each participant P_i has own reference-frame X, Y and Z. In RFI-QKD, frame differences β_i occur between station preparation and projection bases.

outcomes and basic information to estimate parameters for key generation, such as quantum-bit error rate Q. In order to describe the reference frame rotation situation, we set that N-qubit GHZ state is prepared in Pauli basis $\{X_S, Y_S, Z_S\}$. Moreover, participants P_i have their reference frame of $\{X_i, Y_i, Z_i\}$ so that projective measurement is performed with relative reference frame difference of β_i. This relation can be also written as [2]

$$\begin{aligned} Z_S &= Z_i, \\ X_S &= \cos\beta_i X_i + \sin\beta_i Y_i, \\ Y_S &= \cos\beta_i Y_i - \sin\beta_i X_i. \end{aligned} \tag{1}$$

While Z basis of all the participants is invariant under the reference frame rotation, X and Y bases

*fairytale95@kist.re.kr
†shinkj@hyundai.com
‡yosep.kim@kist.re.kr
§hyangtag.lim@kist.re.kr
¶yong-su.kim@kist.re.kr

depend on the uncontrollable frame rotation β_i, and thus, secret key generation can be failed because of varying Q_X values. The main purpose of the RFI-QKD protocol is to use frame rotation invariant parameter C, to prevent key generation failure due to reference frame difference. In the situation of Eq. 1, the projective measurement with frame difference β_i can be regarded as the occurrence of relative phase in the initial GHZ state $|\Psi(\tilde{\beta})\rangle_N = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + e^{i\tilde{\beta}}|1\rangle^{\otimes N})$ where $\tilde{\beta} = \sum_i \beta_i$. Thus, the measurement outcomes belong to the correlation of $|\Psi(\tilde{\beta})\rangle_N$, and the expectation value can be estimated as $\mathrm{tr}(\rho_{\Psi_{\tilde{\beta}}} M)$ where $\rho_x = |x\rangle\langle x|$ and M is Pauli operator consisting of $\{X, Y, Z\}$. In order to define frame rotation invariant parameters, we utilize expectation values, especially the combination of security check basis, $\{X, Y\}$. Thus, C parameter of N-qubit RFI QKD protocol is given as

$$C_N = \sum_{n=1}^{2^N} \langle M_n \rangle^2. \tag{2}$$

2^N corresponds to the number of possible Pauli basis combinations in $\{X, Y\}$. We note that a sinusoidal relation between expectation value and $\tilde{\beta}$ is expected [3], so that the ideal parameter value is $C_N = 2^{N-1}$. Now, we can use the C parameter instead of Q_X for secret key generation. In multiparty RFI-QKD, the asymptotic secret key rate r_N is given as [4]

$$r_N = 1 - H[Q_Z] - I_E[Q_Z, C_N] - h(\max[\lambda_j]), \tag{3}$$

where $H(x)$ and $h(x)$ are Shannon and binary Shannon entropy, respectively. $I_E[Q_Z, C_N]$ is Eve's information $I_E[Q_Z, C_N] = Q_Z H\left[(1+v)/2\right] + (1 - Q_Z) H\left[(1+u)/2\right]$, where $u = \min\left[1/(1-Q_Z)\sqrt{C_N/2^{N-1}}, 1\right]$ and $v = 1/Q_Z\sqrt{C_N/2^{N-1} - (1-Q_Z)^2 u^2}$. λ_j.

3 Experiment

We have also experimentally demonstrated a 4-parties RFI-QKD protocol using single-photon states from spontaneous parametric down-conversion. In order to investigate the effect of reference frame rotating quantum channels, we have performed 4-parties RFI-QKD protocol concerning various $\tilde{\beta}$ cases, some of which are changed while others are fixed. The first and second rows of Fig. 2 present the experimental data of the estimated parameters and secure key rate. The first row of Fig. 2 shows Q_Z (green line) and some expectation value $\langle M_n \rangle$ curves, respectively. The estimated C parameters (red) and secure key rate

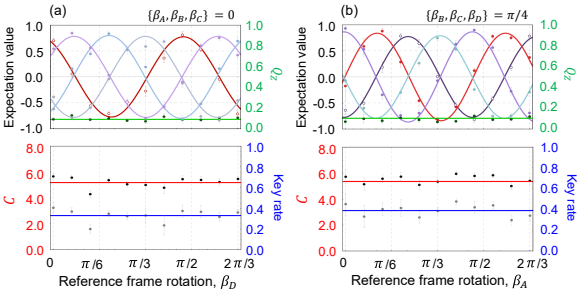


Figure 2: The experimental results of 4-party RFI-QKD in respect of reference frame rotation of (a) $\tilde{\beta} = \{0, 0, 0, \beta_D\}$ and (b) $\tilde{\beta} = \{\beta_A, \pi/4, \pi/4, \pi/4\}$, respectively.

(blue) are presented in the second row of Fig. 2. We have set two $\tilde{\beta}$ cases. Figure 2 (a) and (b) correspond to the cases of rotating β_D while others are fixed at 0 and changing β_A while others are fixed at $\frac{\pi}{4}$, respectively. While Q_Z is invariant under the varying β_D (β_A), expectation values show the sinusoidal oscillation with the visibility of $V = 0.791 \pm 0.024$ ($V = 0.809 \pm 0.028$). The average Q_Z value is $Q_Z^{(a)} = -0.093 \pm 0.018$ ($Q_Z^{(b)} = -0.090 \pm 0.020$), respectively. The C parameter corresponds to the left axis of the second row in Fig. 2. It clearly shows that the C parameters are invariant under the varying $\tilde{\beta}$. In particular, we found that $C^{(a)} = 5.264 \pm 0.356$ and $C^{(b)} = 5.521 \pm 0.305$. Finally, we have presented the secret key rate as $r^{(a)} = 0.339 \pm 0.058$ and $r^{(b)} = 0.395 \pm 0.051$ corresponding to the right axis of Fig. 2. All participants can generate the secret keys through our multiparty RFI-QKD protocol.

References

[1] A. K. Ekert, *Quantum cryptography and bell's theorem,* in *Quantum Measurements in Optics,* (Springer, 1992), pp. 413–418.

[2] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, *Reference-frame-independent quantum key distribution, Physical Review A* **82**, 012304 (2010).

[3] D. Lee, S. Hong, Y.-W. Cho, H.-T. Lim, S.-W. Han, H. Jung, S. Moon, K. J. Lee, and Y.-S. Kim, *Reference-frame-independent, measurement-device-independent quantum key distribution using fewer quantum states,* Opt. Lett. **45**, 2624–2627 (2020).

[4] M. Epping, H. Kampermann, D. Bruß *et al.*, *Multi-partite entanglement can speed up quantum key distribution in networks, New Journal of Physics* **19**, 093012 (2017).

Quantum operations with superposed time axis

Seok Hyung Lie,[1] Hyunseok Jeong,[2] and M.S. Kim[3]

[1]*School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371, Singapore*
[2]*Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea*
[3]*QOLS, Blackett Laboratory, Imperial College London, London, SW7 2AZ, UK.*

(Dated: May 22, 2023)

I. SUMMARY

In the quantum theory, matrix transposition has been known to reverse the order of quantum processe representing time reversal transformations. However, recent discoveries regarding the indefinite causal order of quantum processes propose that there may be other, more general symmetry transformations of time besides complete reversal. In this study, we introduce an expanded concept of matrix transposition, the generalized transposition, that takes into account general bipartite unitary transformations of a quantum operation's future and past Hilbert spaces, allowing for the description of superpositions of the time axes. This approach treats time and space equally and can be used in fields like quantum gravity, where the spatio-temporal structure emerges from quantum mechanics. We apply this generalized transposition to investigate a continuous generalization of perfect tensors, a dynamic version of tracing out a subsystem, and the compatibility of multiple time axes in bipartite quantum interactions. Notably, we demonstrate that when a bipartite interaction is consistent with more distinct local temporal axes, there is a reduced allowance for information exchange between the two parties in order to prevent causality violations.

II. MAIN RESULTS

Matrix transposition, when applied to a composition of matrices, inverts the order of them, i.e.,

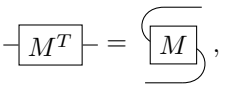
$$(NM)^T = M^T N^T. \tag{1}$$

From this fact, it is natural to model the inversion of time of quantum system by applying the matrix transposition to quantum operations on the system, or more precisely, on the Kraus operators of them:

$$\mathcal{N}^T(\rho) := \sum_i K_i^T \rho K_i^*, \tag{2}$$

where $\mathcal{N}(\rho) = \sum_i K_i \rho K_i^\dagger$ is a quantum channel. Indeed, in Ref. [1], it has been shown that the only order-reversing transformation that works consistently even when it acts on subsystem of joint system processes is the matrix transposition. However, by no means it should be the only symmetry transformation of the temporal structure of quantum processes, considering the recent development of nonclassical causal structure within quantum theory [2, 3].

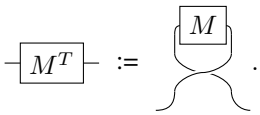
In this work, we construct a symmetry transformation that generalizes the matrix transposition. The transpose operation $M \mapsto M^T$ [1] can be understood as the rotation by 180° in tensor diagram, i.e.



(3)

whose action of quantum channels is given as (2). (Adjoint operation †, on the other hand, is modelled by mirror reflection on tensor diagram.) Geometrically, one can interpret the transpose operation as flipping the direction of time. However, since there are ways to rotate a diagram other than the rotation by 180°, one could naturally become curious after seeing (3) if there is a way to express the general transformation of the direction of the *time axis itself*, not just flipping the time direction for a given time axis as in Ref. [1]. In this section, we propose such a generalization.

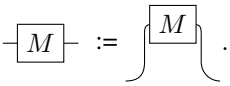
The unitary operator is the complex generalization of the orthogonal matrix, hence it generalizes the action of rotating to complex Hilbert spaces. First, we observe that we can stretch and curve the wires in (3) to transform it into



(4)

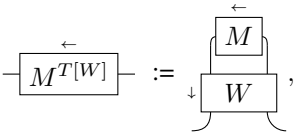
Here, the crossing wires in the right hand side can be interpreted as the swapping operator $F := \sum_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i|$, which is a unitary operator.

On the other hand, we also have the following expression,



(5)

Here, we can say that the swapping operator in (4) is replaced by the identity operator. Comparing (4) and (5), one could understand transpose operation as the exchange of future and past Hilbert space. We can naturally guess that if we substitute them with a general bipartite unitary operator, we can get a generalization of transpose operation. Therefore, we define *the generalized transposition* $T[W]$ for each bipartite unitary operator $W \in \mathfrak{U}(A^{\otimes 2})$ which maps any $M \in \mathfrak{B}(A)$ to $M^{T[W]}$ defined in the following way,



(6)

where the arrow next to each box indicates the flow of time, or the direction from input to output. Concretely, $M^{T[W]}$ is

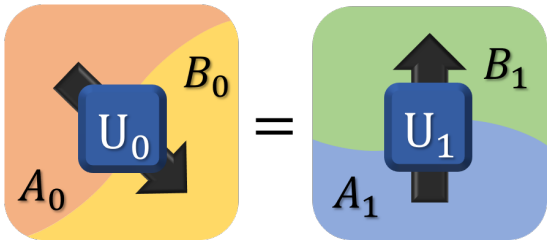


FIG. 1. Consider a unitary operation $U_0 : A_0 \to B_0$. One can interpret A_0 and B_0 as the past and the future Hilbert spaces of a quantum system and U_0 as its time evolution. However, If $A_0 \otimes B_0 = A_1 \otimes B_1$ with W being the bipartite unitary operator connecting two different tensor decompositions, then U_0 can be interpreted as U_1 from A_1 to B_1 if $U_1 = U_0^{T[W]}$.

defined as, with a fixed basis $\{|i\rangle\}$ of A,

$$M^{T[W]} := \sum_{i,j} (\mathbb{1} \otimes \langle j|) W (M|i\rangle \otimes |i\rangle\langle j|). \tag{7}$$

Once we defined how generalized transposition acts on matrices, we can define the corresponding action of generalized transposition on quantum channels, or more generally, on linear maps. We can define the supermap $\mathfrak{T}[W]$ given as

$$\mathfrak{T}[W](\mathcal{N})(\sigma) := |A|^2 \operatorname{Tr}_{BA'}[(\mathbb{1}_A \otimes \phi^+_{BA'})(\mathrm{Ad}_W(J^{\mathcal{N}}_{AB}) \otimes \sigma_{A'})], \tag{8}$$

for any $\sigma \in \mathfrak{B}(A')$ and $\mathcal{N} \in \mathfrak{L}(A)$. For the sake of brevity, we will use the notation $\mathcal{N}^{T[W]} := \mathfrak{T}[W](\mathcal{N})$ interchangeably. This seemingly complicated definition of superchannel $\mathfrak{T}[W]$ is given in this way so that $(\mathrm{Ad}_M)^{T[W]} = \mathrm{Ad}_{M^{T[W]}}$. From this, one can easily see that if

$$\mathcal{N}(\rho) = \sum_n c_n K_n \rho K_n^\dagger, \tag{9}$$

with complex numbers $c_n \in \mathbb{C}$, then

$$\mathcal{N}^{T[W]}(\rho) = \sum_n c_n K_n^{T[W]} \rho K_n^{T[W]\dagger}. \tag{10}$$

Now we have a tool for describing symmetry transformations of the temporal structure of quantum processes, we define the compatibility of a quantum process with multiple temporal structures in terms of the generalized transposition as follows. It is a direct generalization of *bidirectional operations* for the conventional transposition considered in Ref. [1].

Definition 1. A quantum channel $\mathcal{N}$ is compatible with a generalized transposition $T[W]$ when $\mathcal{N}^{T[W]}$ is also a channel.

A particularly important case is when the generalized transposition acts on a subsystem of bipartite quantum process.

Definition 2. A quantum channel $\mathcal{N} \in \mathfrak{C}(AB)$ is compatible with a generalized transposition $T_B[W]$ on B when $\mathcal{N}^{T_B[W]} := (\mathfrak{id}_A \otimes \mathfrak{T}_B[W])(\mathcal{N})$ is also a channel.

This definition enables us to study the meaning of multiple systems sharing the same direction of time by altering the local temporal structure through the generalized transposition. However, the definition of the generalized transposition could be too general for representing the symmetry transformation of purely temporal structure of quantum processes. We thus restrict out attention to a smaller class of generalized transpositions that are *unital*, i.e. $\mathbb{1}^{T[W]} = \mathbb{1}$. Interestingly, a generalized transposition is unital if and only if it is trace-preserving. A generalized transposition $\mathfrak{T}[W]$ being unital is also equivalent to the corresponding bipartite unitary operator W preserving the maximally entangled state $d^{-1/2}\sum_i |i\rangle|i\rangle$. Since this class of generalized transposition preserves the trivial event, i.e., the identity channel, it is rational to assume that they are a good candidate of pure manipulation of temporal structure.

A naturally following question is if it is possible to classify all the generalized transposition according to their locally unitarily similar unital transposition. Proving or disproving it is equivalent to the open problem of showing if every bipartite d^2-dimensional unitary operator has at least one maximally entangled state as its eigenvector [4, 5]. If a bipartite unitary operator U has this property, we say that U preserves ME (maximally entangled state). It has been shown to be true for the case of $d = 2$ [6, 7], but the problem is not so clear for higher dimensions. In this work, we showed that this is indeed true for a large class of bipartite unitary operators, namely, for controlled unitary operators.

Theorem 3. Every qudit-qudit controlled unitary operator W preserves ME.

It has the following implication for generalized transpositions. In other words, for a large class of generalized transpositions, there is actually at least one unitary operation compatible with them.

Corollary 4. For every qudit-qudit controlled unitary operator W, there exists a unitary channel that is compatible with the generalized transposition $T[W]$.

Moreover, in many scenarios, quantum processes do not exist in isolation but are embedded in a context, i.e., superchannels. For example, state preparation and measurement can be interpreted as the surrounding superchannel, too. Say, a quantum channel Φ is fed into a superchannel $\mathfrak{F}$. If Φ is compatible with a generalized transposition $\mathfrak{T}[W]$, then the supermap $\mathfrak{F} \circ \mathfrak{T}[W^\dagger]$ should also a superchannel for the whole picture including the superchannel $\mathfrak{F}$ to be consistent, because

$$\mathfrak{F} \circ \mathfrak{T}[W^\dagger](\mathfrak{T}[W](\Phi)) = \mathfrak{F}(\Phi). \tag{11}$$

This restricts which state preparation is consistent with a given generalized transposition. Especially, not every quantum state can be fed into as a local input of a bipartite quantum interaction that has multiple consistent local temporal structures. This is natural considering that allowing for arbitrary input could violate the causality when two systems do not share a common direction of time.

Proposition 5. A state preparation superchannel given as $\mathfrak{P}^\sigma(\mathcal{N}) := \mathcal{N}(\sigma)$ is compatible with a generalized transposition $T[W]$ of its input channel, i.e., $\mathfrak{P}^\sigma \circ \mathfrak{T}[W^\dagger]$ is a superchannel, if and only if there exists a quantum state τ such

that

$$W(\mathbb{1}_A \otimes \sigma_{A'}^T) = (\mathbb{1}_A \otimes \tau_{A'}^T)W. \tag{12}$$

Our work also includes an extensive discussion on tensor network picture of universe, continuous generalization of perfect tensors and the supertrace with its relation with factorizable maps. Please refer to the technical manuscript for more information and concrete definition of terms used above.

[1] G. Chiribella and Z. Liu, Communications Physics **5**, 190 (2022).

[2] G. Chiribella, G. M. D'Ariano, and P. Perinotti, EPL (Europhysics Letters) **83**, 30004 (2008).

[3] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Physical Review A **88**, 022318 (2013).

[4] Z. Puchała, Ł. Rudnicki, K. Chabuda, M. Paraniak, and K. Życzkowski, Physical Review A **92**, 032109 (2015).

[5] S. Brahmachari, R. N. Rajmohan, S. A. Rather, and A. Lakshminarayan, arXiv preprint arXiv:2210.13307 (2022).

[6] M.-Y. Ye, D. Sun, Y.-S. Zhang, and G.-C. Guo, Physical Review A **70**, 022326 (2004).

[7] B. Kraus and J. I. Cirac, Physical Review A **63**, 062309 (2001).

Characterization of quantum entanglement in Si quantum dot systems: Operational quasiprobability approach

Junghee Ryu[1] Hoon Ryu[1] *

[1] *Division of National Supercomputing, Korea Institute of Science and Technology Information, Daejeon 34141, Republic of Korea*

Abstract. We characterize a bipartite entanglement in a realistic silicon double quantum dot platform. Arbitrary two-qubit entangled states are generated by conducting a single-qubit rotation and a controlled-NOT operation. To quantify the entanglement, we employ a marginal operational quasiprobability (OQ) function, which serves as a reliable entanglement witness even in the presence of significant noise. We here discuss how the entanglement characteristic of the Si DQD structure are affected by charge noises which is omnipresent in semiconductor devices.

Keywords: Entanglement, Silicon quantum dot, Operational quasiprobability

1 Introduction

Quantum correlations, such as entanglement, play a crucial role in quantum information technologies, providing advantages over classical counterparts in quantum computing, quantum communication, quantum metrology, and so on. Thus, the quantification of the quantum correlations is important as it can be used to explore the potential practicality in information processing e.g., suitable states of certain quantum circuits. Especially, we here study the characterization of the quantum entanglement. To this end, we employ a marginal operational quasiprobability (OQ) function that allows negative values of the function if a given state is entangled [1]. We apply the marginal OQ method to the electron-spin qubits in a silicon (Si) double quantum dot (DQD) platform, where a single-qubit rotation and a two-qubit controlled-NOT operation are conducted sequentially in time to generate arbitrary two-qubit entangled states.

2 Method

We use a newly defined quasiprobability function for discrete systems, which is linked to experimental situations in which incompatible observables are measured consecutively. It turns out that the OQ function method identifies the nonclassicality of quantum systems in an operational way. Furthermore, for multipartite systems the marginal OQ function can be used as an entanglement witness. In principle, the OQ approach is advantageous over the entanglement verifications involving the full state tomography process in a sense that our method can be calculated with directly measurable quantities in laboratory and requires less number of measurements to characterize the entanglement.

The N-qubit OQ function is defined by applying a discrete Fourier transform on the composite expectation value $C(\mathbf{n}^1,\ldots,\mathbf{n}^N) \equiv C(\mathbf{n}^1)\otimes\cdots\otimes C(\mathbf{n}^N)$ as

$$\mathcal{W}(\mathbf{a}^1,\ldots,\mathbf{a}^N) \equiv \frac{1}{2^{NK}} \sum_{\mathbf{n}^1,\ldots,\mathbf{n}^N} (-1)^{-\mathbf{a}^1\cdot\mathbf{n}^1\cdots-\mathbf{a}^N\cdot\mathbf{n}^N} \times C(\mathbf{n}^1,\ldots,\mathbf{n}^N), \quad (1)$$

where a tuple $\mathbf{n}^i = (n_1^i, n_2^i, \ldots, n_K^i)$ represents possible measurement configurations for i-th subsystem having K measurement operators and $\mathbf{a}^i\cdot\mathbf{n}^i = \sum_k a_k^i n_k^i$. The expectation value $C(\mathbf{n}^1,\ldots,\mathbf{n}^N)$ represents the measurement configurations that are implemented in a laboratory (see Ref. [2] for more details). We consider the following formula to quantity the entanglement

$$\mathcal{N} \equiv \frac{1}{2}\sum_{\mathbf{a}} \left(|\mathcal{W}(\mathbf{a})| - \mathcal{W}(\mathbf{a})\right). \quad (2)$$

The value $\mathcal{N}$ indicates the sum of the negative components of the OQ function, thus the case of $\mathcal{N} > 0$ can be regarded as the indicator of the entanglement for given quantum systems.

Our working example is the two-qubit time responses that are generated from a Si DQD system. A 2D simulation domain of DQD structure reported in [3] encodes qubits to electron spins that are created with quantum confinement driven by biases imposed on top electrodes, see Figure 1(a). The DQD system is initialized to a $|\downarrow\downarrow\rangle$ state by filling the ground down-spin state of the left and right quantum dot with a single electron. To this end, we set the left (V_{L}) and right gate bias (V_{R}) to 555mV. For the middle gate bias (V_{M}), we consider two cases: (a) 400mV with an exchange energy (J) of 76KHz (weak interaction) and (b) 407.5mV with 18.4MHz (strong interaction) respectively, as shown in Figure 1(b). A spatial distribution of the static magnetic field that is generated by a horseshoe-shaped cobalt micro-magnet in the real case [3] is utilized as an input of simulations. The resulting Zeeman-splitting energy of the left (E_{ZL}) and right spin (E_{ZR}) turn out to be 18.31GHz and 18.45GHz respectively. All these conditions imply that we are able to implement a single-qubit rotation and a two-qubit gate operation to the initial state by controlling the middle gate bias (V_{M}).

*elec1020@kisti.re.kr

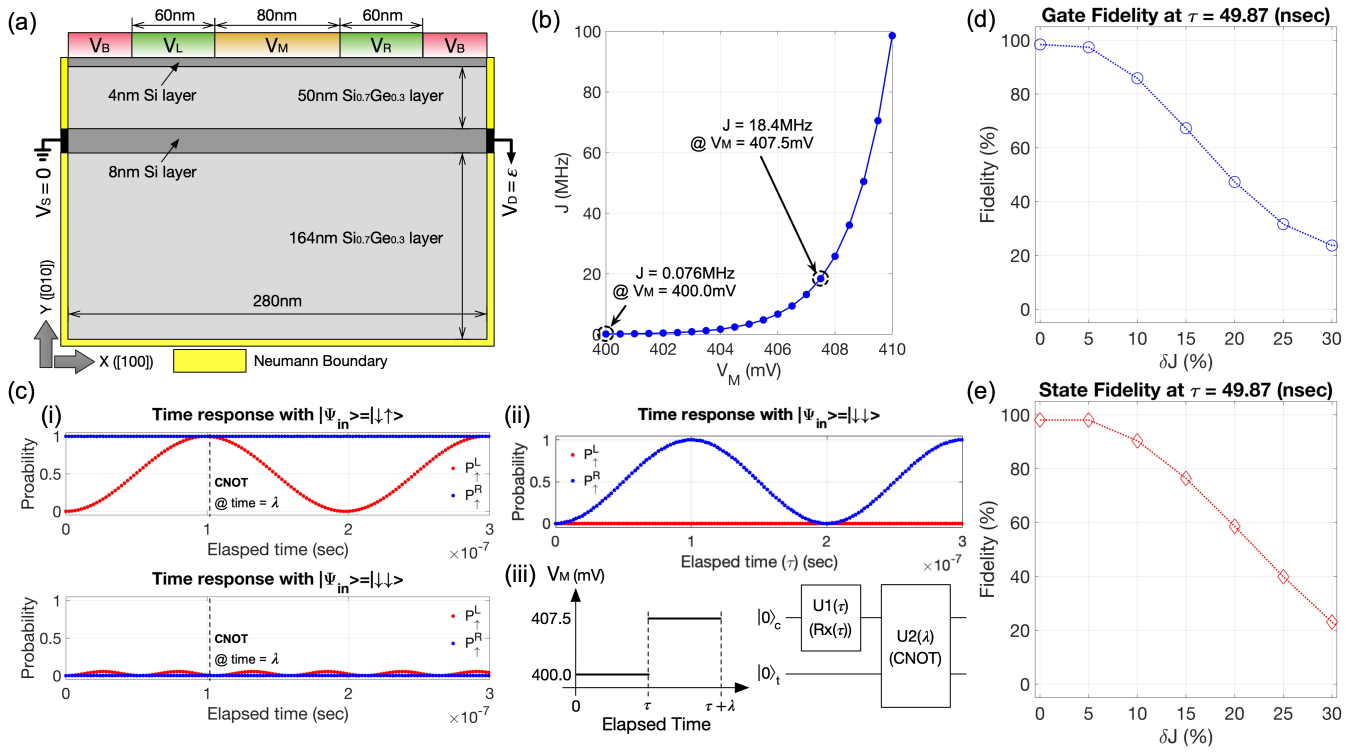


Figure 1: (a) A 2D simulation domain for our case. The real DQD structure [3] is long along the Z([001])-direction, thus it is described in a 2D manner with a periodic boundary condition along the Z-direction. (b) J given as a function V_{M} for $V_{\mathrm{R}} = V_{\mathrm{L}} = 555$mV. In our case, $J \sim 76$KHz and 18.4MHz when $V_{\mathrm{M}} = 400$mV and 407.5mV, respectively. (c) (i) For the strong interaction ($V_M = 407.5$mV), the fastest CNOT operation can be achieved in $\sim 1.05\times10^{-7}$ (λ) seconds upon the system intialization. The gate fidelity of the CNOT operation becomes 98.35%. (ii) For the weak interaction ($V_M = 400$mV), we can make only the right spin oscillate by setting the frequency of AC pulse equal to the Zeeman-splitting energy of the right spin. (iii) A conceptual illustration for time-dependent control of V_M and resulting two-qubit unitary gate that generates the entangled states. (d, e) The fidelity of the two-qubit unitary and the corresponding output state at $\tau = 4.99\times10^{-8}$ seconds (the time spot when the output state is maximally entangled) are shown as a function of δJ, which represents the unintentional variation of J with respect to its noise-free value.

3 Results

In order to characterize the entanglement, we employ the marginal OQ method with the two measurement operators. In general, the OQ function can be constructed by using the positive operator-valued measure (POVM) measurements, but we here consider only two projective measurements defined by the Pauli matrices for cost-efficient calculations [1]. By calculating the negative values of the marginal OQ function, we can quantify the entanglement. The states are generated by the sequential application of a $R_x(\alpha)$ and a CNOT operation, thus the output can be expressed by $|\psi(\alpha)\rangle = \cos(\alpha/2)\,|00\rangle - i\sin(\alpha/2)\,|11\rangle$. The noise-driven characteristic of entanglement is also investigated by changing the noise-free exchange interaction J to $J\times(1+\delta J)$ as we treated to simulate the fidelity shown in Figure 1(c) and Figure 1(d).

Figure 2(a) shows the results of the noise-free case ($\delta J = 0$) as a function of the time τ. The blue (normalized) and green (raw) lines indicate the entanglement strength calculated with the marginal OQ method, and the red line is the one obtained with the negativity method. The maximal strength reads 0.2348 (green line) at $\tau = 4.99\times10^{-8}$ seconds. Note that there exist the intervals of τ where our method cannot characterize the entanglement precisely, which is because the marginal OQ function is constructed by using only two measurement operators for the cost-efficient calculations.

We also explore the behavior of the entanglement characteristic when the Si DQD platform suffers from the charge noises ($\delta J \neq 0$), which is omnipresent in semiconductor devices. Figure 2(b) shows the results of the noise-driven degradation in fidelity and in the marginal OQ method. The noise-driven pattern of entanglement characterization does not necessarily follow that of fidelity, and the output state of the noisy two-qubit operation still has meaningful strength of entanglement. We find that while the charge noise causes huge degradation in the state fidelity, it has a weaker effect on the entanglement resource. In a highly noisy environment, the state fidelity drops to around 20%, but more than 70% of the resource can be retained for maximally entangled Bell states. It should be noted that as shown in Figure 1(d) and 1(e), the gate and state fidelity are sensitive to charge noises, and are sharply reduced as δJ increases.

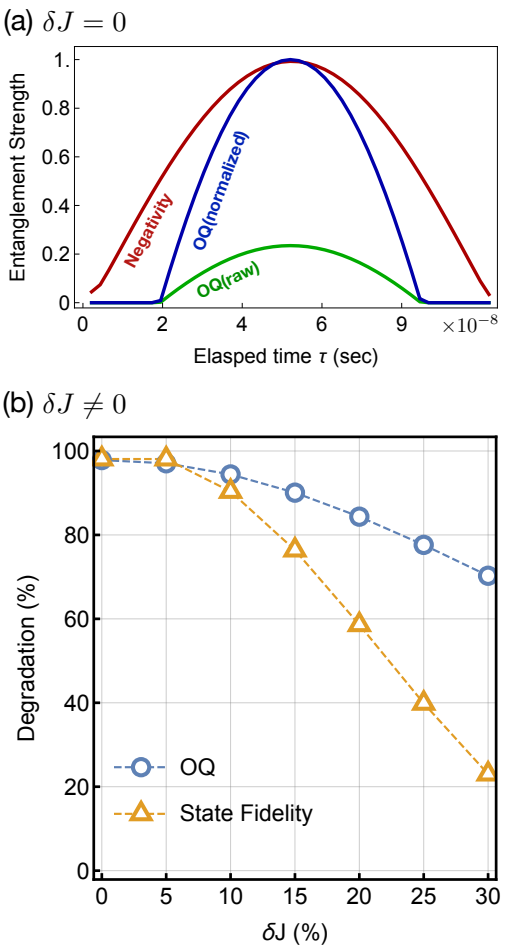


Figure 2: (a) The results of the noise-free case ($\delta J = 0$) as a function of the time τ. (b) The results of the noise-driven degradation in state fidelity and OQ method.

However, Figure 2(b) clearly shows that when the noise is too strong the results we present can be still fairly solid enough to claim the utility of the marginal OQ method as a cost-efficient indicator of entanglement strength, where the cost-efficiency of our method against the negativity method will sharply increase as the size (in qubits) of targeted quantum states increases.

4 Acknowledgements

This work has been carried out under the support of the National Research Foundation of Korea (NRF) grant (NRF-2020M3E4A1079792 and NRF-2022M3K2A1083890).

References

[1] J. Ryu *et al.* Operational quasiprobabilities for qudits *Phys. Rev. A* **88**, 052123 (2013).

[2] J. Ryu *et al.* Exploring entanglement resource in Si quantum dot systems with operational quasiprobability approach *Quantum* **6**, 827 (2022).

[3] D. M. Zajac *et al.* Resonantly driven CNOT gate for electron spins *Science* **359**, 439 (2018).

Quantum public key cryptography using single qubit rotation operators

Ji-Woong Choi†, Sang-Wook Han*

Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea

Abstract In order to implement quantum cryptography that can provide the same functions as modern cryptography, research on quantum public key cryptography is essential. In this paper, we introduce a quantum trapdoor one-way function using the conditions of quantum evolutions, such as cyclic and dynamic evolution of quantum states. Subsequently, we propose a quantum public key cryptography using it.

Keywords: Quantum public key cryptography, quantum trapdoor one-way function, single qubit rotation operator

1. Introduction

Recently, in the field of quantum cryptography, various research has been conducted on quantum authentication, quantum digital signature, and quantum direct communication, in addition to quantum key distribution, which has entered the commercialization step thorough quantum network [1-2]. However, most quantum protocols have been proposed based on symmetric key cryptography because there has not been notarized quantum public key cryptography so far [3-4]. These quantum protocols have disadvantages of using classical information or implementing through complex methods in order to overcome the limitations of symmetric key cryptography [5-6]. In this paper, we introduce quantum trapdoor one-way function using single qubit rotation operators to overcome the limitations of quantum protocols based on symmetric key cryptography. Subsequently, we propose a quantum public key cryptography using proposed quantum trapdoor one-way function.

2. Quantum trapdoor one-way function

We explain the quantum evolution conditions of quantum states, before introducing the quantum trapdoor one-way function. First, we assume that the arbitrary quantum state satisfies eigen value equation as follows.

$$|\Psi\rangle = R_{\hat{n}}^{\dagger}(\theta)R_{\hat{m}}^{\dagger}(\varphi)R_{\hat{n}}(\theta)R_{\hat{m}}(\varphi)|\psi\rangle = \lambda|\psi\rangle, \quad (1)$$

where $R_{\hat{n}}(\theta)$ and $R_{\hat{m}}(\varphi)$ are the single qubit rotation operator with rotation axis $\hat{n}$ and $\hat{m}$, respectively. λ is a complex number. If $\lambda = e^{i\varepsilon}$ $(\neq \pm 1)$, Eq. (1) satisfies the condition of cyclic evolution. Here, the additional global phase $e^{i\varepsilon}$ means the geometric (Berry) phase. The fidelity $F(\rho,\sigma)$ of $|\psi\rangle$ and $|\Psi\rangle$ is as follows.

$$F(\rho,\sigma) = |\langle\psi|\Psi\rangle| = \left|\langle\psi|R_{\hat{n}}^{\dagger}(\theta)R_{\hat{m}}^{\dagger}(\varphi)R_{\hat{n}}(\theta)R_{\hat{m}}(\varphi)|\psi\rangle\right|. \quad (2)$$

If $F(\rho,\sigma) = 1$, it means that $|\psi\rangle$ and $|\Psi\rangle$ are identical except for the global phase. On the other hand, if $F(\rho,\sigma) = 0$, it means that the two quantum states are perpendicular to each other. For example, we consider $\hat{n} = \left(\sin\zeta\cos\frac{\pi}{4}, \sin\zeta\sin\frac{\pi}{4}, \cos\zeta\right)$, $\hat{m} = \left(\sin\frac{\pi}{4}\cos\frac{\pi}{4}, \sin\frac{\pi}{4}\sin\frac{\pi}{4}, \cos\frac{\pi}{4}\right)$, and $\varphi = \frac{3\pi}{4}$ on the Bloch sphere. Figure 1 represents $F(\rho,\sigma)$ according to ζ and θ when $|\psi\rangle = |0\rangle$. The case of $F(\rho,\sigma) = 1$ is satisfied corresponds to the green line, the black line, and the cyan point. In the case of the green line and the black line are satisfied commutation relation $[R_{\hat{n}}(\theta), R_{\hat{m}}(\varphi)] = 0$ and anti-commutation relation $\{R_{\hat{n}}(\theta), R_{\hat{m}}(\varphi)\} = 0$. The cyan point is the case of $\zeta \approx 0.70\pi$ and $\theta \approx 0.79\pi$, and the additional geometric phase $\lambda = e^{i(1.337\pi)}$ is generated after cyclic evolution. Meanwhile, at the white points, $|\psi\rangle$ becomes a perpendicular quantum state $|\psi\rangle_{\perp}$ after dynamic evolution, and an additional dynamic phase $\lambda = e^{i(1.089\pi)}$ or $e^{i(1.907\pi)}$ is generated.

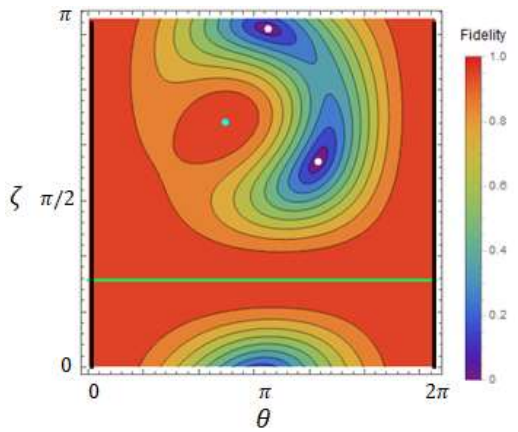


Figure 1. The fidelity $F(\rho,\sigma) = \left|\langle\psi|R_{\hat{n}}^{\dagger}(\theta)R_{\hat{m}}^{\dagger}(\varphi)R_{\hat{n}}(\theta)R_{\hat{m}}(\varphi)|\psi\rangle\right|$ according to ζ and θ when $|\psi\rangle = |0\rangle$.

E-mail: jodol007@kist.re.kr, swhan@kist.re.kr

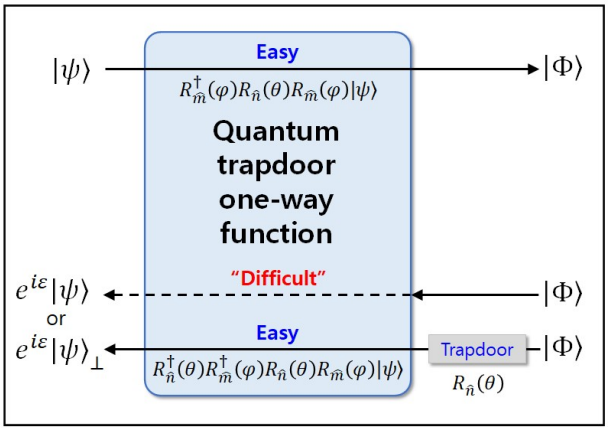


Figure 2. The quantum trapdoor one-way function using single qubit rotation operators

Next, we introduce the quantum trapdoor one-way function using single qubit rotation operators, which is a prerequisite for implementing a quantum public key cryptography. A trapdoor one-way function should provide a function that is easy to compute and difficult to invert without trapdoor information. A quantum trapdoor one-way function should also provide the same functionality. Figure 2 presents the quantum trapdoor one-way function using single qubit rotation operators. The proposed quantum trapdoor one-way function is single qubit rotation operators $R_{\hat{m}}^{\dagger}(\varphi)R_{\hat{n}}(\theta)R_{\hat{m}}(\varphi)$ that satisfies the conditions of cyclic or dynamic evolution in Eq. (1), and $R_{\hat{n}}(\theta)$ is used as the trapdoor information. As shown in Figure 2, the process of $|0\rangle \rightarrow |\Phi\rangle = R_{\hat{m}}^{\dagger}(\varphi)R_{\hat{n}}(\theta)R_{\hat{m}}(\varphi)|0\rangle$ is easy, but the process of $R_{\hat{n}}^{\dagger}(\theta)|\Phi\rangle = e^{i\varepsilon}|0\rangle$ or $e^{i\varepsilon}|1\rangle$ $(e^{i\varepsilon} \neq \pm 1)$ is very difficult without trapdoor information $R_{\hat{n}}(\theta)$. In the proposed quantum trapdoor one-way function, an eavesdropper cannot estimate trapdoor $R_{\hat{n}}(\theta)$ through $R_{\hat{m}}^{\dagger}(\varphi)R_{\hat{n}}(\theta)R_{\hat{m}}(\varphi)$. In addition, since the single qubit rotation operator $R_{\hat{n}}(\theta)$ is used as trapdoor information, it is possible to provide the same functionality as modern cryptography and to secure the security of quantum cryptography.

3. Quantum public key cryptography

We propose a quantum public key cryptography using proposed quantum trapdoor one-way function. Figure 3 show a schematic representation of the quantum public key cryptography.

Preparation step

P1. Alice randomly selects the private key $\otimes_{i=1}^{N} R_{\hat{m}_i}(\varphi_i)$ corresponding to the conditions of cyclic or dynamic evolutions of the quantum state $|0\rangle$.

P2. Alice determines the public key $\otimes_{i=1}^{N} R_{\hat{n}_i}^{\dagger}(\theta_i)R_{\hat{m}_i}(\varphi_i)R_{\hat{n}_i}(\theta_i)$ corresponding to the private of P1 step. Subsequently, she announces the public key.

Encryption step

E1. Bob randomly generates message $\otimes_{j=1}^{N}|m_j\rangle \in \{|0\rangle, |1\rangle\}$ and decoy qubits $\otimes_{k=1}^{M}|d_k\rangle \in \{|+\rangle, |-\rangle\}$ randomly to send to Alice.

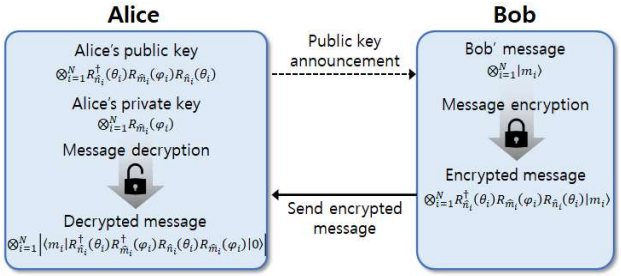


Figure 3. A schematic representation of the quantum public key cryptography using single qubit rotation operators.

E2. Bob encrypts $|\psi_i\rangle \in \{|m_j\rangle, |d_k\rangle\}$ using Alice's public key as follows.

$$|E\rangle = \otimes_{i=1}^{N+M} R_{\hat{n}_i}^{\dagger}(\theta_i)R_{\hat{m}_i}(\varphi_i)R_{\hat{n}_i}(\theta_i)|\psi_i\rangle. \quad (3)$$

Then, Bob transmits $|E\rangle$ of Eq. (3) to Alice.

Decryption step

D1. Bob informs the information of decoy qubits, and Alice decrypts as follows.

$$\otimes_{i=1}^{M} R_{\hat{n}_i}^{\dagger}(\theta_i)R_{\hat{m}_i}^{\dagger}(\varphi_i)R_{\hat{n}_i}(\theta_i) R_{\hat{n}_i}^{\dagger}(\theta_i)R_{\hat{m}_i}(\varphi_i)R_{\hat{n}_i}(\theta_i)|\psi_i\rangle. \quad (4)$$

Then, Alice measure decoy qubits using x-basis, and verifies the security of the quantum channel.

D2. Alice generates a quantum state $|D\rangle = \otimes_{i=1}^{N} R_{\hat{m}_i}(\varphi_i)|0\rangle$ for decryption using the private key. Subsequently, she performs the decryption process using $|E\rangle$ as follows.

$$|\langle E|D\rangle| = \otimes_{i=1}^{N} \left|\langle m_i|R_{\hat{n}_i}^{\dagger}(\theta_i)R_{\hat{m}_i}^{\dagger}(\varphi_i)R_{\hat{n}_i}(\theta_i)R_{\hat{m}_i}(\varphi_i)|0\rangle\right|. \quad (5)$$

D3. In the case of Alice's private key satisfies cyclic evolution, Eq. (4) is $\otimes_{i=1}^{N}|e^{i\varepsilon}||\langle m_i|0\rangle|$. If $F(\rho,\sigma) = 1$, Bob's message is $|m_i\rangle = |0\rangle$. Otherwise, if $F(\rho,\sigma) = 0$, $|m_i\rangle = |1\rangle$.

D4. In the case of Alice's private key satisfies dynamic evolution, Eq. (4) is $\otimes_{i=1}^{N}|e^{i\varepsilon}||\langle m_i|1\rangle|$. If $F(\rho,\sigma) = 1$, Bob's message is $|m_i\rangle = |1\rangle$. Otherwise, if $F(\rho,\sigma) = 0$, $|m_i\rangle = |0\rangle$.

4. Conclusion

In this paper, we introduced a quantum trapdoor one-way function, which is a prerequisite for a quantum public key cryptography, using cyclic and dynamic evolution of quantum states. Since the quantum state encrypted using the proposed quantum trapdoor one-way function randomly, it is very difficult to generate the final quantum state without a single qubit rotation operator corresponding to trapdoor information. However, if trapdoor information is used, it is possible to generate final quantum state easily. The proposed encryption method guarantees safety by the principles of quantum

mechanics. In addition, the quantum trapdoor one-way function has the advantage of being easy to implement because it uses single qubit operators and a single qubit instead of multi-dimensional quantum operator and entangled states. Finally, we propose a quantum public key cryptography using the quantum trapdoor one-way function. The proposed quantum public key cryptography uses single qubit rotation operators as public and private key, and uses them to encrypt and decrypt messages. It is possible to provide security of quantum cryptography and the same function as public key cryptography of modern cryptography. The proposed quantum public key cryptography is expected to enable efficient system design in the field of quantum cryptography where there is no alternative other than symmetric key cryptography.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) (2021M1A2A2043892, 2022M3K4A1097119), Institute for Information and Communications Technology Promotion (IITP) (2020-0-00890), the Commercializations Promotion Agency for R&D Outcomes (2022SCPO_B_0210), KREONET Advanced Research Program Grant from KISTI, and KIST research program (2E31531, 2E32801).

References

[1] Gisin, Nicolas, et al. Quantum cryptography. Reviews of modern physics 74.1: 145, 2002.

[2] Pirandola, Stefano, et al. Advances in quantum cryptography. Advances in optics and photonics 12.4: 1012-1236, 2020.

[3] Dušek, Miloslav, et al. Quantum identification system. Physical Review A 60.1: 149, 1999.

[4] Zeng, Guihua, and Christoph H. Keitel. Arbitrated quantum-signature scheme. Physical review A 65.4: 042312, 2002.

[5] Forouzan, Behrouz A., and Debdeep Mukhopadhyay. Cryptography and network security. McGraw Hill, 2015.

[6] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.

Objectivity in a simple harmonic oscillator in spin environment

Tae-Hun Lee[1] * Jarosław K. Korbicz[1] †

[1] *Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland.*

Abstract. We investigate an objective quantum state for a system of a simple harmonic oscillator interacting with the large collections of spin-1/2 environment, a so-called spectrum broadcast structure (SBS). Spin dynamics is assumed to be effectively described by a time-dependent effective Hamiltonian corresponding to a classical trajectory of a harmonic oscillator. The objectivity measures for the SBS, a decoherence factor and a generalized overlap (fidelity), are calculated on the high frequency expansion in the Floquet theory.

Keywords: spectrum broadcast structure, objectivity, decoherence factor, generalized overlap, fidelity, high frequency expansion.

1 Introduction

Although quantum mechanics is believed to be the most fundamental framework to describe any physical systems, our daily perceived world seems to sharply contrast with quantum mechanical predictions based on counter-intuitive natures like superposition, interference, disturbance, non-locality, etc. More concretely, this puzzle boils down to a so-called "measurement problem". However, it is not even clear whether it is a real, well-posed problem in quantum theory or a reflection of our misunderstanding of the theory. In this sense it is important to attempt how much the problem can be explained within the current framework of quantum mechanics.

One of the characteristics of classicality is "objectivity" [2], analogous to "invariance" of physics in relativity principle. It turned out that environmental interactions, which were believed to be minimized, play a significant role driving a quantum systems to have classicality. This mechanism is called "Quantum Darwinism" [1]. Furthermore, "Spectrum Broadcast Structure"(SBS) is introduced for an objective quantum state [2].

In this presentation, we consider a simple harmonic oscillator interacting with qubit enviroments to investigate whether a simple harmonic oscillator evolves into a classical objective state, the SBS structure. The Hamiltonian of the system is in a form of one for a system of a photon-two-level atom, i.e. the Jaynes-Cummings model [3]. The SBS structure is characterized by two measures, a decoherence factor and a generalized overlap (fidelity). These two quantities are calculated based on high frequency expansion in the Floquet theory [4].

2 Dynamics of System

The Hamiltonian H for a composite system, where a simple harmonic oscillator bilinearly interacts with individual spin environment is given by

$$H = H_S + \sum_i H_E^{(i)} + \sum_i H_{int}^{(i)}, \tag{1}$$

where

$$\begin{aligned} H_S &= \frac{P^2}{2M} + \frac{1}{2}M\Omega^2\hat{X}^2, \\ H_E^{(i)} &= -\frac{\Delta_i}{2}\sigma_x^{(i)}, \\ H_{int}^{(i)} &= g_i\hat{X}\otimes\sigma_z^{(i)}, \end{aligned} \tag{2}$$

where M and Ω are a mass and an angular frequency of an oscillator, respectively and g_i is an interaction coupling between an oscillator and ith spin-environment and Δ_i is a self-dynamic coupling. For interaction we consider only a bilinear interaction $H_{int}^{(i)}$ between the ith spin and a harmonic oscillator without mutual interactions among other spins. First, we approximate a dynamics of qubits, based on classical influence of a harmonic oscillator (Born-Oppenheimer approximation) by using the effective Hamiltonian for qubits H_{eff},

$$H_{eff} = \sum_i \left(-\frac{\Delta_i}{2}\sigma_x^{(i)} + g_i X_0 \sigma_z^{(i)}\cos\Omega t\right), \tag{3}$$

Then we put the effective spin dynamics back into a total state.

3 Objective Quantum State

Here we introduce an objective quantum state, a so-called Spectrum Broadcast Structure (SBS) [2],

$$\rho_{S:fE} = \sum_i p_i |i\rangle_S\langle i| \otimes \rho^{E_1} \otimes \cdots \otimes \rho^{E_{fN}} \tag{4}$$

After unobserved degrees of freedom traced out, the SBS structure of a total density matrix is an orthogonal convex combination. The SBS structure is characterized by a vanishing decoherence factor and a vanishing generalized overlap(fidelity).

4 Decoherence Factor and Generalized Overlap

When our effective description of spin environmental systems is translated back into the density matrix for the

*taehunee@cft.edu.pl
†jkorbicz@cft.edu.pl

total system, ρ_{SE} is effectively written as

$$\rho_{SE}(t) = \int dX_0 dX_0' e^{-iH_S t/\hbar}|X_0\rangle\langle X_0'|e^{iH_S t/\hbar} \quad (5)$$
$$\langle X_0|\rho_S(0)|X_0'\rangle \bigotimes_k U_k(X_0,t)\rho_E^{(k)}(0)U_k^\dagger(X_0',t),$$

where $U_k(X_0,t) = Te^{-\frac{i}{\hbar}\int_0^t H_{eff}^{(k)}dt'}$. After unobserved environmental degrees of freedom traced out, we wish see two aspects of a total state, which characterize the SBS structure. One is how much off-diagonal elements (coherence) decrease and the other is how much diagonal elements are orthogonal to each other. the decoherence factor is defined as,

$$\Gamma_{X_0.X_0'} = \mathrm{Tr}_{uE}[\bigotimes_{k\in uE} U_k(X_0,t)\rho_E^{(k)}(0)U_k^\dagger(X_0',t)]$$
$$= \prod_{k\in uE}\Gamma^{(k)}_{X_0.X_0'}, \quad (6)$$

where $\Gamma^{(k)}_{X_0.X_0'} = \mathrm{Tr}_k[\rho^{(k)}(0)U^{(k)}_{X_0,X_0'}]$ and with $U^{(k)}_{X_0,X_0'} \equiv U_k^\dagger(X_0')U_k(X_0)$. A decoherence factor is responsible for how off-diagonal elements in a total state change. The diagonal elements in a total state Together with a decoherence factor, a so-called generalized overlap (fidelity) $B(\rho,\rho')$ is a measure to characterize the orthogonality (distinguishability) of two states (ρ,ρ'), which is required for objectivity in the SBS structure, defined by

$$B(\rho,\rho') \equiv \mathrm{Tr}\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}}. \quad (7)$$

5 Representation

For a single spin in the Pauli matrix basis $\rho_0 = \rho(0)$ is written with the Bloch vector parametrization,

$$\rho_0 = \frac{1}{2}\left(\mathbb{I} + \sum_i a_i\sigma_i\right), \quad (8)$$

where a_i is a real number with $|\vec{a}| \le 1$ and

$$U_{X_0,X_0'} = u_0\mathbb{I} + i\sum_i u_i\sigma_i, \quad (9)$$

where u_0 and u_i are a real number satisfying $u_0^2+|\vec{u}|^2 = 1$. The magnitude of a decoherence factor is expressed by $|\Gamma_{X_0.X_0'}|^2$ is

$$|\Gamma_{X_0,X_0'}|^2 = u_0^2 + (\vec{a}\cdot\vec{u})^2 \le 1. \quad (10)$$

A generalized overlap $B^2_{X_0,X_0'}$ is obtained as

$$B^2_{X_0,X_0'} = 1 - |\vec{a}\times\vec{u}|^2 \le 1. \quad (11)$$

The relation between $|\Gamma_{X_0.X_0'}|^2$ and $B^2_{X_0,X_0'}$ is given by

$$B^2_{X_0,X_0'} = (1-|\vec{a}|^2)(1-u_0^2) + |\Gamma_{X_0,X_0'}|^2. \quad (12)$$

6 Complementarity

According to the relation Eq.(12), the relation between $|\Gamma_{X_0,X_0'}|$ and $B_{X_0,X_0'}$ is hyperbolic,

$$B^2_{X_0,X_0'} - |\Gamma_{X_0,X_0'}|^2 = (1-|\vec{a}|^2)(1-u_0^2). \quad (13)$$

In order to make both a perfect decoherence and a perfect distinguishability, i.e. $|\Gamma_{X_0,X_0'}| = B_{X_0,X_0'} = 0$, a particular condition i.e. an initial state is a pure state $|\vec{a}| = 1$ and $u_0 = 0$ and $\vec{a}\perp\vec{u}$ must be satisfied.

7 Periodic Hamiltonian

H_{eff} is periodic with period $T = 2\pi/\Omega$. According to the Floquet Theory, the corresponding a unitary evolution operator is split into periodic part and non-periodic part [4],

$$U(t,t_0) = e^{-iK(t)/\hbar}e^{-i(t-t_0)H_e/\hbar}e^{iK(t_0)/\hbar}, \quad (14)$$

where H_e is a time-independent Hamiltonian responsible for slow dynamics while $K(t)$ for fast dynamics and has the same periodicity $K(t) = K(t+T)$ as the given periodic Hamiltonian H_{eff}.

8 Higher Frequency Expansion

In Eq.(14) the effective Hamiltonian H_e and $K(t)$ are expanded in $1/\Omega$ for large frequency $\Omega \gg 1$ up to $O(1/\Omega^2)$ [4],

$$H_e = H_0 + \frac{1}{\hbar\Omega}\sum_{j=1}^\infty \frac{1}{j}[V^{(j)},V^{(-j)}]$$
$$+ \frac{1}{2\hbar^2\Omega^2}\sum_{j=1}^\infty\frac{1}{j^2}([[V^{(j)},H_0],V^{(-j)}] + h.c.) + \cdots$$
$$= -\tilde{\Delta}(1-\xi^2)\sigma_x\hbar\Omega + \cdots \quad (15)$$

and

$$K = \frac{\hbar}{i\hbar\Omega}\sum_j^\infty\frac{1}{j}(V^{(j)}e^{ij\Omega t} - V^{(-j)}e^{-ij\Omega t})$$
$$+ \frac{\hbar}{i\hbar^2\Omega^2}\sum_j^\infty\frac{1}{j^2}([V^{(j)},H_0]e^{ij\Omega t} - h.c.) + \cdots$$
$$= \hbar(\xi\sigma_z\sin\Omega t - 2\tilde{\Delta}\xi\sigma_y\cos\Omega t) \quad (16)$$

where $V^{(j)}$ is a Fourier coefficient of H_{eff} as

$$H_{eff} = H_0 + \sum_{j=1}^\infty (V^{(j)}e^{ij\Omega t} + V^{(-j)}e^{-ij\Omega t}).$$

and $\xi \equiv \frac{gX_0}{\hbar\Omega}$ and $\tilde{\Delta} \equiv \frac{\Delta}{2\hbar\Omega}$.

9 Numerical Results

The decoherence factor and the generalized overlap are characterized by the parameters:

$$\tau \equiv \Omega t,\ \xi_i \equiv \frac{g_iX_0}{\hbar\Omega},\ \xi_i' \equiv \frac{g_iX_0'}{\hbar\Omega}, d\xi \equiv \xi_i - \xi_i',\ \tilde{\Delta}_i \equiv \frac{\Delta_i}{2\hbar\Omega}.$$

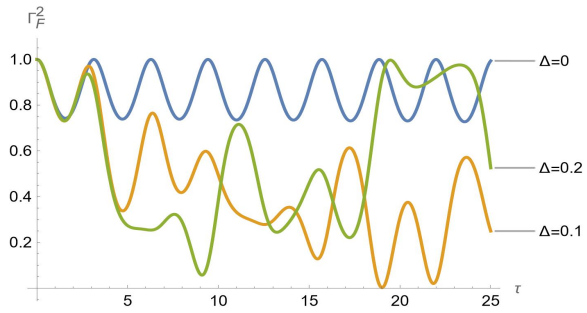


Figure 1: Decoherence increases as a self dynamics coupling increases.

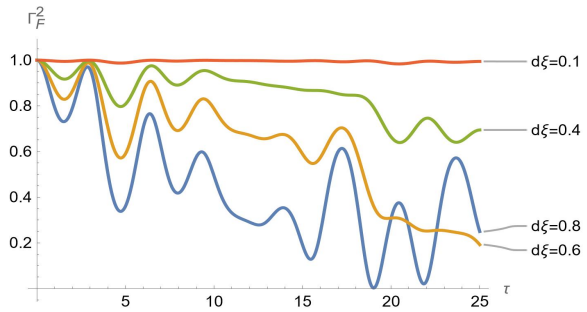


Figure 2: Decoherence increases as an interaction/separation increases.

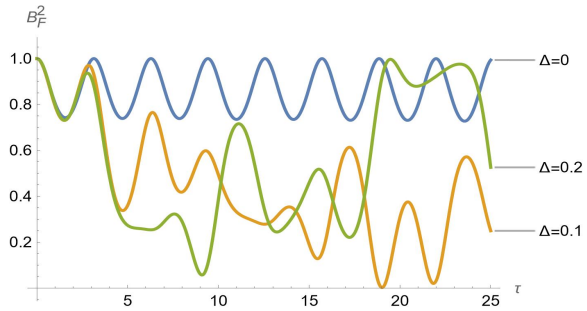


Figure 3: Orthogonality increases as a self dynamics coupling increases.

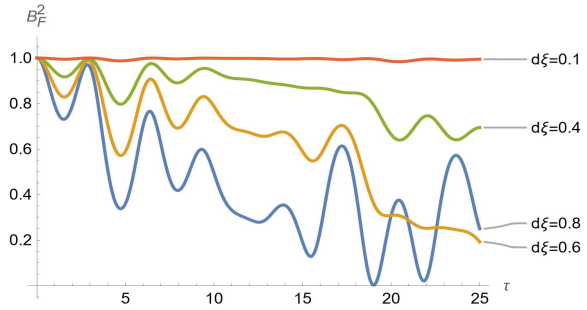


Figure 4: Orthogonality increases as an interaction/separation increases.

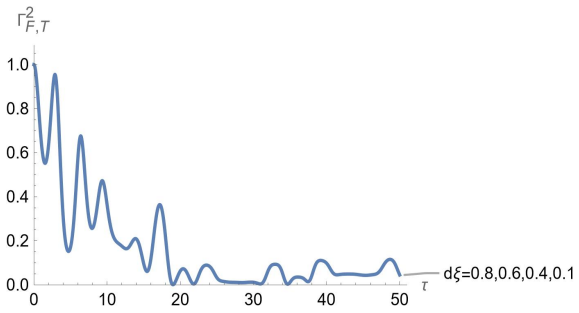


Figure 5: Total decoherence factor.

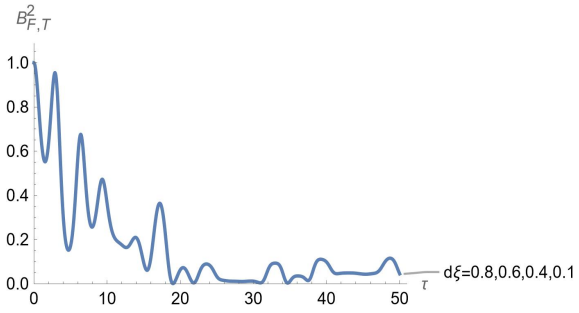


Figure 6: Total generalized overlap.

10 Summary

- Interaction/separation between two positions of a harmonic oscillator ($d\xi$) increases decoherence and distinguishability.
- A self-dynamics ($\tilde{\Delta}$) also increase decoherence and distinguishability.
- An emergent periodicity remains for an individual qubit but thanks to the product rule it dies out for a large qubit environment with different strength of interactions.
- Purity $|\vec{a}| = 1$ leads to $B_{X_0,X_0'} = |\Gamma_{X_0,X_0'}|$.
- Both conditions purity $|\vec{a}| = 1$ and $\vec{a} \perp \vec{u}$ lead to $B_{X_0,X_0'} = |\Gamma_{X_0,X_0'}| = 0$.

References

[1] W. H. Zurek. Quantum Darwinism, classical reality, and the randomness of quantum jumps. *Physics Today*, 67(10):44-50, 2014.

[2] R. Horodecki, K. Korbicz, and P. Horodecki. Quantum origins of objectivity. *Phys. Rev. A*, 91:032122, 2015.

[3] E. T. Jaynes and F. W. Cummings. Comparison of quantum and semiclassical radiation theories with application to the beam maser. *IEEE Proc.*, 51:89-109, 1963.

[4] N. Goldman and J. Dalibard. Periodically Driven Quantum Systems: Effective Hamiltonians and Engineered Gauge Fields. *Phys. Rev. X*, 4: 031027, 2014.

Quantum-Secured Single-Pixel Imaging with Advanced Security

Jaesung Heo[1] * Junghyun Kim[1] Taek Jeong[1] Yong Sup Ihn[1] Duk Y. Kim[1]
Zaeill Kim[1] Yonggi Jo[1] †

[1] *Agency for Defense Development, Daejeon, Republic of Korea*

Abstract. In this presentation, we introduce a novel quantum-secured single-pixel imaging method. Based on non-classical correlations of a photon pair, our method can detect deceiving attempts, while rejecting strong chaotic light through photon heralding. In our demonstration, we used polarization-correlation for a security analysis. Mixture of true and false signal lowers the error rate below detection threshold, which can be revealed by our method. Proof-of-principle demonstrations of our method and trustworthy image reconstruction will be presented. The method can be developed using matured techniques used in quantum secure communication, thus offering a promising direction for practical applications in secure imaging.

Keywords: secure imaging, ghost imaging, sinlge-pixel imaging, correlation

1 Introduction

In various quantum information protocols, non-classical correlations between quantum systems played key role in realizing quantum advantage. Quantum key distribution exploits entanglement for security against potential eavesdropping attacks. Quantum ghost imaging uses correlations to enhance the signal-to-noise ratio of an image beyond the classical limit. Applying security analysis methods of quantum key distribution to quantum imaging, various quantum-secured imaging protocols were proposed [1, 2, 3]. Experimentally realized ones focused only on rudimentary attack methods. Moreover, imaging and security check were performed sequentially. However, it is possible to deceive the imaging system with errors lower than detection threshold of rudimentary attack. Moreover, sequential process loses the close relationship between obtained images and security.

We present a novel quantum-secured single-pixel imaging (QS-SPI) method that exploits non-classical correlations of a photon pair for imaging and security checking, simultaneously. Our imaging method is based on single-pixel imaging (SPI), also known as computational ghost imaging (CGI). Compared to the existing quantum-secured imaging methods, our proposed method offers enhanced security against potential attacks. Based on intercept-and-resend attack, we additionally considered a partial deceiving attack that constructs a fraud image by mixing genuine signals and false signals, resulting in errors below detection threshold. Our method can expose the presence of such attack. In addition, as obtained images are closely related to the security of the protocol, extracting trustworthy information under the attack is possible. Experimental demonstration of enhanced security analysis method under deceiving attacks is presented. We expect that advanced techniques used in quantum secure communication can further improve the security of QS-SPI. Detailed information can be found in [4].

*jayh@add.re.kr
†yonggi@add.re.kr

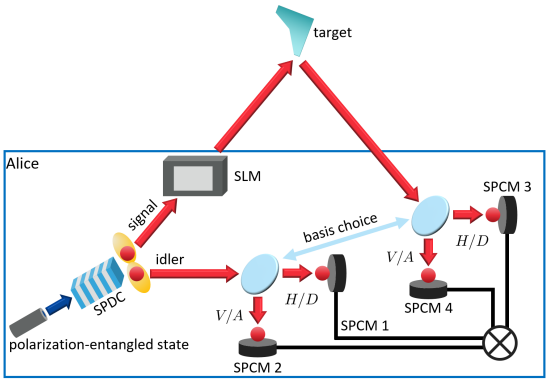


Figure 1: A schematic diagram of QS-SPI. Polarization-entangled photons are generated as the source beam. The signal photon is sent to an SLM to be filtered according to an imaging pattern. Then, it interacts with a target and detected by single photon counting modules (SPCMs) in polarization discrimination manner. The idler photon, the other entangled party, is also measured with polarization discrimination. Correlation between imaging patterns and corresponding detected intensities constructs target image. Simultaneously, the time-correlation and polarization-correlation of the two modes are analyzed.

2 Quantum-Secured Single-Pixel Imaging

In SPI, the main purpose of an attack is to deceive an imaging system to construct a fake image. In this sense, precise extraction of signal information is not important for enemy. Rather, it is important to send false signal containing fake image information to imaging system within detection window for incurring construction of a deceiving image. The meaningful attack of this purpose is to modulate the intensity (photon number) of the light for the formulation of a fake image. Under this circumstance, an intercept-and-resend attack is the probable attack strategy for image-deceiving attacks [2].

Typical error bound of intercept-and-resend attack is 25%. However, if partial deceiving attack is conducted,

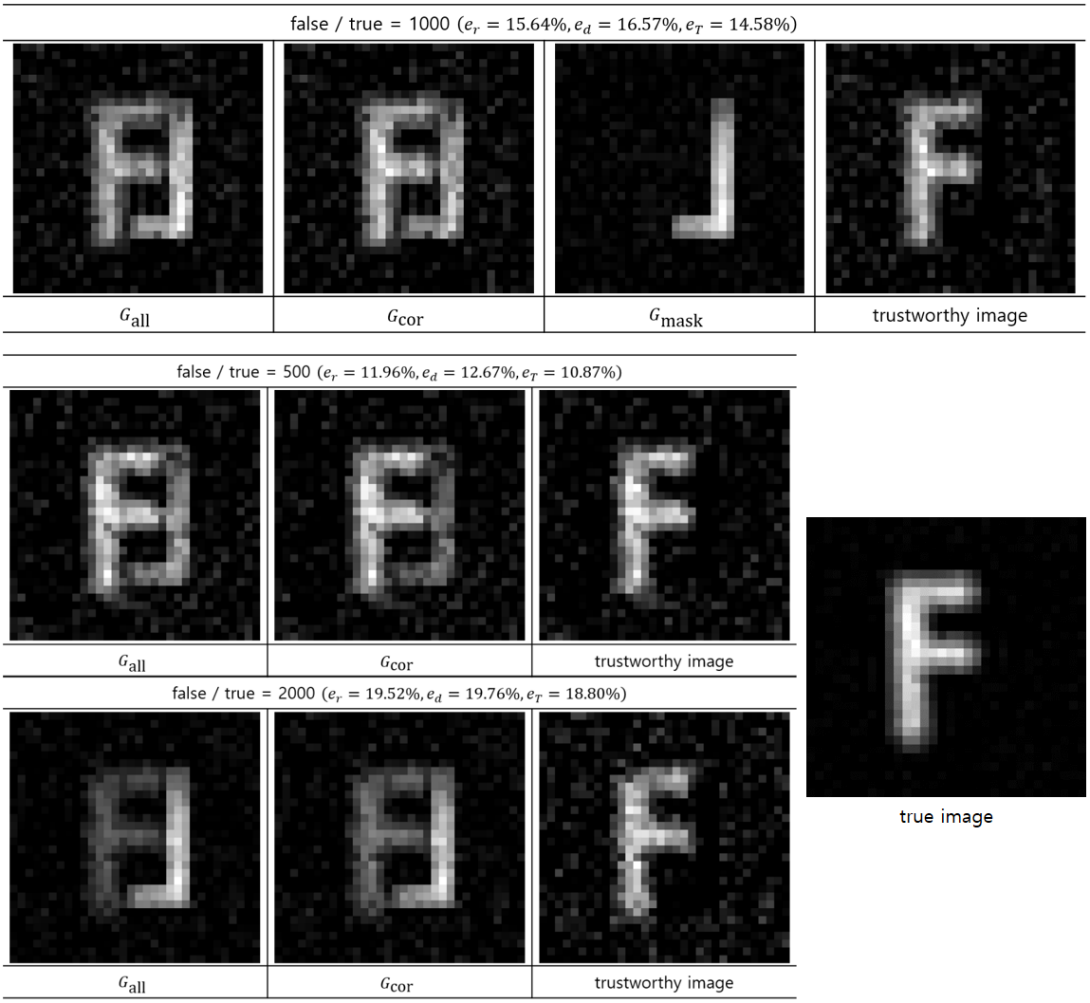


Figure 2: Images obtained by QS-SPI under a partial deceiving attack where true target profile has no overlap with false target profile.

an attack of an enemy sending mixture of true and false signal, error rate can be below 25% but still forming deceiving images. Based on non-classical correlations, QS-SPI can partially discriminates false signal. Under intercept-and-resend attack, a quarter of it is discriminated. From this, threshold error rate under ideal attack can be calculated [4],

$$e_T = \frac{\sum_{i,j} G_{\mathrm{mask}}(i,j)}{\sum_{i,j} G_{\mathrm{all}}(i,j)}, \tag{1}$$

where G_{mask} is an image obtained by partially discriminated false signal and G_{all} is the one by all incoming signal. Partial deceiving attack can be exposed when the error is beyond e_T. When the attack is confirmed, trustworthy image can be reconstructed through

$$G_A(i,j) = G_{\mathrm{cor}}(i,j) - 3G_{\mathrm{mask}}(i,j), \tag{2}$$

where G_A is an image of true target and G_{cor} is an image obtained by coincidence counts heralded by non-classical correlation of source beam.

3 Result and Discussion

Proof-of-principle demonstration of QS-SPI under a partial deceiving attack is presented in Fig. 2. Ratio of false signal to true signal intensity was controlled as 500, 1000, and 2000. Errors below 25% are obtained in all cases and G_{all} shows deceived image of digital number "8". However, QS-SPI detects partial deceiving attack as the error rates, $e_{r(d)}$ for error rate in retilinear (diagonal) basis, are over the threshold error rate e_T. G_{mask} revealed the false image, left-and-right inverse of alphabet letter "L". Following Eq. 2, trustworthy image is reconstructed, alphabet letter "F", indicating that digital number "8" was not a true target but "F" was. Due to suppression of true signal compared to false signal, degrade in image quality can be observed as the false signal intenisty gets stronger.

QS-SPI can further be applied to ghost imaging, quantum-secured optical ranging protocol, and its security analysis can be enhanced by adopting hyper-entangled states. Device-independent security can be achieved by observing Bell parameter as a security checking method.

Acknowledgments - This work was supported by a

grant to Defense-Specialized Project funded by Defense Acquisition Program Administration and Agency for Defense Development.

References

[1] M. Malik and R. W. Boyd, In *2012 Conference on Lasers and Electro-Optics (CLEO)*, pp. 1-2 (2012).

[2] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, *Appl. Phys. Lett.* **101**, 241103 (2012).

[3] X. Yao, X. Liu, L. You, Z. Wang, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang, *Phys. Rev. A.* **98**, 063816 (2018).

[4] J. Heo, J. Kim, T. Jeong, Y. S. Ihn, D. Y. Kim, Z. Kim, and Y. Jo, arXiv:2209.06365 [quant-ph].

Observing shareability of multipartite Einstein-Podolsky-Rosen steering

Kai Sun[1 2 *] Ze-Yan Hao[1 2] Jin-Shi Xu[1 2 †] Chuan-Feng Li[1 2 ‡]
Guang-Can Guo[1 2]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[2] *CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

Abstract. Einstein-Podolsky-Rosen (EPR) steering, different from both entanglement and Bell nonlocality, describes the ability of one observer to affect another party's state via local measurements. For multipartite EPR steering, the monogamous situation, where two observers cannot simultaneously steer states of the third party, limits the shareability of EPR steering in reduced subsystems. Here, in an optical experiment, we observe the shareability of EPR steering in a three-qubit system without the monogamous limitation. Moreover, based on reduced bipartite EPR steering detection results, we verify genuine three-qubit entanglement results. This work provides a basis for an improved understanding of multipartite EPR steering and has potential applications in many quantum information protocols.

Keywords: EPR steering, multipartite, shareability, monogamy

1 Introduction

Einstein-Podolsky-Rosen (EPR) steering, describing the process in which one observer can steer another observe's state through local measurements, was reformulated by Wiseman *et al*. in 2007 with an operational definition stating that the assemblage of conditional states at the steered party cannot be explained via a local hidden state model [1]. Regarded as a term of quantum nonlocal correlations, EPR steering lies between quantum entanglement and Bell nonlocality hierarchically. Due to its unique directional property, EPR steering indicates an asymmetric manifestation, which further leads to one-way EPR steering meaning Alice can steer Bob but not vice versa. Expanding the directional property to the multipartite system, monogamous relations in EPR steering limits the quantum correlations shared arbitrarily [2]. Taking a three-qubit system (e.g., Alice, Bob, and Charlie) as an illustration, the monogamy of EPR steering refers to the impossibility of Alice and Bob simultaneously steering the state of Charlie. As a significant property in multipartite EPR steering, in continuous variable optical systems, the monogamous relations of multipartite EPR steering have been demonstrated in many experiments [3, 4]. Beyond the monogamy of multipartite EPR steering, the shareability of EPR steering in reduced subsystems reveals that the shared correlations are not monogamous, which means that Alice and Bob can steer Charlie simultaneously with increasing the number of observer measurement settings [5]. This illustration allows us to observe different shareability configurations of EPR steering in a multipartite system, which enrich the scenarios of tasks based on multipartite steering.

Here, based on a three-qubit system constructed with the three degrees of freedom (DOF) of a single photon, namely, the polarization, path, and orbital angular momentum, different configurations of shareability for EPR steering are experimentally observed beyond the constraint of monogamy [6]. Considering the directional property of EPR steering, these relations are observed by exploiting the uncertainty relation criterion with three measurement settings. Moreover, the detection of EPR steering shareability relations facilitates the verification of genuine three-qubit entanglement. Our results can be a significant step forward toward extending the understanding of multipartite relationships and have potential applications in quantum information protocols.

2 Results

Alice can steer Bob if the inequality

$$P_{AB} = \sum_i \delta^2 (\alpha_i A_i + B_i) \geq \min_{\rho_B} \sum_i \delta^2 (B_i) \qquad (1)$$

is violated, where δ denotes the variance of the measurement outcomes and $\alpha_i = -\frac{C(A_i,B_i)}{\delta^2(A_i)}$ in which $C(A_i, B_i) = \langle A_i B_i \rangle - \langle A_i \rangle \langle B_i \rangle$. For a three-qubit system (Alice, Bob, and Charlie), in the case where the number of measurement settings $n = 2$, the monogamous relation is valid. However, by increasing n to 3, the monogamy violations are possible, which means that more shareability configurations of EPR steering can be observed. Here, three measurement settings are chosen as $\{\sigma_x, \sigma_y, \sigma_z\}$. We can confirm that $\min_{\rho_A} \sum_i \delta^2 (A_i) = \min_{\rho_A} \sum_{i=x,y,z} \left(1 - \langle \sigma_i \rangle^2\right) = 2$, similarly, $\min_{\rho_B} \sum_i \delta^2 (B_i) = \min_{\rho_C} \sum_i \delta^2 (C_i) = 2$. The parameter $P_{AB} < 2$ violates the inequality (1) and indicates that Bob can be steered by Alice.

Taking the W-like states as an illustration,

$$|\psi_{ABC}\rangle = \alpha |0\rangle |0\rangle |1\rangle + \beta |0\rangle |1\rangle |0\rangle + \gamma |1\rangle |0\rangle |0\rangle , \qquad (2)$$

where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$. For the state $|\psi_{ABC}\rangle = 0.2|001\rangle + 0.4|010\rangle + \sqrt{0.8}|100\rangle$, the parameters P_{BA}, P_{AB}, and P_{AC} violate the steering inequality (1), which means that monogamy can be observed when no one can be steered by the others at the same time.

*ksun678@ustc.edu.cn
†jsxu@ustc.edu.cn
‡cfli@ustc.edu.cn

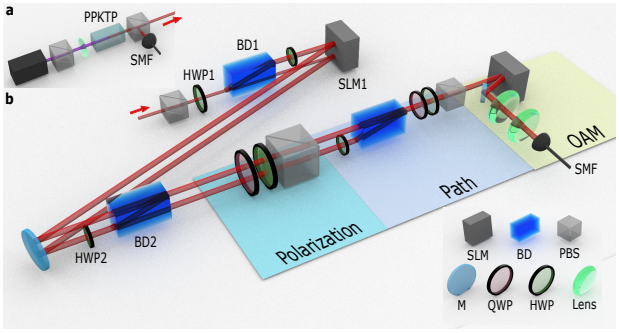


Figure 1: Illustration of the process of preparation and measurement of three-qubit states. **a**. A heralded single-photon source generates a pair of photons via a PPKTP crystal. **b**. The main optical system. The initial photon is divided into two optical paths through the half wave plate (HWP1) and the beam displacer (BD1). The first spatial light modulator (SLM1) then generates an orbital angular momentum (OAM) via the phase-only hologram. The GHZ-like states can be prepared when the angle of the HWP2 is set to 45°. The BD2 is positioned to generate W-like states and adjust their parameters in Eq. (2) by changing HWP1 and HWP2. The measurement apparatus is composed of three independent parts that can achieve separate projective measurements of states with different degrees of freedom (polarization, path, and OAM).

For the state $|\psi_{ABC}\rangle = (|001\rangle + |010\rangle + \sqrt{2}|100\rangle)/2$, we can obtain $P_{BA} = P_{CA} < 2$, which indicates that Alice can be steered by Bob and Charlie simultaneously. In this assessment, more EPR steering configurations can be observed. For instance, the steering parameters of state $|\psi_{ABC}\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ all have the theoretical values of $16/9 < 2$.

Experimental setup. As shown in Fig. 1**a**, the heralded single photons is generated from a 20 mm long periodically poled $KTiOPO_4$ (PPKTP) crystal which is pumped by a 404-nm continuous-wave laser. The initial photon polarization state is prepared to be $\mu|H\rangle + \nu|V\rangle$ ($|\mu|^2 + |\nu|^2 = 1$), in which $|H\rangle$ and $|V\rangle$ correspond to the horizontal and vertical polarization bases, respectively. A half-wave plate (HWP1) is used to adjust μ and ν. Using a beam displacer (BD1), which can split the input into two orthogonally polarized beams, the $|H\rangle$ and $|V\rangle$ states are separated into different paths, $|H\rangle$ for the down-path and $|V\rangle$ for the up-path. The first DOF can then be represented by the orthogonal path-basis $|U\rangle$ (up-path) and $|D\rangle$ (down-path). After passing through the BD1, the initial state becomes $\mu|D\rangle + \nu|U\rangle$. The second DOF is given by orbital angular momentum (OAM) generated via the spatial light modulator (SLM1). The upside hologram exhibits a $|-l\rangle$ grating, whereas the downside hologram generates a $|+l\rangle$ grating, where $|\pm l\rangle$ correspond to the Laguerre-Gaussian (LG) modes and represent the states with orbital angular momentum $\pm l\hbar$. In this experiment, l is set to be 2. Since the SLM only works for the $|H\rangle$ polarization, a 45° HWP is used in front of the SLM1 to turn the polarization of the up-path into $|H\rangle$. After passing through the SLM1, the state evolves to $\mu|D\rangle|+l\rangle + \nu|U\rangle|-l\rangle$. The HWP2 after the SLM1 is then used to transform the down-path polarization into $|V\rangle$. In this way, a Greenberger-Horne-Zeilinger (GHZ) like state, namely, $|G\rangle = \mu|V\rangle|D\rangle|+l\rangle + \nu|H\rangle|U\rangle|-l\rangle$ could be prepared using the three DOF of the single photon which is equivalent to the states generated with three photons. To obtain the target W-like states, another beam displacer (BD2) is used to generate more components. After passing through BD2, the path of the $|H\rangle$ polarization remains unchanged, and the path of the $|V\rangle$ polarization deviates into a higher path ($|V\rangle|D\rangle \rightarrow |V\rangle|U\rangle$). By rotating the angle θ of the HWP2, the state $|V\rangle|D\rangle$ could be prepared to be $\sin 2\theta|V\rangle|D\rangle + \cos 2\theta|H\rangle|D\rangle$. Thus, the state $|V\rangle|D\rangle|+l\rangle$ becomes $\cos 2\theta|H\rangle|D\rangle|+l\rangle + \sin 2\theta|V\rangle|U\rangle|+l\rangle$, whereas the states $|H\rangle|U\rangle|-l\rangle$ does not change. With encoding $|H\rangle \rightarrow |0\rangle_s$, $|V\rangle \rightarrow |1\rangle_s$, $|U\rangle \rightarrow |0\rangle_p$, $|D\rangle \rightarrow |1\rangle_p$, $|+l\rangle \rightarrow |0\rangle_m$, and $|-l\rangle \rightarrow |1\rangle_m$, the W-like states in Eq. (2) are prepared in which the parameters α, β, and γ are determined by the angles of HWP1 and HWP2.

The measurement process can be divided into three independent projective measurements, namely, polarization, path, and OAM analyzer. The unit of a polarization analyzer is composed of a quarter-wave plate (QWP), an HWP, and a polarization beam splitter (PBS). The path measurement contains an HWP, a BD, and a polarization analyzer, in which the HWP and the BD are used to convert path information into polarization information. After passing through the BD, the $|U\rangle$ path changes into the $|H\rangle$, and the $|D\rangle$ path is converted into $|V\rangle$. Therefore, the polarization analyzer is used after the BD to realize a projective path measurement. The OAM measurement consists of an SLM loading phase-only hologram and a single mode fiber (SMF). Different projective measurements of the OAM qubit can be achieved by transforming target states (like $(|+l\rangle + |-l\rangle)/\sqrt{2}$) into the $l = 0$ mode with different holograms generated by the SLM. The SMF is then used to couple the $l = 0$ mode and filter out the other modes. Before being detected by the single-photon detectors, the photons in Fig. 1**a** and Fig. 1**b** are filtered through interference filters with a bandwidth of 3 nm, and the resulting signals are then sent to coincidence counting.

Experimental results. Seven W-like states are experimentally prepared as in Eq. (2) with an average fidelity $F = \mathrm{Tr}\left(\sqrt{\sqrt{\rho_{\mathrm{th}}}\rho_{\mathrm{ex}}\sqrt{\rho_{\mathrm{th}}}}\right)$ of 0.960(3). Here, ρ_{ex} is obtained through the experimental results, whereas ρ_{th} represents the ideal theoretical state. The parameter $P_{BA} < 2$ indicates that Alice can be steered by Bob. The red dots in Fig. 2**a** demonstrate the shareability of EPR steering without the constraint of monogamy in cases with three measurement settings. The shareability relations transcending the constraint of EPR steering monogamy are verified via the uncertain relation criterion. For state "3" with parameters $P_{BA} = 1.99(3)$, $P_{AB} = 2.00(3)$, $P_{CA} = 1.60(4)$, $P_{AC} = 1.65(5)$, $P_{CB} = 1.61(5)$, and $P_{BC} = 1.64(4)$, violation of

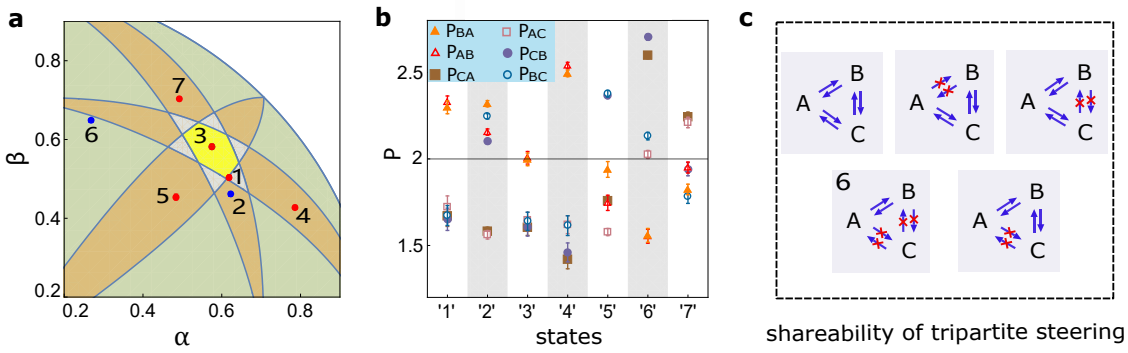


Figure 2: Experimental results. **a**. The horizontal and vertical coordinates are α and β in Eq. (2). The background of this figure is divided into different areas to indicate different relationships. The red experimental dots demonstrate the EPR steering shareability relations existing beyond the monogamy constraint. The states exhibiting monogamous relations are marked by blue dots. The experimentally prepared three-qubit states are distinguished by the numbers marked beside them. **b** indicates the results obtained based on the uncertainty relation criterion. Different parameters are labeled by different colors and shapes. Alice can steer Bob when the steering parameter $P_{AB} < 2$, whereas $P_{BA} < 2$ indicates that Bob can steer Alice. **c**. The different shareability relations of tripartite EPR steering correspond to the states shown in **a**.

Table 1: Results of the detected of EPR steering shareability relations (SR) beyond the monogamous relationship and witness detection. The "Y" and "N" of "SR" indicate whether genuine entanglement has been detected by shareability relations. The negative values of the witness represent a double confirmation of the genuine entanglement.

state	SR	witness
1	Y	-0.27(1)
2	N	-0.23(1)
3	Y	-0.26(1)
4	Y	-0.14(1)
5	Y	-0.21(1)
6	N	-0.15(1)
7	Y	-0.23(1)

the monogamy relation by the shareability of EPR steering can then be presented. The error bars in the figures are handled by Poisson counting statistics. We also employ another criterion that can detect the shareability of EPR steering via only the tomographic measurements of reduced single-qubit states (RSQSs) [5]. Compared to the uncertainty relation criterion, this method needs fewer projectors but sacrifices some valid ranges.

Furthermore, the verification results of the EPR steering shareability relations are used to test whether the states are genuinely entangled. As a comparison, the three-qubit witness is employed for double verification. The witness $\mathcal{W} = \frac{2}{3}\mathcal{I} - P_W$ is used, where P_W is the projector of $|W\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$, and $\mathcal{I}$ is the identity matrix. The result that $\mathrm{Tr}(\rho\mathcal{W}) < 0$ indicates a correlation of genuine entanglement. The experimental results are presented in Table 1, where conclusions regarding the detection of EPR steering shareability relations and witness detection are listed. All the states have negative witness values, whereas only the states represented by red dots in Fig. 2**a** can be verified as being genuinely entangled since they support the EPR steering shared among the three observers. The criterion of Eq. (1) leads to the fact that several W-like states, which are genuinely three-qubit entangled states that have the property of EPR steering being shared only between two observers, such as states "2" and "6", cannot be detected by the proposed method. This indicates that the verification of EPR steering shareability relations is a sufficient and unnecessary method to test for genuine three-qubit entanglement.

3 Discussions

Our results contribute to a significant step forward in the study of multipartite systems. The exploitation of multisetting scenarios provides a deeper understanding of the steerability shared among reduced subsystems. It would be interesting to extend the proposed method to more complex multipartite systems and observe the EPR steering shareability relations therein. The results of this work provide a valuable method for realizing multipartite genuine entanglement testing. Since monogamy implies security limits on quantum cryptography [7], our results may provide a basis for more applications of cryptographic protocols based on EPR steering. Furthermore, as this work demonstrates the abundant configurations of EPR steering shared in a multipartite system, we hope that it can be helpful for building a future multipartite EPR steering network.

References

[1] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, Entanglement, Nonlocality, and the Ein-

steinCPodolskyCRosen Paradox. *Phys. Rev. Lett.* 98, 140402 (2007).

[2] M. D. Reid. Monogamy inequalities for the Einstein-Podolsky-Rosen paradox and quantum steering. *Phys. Rev. A* 88, 062108 (2013).

[3] S. Armstrong *et. al.* Multipartite EinsteinCPodolsky-CRosen steering and genuine tripartite entanglement with optical networks. *Nat. Phys.* 11, 167 (2015).

[4] M. Wang *et. al.* Deterministic Distribution of Multipartite Entanglement and Steering in a Quantum Network by Separable States. *Phys. Rev. Lett.* 125, 260506 (2020).

[5] B. Paul and K. Mukherjee. Shareability of quantum steering and its relation with entanglement. *Phys. Rev. A* 102, 052209 (2020).

[6] Z.-Y. Hao *et. al.* Demonstrating Shareability of Multipartite Einstein-Podolsky-Rosen Steering. *Phys. Rev. Lett.* 128, 120402 (2022).

[7] C.-Y. Huang, N. Lambert, C.-M. Li, Y.-T. Lu, and F. Nori. Securing quantum networking tasks with multipartite Einstein-Podolsky-Rosen steering. *Phys. Rev. A* 99, 012302 (2019).

Transversal Injection: A method for direct encoding of ancilla states for non-Clifford gates using stabiliser codes.

Jason Gavriel,[1,2,*] Daniel Herr,[3] Alexis Shaw,[1,2] Michael J. Bremner,[1,2] Alexandru Paler,[4] and Simon J. Devitt[2]

[1]*Centre for Quantum Computation and Communication Technology.*
[2]*Centre for Quantum Software and Information, University of Technology Sydney. Sydney, NSW, 2007, Australia.*
[3]*d-fine GmbH, An der Hauptwache 7, 60213, Frankfurt, Germany.*
[4]*Aalto University, 02150 Espoo, Finland.*

Quantum Error Correction (QEC) forms a crucial component of large-scale quantum computing systems [1, 2]. The difficulty in fabricating ultra-low error rate qubits and quantum gates at scale necessitates active techniques to mitigate errors caused by environmental decoherence, fabrication errors, measurement and control errors, and components that are always probabilistic [3]. While there is currently a focus on the so called NISQ regime [4] - where it is hoped that a scientifically or commercially valuable quantum algorithm can be found that is small enough to not require QEC on the current or next generation quantum computing chipsets - most theoretical work suggests that the true value in quantum computing will lie with large simulation algorithms that will unarguably require extensive error correction [5–7], unless we see a significant revolution in hardware technology.

While work on QEC is extensive [8], the physical constraints on quantum hardware architectures has resulted in the dominance of one type of QEC code, namely the surface code [9]. Defined over a 2D nearest neighbour array of physical qubits, it is now the most studied QEC code and the preferred model for numerous architecture blueprints in multiple hardware platforms [10–14]. However, the implementation of QEC for *any* quantum algorithm, large or small, comes with a significant overhead in physical qubits and/or computational time [15]. This is not surprising as the goal of QEC is often to take a physical error rate of the hardware of between $p = 10^{-3} \rightarrow 10^{-4}$ and reduce it by many orders of magnitude, with large-scale quantum simulation estimated to require error rates of 10^{-20} or even lower [6, 16].

Theoretical work in QEC, algorithmic design, compilation and resource optimisation has done a surprising job of figuring out better and better ways to implement error corrected algorithms [17–19], with one of the most studied algorithms, Shor's algorithm, a useful example. Early compilation efforts, with the surface code, benchmarked Shor's algorithm at the beginning of the 2010's, showing that upwards of 30 billion components would be required to implement Shor-2048 [20]. By focusing entirely on better ways to implement both the algorithm itself and the underlying QEC protocols, this has been reduced to 20 Million qubits by the end of the 2010's without changing any assumptions at the physical hardware level [15].

How much this can still be reduced depends on several factors - even when we still do not change the hardware assumptions of the underlying micro-architecture. The first is just the raw qubit overhead to encode a logical qubit of information up to some desired logical error rate. For a distance d error correction code, the logical error rate scales as $p_L \approx O(p^{\lfloor \frac{d-1}{2} \rfloor})$, under a simple symmetric Pauli model. This assumes that the physical error rate of all parts of the hardware system (decoherence, control, measurement etc...) is under the fault-tolerant threshold of the code, approximately $p \approx 0.67\%$ for the surface code [21]. If we take a square, un-rotated, planar surface code, the total number of qubits (data + syndrome qubits) scales as $N = (2d-1)^2$, hence $p_L \approx O(p^{\lfloor \frac{\sqrt{N}-1}{4} \rfloor})$. This exponential scaling means that for a heavily error corrected code, a lattice of $N > 1000$ is required [21]. How much this base level logical qubit overhead can be reduced, while still having a code that is architecturally feasible is still an open question.

TRANSVERSAL INJECTION PROTOCOL

This work introduces a simple new way to produce encoded non-Pauli Eigenstates. This process we dub 'Transversal Injection' modifies the way in which non-Clifford ancillary states are encoded. Transversal injection involves performing a transversal rotation - a uniform single qubit rotation on all data qubits individually - initialising them in some non-Pauli state. This is followed on by the standard stabiliser measurement procedure. During the encoding state, the stabilisers will either commute or anti-commute and the encoded logical state will now be some non-Pauli eigenstate. The string of all stabiliser measurements forms what we will call a *stabiliser trajectory*, and can be used to determine the resultant state. As we are no longer in eigenstates of the logical Z operator of the surface code, we will be left with some non-trivial logically encoded state. The probabilistic nature of the X and Z-type stabiliser measurements means that the resultant encoded state from transversal

injection is *probabilistic*, but *heralded*.

Using the stabilisers of the surface code, the initial transversal rotation and the stabiliser trajectory, we use a classical algorithm to calculate the encoded state that has been heralded by the protocol. This algorithm can be feasibly run on the fly for code distances < 6 which allows us to do numerical simulations. When only syndromes with trivial X syndromes are observed, the classical algorithm can be run efficiently at higher distances. We present this new technique in the context of the surface code, but it should be stressed that it is applicable to all stabiliser based QEC codes. This new method can be looked at as the qubit extension of what was found in the continuous variable context [22], where all-Gaussian universality was discovered in the context of the GKP code.

We verify the protocol through numerical simulation under a balanced Pauli noise model. At a physical error rate p, a Pauli X, Z or Y operator is applied with equal probability for a single qubit gate. For the two-qubit CNOT gate for syndrome extraction and measurement, a random combination of I, X, Z and Y operators (excluding II) is applied. This generally results in an encoded error rate greater than the physical error rate p. The relationship between physical error rate and logical rate are linearly proportional, it appears that higher distance codes perform worse than lower distance codes, and logical error rate always exceeds the physical error rate. For each distance and physical error rate, a second experiment was run where a simple post-selection strategy was employed in an attempt to improve fidelity. Post-selection does appear to yield improvements in fidelity by filtering out trajectories of simulated runs with a naive, pre-computed lookup table. Distance 4 with post-selection appears to yield a significant improvement in fidelity, dropping *below* the physical error rate to roughly $0.39p$.

Transversal injection circumvents the Eastin-Knill no-go theorem [23] as it is a method for preparing non-Clifford resources, such as a T-gate, to achieve universal quantum computation on the planar surface code. This new technique does not violate the Eastin-Knill theorem and is in fact still limited by the implications of the theorem. A T-gate still can't be implemented transversally on the code and the encoding step in this technique has a diminished error detecting ability. The first round of stabilisers themselves are not fault tolerant and this round is susceptible to two-qubit correlated errors without a detection event. If these errors occur before the first stabiliser measurements are extracted, the initial state will be altered without detection events. Single qubit errors on ancillary qubits are either detected in subsequent syndrome extractions or change the logical state in a way that is heralded by its measurement (i.e. once the initial Pauli frame of an encoded state is known, the encoded state is defined).

Current methods of magic state encoding similarly exhibit a linear scaling between the encoded state's fidelity and physical error rate[24]. Generally, the fidelity of output states from transversal injection is worse until a post-selection strategy is applied. Once post selection is applied on our distance 4 simulations, the logical error rate is comparable with the lower bound of other results even at much larger distances. To achieve the same fidelity, transversal injection has a much smaller qubit footprint and only requires a moderate amount of post-selection. Further analysis is needed to evaluate this protocol at distance 5 and higher to determine how fidelity scales beyond these results.

While a large number of states on the *logical Bloch Sphere* are available using this technique, the number of possible stabiliser trajectories scales exponentially as a function of the number of qubits and hence code distance. In our preliminary analysis, the probability of a particular state being prepared becomes exponentially unlikely as the code distance is scaled. There are potential redundancies at higher distances, but so far we have not identified any exploitable patterns. This implies that when a specific ancillary state is required for a teleported gate, it will need to be constructed through an effective random walk over the Bloch sphere. The exponential number of states on the Bloch Sphere that are available implies that rather than compiling to simply the non-Clifford T-gate in an error corrected system, we should be able to compile to any Z or X axis rotation we want by producing random logical states and approximating the required ancillary state needed for a given $R_z(\theta)$ or $R_x(\theta)$. Transversal injection can be used to produce magic states which we can then distil to an arbitrary accuracy, although this is only a subset of the possible output states. Hence, there is motivation to research distillation methods that are effective on other non-Pauli states. This has clear implications for circuit level compilation as the Clifford + T alphabet for a fault-tolerant compatible circuit will no longer be a constraint.

There are various techniques developed in the literature in approximating single qubit gates via a random walk around SU(2) that can be exploited to find a systematic solution to the gate compilation issue [25], but this is relegated to further work. While a direct resource comparison to a compiled algorithm using magic state distillation, such as Shor-2048 [15] will require a systematic solution to compiling arbitrary single qubit logical rotations, there is a potential for reduced qubit requirements for any large-scale algorithm by utilising this new technique.

* Electronic address: jason@gavriel.au

[1] Simon J Devitt, William J Munro, and Kae Nemoto. Quantum error correction for beginners. 76(7):076001, 2013.

[2] Barbara M. Terhal. Quantum error correction for quantum memories. *Reviews of Modern Physics*, 87:307, 2015.

[3] Terry Rudolph. Why i am optimistic about the silicon-photonic route to quantum computing. *APL Photonics*, 2(3):030901, 2020/09/28 2017.

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

[5] Markus Reiher, Nathan Wiebe, Krysta M. Svore, Dave Wecker, and Matthias Troyer. Elucidating reaction mechanisms on quantum computers. *Proceedings of the National Academy of Sciences*, 114(29):7555, 07 2017.

[6] Ryan Babbush, Craig Gidney, Dominic W. Berry, Nathan Wiebe, Jarrod McClean, Alexandru Paler, Austin Fowler, and Hartmut Neven. Encoding electronic spectra in quantum circuits with linear t complexity. *Phys. Rev. X*, 8:041015, Oct 2018.

[7] Vera von Burg, Guang Hao Low, Thomas Häner, Damian S. Steiger, Markus Reiher, Martin Roetteler, and Matthias Troyer. Quantum computing enhanced computational catalysis. *Phys. Rev. Research*, 3:033055, Jul 2021.

[8] Daniel A. Lidar and Todd A. Brun. *Quantum Error Correction*. Cambridge University Press, Cambridge, 2013.

[9] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86:032324, 2012.

[10] Bjoern Lekitsch, Sebastian Weidt, Austin G. Fowler, Klaus Mølmer, Simon J. Devitt, Christof Wunderlich, and Winfried K. Hensinger. Blueprint for a microwave trapped ion quantum computer. *Science Advances*, 3(2):e1601540, 02 2017.

[11] N. Cody Jones, Rodney Van Meter, Austin G. Fowler, Peter L. McMahon, Jungsang Kim, Thaddeus D. Ladd, and Yoshihisa Yamamoto. Layered architecture for quantum computing. *Physical Review X*, 2:031007, 2012.

[12] Hiroto Mukai, Keiichi Sakata, Simon J Devitt, Rui Wang, Yu Zhou, Yukito Nakajima, and Jaw-Shen Tsai. Pseudo-2d superconducting quantum computing circuit for the surface code: proposal and preliminary tests. 22(4):043013, 2020.

[13] Charles D. Hill, Eldad Peretz, Samuel J. Hile, Matthew G. House, Martin Fuechsle, Sven Rogge, Michelle Y. Simmons, and Lloyd C. L. Hollenberg. A surface code quantum computer in silicon. *Science Advances*, 1, 2015.

[14] Hector Bombin, Isaac H. Kim, Daniel Litinski, Naomi Nickerson, Mihir Pant, Fernando Pastawski, Sam Roberts, and Terry Rudolph. Interleaving: Modular architectures for fault-tolerant photonic quantum computing. *arXiv:2103.08612*, 2021.

[15] C. Gidney and M. Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5(433), 2021.

[16] O. D. Matteo, V. Gheorghiu, and M. Mosca. Fault-tolerant resource estimation of quantum random-access memories. *IEEE Transactions on Quantum Engineering*, 1:1–13, 2020.

[17] Daniel Litinski. A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery. *Quantum*, 3:128, March 2019.

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

[19] C. Gidney and A.G. Fowler. Efficient magic state factories with a catalyzed $|ccz\rangle$ to $2|t\rangle$ transformation. *Quantum*, 3(135), 2019.

[20] Simon J. Devitt, Ashley M. Stephens, William J. Munro, and Kae Nemoto. Requirements for fault-tolerant factoring on an atom-optics quantum computer. *Nature Communications*, 4(1):2524, 2013.

[21] Ashley M. Stephens. Fault-tolerant thresholds for quantum error correction with the surface code. *Physical Review A*, 89:022321, 2014.

[22] Ben Q. Baragiola, Giacomo Pantaleoni, Rafael N. Alexander, Angela Karanjai, and Nicolas C. Menicucci. All-gaussian universality and fault tolerance with the gottesman-kitaev-preskill code. *Physical Review Letters*, 123(20):200502–, 11 2019.

[23] B. Eastin and E. Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102:110502, 2009. arXiv:0811.4262.

[24] Ying Li. A magic state's fidelity can be superior to the operations that created it. *New Journal of Physics*, 17(2):023037, feb 2015.

[25] S. Bravyi and A. Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, 2005. quant-ph/0403025.

Reducing T-count in Quantum Boolean Circuits by Exploiting Relative Phase Boolean Functions

David Clarino[1] * Naoya Asada[1] † Shigeru Yamashita[1] ‡

[1] *Graduate School of Information Science and Engineering Ritsumeikan University*

Abstract. LUT-based synthesis methods have recently been proposed as a way to synthesize Quantum Boolean Circuits in a qubit constrained environment. Other results have also shown that allowing a relative phase when implementing Quantum Boolean Circuits yields an advantage in T-count without additional ancilla qubits, which is advantageous in the fault-tolerant quantum computing paradigm. We propose a method that utilizes both LUT-based synthesis and Relative Phase Quantum Boolean Circuits that minimize the T-count while minimizing the ancilla required to implement them. We leverage recent results regarding Relative Phase versions of Boolean functions and the Shannon decomposition to propose a novel method to synthesize arbitrary Boolean functions up to a Relative Phase. We then utilize this method to synthesize Boolean logic inside each LUT as a relative phase Quantum Boolean Circuit and show that the resulting Quantum Circuit has a clear advantage in T-count to using it over more naive methods.

1 Introduction

Quantum Boolean circuits are a circuit model to implement Boolean functions as quantum circuits. Toffoli gates are an essential component in these; however, they are composite from other, more fundamental gates [2] as depicted in Fig 1. In the fault tolerant paradigm, the Clifford+T set [4] is often used. However, T-gates incur much higher cost to implement fault tolerantly than the rest of that set, so we want to reduce their number as much as possible

We observe that it is possible to reduce the T-count if we implement Boolean functions, only up to a *relative phase* i.e. a phase that is state dependent. By ignoring any phase logic that is not dependent on the target, the method can reduce the T-count of implementing a Boolean map in quantum computing, but at the cost of a relative phase. However, a relative phase poses problems if the subsequent state were used in another quantum state, as it induces a rotation especially in a linear combination of state

Previous research has suggested that alternating pairs of gates have the potential to greatly reduce the number of T-gates, so generating logic that cascades into one output maximizes such pairs. Our research seeks to leverage recent results in relative phase implementations of Boolean functions [3] [1] and LUT-based quantum circuit synthesis [5] to generate such circuits in order to reduce T-count in a a qubit constrained environment.

Our Contribution. We propose a method that reduces the number of T-gates in a quantum Boolean circuit by exploiting relative phase Boolean functions. Among our contributions:

- A novel method to synthesize a Boolean function up to a relative phase by utilizing relative phase constructions and Shannon Decomposition.
- A method to generate a Quantum Boolean Circuit from a Boolean Logic Network representation leveraging the above method to reduce T-count.

Our methods are compared to a naive synthesis of each LUT node that utilizes an ESOP-based method to synthesize each Boolean function exactly as a Quantum Boolean Circuit. While there remain a few exceptions to its advantage, its advantage in the majority of cases we have tested suggests that further research into this area might turn fruitful.

The paper is structured as follows. Section 2 outlines preliminary information for understanding this paper. Then Section 5 lays out some motivations for the research we are going to conduct. Section 4 follows with our proposed method, including our novel method to realize functions up to a relative phase without any additional ancillae, and then its use with the LUT-based synthesis. Then, our experimental results in Section 5 can confirm that our method can indeed reduce the T-count of quantum Boolean circuits. Finally Section 5 contains our conclusions and future work.

2 Preliminary

2.1 Boolean Logic Network

A *Boolean logic network* is a simple dag whose vertices are primary inputs, primary outputs, and nodes which represent logic gates, whose arcs connect gates to inputs,

*dizzy@ngc.is.ritsumei.ac.jp
†accel@ngc.is.ritsumei.ac.jp
‡ger@ngc.is.ritsumei.ac.jp

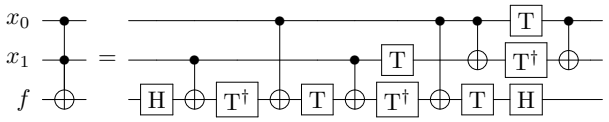


Figure 1: A Toffoli gate in Clifford+T basis

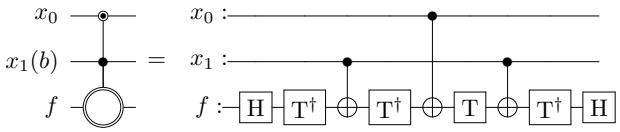


Figure 2: An RTOF gate in Clifford+T basis

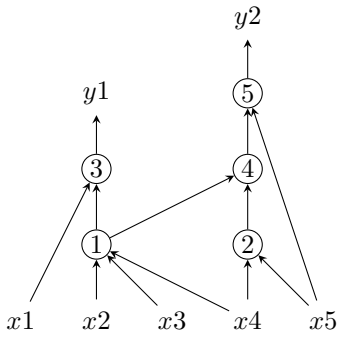


Figure 3: A Boolean logic network

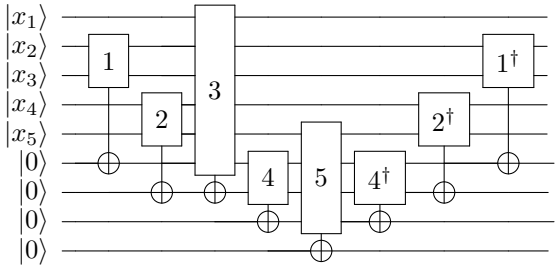


Figure 4: The Quantum Circuit implementing Fig 3

outputs, and other gates. A logic function can be decomposed into such a Boolean logic network, and its nodes subsequently implemented as LUTs or logic gates. We see an example in Fig 3

3 Existing Research and Motivation

Facts we use from existing research are found below

- Replacing pairs of computing and uncomputing gates with RTOF gate and its inverse will lead to T gate savings in most cases.
- Using the above, it is possible to use clean-ancilla to decompose an MCT with fewer T gates than the known methods.
- A recursive procedure to generate MCT gates up to a relative phase.

4 Proposed Method

4.1 Using Shannon Decomposition To Realize Arbitrarily Controlled Single Target Gates

Recall the Shannon decomposition $f(x_n, ..., x_1) = x_n \cdot f(x_n = 1, x_{n-1}, \cdots, x_0) + \bar{x_n} \cdot f(x_n = 0, x_{n-1}, \cdots, x_0)$. Because $x \cdot a + \bar{x} \cdot b = x \cdot a \oplus \bar{x} \cdot b$, this means that we can implement this function as a series of Relative Phase U-controlled NOT gates (UCNOT).

First, from the Shannon decomposition $f(x_n, ..., x_1) = x_n \cdot f(x_n = 1, x_{n-1}, \cdots, x_0) + \bar{x_n} \cdot f(x_n = 0, x_{n-1}, \cdots, x_0)$ where we can take $g = f(x_n = 1, x_{n-1}, \cdots, x_0)$ and $g' = f(x_n = 0, x_{n-1}, \cdots, x_0)$. As with any Shannon decomposition, we can decompose using an arbitrary variable order. It is easy to see that this expression implements the Sum of Products (SOP) expression of the Shannon decomposition. We then take each of g and g' and repeat the process recursively until we are left with a simple CNOT as our U-controlled NOT expression.

If it is "False", we have a False-controlled-NOT, meaning an identity function. This means that if one side of the Shannon decomposition evaluates to either "True" or "False", we can merely replace it with a CNOT gate or an identity (meaning nothing at all), respectively, without expending any additional T-gates to implement the function. As we will see in the next example, we can express the relative-phase Toffoli gate construction in [1] as a special case of this construction

4.2 Shannon Decomposition Cost and BDD representation

As is already apparent from the diagram, each variable that the function is dependent on roughly doubles the T-count, such that the total cost $C \propto 2^n$. This is in line with Barenco et al [2], who posit that the T-count of a gate is exponential with respect to the number of inputs in the absence of ancilla. As can also be seen from the diagram, each level has a linear dependence on the number of nodes at each level, so the relative complexity of the function also factors into the cost. In an environment where dirty ancilla are assumed to be plentiful, it is therefore desireable to limit these implementations to smaller numbers of input qubits i.e. smaller LUT-sizes.

As can already be seen, the Shannon decomposition method lends itself naturally to representation by Binary Decision Diagrams (BDDs). Representing our Boolean functions as BDDs gives us an easy way to traverse down the Shannon decomposition tree merely by traversing the BDD in the same direction and feeding the next node in the traversal as your input function to the next iteration

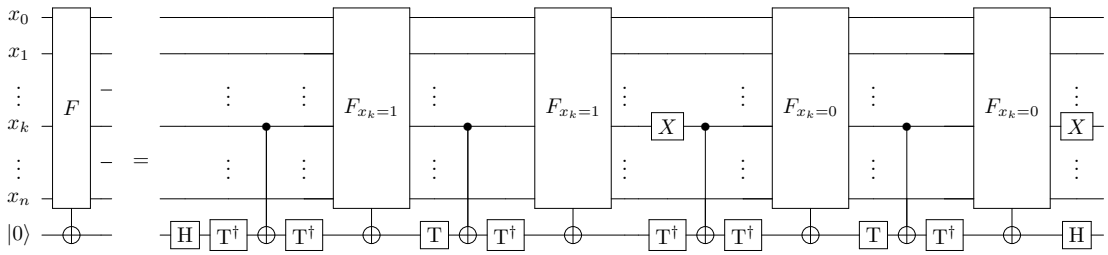


Figure 5: The circuit for Shannon Decomposition

of the recursive loop. As the cost is directly proportional to the number of nodes in the BDD, we can merely choose the variable order that minimizes the node count to minimize our generated quantum circuit

Knowing this, we are now ready to define our algorithm to define an arbitrary Boolean function up to a relative phase. First we convert the Boolean function to a BDD. We then find a suitable variable order that minimizes the number of nodes in the BDD (We leave the calculation up to the implementater depending on the scale of the problem. We present a solution in 5 that works for the problems we used in our experiments, but this is not meant to be a part of the main algorithm). We then proceed with our Shannon decomposition recursively in the variable order. However, we reevaluate the optimality of the BDD order at every level and rearrange the variables depending on which minimizes the function. The algorithm terminates when all branches reach either leaves or True/False.

4.3 Synthesizing A Boolean Function Using LUT-networks and Shannon Decomposition RTOF

Using the algorithm defined in the previous subsection, we are now ready to define our LUT-based synthesis method. First, we take as input a LUT network synthesized from a Boolean expression using existing LUT-Network decomposition methods. Then this LUT network is parsed by the algorithm to create a quantum circuit of UCNOT gates. Any intermediate node is decomposed as two UCNOTs: one to compute, and the other to uncompute, acting on the same dirty ancilla. Any node that acts only on output qubits (output node i.e. an endpoint to the cascading logic) is given only one UCNOT.An example of the result of this type of processing is depicted in Fig 4.

This QC is then parsed by our algorithm, synthesizing each UCNOT into relative phase versions of the partial Boolean functions in each intermediate node (as well as their inverse), and exact versions in each output node. These are then recombined into a quantum circuit.

5 Experimental Results and Conclusion

We generated Boolean Logic Netowrks using the ABC tool from the EPFL Combinational Benchmark Suite benchmark functions and, with LUT-sizes of 3,4,5,6. We then implemented them as quantum Boolean circuits both using the proposed method, as well as an exact synthesis using ESOP based methods and constructed conventionally. We found that on average the proposed method outperforms the ESOP methods by 22% with high variation. We also found that decreasing both the cost and the LUT-SIZE shows an average improvement of 62% over the LUT6 ESOP generated circuit. Thus our primary target of interest to improve this seems to be the cost of the Shannon Decomposition

References

[1] Matthew Amy and Neil J. Ross. Phase-state duality in reversible circuit design. *Phys. Rev. A*, 104:052602, Nov 2021.

[2] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.

[3] Dmitri Maslov. Advantages of using relative-phase toffoli gates with an application to multiple control toffoli optimization. *Physical Review A*, 93(2):022311, 2016.

[4] Michael A Nielsen and Isaac Chuang. *Quantum Computation*. 2010.

[5] Mathias Soeken, Martin Roetteler, Nathan Wiebe, and Giovanni De Micheli. Lut-based hierarchical reversible logic synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 38(9):1675–1688, 2018.

Energy-Consumption Advantage of Quantum Computation [1]

Florian Meier[1] * Hayata Yamasaki[2] †

[1] *Technische Universität Wien*
[2] *The University of Tokyo*

Abstract. Energy consumption in solving computational problems has been gaining growing attention as a part of the performance measures of computers. Quantum computation is known to offer advantages over classical computation in terms of various computational resources; however, its advantage in energy consumption has been challenging to analyze due to the lack of a theoretical foundation to relate the physical notion of energy and the computer-scientific notion of complexity for quantum computation with finite computational resources. To bridge this gap, we introduce a general framework for studying energy consumption of quantum and classical computation based on a computational model with a black-box oracle, as conventionally used for studying query complexity in computational complexity theory. With this framework, we derive an upper bound of energy consumption of quantum computation with covering all costs, including those of initialization, control, and quantum error correction; in particular, our analysis shows an energy-consumption bound for a finite-step Landauer-erasure protocol, progressing beyond the existing asymptotic bound. We also develop techniques for proving a lower bound of energy consumption of classical computation based on the energy-conservation law and the Landauer-erasure bound; significantly, our lower bound can be gapped away from zero no matter how energy-efficiently we implement the computation and is free from the computational hardness assumptions. Based on these general bounds, we rigorously prove that quantum computation achieves an exponential energy-consumption advantage over classical computation for Simon's problem. These results provide a fundamental framework and techniques to explore the physical meaning of quantum advantage in the query-complexity setting based on energy consumption, opening an alternative way to study the advantages of quantum computation.

Keywords: quantum thermodynamics, energy consumption, exponential advantage of quantum computation, query complexity, Landauer's principle

With growing interest in the sustainability of our society, energy consumption is nowadays considered an important part of performance measures for benchmarking computers. It is expected that quantum computation will be no exception; its energy efficiency will ultimately be one of the deciding factors as to whether quantum computers will be used on a large scale [2–4]. Originally, quantum computers emerged as a promising platform to solve certain computational problems that would otherwise be unfeasible to solve on classical computers. The advantage of quantum computation is generally examined in terms of computational complexity, which quantifies computational resources required for solving the problems, such as time complexity, communication complexity, and query complexity [5]. Energy is, however, a different computational resource from the above ones. A priori, an advantage in some computational resource does not necessarily imply that in another; for example, quantum computation is believed to achieve an exponential advantage in time complexity over classical computation but does not provide such an advantage in the required amount of memory space [6]. Whether quantum computation can offer a significant energy-consumption advantage over classical computation is a fundamental question but has not been explored rigorously as of now due to the lack of theoretical foundation to relate the known advantages of quantum computation and that in its energy consumption.

*florianmeier256@gmail.com
†hayata.yamasaki@gmail.com

Challenges in studying energy-consumption advantage. To analyze the energy-consumption advantage of quantum computation, there are two inequalities to be shown: first, an upper bound of energy consumption for performing a quantum algorithm, and secondly, a lower bound of energy consumption for *all* classical algorithms to solve the same problem.

As for the former, previous works mostly investigate energy consumption in implementing a single quantum gate [7–12], but the analysis of the quantum advantage requires an upper bound of energy consumption of the overall quantum computation composed of many quantum operations. Such an analysis has been challenging because, to account for the energy consumption of quantum computation, we need to take into account all the operations included in the computation, e.g., not only the gates but also the cost of initializing qubits and performing quantum error correction. A challenge here arises since, unlike quantum gates, some other quantum operations, such as measurements and initialization, may consume an infinitely large amount of energy as we increase the accuracy in their implementation [13, 14]. Thus, we need to formulate the framework of quantum computation properly to avoid the operations requiring infinite energy consumption and to establish finite achievability results of energy consumption for all the operations used for the quantum computation within the framework.

The latter is even more challenging since it is in general hard to derive a lower bound of energy consumption of overall computation from the lower bound of each individual operation; after all, we may be able to perform multiple operations in the computation collectively

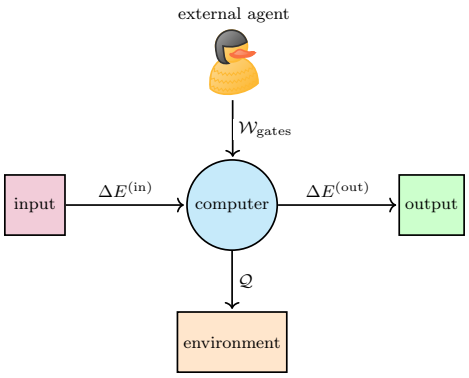


Figure 1: Illustration of our thermodynamic model for quantum and classical computation.

to save energy consumption. In the first place, the energetic cost of performing reversible operations, be it on a quantum or classical computer, can be either positive or negative. For example, consider the cost of performing a bit-flip gate on a two-level system with states 0 and 1 and energies $E_0 < E_1$. If the bit initially starts in 0, then we need to invest a positive amount of energy $E_1 - E_0 > 0$ to obtain 1 by the bit-flip gate. By contrast, if the bit initially starts in the state 1 and is flipped into 0, one can also gain energy $E_1 - E_0$ from the bit-flip gate at best; in other words, the energetic cost of performing a reversible operation can be negative in general. Apart from this energetic cost, the implementation of the bit-flip gate may also require an additional control cost arising from heat dissipation, which is caused by, e.g., friction and electrical resistance. The control cost may be positive in reality, but in the limit of energy-efficient implementation, it is hard to rule out the possibility that the control cost may be negligibly small; in particular, it is unknown whether the infimum of the control cost over any possible implementation of computation can still be lower bounded by a strictly positive constant gapped away from zero. Thus, the analysis requires a novel technique for deriving a nonzero lower bound of energy consumption of the overall computation, which needs to be applied independently of the detail of the implementation.

Summary of main results. We address the above challenges by combining and developing techniques on computational complexity theory [5], quantum information theory [15], and quantum thermodynamics [16]. In particular, our results are as follows.

1. We formulate a framework within which the energy consumption of quantum and classical computation can be rigorously studied (Sec. II of Technical Version [1]). We will describe its core idea with Fig. 1 in the following.

2. We derive a general upper bound on the energy consumption that is achievable by the quantum computation in our framework (Sec. IIIA of Technical Version [1]). For this analysis, extending upon the existing asymptotic results [14, 17, 18] on Landauer erasure [19], we show a novel result on the achievability of finite-fidelity and finite-step Landauer erasure. Apart from the finite Landauer erasure, we derive our achievability bound using complexity-theoretic considerations and also taking into account overheads from quantum error correction, so as to cover all the contributions to the energy consumption.

3. We further develop a technique for obtaining an implementation-independent lower bound on the energy consumption of the classical computation in our framework (Sec. IIIB of Technical Version [1]). The bound is derived using energy conservation and the Landauer-erasure bound.

4. Lastly, we show an explicit example where the energy consumption of quantum and classical computation for solving a computational problem is exponentially separated (Sec. IV of Technical Version [1]). To prove this rigorously, we apply the above techniques to Simon's problem [20, 21].

To establish the framework for studying energy consumption, we view quantum and classical computations as thermodynamic processes, as shown in Fig. 1. In our computational model, the agent uses the computer to carry out the computation to solve a decision problem. Performing operations on the computer comes at a work cost for this external agent, which we summarize as $\mathcal{W}_{\rm gates}$. This cost includes *energetic costs* arising from the change of energy of the internal states of the computer, and *control costs* caused by energetic losses in implementing these operations due to heat dissipation. As in a conventional setting of studying query complexity [5, 15, 22], we use an oracle as an input model, which provides the input to the computer via oracle queries. In our model, the oracle is an irreversible black box whose internals are unknown. Still, there is some transfer of energy between the input and the computer, namely $\Delta E^{(\rm in)}$, due to the states the oracle generates and inputs into the computer. On the other hand, working on decision problems means that the output is a two-level system where the decision is stored as either 0 or 1. Generating this single-bit output comes at an energy exchange of $\Delta E^{(\rm out)} = O(1)$ and is practically negligible compared to the growing sizes of the computer, the input, and the thermal environment surrounding around the computer. Throughout the computation, the energy corresponding to the control cost may flow into the environment, which in parts contributes to the heat $\mathcal{Q}$ dissipated to the environment. The other contribution to $\mathcal{Q}$ arises from reinitializing the internal state of the computer at the end of the computation. In contrast to the control cost that may approach zero in the limit of energy-efficient implementation, nonzero energy consumption in reinitializing the computer is inevitable in our framework due to Landauer's principle [19]. All in all, we demand that the reinitialization make the computation cyclic on the computer so that this computer could be used for solving another task after conducting the current computation.

With this model, we define the *energy consumption* $\mathcal{W}$ in computation as the sum of all the contributions of the external agent, the input, and the output in Fig. 1, i.e.,

$$\mathcal{W} \coloneqq \mathcal{W}_{\text{gates}} + \Delta E^{(\text{in})} - \Delta E^{(\text{out})}. \tag{1}$$

The demand of the computation being cyclic is critical to energy conservation; i.e., in the limit of closing this thermodynamic cycle ideally without error, the energy conservation leads to $\mathcal{W} = \mathcal{Q}$. The energy consumption $\mathcal{W}$ is the sum of he non-dissipative energy exchanges between external systems and the computer, which can be understood as the work cost of performing the computation. The contributions to $\mathcal{W}$ are detailed further in Sec. II of Technical Version [1].

With this framework, we analyze all contributions to $\mathcal{W}$ to derive an upper bound of energy consumption for quantum computation. Our analysis argues that the work cost of performing unitary operations on the computer scales at most with the size of the circuit for their implementation. However, a challenge arises since the computation in Fig. 1 is realized by a thermodynamic cycle, and thus, the states of the computer have to be reinitialized by the end of the computation. Protocols for Landauer erasure [19] can be used for the reinitialization in our framework, but the existing asymptotic results [14, 17, 18] on the required cost of the Landauer-erasure protocols are insufficient for our analysis of finite work cost. Problematically, it may require infinite time steps to exactly reset a given state into a target pure state by the Laudauer-erasure protocols, and the control cost required for the infinite time steps may also diverge; indeed, based on the third law of thermodynamics (Nernst's unattainability principle [23]), cooling a quantum state to absolute zero and thereby erasing its previous state inevitably comes at divergent resource costs in some form [14, 24–26]. By contrast, our main contribution is to derive an upper bound of energy consumption for the Laudauer-erasure protocol with finite step to achieve finite infidelity to a target pure state. With this bound, we also take into account the finite overhead of quantum error correction by arguing that the infidelity for this Laudauer erasure can be set as the threshold constant for fault-tolerant quantum computation, leading to the general upper bound of energy consumption.

On the other hand, we analyze the heat $\mathcal{Q}$ ($= \mathcal{W}$ due to the energy conservation) to derive a lower bound on the energy consumption for classical computation. The decomposition of $\mathcal{W}$ in (1) into the respective contributions (e.g., energetic cost and control cost) would not directly help us in finding the lower bound since no fundamentally positive lower bound is known for the cost of performing a gate; after all, in the limit of energy-efficient implementation, a single gate may be performed at as close to zero control cost as possible. Moreover, without oracle, any classical algorithm could be written in a reversible way, but reversible computation would make it possible to perform uncomputation after the result of the computation has been output from the computer, where the invested energy for the computation could be returned in principle via the uncomputation [27, 28]. To avoid this uncomputation, it is essential for our framework to assume that the oracle is a black box whose inverse is inaccessible, guaranteeing that part of the computation may not be inverted. The crucial assumption in our framework is that the knowledge on the oracle obtained from the queries during the computation remains in the computer until erased with the thermodynamical cost in an irreversible way. By analyzing the heat dissipation $\mathcal{Q}$ required for the Laudauer erasure, we obtain a general lower bound on the energy consumption of computation.

Using these general bounds, we prove that the energy consumption of quantum computation can be exponentially smaller than that of classical computation for solving Simon's problem [20, 21]. Simon's problem is an exemplary case where the query complexity in quantum computation is exponentially separated from any classical computation. The structure of the quantum algorithm to solve Simon's problem is closely related to the ones to solve the non-oracle-based (i.e., non-relativized) problems of the discrete logarithm and the integer factorization [29]. The issue with the latter non-relativized problems is that lower bounds on the complexity of classical algorithms to solve them are notoriously hard to show in general because they mainly boil down to the open question of whether there exists a classical polynomial-time algorithm to solve the integer factorization. By contrast, applying our energy-consumption bounds to Simon's problem, we rigorously prove the exponential energy-consumption advantage of quantum computation, where the bound for classical algorithms do not depend on the conjectured hardness of a computational task.

Impact. Our study provides a fundamental framework and techniques for exploring a novel quantum advantage in terms of energy consumption. The framework is designed so that a quantum advantage in query complexity can be employed for proving the energy-consumption advantage of quantum computation over classical computation. These results clarify the physical meaning of the quantum advantage in the query-complexity setting in terms of energy consumption. Also from a broader perspective, beyond solving decision problems, quantum computers may have promising applications in learning properties of physical dynamics described by an unknown map within the law of quantum mechanics [30]. The physical dynamics that are input to the learning algorithms by themselves can be considered a black-box oracle, and the framework and techniques developed here are also expected to serve as a theoretical foundation to realize the energy-consumption advantage of quantum computation in such physically well-motivated applications. Finally, a potential drawback of our current analysis would be that some part of our analysis ignores constant factors of the bounds; thus, the actual energy consumption required for experimental demonstration of the energy-consumption quantum advantage may be still unclear at a small scale. It would also be important in practice to evaluate the constant factors more explicitly, but our results have opened a route toward further studies in this direction with a solid theoretical foundation.

References

[1] Technical version attached to this submission, arXiv:2305.11212, 2023.

[2] J. Preskill, Quantum Computing in the NISQ era and beyond, Quantum **2**, 79 (2018).

[3] A. Auffèves, Quantum Technologies Need a Quantum Energy Initiative, PRX Quantum **3**, 020101 (2022).

[4] D. Jaschke and S. Montangero, Is quantum computing green? an estimate for an energy-efficiency quantum advantage, Quantum Science and Technology **8**, 025001 (2023).

[5] J. Watrous, Quantum Computational Complexity, in *Encyclopedia of Complexity and Systems Science*, edited by R. A. Meyers (Springer New York, New York, NY, 2009) pp. 7174–7201.

[6] J. Watrous, On the complexity of simulating space-bounded quantum computations, Comput. Complex. **12**, 48–84 (2004).

[7] M. Ozawa, Conservative Quantum Computing, Phys. Rev. Lett. **89**, 057902 (2002).

[8] J. Gea-Banacloche and M. Ozawa, Minimum-energy pulses for quantum logic cannot be shared, Phys. Rev. A **74**, 060301 (2006).

[9] J. Ikonen, J. Salmilehto, and M. Möttönen, Energy-efficient quantum computing, npj Quantum Information **3**, 17 (2017).

[10] J. Stevens, D. Szombati, M. Maffei, C. Elouard, R. Assouly, N. Cottet, R. Dassonneville, Q. Ficheux, S. Zeppetzauer, A. Bienfait, A. N. Jordan, A. Auffèves, and B. Huard, Energetics of a Single Qubit Gate, Phys. Rev. Lett. **129**, 110601 (2022).

[11] G. Chiribella, Y. Yang, and R. Renner, Fundamental Energy Requirement of Reversible Quantum Operations, Phys. Rev. X **11**, 021014 (2021).

[12] Y. Yang, R. Renner, and G. Chiribella, Energy requirement for implementing unitary gates on energy-unbounded systems, Journal of Physics A: Mathematical and Theoretical **55**, 494003 (2022).

[13] Y. Guryanova, N. Friis, and M. Huber, Ideal Projective Measurements Have Infinite Resource Costs, Quantum **4**, 222 (2020).

[14] P. Taranto, F. Bakhshinezhad, A. Bluhm, R. Silva, N. Friis, M. P. Lock, G. Vitagliano, F. C. Binder, T. Debarba, E. Schwarzhans, F. Clivaz, and M. Huber, Landauer versus nernst: What is the true cost of cooling a quantum system?, PRX Quantum **4**, 010332 (2023).

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, 2010).

[16] J. Goold, M. Huber, A. Riera, L. d. Rio, and P. Skrzypczyk, The role of quantum information in thermodynamics–a topical review, Journal of Physics A: Mathematical and Theoretical **49**, 143001 (2016).

[17] D. Reeb and M. M. Wolf, An improved Landauer principle with finite-size corrections, New Journal of Physics **16**, 103011 (2014).

[18] A. Rolandi and M. Perarnau-Llobet, Finite-time landauer principle at strong coupling, 2211.02065v2 [quant-ph] (2022).

[19] R. Landauer, Irreversibility and Heat Generation in the Computing Process, IBM Journal of Research and Development **5**, 183 (1961).

[20] D. Simon, On the power of quantum computation, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994) pp. 116–123.

[21] D. R. Simon, On the power of quantum computation, SIAM Journal on Computing **26**, 1474 (1997).

[22] H. Buhrman and R. de Wolf, Complexity measures and decision tree complexity: a survey, Theoretical Computer Science **288**, 21 (2002), complexity and Logic.

[23] W. Nernst, Ueber die Berechnung chemischer Gleichgewichte aus thermischen Messungen, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1906**, 1 (1906).

[24] H. Wilming and R. Gallego, Third Law of Thermodynamics as a Single Inequality, Phys. Rev. X **7**, 041033 (2017).

[25] L. Masanes and J. Oppenheim, A general derivation and quantification of the third law of thermodynamics, Nature Communications **8**, 14538 (2017).

[26] N. Freitas, R. Gallego, L. Masanes, and J. P. Paz, Cooling to Absolute Zero: The Unattainability Principle, Thermodynamics in the Quantum Regime , 597–622 (2018).

[27] C. H. Bennett, Logical reversibility of computation, IBM journal of Research and Development **17**, 525 (1973).

[28] C. H. Bennett, The thermodynamics of computation—a review, International Journal of Theoretical Physics **21**, 905 (1982).

[29] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing **26**, 1484 (1997).

[30] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, Challenges and opportunities in quantum machine learning, Nature Computational Science **2**, 567 (2022)
.

Quantum Circuit Autoencoder

Jun Wu[1] * Hao Fu[1] † Mingzheng Zhu[1] ‡ Wei Xie[1] § Xiang-Yang Li[1 2] ¶

[1] *University of Science and Technology of China, Hefei 230027, China*
[2] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

Abstract. In this study, we introduce the concept of a quantum circuit autoencoder as a means to compress and encode information within quantum circuits. This serves as a generalization of the quantum state autoencoder. Our first step involves presenting a protocol for the quantum circuit autoencoder and designing a variational quantum algorithm named QCAE that can implement it. We then explore the conditions necessary for lossless compression and establish an upper bound on recovery fidelity of QCAE. Furthermore, we identify how the lossless condition enables us to construct a loss function and avoid the Barren Plateau problem. Following the classical autoencoder approach, we apply QCAE to dimension reduction and anomaly detection for quantum circuits. Finally, we evaluate the effectiveness of our proposed quantum circuit autoencoder through numerical simulations. Our results show that QCAE can efficiently compress and recover quantum circuits with high fidelity while identifying circuit outliers precisely.

Keywords: quantum machine learning, variational quantum algorithms, autoencoder, quantum circuit compression

1 Introduction

Quantum technologies have made significant progress in the past several years, with notable examples including quantum supremacy experiments [1, 2, 3] on Noisy Intermediate-Scale Quantum (NISQ) devices [4]. However, NISQ devices suffered from severe noise and limited qubits. Therefore, in order to fully utilize NISQ resources, it is essential to implement techniques for compressing quantum information to reduce the number of resources required for a particular task.

Autoencoder is an artificial neural network widely used to compress and encode information [5]. The main idea is to reduce the dimension of information through bottleneck while maintaining the reconstructed fidelity of the data. Ref. [6] proposed a quantum autoencoder (QAE), a quantum extension of autoencoder, to reduce the input states' dimension and widely investigated in quantum machine learning and other areas [7, 8, 9]. QAE reduces the state's dimension by discarding the "trash" system in the encoding step and then reconstructs the state with the help of the "reference" state.

However, the reconstructed fidelity is limited when the number of input states is large [10]. Moreover, quantum information is often stored in quantum circuits instead of quantum states due to the state store technologies are not mature [11, 12]. In order to address these issues, there is a need for an elaborate study on quantum circuit autoencoder. Quantum circuit autoencoder can also as a generalization of QAE, for example, it can subsume QAE in some cases such as purified quantum query access model.

Ref. [13] and Ref. [14] proposed a gate compression model that uses two unitary operators to reduce the input gate's dimension and another two unitary operators to reconstruct the original gate. This model can be seen as a simple prototype of a quantum circuit autoencoder. The authors also provided a method to achieve exponential reduction in dimension. However, this approach only considers gates consisting of single-qubit gates in the IID form, whereas general quantum circuits in practice consist of multiple qubits and not just single-qubit gates.

In this work, we proposed a quantum circuit autoencoder model as depicted in Fig. 1. For a mixed quantum channel $\mathcal{E}$, which is a convex combination of a batch of quantum circuits acting on D-qubits, we construct encoders $\mathcal{U}_1$ and $\mathcal{V}_1$ to obtain $\mathcal{F} = \mathrm{tr}_{trash}(\mathcal{V}_1 \circ \mathcal{E} \circ \mathcal{U}_1)$ acting on d-qubit system ($d < D$), where tr_{trash} meaning discarding the $D - d$ system, i.e. the "trash" system. The goal is to maximize the reconstruc fidelity between $\tilde{\mathcal{E}} = \mathcal{V}_2 \circ (\mathcal{F} \otimes \mathrm{id}) \circ \mathcal{U}_2$ and $\mathcal{E}$.

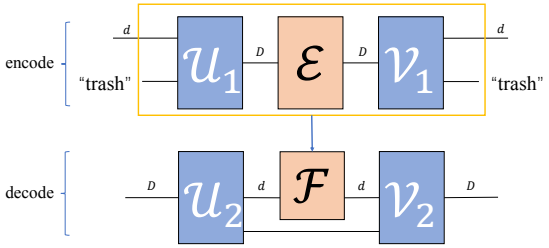


Figure 1: the quantum circuit autoencoder encodes a 2^D-dimensional quantum circuit into a 2^d-dimensional circuit and reconstructs the original 2^D-dimensional quantum circuit through the encoding process.

In order to implement a quantum circuit autoencoder on NISQ devices, we have designed a variational quantum algorithm [15] named QCAE. Specifically, we have made use of parameterized quantum circuits (PQCs) [16] to find the encoders and decoders required for the implementation of the quantum circuit autoencoder. We have also utilized QCAE for some quantum circuit tasks, including dimension reduction and anomaly detection on quantum circuits.

*jun_wu@mail.ustc.edu.cn
†hflash@mail.ustc.edu.cn
‡zmzming@mail.ustc.edu.cn
§xxieww@ustc.edu.cn
¶xiangyangli@ustc.edu.cn

2 Method

2.1 Sketch of our method

We present the diagram of our quantum circuit autoencoder model. The goal is to find encoders and decoders to encode $\mathcal{E}$ through a bottleneck and decode it to original circuits as faithfully as possible. Our algorithm uses the parameterized quantum circuit controlled by a set of parameters to represent the encoders and decoders. Therefore, QCAE aims to find the optimal control parameters to maximize the similarity between original and reconstructed quantum circuits.

The typical quantum circuits autoencoder is shown in Fig. 1 consists of two separated processes: encoding and decoding. During the encoding process, the training data set $\{\mathcal{E}_i\}_{i=1}^{N_{train}}$ is encoded as a mixed quantum channel $\mathcal{E}$ on D-qubits system. Then, the encoders $U(\theta)$ and $V(\theta)$ act on the channel $\mathcal{E}$ and get the reduced channel $\mathcal{F}$ by partially tracing the last $(D-d)$ qubits (i.e. "trash" systems). As a result, return the channel $\mathcal{F}$ on the d-qubit system. In the reconstruction process, the decoders $U(\theta)^\dagger$ and $V(\theta)^\dagger$ are applied to the channel $\mathcal{F} \otimes \mathrm{id}$ to yield a new quantum circuit $\tilde{\mathcal{E}}$. Finally, we feed the similarity between $\mathcal{E}$ and $\tilde{\mathcal{E}}$ to the classical optimizer to update parameters θ. Note that the decoders in the reconstruction process are the conjugate transpose of the encoders. Therefore, we only consider the encoding process for convenience. And we use the product state between maximally mixed ω and maximally entangled state ϕ^+ as the initial state. Fig. 2 is the diagram of QCAE.

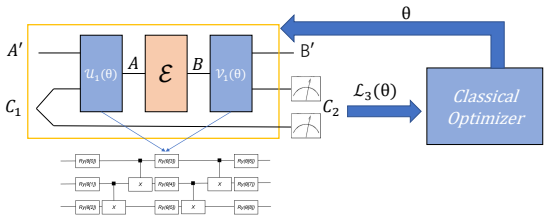


Figure 2: The diagram of the QCAE.

2.2 Loss Function

Given the data set $\mathcal{D} := \{\mathcal{E}_m\}_{m=1}^N$ and encoders $U(\theta)$ and $V(\theta)$, we obtain the mixed quantum channel $\mathcal{E} = \frac{1}{N}\sum_m \mathcal{E}_m$, the loss function is designed as:

$$\mathcal{L}_1 := 1 - y(\mathcal{E}, \tilde{\mathcal{E}}), \tag{1}$$

here, the error function $y(\mathcal{E}, \tilde{\mathcal{E}})$ is defined as:

$$y(\mathcal{E}, \tilde{\mathcal{E}}) = F(J^{\mathcal{E}}, J^{\tilde{\mathcal{E}}}), \tag{2}$$

where $F(\cdot)$ is the state fidelity function, $\tilde{\mathcal{E}} = \mathcal{V}^\dagger \circ (\mathcal{F} \otimes \mathrm{id}) \circ \mathcal{V}^\dagger$ and $\mathcal{F} = \mathrm{tr}_{C_1C_2}[\mathcal{V} \circ \mathcal{E} \circ \mathcal{U}]$.

The error function in Eq. 2 is to calculate the fidelity between two 4^D quantum states, which is an unaffordable computation cost. We propose Prop. 1 and given the loss function:

$$\mathcal{L}_2(\mathcal{D}, \theta) := 1 - [F(\phi^+_{C_1}, \phi^+_{C_2})], \tag{3}$$

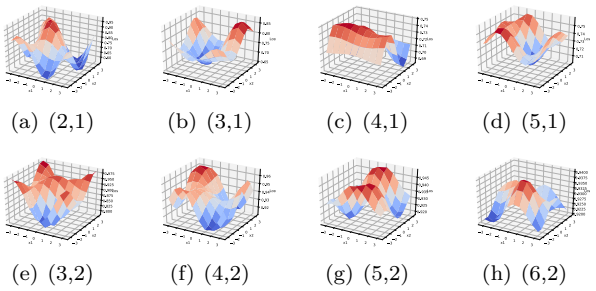


Figure 3: The slice of loss landscape with respect to the first two circuit parameters by changing the input channels' size D and latent channel size d. Here, the binary list represents (D, d).

where $F(\cdot)$ is also the state fidelity function and only considers the state on the "trash" system,

$$F^(\phi^+_{C_1}, \phi^+_{C_2}) = \\ \mathrm{tr}(\phi^+ \mathrm{tr}_{B'}[(\mathcal{V}(\theta) \circ \mathcal{E} \circ \mathcal{U}(\theta))(\omega_{A'} \otimes \phi^+_{C_1})])). \tag{4}$$

Furthermore, to escape Barren Plateau (BP) [17], we use the following loss function:

$$\mathcal{L}_3(\mathcal{D}, \theta) := \\ 1 - [\mathrm{tr}(O\,\mathrm{tr}_{B'}[(\mathcal{V}(\theta) \circ \mathcal{E} \circ \mathcal{U}(\theta))(\omega_{A'} \otimes \phi^+_{C_1})])], \tag{5}$$

where O is a local observable and

$$O = \sum_{m=1}^{N-1} \phi^+_{m,m+1} \otimes \mathbb{1}_{\overline{m,m+1}}. \tag{6}$$

Analytical Gradients and Barren Plateau: Given the QCAE, we briefly discuss analytic gradient and the barren plateau issues that the expectation gradient is approximate to zero exponentially. The ansatz we use is a 2-local parameterized quantum circuit deployed as the sequence of single-qubit rotations and two-qubit gates. Therefore, we can use the parameter-shift rule[18] to obtain the partial derivative:

$$\frac{\partial \mathcal{L}_3}{\partial \theta_j} = \mathcal{L}_3(\theta_+) - \mathcal{L}_3(\theta_-), \tag{7}$$

where θ_+ and θ_- are different from θ only at the j-th parameter: $\theta_j \to \theta_j \pm \frac{\pi}{4}$.

As for the Barren Plateau(BP) [17] from which many variational quantum algorithms may suffer. We remark on two points: First, our QCAE performs $(D-d)$-qubit measurements and takes the result as the loss function. Second, the observable of loss function in Eq. 5 is local. These two points keep the loss function local, which has been proved to have, at worst, a polynomially vanishing gradient with a shallow PQC [19]. In this sense, our QCAE could release the barren plateau issue when the number of layers $L \in \mathcal{O}(\log(D))$. Fig. 3 shows the landscape of QCAE, where the target channel is a combination of ten PQCs.

3 Theoretical Analysis

In this section, we give two propositions. One is the Faithful Compression Condition, which is essential in designing the loss function in Eq. 3. Another provides an upper bound on reconstructed fidelity of QCAE.

3.1 Faithful Compression Condition

Proposition 1. *(Faithful compression condition) The channel $\mathcal{E}$ can be recovered from $\mathcal{F}$ by recovery scheme if and only if*

$$\mathrm{tr}_{B'}\,\Pi(\omega_{A'}\otimes\phi^{+}_{C_1})=\phi^{+}_{C_2}, \tag{8}$$

where ϕ^+ is the maximally entangled state, ω denotes the maximally mixed state, and $\Pi=\mathcal{V}\circ\mathcal{E}\circ\mathcal{U}$ is the channel after applying encoders to $\mathcal{E}$.

Prop. 1 tells us that we can recover a quantum channel after compression if the origin channel can be written as a product of a compressed channel and an identity channel. Prop. 1 implies that it is possible to accomplish the learning task of finding the ideal $\mathcal{U}$ and $\mathcal{V}$ by training only on the "trash" state.

3.2 Upper Bound on Recovery Fidelity of QCAE

Lemma 1. *Let ρ and σ be the quantum state, and let r be the rank of σ. Then the fidelity between ρ and σ is upper bounded by the sum of the largest r eigenvalues of ρ, and the bound is achieved if and only if $\rho=\sigma$.*

Lemma 1 gives us an upper bound on the fidelity between any two quantum states, and it can be used to prove the following proposition.

Proposition 2. *Let $\tilde{\mathcal{E}}$ be the recovered quantum channel from $\mathcal{V}\circ\mathcal{E}\circ\mathcal{U}$, the recovery fidelity $F(\tilde{\mathcal{E}},\mathcal{E})$ is upper bounded by the sum of the largest d^2 eigenvalues of Choi state of $\mathcal{E}$, where d is the dimension of the reduced quantum channel $\mathcal{F}=\mathcal{V}\circ\mathcal{E}\circ\mathcal{U}$.*

Inspired by this proposition, we know that the reconstruct fidelity via QCAE could be not good with a rank larger than d^2. For example, let us consider the completely depolarizing quantum channel Δ whose input and output dimensions are D and compress it to D/d dimension. The Choi state of Δ is $\mathrm{diag}(\frac{1}{D^2},\cdots,\frac{1}{D^2})$. Based on the above proposition, even for the best case of training, the fidelity of reconstruction is always no larger than $\frac{d^2}{D^2}$.

4 Numerical Results

This section presents some practical applications of QCAE, such as dimension reduction and anomaly detection for quantum circuits.

In the compression experiments, we choose a set of PQCs with parameters generated by the same distribution, and using the reconstructed infidelity as the validation. We can achieved low reconstruct error rates of less than 0.2, as show in Fig. 4 and Tab. 4.

In the anomaly detection experiments, we set the PQCs with parameters generated by $norm(0,0.1)$ as normal data and the PQCs with parameters generated by

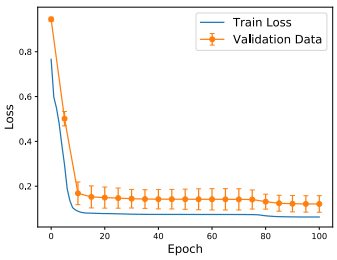


Figure 4: Training and validation processes of quantum circuits compression.

Table 1: Compression performance of multiple parameterized quantum circuits.

m*	distribution	n†	d‡	$\mathcal{L}_3$	val_mean	val_std
10	$norm(0,0.1)$	4	3	0.016	0.031	0.019
10	$norm(0,0.2)$	4	3	0.063	0.121	0.037
10	$norm(0,0.3)$	4	3	0.104	0.194	0.086
20	$norm(0,0.1)$	4	3	0.022	0.044	0.020
10	$norm(0,0.1)$	4	2	0.027	0.048	0.011
10	$norm(0,0.1)$	5	3	0.038	0.074	0.033
10	$norm(0,0.1)$	6	4	0.051	0.099	0.030

* m is the number of circuits
† n is the number of qubits
‡ d is the number of latent qubits

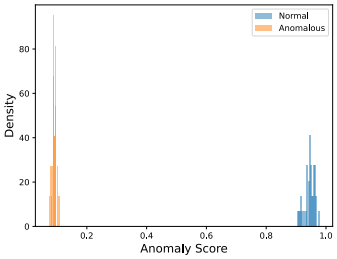


Figure 5: The results of quantum circuits anomaly detection.

$norm(0,0.5)$ as abnormal data. We use the reconstructed fidelity as the anomalous scores to detect the outliers. QCAE is proved to be highly effective in distinguishing abnormal data from normal data, see Fig. 5.

5 Discussion

The reconstruct fidelity of QCAE is bounded in Proposition 2. This limitation arises from the fact that the rank of the mixed quantum channel increases as the number of circuits grows. To address this, we can use an effective ansatz and pad a noise channel instead of an identity channel when reconstructing the channel from the reduced channel. An interesting research direction is to estimate the performance of QCAE on random input quantum channels. There is a lot of potential for further progress in determining tasks that are suitable for QCAE. For example, quantum circuit autoencoders have applications in denoising, data generation, and feature extraction for information in quantum circuits. In addition, finding more practical tasks beyond anomaly detection using Parameterized Quantum Circuits (PQCs) with different parameters and distributions is also appealing.

References

[1] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[2] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[3] Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, et al. Strong quantum computational advantage using a superconducting quantum processor. *Physical review letters*, 127(18):180501, 2021.

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

[5] Cheng-Yuan Liou, Jau-Chi Huang, and Wen-Chie Yang. Modeling word perception using the elman network. *Neurocomputing*, 71(16-18):3150–3157, 2008.

[6] Jonathan Romero, Jonathan P Olson, and Alan Aspuru-Guzik. Quantum autoencoders for efficient compression of quantum data. *Quantum Science and Technology*, 2(4):045001, 2017.

[7] Kwok Ho Wan, Oscar Dahlsten, Hlér Kristjánsson, Robert Gardner, and MS Kim. Quantum generalisation of feedforward neural networks. *npj Quantum information*, 3(1):1–8, 2017.

[8] Guillaume Verdon, Jason Pye, and Michael Broughton. A universal training algorithm for quantum deep learning. *arXiv preprint arXiv:1806.09729*, 2018.

[9] Dmytro Bondarenko and Polina Feldmann. Quantum autoencoders to denoise quantum data. *Physical review letters*, 124(13):130502, 2020.

[10] Chenfeng Cao and Xin Wang. Noise-assisted quantum autoencoder. *Physical Review Applied*, 15(5):054012, 2021.

[11] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum random access memory. *Physical review letters*, 100(16):160501, 2008.

[12] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S Kottmann, Tim Menke, et al. Noisy intermediate-scale quantum algorithms. *Reviews of Modern Physics*, 94(1):015004, 2022.

[13] Giulio Chiribella, Yuxiang Yang, and Cupjin Huang. Universal superreplication of unitary gates. *Physical review letters*, 114(12):120504, 2015.

[14] W Dür, P Sekatski, and M Skotiniotis. Deterministic superreplication of one-parameter unitary transformations. *Physical review letters*, 114(12):120503, 2015.

[15] M Cerezo, Kunal Sharma, Andrew Arrasmith, and Patrick J Coles. Variational quantum state eigensolver. *arXiv preprint arXiv:2004.01372*, 2020.

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

[17] Jarrod R McClean, Sergio Boixo, Vadim N Smelyanskiy, Ryan Babbush, and Hartmut Neven. Barren plateaus in quantum neural network training landscapes. *Nature communications*, 9(1):1–6, 2018.

[18] Maria Schuld, Ville Bergholm, Christian Gogolin, Josh Izaac, and Nathan Killoran. Evaluating analytic gradients on quantum hardware. *Physical Review A*, 99(3):032331, 2019.

[19] M Cerezo, A Sone, T Volkoff, L Cincio, and PJ Coles. Cost-function-dependent barren plateaus in shallow quantum neural networks (2020). *arXiv preprint arXiv:2001.00550*, 2001.

Tensor Network Assisted Variational Quantum Algorithm

Junxiang Huang[1] * Wenhao He[1 2] Yukun Zhang[1] Yusen Wu[3] Bujiao Wu[1 4] †
Xiao Yuan[1] ‡

[1] *Center on Frontiers of Computing Studies, Peking University, Beijing 100871, China*
[2] *School of Physics, Peking University, Beijing 100871, China*
[3] *Department of Physics, The University of Western Australia, Perth, WA 6009, Australia*
[4] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin 14195, Germany*

Abstract. Near-term quantum devices generally suffer from shallow circuit depth and hence limited expressivity due to noise and decoherence. To address this, we propose tensor network assisted parameterized quantum circuits, which concatenate a classical tensor network operator with a quantum circuit to effectively increase the circuit's expressivity without requiring a physically deeper circuit. We present a framework for tensor network-assisted variational quantum algorithms that can solve quantum many-body problems using shallower quantum circuits. We demonstrate the efficiency of this approach by considering two examples of unitary matrix product operators and unitary tree tensor networks, showing that they can both be implemented efficiently. Through numerical simulations, we show that the expressivity of these circuits is greatly enhanced with the assistance of tensor networks. We apply our method to 2D Ising models and 1D time crystal Hamiltonian models with up to 16 qubits, and demonstrate that our approach consistently outperforms conventional methods using shallow quantum circuits.

Keywords: tensor network, quantum circuit, variational quantum algorithm

1 Introduction

Tensor networks (TNs) and parameterized quantum circuits (PQCs) are powerful tools for representing quantum many-body states, respectively in classical and quantum approaches. The density matrix renormalization group (DMRG) algorithm, based on TNs, has achieved great success in solving ground state properties for one-dimensional systems [1, 2, 3]. However, the expressivity of TNs is limited by the area law with limited bond dimensions. PQCs, on the other hand, offer a more natural representation of quantum states on quantum computers, and many quantum algorithms [4, 5] have been proposed to take advantage of this. Nevertheless, near-term quantum computers are inherently noisy, which could also limit the circuit depth and expressivity of PQCs. Therefore, solving systems with non-trivial entanglement structures, such as strongly correlated matters and molecules, using either TNs or PQCs remains a challenging task.

TNs and PQCs are commonly considered as distinct classical and quantum computation methods, each with its own set of advantages and limitations. While TNs are relatively easy to implement, they have limited expressivity due to the area law, while PQCs offer much larger expressivity but are limited by noise and shallow circuit depth. Nevertheless, TNs and PQCs have been shown to have close interactions with each other. PQCs, for example, can be designed as classically unrealizable TNs with exponentially large bond dimensions [6, 7, 8, 9, 10]. At the same time, TNs that are classically realizable can represent special unitary operations and be used as a particular type of PQCs. This raises the question of whether we can integrate these two methods under a unified framework.

Here, we present a framework for tensor network assisted variational quantum algorithms. Our proposal involves tensor network-parametrized quantum circuits (TN-PQC), which consist of a standard PQC with an appended TN unitary operator. By augmenting the PQC with the TN unitary, which mainly performs classical rotations of the Hamiltonian, the TN-PQC can significantly enhance circuit depth and thereby improve expressiveness without requiring the physical implementation of deeper circuits. We then proceed to examine three key questions pertaining to our framework: (i) how to design the TN-PQC structure; (ii) optimization strategies for TN-PQC; and (iii) the comparative benefits of this hybrid architecture. To address (i), we present two examples of unitary matrix product operator (uMPO) and unitary tree tensor network (uTTN) and demonstrate their efficacy. We address (ii) with various optimization strategies and tackle (iii) through numerical experiments. We implement our method to numerically estimate the ground energy of the 2D Ising model with 16 qubits and the 1D time crystal Hamiltonian with 11 to 16 qubits. We compare the performance of TN-PQC (uMPO), TN-PQC (uTTN), and VQE algorithms. Our numerical results highlight the significant advantages of TN-PQC methods over conventional methods, with TN-PQC (uMPO) exhibiting the best performance, suggesting the benefits of uMPO integration.

2 Framework of TN-PQC

The problem of finding the ground state and ground energy of the Hamiltonian H can be expressed as the minimization problem:

$$\arg\min_{\psi} \langle\psi| H |\psi\rangle , \tag{1}$$

*jxhuang@stu.pku.edu.cn
†bujiaowu@gmail.com
‡xiaoyuan@pku.edu.cn

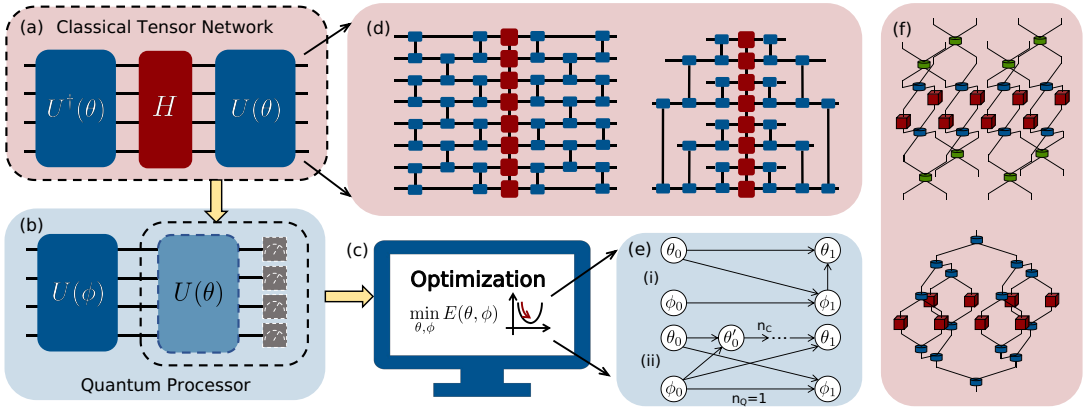


Figure 1: The TN-PQC framework: (a) A classical tensor network can represent part of the parameterized circuits and the Hamiltonian $U^\dagger(\theta)HU(\theta)$. (b) The quantum processor measures the remaining parameterized circuits using an effective Hamiltonian represented by a TN. (c) The gradient descent method is employed to find classical and quantum parameters corresponding to the lowest measurement results. (d) Contraction strategies for 1D uMPO and uTTN when combined with the Hamiltonian in a TN form. (e) Two optimization strategies for different parameters. i) The iteration of the quantum parameter $\boldsymbol{\phi}_1$ is obtained by computing the gradient from the previous classical and quantum parameters $\boldsymbol{\theta}_0$ and $\boldsymbol{\phi}_0$, while the parameter $\boldsymbol{\theta}_1$ is obtained from $\boldsymbol{\theta}_0$ and $\boldsymbol{\phi}_1$. ii) The parameter updating process is similar, but with the introduction of $n_C > 1$ intermediate steps between the initial and final classical parameters θ_0 and $\boldsymbol{\theta}_1$ to update classical parameters. (f) 2D uMPO and uTTN combined with the Hamiltonian in a 2D TN form.

where different parametrizations of ψ result in different methods. One example is to set $|\psi\rangle = U(\boldsymbol{\phi})|\mathbf{0}\rangle$, where $U(\boldsymbol{\phi})$ is a parameterized quantum circuit (PQC) with tunable parameters $\boldsymbol{\phi}$. This method is known as traditional VQE. In the framework of this article, we set $|\psi\rangle = U(\boldsymbol{\theta})U(\boldsymbol{\phi})|\mathbf{0}\rangle$, which transforms the minimization problem into:

$$\min_{\boldsymbol{\theta},\boldsymbol{\phi}} \langle \mathbf{0}| U^\dagger(\boldsymbol{\phi})U^\dagger(\boldsymbol{\theta})HU(\boldsymbol{\theta})U(\boldsymbol{\phi})|\mathbf{0}\rangle, \tag{2}$$

where $U(\boldsymbol{\phi})$ represents a quantum circuit with parameters $\boldsymbol{\phi}$, and $U(\boldsymbol{\theta})$ represents a unitary tensor network with parameters $\boldsymbol{\theta}$. By optimizing both classical and quantum parameters, the limited circuit depth of $U(\boldsymbol{\phi})$ can be compensated by the higher expressive power of $U(\boldsymbol{\theta})$. We aim to disentangle Hamiltonian H using the similarity transformation $U(\boldsymbol{\theta})$ and make the VQE circuit more efficient.

When both $U(\boldsymbol{\theta})$ and H are expressed in TNs, the parameterized Hamiltonian $H(\boldsymbol{\theta}) := U^\dagger(\boldsymbol{\theta})HU(\boldsymbol{\theta})$ in Eq.(2) can be considered as a TN with some legs contracted. The entire parameterized TN $H(\boldsymbol{\theta})$ is referred to as the TN part in the following sections, while $U(\boldsymbol{\phi})|\psi_0\rangle$ in Eq.(2) is referred to as the VQE part. When parameter $\boldsymbol{\theta}$ is fixed, Eq. (2) reduces to a traditional VQE method, whereas when $\boldsymbol{\phi}$ is fixed, it becomes a classical parameter optimization method. The entire process described above is illustrated in Fig. 1(a-c).

One issue to consider is how to choose the PQC $U(\boldsymbol{\phi})$ and the TN $U(\boldsymbol{\theta})$. In principle, the structure of PQC $U(\boldsymbol{\phi})$ can be arbitrary, and in this paper, we utilize some existing VQE ansatzes [11]. However, designing the TN requires more expertise to avoid the explosion of the Pauli decomposition of the TN part $H(\boldsymbol{\theta})$, since VQE requires measuring the Pauli basis. With the Pauli expansion form of the TN part, the resulting energy can be expressed as a linear combination of expectation values:

$$E(\boldsymbol{\theta},\boldsymbol{\phi}) = \sum_P c_P(\boldsymbol{\theta})\langle P\rangle_{\boldsymbol{\phi}}, \tag{3}$$

where $c_P(\boldsymbol{\theta}) = \mathrm{Tr}[PU^\dagger(\boldsymbol{\theta})HU(\boldsymbol{\theta})]$ is the Pauli decomposition coefficient of the classical part, and the summation iterates over all operators P with non-zero coefficients. The notation $\langle P\rangle_{\boldsymbol{\phi}}$ denotes the measurement results of operator P on the PQC, with the subscript indicating the parameter in PQC.

We propose three conditions for selecting an appropriate TN $U(\boldsymbol{\theta})$ in the classical part:

(i) $U^\dagger(\boldsymbol{\theta})HU(\boldsymbol{\theta})$ must share the same ground state and energy as H.

(ii) Either the number of Pauli decomposition terms remains small, which is polynomial in terms of qubit number, or the Pauli operators can be effectively sampled.

(iii) The coefficients $c_P(\boldsymbol{\theta})$ must be able to be computed efficiently.

Following these general principles, we could construct several kinds of $U(\boldsymbol{\theta})$ efficiently as shown in Figure 1(d).

3 Numerical Results

We test the efficacy of TN-PQC for determining the ground states of 2D spin-lattice systems with nearest-neighbor interactions, specifically the Ising model. We choose the Hamiltonian as $H = -J\sum_{\langle ij\rangle} Z_iZ_j - g\sum_j X_j$,

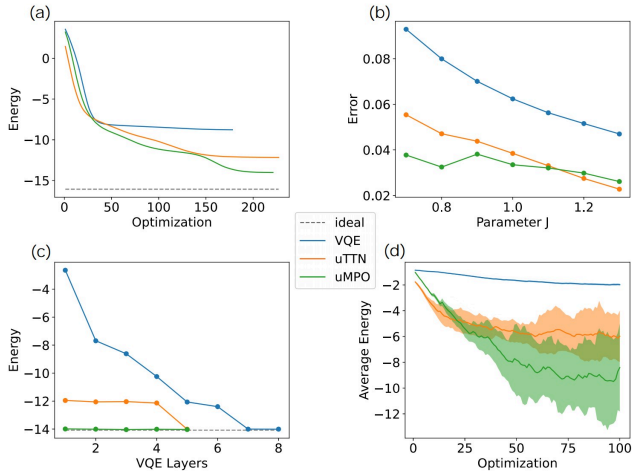


Figure 2: The numerical results demonstrate the superior accuracy and scalability of TN-PQC. (a) Performance comparison of pure VQE, uTTN-assisted VQE, and uMPO-assisted VQE on a (4×4)-qubit 2D transverse field Ising model. (b) Lowest energy error achieved by pure VQE, uTTN-assisted VQE, and uMPO-assisted VQE as the time crystal model parameter J varies. (c) Estimated ground state energy of a 16-qubit time crystal model using different algorithms with an increasing number of layers of PQC. (d) Estimated energy after 1-100 optimization steps for the iterative experiment of pure VQE, uTTN-assisted VQE, and uMPO-assisted VQE on a noisy 16-qubit time crystal model.

which is the well-known transverse field Ising model, where Z_i and X_j are local Pauli operators, $\langle ij \rangle$ denotes the summation over nearest neighbors and g represents the interaction strength between the system and the external magnetic field. The parameter set we use is $\{J = 0.1, g = 1\}$, and numerical experiments are performed on a 4×4 qubit 2D Ising model. We experimentally compare the performance of the VQE-only circuit, TN-PQC with TN being a uTTN, and TN-PQC with TN being a uMPO (2 layers), respectively, in determining the ground state of these models, as shown in Fig. 2(a). All of these algorithms have the same parameterized quantum circuit, consisting of a layer of parameterized rotations in Pauli Y-basis gates and n similar layers of CZ gates for entanglement, as before.

We optimize these circuits using the gradient descent algorithm and find that TN-PQC has a much better convergence estimation value of the ground energy, and TN-PQC with TN being a uMPO performs better than a uTTN. This suggests that MPOs may be more appropriate for the Hamiltonians with the spin-lattice model.

We compare the performance of VQE, TN-PQC with an uTTN, and TN-PQC with an MPO on various parameter models of the time-crystal Hamiltonian, which is given by $H = -\sum_k [J_k Z_{k-1} X_k Z_{k+1} + V_k X_k X_{k+1} + h_k X_k]$. In particular, we vary the parameter J from 0.7 to 1.3 with fixed $V = 0.1$ and $h = 0.1$, as shown in Fig. 2(b). To handle this more complex Hamiltonian, we use a deeper circuit consisting of 2 layers of parameterized rotation in Pauli Y-basis gates and Pauli X-basis gates, and n layers of CNOT gates ($\text{CNOT}_{i,i+1}$ for $1 \leq i \leq n-1$) to induce more entanglement. The figure demonstrates that TN-PQC maintains a distinct advantage as J varies.

To better understand the capabilities of different approaches in improving accuracy, we investigate the achievable energy accuracy by increasing the number of layers in a parameterized quantum circuit with repeating structures. We employ the 1D 16-qubit time crystal Hamiltonian to compare the ability of different methods in reducing the number of layers in parameterized quantum circuits. We set the parameter values to $\{J = 1, V = 0.1, g = 0.1\}$ and use a layer of rotation in Y-basis gates, followed by n layers of CNOT gates ($\text{CNOT}_{i,i+1}$ for $1 \leq i \leq n-1$) in our parametric quantum circuit. Fig. 2(c) shows the estimated ground energy for different algorithms as the number of layers increases. Our results demonstrate that a pure VQE circuit with 7 repetitions of the original structure performs as well as the uTTN-assisted VQE circuit with 5 repetitions and the MPO-assisted original VQE circuit, with all three approaches approaching the theoretical value of the time crystal Hamiltonian ground state energy within an error of 1×10^{-2}.

We also assess the robustness of TN-PQC to noise by introducing depolarization noise to the single-qubit and two-qubit gates. Multiple fixed 100-step iterative experiments are conducted on the same initial quantum state to obtain the estimation and error bar. The error is estimated using the formula $\varepsilon = 3\sqrt{\sum_{i=1}^{S} (v_i - \bar{v})^2 / S^2}$, where v_i denotes the ith estimate, $\bar{v}$ denotes the mean, and S denotes the total number of experiment times.

In practice, the depolarization noise probability for the single-qubit and two-qubit gates (specifically, the rotation Y and CNOT gate) is set at 2×10^{-5} and 5×10^{-5}, respectively. The same set of parameters is chosen, and the experiment is repeated for $S = 40$ times. The mean values and error bars are calculated for each step. Fig. 2(d) shows the estimation results with increasing optimization steps. We observe that while the TN assistance amplifies the noise fluctuation, TN-PQC still outperforms pure VQE even when considering the effect of the estimation error bar.

4 Why AQIS?

We propose a hybrid framework that can take full advantage of the respective strengths of tensor networks and quantum circuits, and present numerical simulations which show that the TN-PQC consistently and significantly outperforms the VQE algorithm with shallow depth of quantum circuits. We also numerically show that the expressivity is greatly enhanced with the assistance of tensor networks for the original shallow-depth VQE algorithm. We believe our work would inspire the AQIS audience to explore the possibility of more hybrid frameworks.

References

[1] Steven R White. Density matrix formulation for quantum renormalization groups. *Physical review letters*, 69(19):2863, 1992.

[2] Steven R White. Density-matrix algorithms for quantum renormalization groups. *Physical review b*, 48(14):10345, 1993.

[3] Stefan Rommer and Stellan Östlund. Class of ansatz wave functions for one-dimensional spin systems and their relation to the density matrix renormalization group. *Physical review b*, 55(4):2164, 1997.

[4] Yudong Cao, Jonathan Romero, Jonathan P Olson, Matthias Degroote, Peter D Johnson, Mária Kieferová, Ian D Kivlichan, Tim Menke, Borja Peropadre, Nicolas PD Sawaya, et al. Quantum chemistry in the age of quantum computing. *Chemical reviews*, 119(19):10856–10915, 2019.

[5] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C Benjamin, and Xiao Yuan. Quantum computational chemistry. *Reviews of Modern Physics*, 92(1):015003, 2020.

[6] William Huggins, Piyush Patil, Bradley Mitchell, K Birgitta Whaley, and E Miles Stoudenmire. Towards quantum machine learning with tensor networks. *Quantum Science and technology*, 4(2):024001, 2019.

[7] Michael Foss-Feig, David Hayes, Joan M Dreiling, Caroline Figgatt, John P Gaebler, Steven A Moses, Juan M Pino, and Andrew C Potter. Holographic quantum algorithms for simulating correlated spin systems. *Physical Review Research*, 3(3):033002, 2021.

[8] Bela Bauer, Sergey Bravyi, Mario Motta, and Garnet Kin-Lic Chan. Quantum algorithms for quantum chemistry and quantum materials science. *Chemical Reviews*, 120(22):12685–12717, 2020.

[9] Michael Lubasch, Jaewoo Joo, Pierre Moinier, Martin Kiffner, and Dieter Jaksch. Variational quantum algorithms for nonlinear problems. *Physical Review A*, 101(1):010301, 2020.

[10] Fergus Barratt, James Dborin, Matthias Bal, Vid Stojevic, Frank Pollmann, and Andrew G Green. Parallel quantum simulation of large systems on small nisq computers. *npj Quantum Information*, 7(1):1–7, 2021.

[11] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021.

Characterising and Controlling Complex Quantum Processes with Classical Memory

Philip Taranto[1] * Marco Túlio Quintino[2] Mio Murao[1] Simon Milz[3]

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo, Tokyo 113-0033, Japan*
[2] *Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*
[3] *School of Physics, Trinity College Dublin, Dublin 2, Ireland*

Abstract. Memory is the fundamental form of temporal complexity: when present but uncontrollable, it manifests as non-Markovian noise; conversely, if memory can be controlled, it can provide a powerful resource for information processing. Memory effects arise via interactions between a system and its environment; as such, they can be either classical or quantum. From a practical standpoint, quantum processes with classical memory promise near-term applicability: they are more powerful than their memoryless counterpart, yet at the same time can be sufficiently controlled without being spoiled by decoherence. However, despite practical and foundational value, apart from simple two-time scenarios, the distinction between quantum and classical memory remains unexplored. We first analyse various physically-motivated candidates regarding a suitable definition for classical memory that lead to remarkably distinct phenomena in the multi-time setting. Subsequently, we develop witnesses to determine the exclusion of a process from each set, thereby systematically characterising the hierarchy multi-time memory effects.

Keywords: Quantum Information Theory; Quantum and Classical Memory; Multi-Time Quantum Phenomena.

1 Introduction

Memory is the fundamental form of temporal complexity, appearing ubiquitously across natural and engineered processes [1]. Most prominently, memory can be controlled to reliably prepare states [2, 3], simulate non-Markovian phenomena [4–6], enhance information processing [7, 8], and control circuit architectures [9–12]. Such primitives are routinely used in classical computers to improve performance and will be necessary for robust quantum devices [13]. Only recently has a consistent understanding of memory in quantum processes been developed via the "process tensor" formalism [14, 15]. The process tensor has been shown to correctly generalise classical stochastic processes to the quantum realm [16–18] and encode key memory properties—length [19], structure [20] and strength [21]—providing a framework for analysing complex multi-time quantum dynamics [22, 23]. Such results have been tested experimentally [12, 24], evidencing their immediate applicability.

Nonetheless, from a practical standpoint, control over *quantum* memory might be out of reach (beyond laboratory settings) since it requires delicate experimental setups. Manipulating quantum processes with *classical* memory seems more manageable (yet still powerful) [25, 26]; however, the resourcefulness of classical memory remains largely unexplored. Here we ask: *What is truly quantum about quantum memory, and what can be achieved with processes controlled by only classical memory?* Our interrogation is operational and inspired by the spatial setting, where genuinely quantum correlations have been identified as a fundamental resource [27, 28]. At the same time, there exist tasks that can be performed optimally using only classical correlations, providing a simpler strategy in practice. Here, we develop a systematic understanding of quantum processes with both quantum and classical memory, focusing on the ability of the latter to demonstrate advantages in information processing tasks.

*philipguy.taranto@phys.s.u-tokyo.ac.jp

2 Results

We consider a system S that is sequentially interrogated N times; in between the probings, the system interacts with its environment E, together evolving unitarily (see Fig. 1). An object that permits the computation of all possible multi-time correlations—the "process tensor"—can be built up (in the Choi representation[1]) from these parts via the *link product* $\star$ [10]. An N-time quantum process can then be defined via:

Definition 1 (Multi-time quantum process)**.** An N-time quantum process is represented by $\mathsf{C}_{N:1} \geq 0$ that can be written as

$$\mathsf{C}_{N:1} = \mathbb{1}_{E_{N^{\mathrm{i}}}} \bigstar_{j=1}^{N-1} \mathsf{U}_{(ES)_{j+1^{\mathrm{i}}j^{\circ}}} \star \mathrm{I}_{E_j} \star \rho_{(ES)_{1^{\mathrm{i}}}}, \quad (1)$$

with $\rho_{(ES)_{1^{\mathrm{i}}}}$ a state, each $\mathsf{U}_{(ES)_{j+1^{\mathrm{i}}j^{\circ}}}$ a unitary channel, each I_{E_j} an identity map, and $\mathbb{1}_{E_{N^{\mathrm{i}}}}$ representing the partial trace. We denote the set of such processes by $\mathtt{QM}$.

The Choi state of an N-time process is a many-body state $\mathsf{C}_{N:1} \in \mathcal{L}(\mathcal{H}_{S_{N^{\mathrm{i}}}} \bigotimes_{j=1}^{N-1} \mathcal{H}_{S_{j^{\circ}}} \otimes \mathcal{H}_{S_{j^{\mathrm{i}}}})$ which satisfies causality constraints that encode the impossibility of sending information from the future to the past [10]. We will later use the violation of similar no-signalling conditions to establish the distinction between certain types of memory.

In this representation, correlations of the Choi state encode temporal correlations of the process. Recent work has demonstrated various features that arise from the interplay between memory effects and sequential measurements in quantum theory [17–21, 31–33]. Here, we examine meaningful ways to characterise multi-time quantum processes with different types of memory, particularly focusing on the case where the memory is restricted to being classical. Starting from a system-environment dynamics, there are various ways to impose classicality on the memory, each justified within their own right but which lead to distinct consequences that can be determined by probing the system alone.

[1] Just as channels can be represented as bipartite states via the *Choi-Jamiołkowski isomorphism* [29, 30], multi-time quantum processes can be represented as multi-partite states [15], as we use throughout.

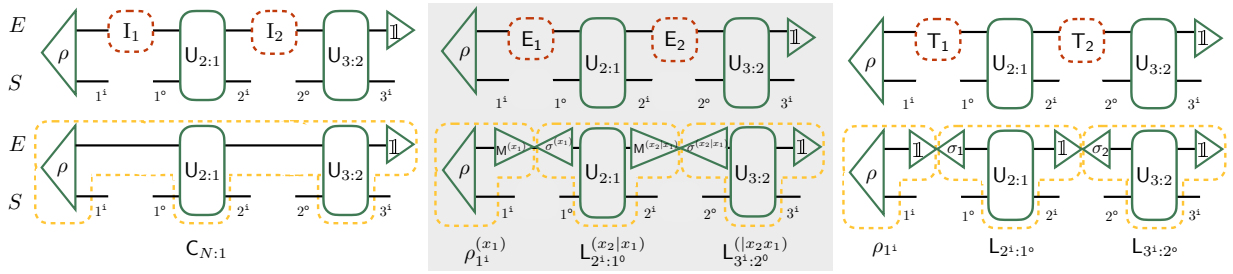


Figure 1: *Types of Memory.* Quantum processes can have quantum memory (left; Def. 1), classical memory (middle; Def. 3), or no memory (right; Def. 2). In the upper panels, we show the system-environment dilation. In the lower panels, we invoke the structure of the relevant environment channels to deduce the process tensor form (yellow dashed outlines). The general case cannot be broken up; the classical memory case leads to a sequence of conditional instruments [Eq. (5)], which is more general than convex mixtures of memoryless processes (Def. 4) and a special case of separable processes (Def. 5); the memoryless case leads to a sequence of independent CPTP channels [Eq. (3)].

2.1 Types of Memory

We aim to delineate different types of memory, i.e., temporal correlations. On the foundational side, similar hierarchies have been developed in the spatial setting [27, 28]; hence, there is interest in extending such notions to the temporal realm. From a practical perspective, different experimental setups can generate distinct memory effects, and so it is crucial to distinguish between them and figure out their resourcefulness. To achieve such goals, meaningful definitions, witnesses, and physical interpretations are necessary.

The memory effects that can be exhibited are contingent upon what type of information the process can transmit in time. This, in turn, depends upon what happens to the *environment*—the carrier of information about previous system states—in between portions of global evolution. In general, the environment evolves coherently, propagating quantum information forward in time. Mathematically, this is modelled by evolving the environment *trivially* between times [I_{E_j} in Eq. (1)]. By imposing different environment dynamics, one can actively restrict the type of memory exhibited (see Fig. 1).

Memoryless Quantum Processes.—For instance, the environment could be erased and prepared anew in between times, thereby not transmitting *any* historic information. Such behaviour occurs whenever the environment completely rethermalises between interrogations and is a key assumption leading to GKSL / Markovian master equations [34, 35]. Mathematically, this physical situation corresponds to a *trace-and-replace* map being applied to the environment between times. Such maps are represented by uncorrelated Choi states, i.e., $\mathsf{T}_{\circ\mathtt{i}} = \sigma_\circ \otimes \mathbb{1}_\mathtt{i}$, where $\sigma_\circ$ is an arbitrary quantum state (which, in the picture described above, could be the thermal state of the environment). This leads to:

Definition 2. An N-time *memoryless quantum process* is represented by $\mathsf{C}^{\mathsf{M}}_{N:1} \geq 0$ that can be written as

$$\mathsf{C}^{\mathsf{M}}_{N:1} = \mathbb{1}_{E_{N^\mathtt{i}}} \bigstar_{j=1}^{N-1} \mathsf{U}_{(ES)_{j+1^\mathtt{i} j^\circ}} \star \mathsf{T}_{E_j} \star \rho_{(ES)_{1^\mathtt{i}}}, \qquad (2)$$

with each T_{E_j} a trace-and-replace channel and the other objects as before. We denote the set of such processes by $\mathtt{M}$.

By invoking the form of each trace-and-replace channel $\mathsf{T}_{E_j} := \sigma_{E_{j^\circ}} \otimes \mathbb{1}_{E_{j^\mathtt{i}}}$, noting that $\mathsf{L}_{j+1^\mathtt{i}:j^\circ} := \mathbb{1}_{E_{j+1^\mathtt{i}}} \star \mathsf{U}_{(ES)_{j+1^\mathtt{i} j^\circ}} \star \sigma_{E_{j^\circ}}$ induces a channel on the system, and defining $\rho_{1^\mathtt{i}} := \rho_{(ES)_{1^\mathtt{i}}} \star \mathbb{1}_{E_{1^\mathtt{i}}}$ (see Fig. 1), we have the equivalent form of a memoryless quantum process as a sequence of *independent* quantum channels [14, 36]:

$$\mathsf{C}^{\mathsf{M}}_{N:1} = \mathsf{L}_{N^\mathtt{i}:N-1^\circ} \otimes \ldots \otimes \mathsf{L}_{2^\mathtt{i}:1^\circ} \otimes \rho_{1^\mathtt{i}}. \qquad (3)$$

Here, each $\mathsf{L}_{j+1^\mathtt{i}:j^\circ}$ represents a *completely positive and trace preserving* **(CPTP)** channel evolving the system from t_j to t_{j+1}; in the Choi representation, these properties are respectively reflected by $\mathsf{L}_{j+1^\mathtt{i}:j^\circ} \geq 0$ and $\mathrm{tr}_{j+1^\mathtt{i}}\left[\mathsf{L}_{j+1^\mathtt{i}:j^\circ}\right] = \widetilde{\mathbb{1}}_{d_{j^\circ}}$. Memorylessness of the process is clear from this uncorrelated structure, as all of the CPTP maps are mutually independent.

Classical Memory Quantum Processes.—In more general scenarios, e.g., when the environment does not fully rethermalise between times, some memory can be transported. Depending on the particularities of the environment and its interactions with the system, said memory can be either classical or quantum. Here, we model classical memory effects by interpolating between the memoryless case (where the environment rethermalises between times) and the quantum memory case (where the environment coherently propagates) by interspersing the global dynamics with channels that transmit only classical information through the environment. This scenario can be modelled by subjecting the environment to an *entanglement-breaking channel* **(EBC)** between times. In each run, any EBC can simply measure the system and feed forward classical information pertaining to the outcome. Mathematically, EBCs are described by measure-and-prepare channels, i.e., $\mathsf{E}_{\circ\mathtt{i}} = \sum_x \sigma^{(x)}_\circ \otimes \mathsf{M}^{(x)}_\mathtt{i}$ where each $\sigma^{(x)}_\circ$ is an arbitrary state and $\{\mathsf{M}^{(x)}_\mathtt{i}\}$ forms a POVM [27]. This leads to:

Definition 3. An N-time *classical memory quantum process* is represented by $\mathsf{C}^{\mathrm{CM}}_{N:1} \geq 0$ that can be written as

$$\mathsf{C}^{\mathrm{CM}}_{N:1} = \mathbb{1}_{E_{N^\mathtt{i}}} \bigstar_{j=1}^{N-1} \mathsf{U}_{(ES)_{j+1^\mathtt{i} j^\circ}} \star \mathsf{E}_{E_j} \star \rho_{(ES)_{1^\mathtt{i}}}, \qquad (4)$$

with each E_{E_j} an EBC and the other objects as before. We denote the set of such processes by $\mathtt{CM}$.

By invoking the structure of EBCs, we yield the form [25]:

$$\mathsf{C}^{\mathrm{CM}}_{N:1} = \sum p_{x_{N:1}} \mathsf{L}^{(x_N|x_{N-1:1})}_{N^\mathtt{i}:N-1^\circ} \otimes \ldots \otimes \mathsf{L}^{(x_2|x_1)}_{2^\mathtt{i}:1^\circ} \otimes \rho^{(x_1)}_{1^\mathtt{i}}, \qquad (5)$$

where $x_{k:j} := \{x_j, \ldots, x_j\}$, $p(x_{N:1})$ is a probability distribution, $\{\rho^{(x_1)}_{1^\mathtt{i}}\}$ forms a state ensemble, i.e., each $\rho^{(x_1)}_{1^\mathtt{i}} \geq 0$ and $\rho_{1^\mathtt{i}} := \sum_{x_1} \rho^{(x_1)}_{1^\mathtt{i}}$ has unit trace, and $\mathsf{L}^{(x_{j+1}|x_{j:1})}_{j+1^\mathtt{i}:j^\circ} := \mathsf{M}^{(x_{j+1})}_{E_{j+1^\mathtt{i}}} \star \mathsf{U}_{(ES)_{j+1^\mathtt{i} j^\circ}} \star \sigma^{(x_{j:1})}_{E_{j^\circ}}$ forms an instrument for each conditioning argument, reflecting the fact that every outcome observed can condition the choice of future EBCs.

Classical Direct Cause Quantum Processes.—The above definition notwithstanding, other sets of processes could meaningfully be considered to have classical memory. The simplest such is that in which a coin toss determines which of a different memoryless process ensues. This leads to:

Definition 4. An N-time *classical direct cause quantum process* is represented by $\mathsf{C}^{\mathrm{CDC}}_{N:1} \geq 0$ that can be written as

$$\mathsf{C}^{\mathrm{CDC}}_{N:1} = \sum p_x \mathsf{L}^{(x)}_{N^{\mathrm{i}}:N-1^{\mathrm{o}}} \otimes \ldots \otimes \mathsf{L}^{(x)}_{2^{\mathrm{i}}:1^{\mathrm{o}}} \otimes \rho^{(x)}_{1^{\mathrm{i}}}, \quad (6)$$

where p_x is a probability distribution and each $\mathsf{L}^{(x)}_{j+1^{\mathrm{i}}:j^{\mathrm{o}}}$ is a CPTP channel. We denote the set of such processes by CDC.

The classical analogues of Defs. 3 and 4 are equivalent (due to the fact that measurements are non-invasive), so it may be surprising that they differ in the quantum realm.

Separable Quantum Processes.—Classical memory quantum processes have been explored in Ref. [25]. Since characterising the set CM is difficult, the authors relaxed the condition that each conditional dynamics must be trace preserving, leading (not obviously) to a superset of CM [26]. Precisely, they drop the demand that each $\mathsf{L}^{(x_{j-1:1})}_{j^{\mathrm{i}}:j-1^{\mathrm{o}}} := \sum_{x_j} \mathsf{L}^{(x_j|x_{j-1:1})}_{j^{\mathrm{i}}:j-1^{\mathrm{o}}}$ is TP [see Eq. (5)], only retaining positivity of each element and overall causality. This leads to:

Definition 5. An N-time *separable quantum process* is represented by $\mathsf{C}^{\mathrm{SEP}}_{N:1} \geq 0$ that can be written as

$$\mathsf{C}^{\mathrm{SEP}}_{N:1} = \sum p_x \mathsf{L}^{(x)}_{N^{\mathrm{i}}:N-1^{\mathrm{o}}} \otimes \ldots \otimes \mathsf{L}^{(x)}_{2^{\mathrm{i}}:1^{\mathrm{o}}} \otimes \rho^{(x)}_{1^{\mathrm{i}}}, \quad (7)$$

where p_x is a probability distribution, each $\rho^{(x)}_{1^{\mathrm{i}}} \geq 0$ and $\mathsf{L}^{(x)}_{j+1^{\mathrm{i}}:j^{\mathrm{o}}} \geq 0$. We denote the set of such processes by SEP.

Note the lack of constraints on the elements in this decomposition compared to Defs. 3 and 4, where they must represent conditional instruments or CPTP channels, respectively.

A priori, it is unclear if these sets of processes (Defs. 3–5)—each representing a distinct physical situation—coincide on the level of what is observable on the system; we now move to demonstrate a clear distinction between them.

2.2 Strict Hierarchy for Multi-Time Processes

By imposing certain dynamics on the environment one can "kill off" certain types of memory—be it erasing the history (Def. 2) or destroying coherent information (Def. 3)—to yield distinct memory classes (note, though, that the physical picture corresponding to SEP is unclear). However, from a practical perspective, one cannot access the environment; thus, we develop methods to distinguish these sets by probing the system alone, demonstrating the strict hierarchy (see Fig. 2):

$$\mathtt{M} \subsetneq \mathtt{CDC} \subsetneq \mathtt{CM} \subsetneq \mathtt{SEP} \subsetneq \mathtt{QM}. \quad (8)$$

It is straightforward to note that $\mathtt{M} \subsetneq \mathtt{CDC}$ due to the non-convexity of the set of memoryless processes. Similarly, $\mathtt{SEP} \subsetneq \mathtt{QM}$ holds since not all quantum processes are separable in time [25, 37]. However, the relationship between the

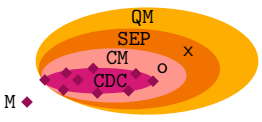


Figure 2: *Memory Hierarchy.* We present a process in CM but outside CDC (o). For two-time processes, CM and CDC coincide, making our demonstration one of a genuinely multi-time phenomenon. Furthermore, a process that is in SEP but outside CM (×) was demonstrated in Ref. [26]. We develop witnesses to systematically detect such processes (which bypass previous entanglement-based criteria [25]).

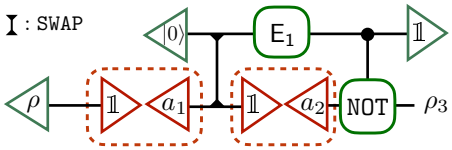


Figure 3: *A* CM *process with no* CDC *realisation.* The process (green) above can signal from t_1 to t_3, which can be tested by tracing out the system at times t_1 and t_2, fixing a state a_2, and feeding in an arbitrary state a_1 (red). For instance, $\rho_3(a_1 = |0\rangle) = a_2$ whilst $\rho_3(a_1 = |1\rangle) = \mathtt{NOT}(a_2)$. Such signalling is incompatible with a CDC realisation, although the process is in CM by construction.

middle three sets—each of which positing a meaningful notion of "classical memory quantum processes"—is more intricate. Interestingly, for processes defined on only two times, CDC and CM coincide [26]. However, in extending to more than two times, we construct a process that is in CM but outside CDC (see Fig. 3). The intuitive reason for this strict inclusion lies in the fact that any CDC process cannot signal between times (except between neighbours), since the choice of 'what process' is made at the very beginning; on the other hand, processes in CM can signal arbitrarily far into the future by feeding forward classical information. The witnesses we develop are based upon violations of such signalling conditions. Lastly, note that such a distinction does not exist in the classical realm, where the analogues of CDC and CM coincide. This result thereby constitutes a genuinely multi-time quantum effect.

Finally, $\mathtt{CM} \subsetneq \mathtt{SEP}$ was conjectured in Ref. [25] and proven in Ref. [26] (see Fig. 2). This distinction is akin to the existence of maps that preserve separable states but cannot be implemented by LOCC [27]; although the former are easier to characterise, the latter are more operationally meaningful. Similarly here regarding multi-time processes: SEP is straightforward to characterise and exclusion from it can be determined via entanglement witnesses [25]. However, given a process in SEP, there does not generally exist a realisation using only classical memory. Here, we provide systematic criteria to witness such processes—a distinction that cannot be made by previous criteria based on entanglement detection. The intuition behind our criteria comes from the fact that, although a dynamics may lead to a separable process tensor once the environment is traced out, some such dynamics nonetheless *require* temporal entanglement, i.e., quantum memory; this requirement can be witnessed on the level of the system alone.

3 Concluding Discussion & Outlook

Our results are of central importance in two ways. From a foundational standpoint, they distinguish quantum and classical memory, outlining the ultimate limitations of quantum information processing and providing a holistic characterisation of the hierarchy of possible memory structures in quantum theory. On the practical side, since noise in quantum devices—and thus the observed memory effects—will predominately be classical in the near future, our results provide a methodological framework upon which efficient and reliable quantum devices can be built. Accordingly, the concepts explored and results presented here should have immediate impact on various fields of quantum science, including quantum information theory, optimal control, open quantum systems, and quantum foundations, to name but a few.

References

[1] N. van Kampen. *Stochastic Processes in Physics and Chemistry*. Elsevier, New York, 2011.

[2] C. Sayrin, I. Dotsenko, X. Zhou, B. Peaudecerf, T. Rybarczyk, S. Gleyzes, P. Rouchon, M. Mirrahimi, H. Amini, M. Brune, J.-M. Raimond, and S. Haroche. Real-time quantum feedback prepares and stabilizes photon number states. *Nature* **477**:73–77, 2011.

[3] L. Magrini, P. Rosenzweig, C. Bach, A. Deutschmann-Olek, S. G. Hofer, S. Hong, N. Kiesel, A. Kugi, and M. Aspelmeyer. Real-time optimal quantum control of mechanical motion at room temperature. *Nature* **595**:373-377, 2021.

[4] A. L. Grimsmo. Time-Delayed Quantum Feedback Control. *Phys. Rev. Lett.* **115**:060402, 2015.

[5] A. Luchnikov, S. V. Vintskevich, H. Ouerdane, and S. N. Filippov. Simulation Complexity of Open Quantum Dynamics: Connection with Tensor Networks. *Phys. Rev. Lett.* **122**:160401, 2019.

[6] M. R. Jørgensen and F. A. Pollock. Exploiting the Causal Tensor Network Structure of Quantum Processes to Efficiently Simulate Non-Markovian Path Integrals. *Phys. Rev. Lett.* **123**:240602, 2019.

[7] K. Banaszek, A. Dragan, W. Wasilewski, and C. Radzewicz. Experimental Demonstration of Entanglement-Enhanced Classical Communication over a Quantum Channel with Correlated Noise. *Phys. Rev. Lett.* **92**:257901, 2004.

[8] J. Bavaresco, M. Murao, and M. T. Quintino. Strict Hierarchy between Parallel, Sequential, and Indefinite-Causal-Order Strategies for Channel Discrimination. *Phys. Rev. Lett.* **127**:200504, 2021.

[9] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Quantum Circuit Architecture. *Phys. Rev. Lett.* **101**:060401, 2008.

[10] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Theoretical framework for quantum networks. *Phys. Rev. A* **80**:022339, 2009.

[11] S. Mavadia, C. L. Edmunds, C. Hempel, H. Ball, F. Roy, T. M. Stace, and M. J. Biercuk. Experimental quantum verification in the presence of temporally correlated noise. *npj Quantum Inf.* **4**:7, 2018.

[12] G. A. L. White, C. D. Hill, F. A. Pollock, L. C. L. Hollenberg, and K. Modi. Demonstration of non-Markovian process characterisation and control on a quantum processor. *Nat. Commun.* **11**:6301, 2020.

[13] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. F. Riedel, P. O. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F. K. Wilhelm. The quantum technologies roadmap: a European community view. *New J. Phys.* **20**:080201, 2018.

[14] F. A. Pollock, C. Rodríguez-Rosario, T. Frauenheim, M. Paternostro, and K. Modi. Operational Markov Condition for Quantum Processes. *Phys. Rev. Lett.* **120**:040405, 2018.

[15] F. A. Pollock, C. Rodríguez-Rosario, T. Frauenheim, M. Paternostro, and K. Modi. Non-Markovian quantum processes: Complete framework and efficient characterization. *Phys. Rev. A* **97**:012127, 2018.

[16] S. Milz, F. Sakuldee, F. A. Pollock, and K. Modi. Kolmogorov extension theorem for (quantum) causal modelling and general probabilistic theories. *Quantum* **4**:255, 2020.

[17] P. Strasberg and M. G. Díaz. Classical quantum stochastic processes. *Phys. Rev. A* **100**:022120, 2019.

[18] S. Milz, D. Egloff, P. Taranto, T. Theurer, M. B. Plenio, A. Smirne, and S. F. Huelga. When Is a Non-Markovian Quantum Process Classical? *Phys. Rev. X* **10**:041049, 2020.

[19] P. Taranto, F. A. Pollock, S. Milz, M. Tomamichel, and K. Modi. Quantum Markov Order. *Phys. Rev. Lett.* **122**:140401, 2019.

[20] P. Taranto, S. Milz, F. A. Pollock, and K. Modi. Structure of quantum stochastic processes with finite Markov order. *Phys. Rev. A* **99**:042108, 2019.

[21] P. Taranto, F. A. Pollock, and K. Modi. Non-Markovian memory strength bounds quantum process recoverability. *npj Quantum Inf.* **7**:149, 2021.

[22] G. A. L. White, F. A. Pollock, L. C. L. Hollenberg, C. D. Hill, and K. Modi. From many-body to many-time physics. arXiv:2107.13934, 2021.

[23] G. A. L. White, F. A. Pollock, L. C. L. Hollenberg, K. Modi, and C. D. Hill. Non-Markovian Quantum Process Tomography. *PRX Quantum* **3**:020344, 2022.

[24] Y. Guo, P. Taranto, B.-H. Liu, X.-M. Hu, Y.-F. Huang, C.-F. Li, and G.-C. Gu. Experimental Demonstration of Instrument-Specific Quantum Memory Effects and Non-Markovian Process Recovery for Common-Cause Processes. *Phys. Rev. Lett.* **126**:230401, 2021.

[25] C. Giarmatzi and F. Costa. Witnessing quantum memory in non-Markovian processes. *Quantum* **5**:440, 2021.

[26] M. Nery, M. T. Quintino, P. A. Guérin, T. O. Maciel, and R. O. Vianna. Simple and maximally robust processes with no classical common-cause or direct-cause explanation. *Quantum* **5**:538, 2021.

[27] M. Horodecki, P. W. Shor and M. B. Ruskai. Entanglement Breaking Channels. *Rev. Math. Phys.* **15**:629, 2003.

[28] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.* **86**:419, 2003.

[29] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.* **3**:275, 1972.

[30] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Its Appl.* **10**:285, 1975.

[31] A. A. Budini. Quantum Non-Markovian Processes Break Conditional Past-Future Independence. *Phys. Rev. Lett.* **121**:240401, 2018.

[32] A. A. Budini. Quantum Non-Markovian Processes Break Conditional Past-Future Independence. *Entropy* **24**:649, 2022.

[33] P. Taranto, T. J. Elliot, and S. Milz. Hidden Quantum Memory: Is Memory There When Somebody Looks? *Quantum* **7**:991, 2023.

[34] V. Gorini, A. Kossakowski, and E. C. G. Sudarshan. Completely positive semigroups of N-level systems. *J. Math. Phys.* **17**:821, 1976.

[35] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.* **48**:119, 1976.

[36] F. Costa and S. Shrapnel. Quantum causal modelling. *New J. Phys.* **18**:063032, 2016.

[37] S. Milz, C. Spee, Z.-P. Xu, F. A. Pollock, K. Modi, and O. Gühne. Genuine multipartite entanglement in time. *SciPost Phys.* **10**:141, 2021.

Improving D2p Grover's algorithm to reach performance upper bound under phase noise

Jian Leng[1] * Fan Yang[1] † Xiang-Bin Wang[1 2 3 4 5] ‡

[1] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*

[2] *Jinan Institute of Quantum technology, SAICT, Jinan 250101, China*

[3] *Shanghai 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*

[4] *Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China*

[5] *Frontier Science Center for Quantum Information, Beijing, China*

Abstract. The original Grover's algorithm has a success probability to output a correct solution, while deterministic Grover's algorithms improve the success probability to 100%. However, the success probability of deterministic Grover's algorithm decreases in noisy environment. Here we improve the deterministic two-parameter (D2p) Grover's algorithm to reach the upper bound for success probability under phase noise. We prove that it is not possible to design any deterministic Grover's algorithm whose success probability is higher than our improved D2p protocol's under phase noise.

Keywords: deterministic Grover's algorithm, upper success probability bound, phase noise

Grover's quantum search algorithm [1] provides a quadratic speedup against classical search algorithms and it outputs a correct result with success probability better than 50%. Grover's algorithm can be described as the iterations of two modules: the black box oracle which is untunable [2] and the reflection operator with a tunable phase β. The original Grover's algorithm simply chooses $\beta = \pi$. Very recently, a novel result named as deterministic two-parameter (D2p) Grover's algorithm [3] is presented. This D2p protocol can deterministically give a correct solution by choosing two well-designed phases β_1, β_2 for reflection operator. There is an important problem that noise is inevitable for practical quantum circuit. It is meaningful to find such a robust algorithm with success probability as high as possible. In particular, phase noise $\delta\beta$ is caused by implement's imperfection and, to our knowledge, designing a quantum error correction code for phase noise is still an open problem. The effect of phase noise [4] to the original Grover's algorithm has been investigated. However, the optimal result of Grover's algorithm is unknown. Here we improve the D2p algorithm to reach the upper bound for success probability under phase noise: Firstly, we present a new method to study noise effect in Grover's algorithm that studying geometrical properties of noise on Bloch sphere. Then we show our improved protocol for D2p Grover's algorithm. Finally, we prove that the success probability of our improved D2p protocol is the highest among all possible deterministic Grover's algorithms, which cannot be surpassed in principle. It is an important progress for Grover's algorithm working in practical environment, especially in the cases such as high cost of system initialization and quantum measurement.

*lengj20@mails.tsinghua.edu.cn

†yangf20@mails.tsinghua.edu.cn

‡xbwang@mail.tsinghua.edu.cn

Here we illustrate the comparisons between original Grover's algorithm, D2p algorithm and our improved D2p algorithm under phase noise. In Fig. 1 (a), we show our improved D2p algorithm by a brief 3D image. Define $\lambda = M/N$ where M and N are the amount of target states and total states respectively. In Fig. 1 (b) and (c), we apply the Gaussian distributed phase noise $\delta\beta = \mathcal{N}(\mu, \sigma^2)$ to the original Grover's algorithm, D2p protocol and our improved D2p algorithm, while the mean value μ is different for Fig. 1 (b) and (c). Fig. 2 shows that how variation parameter σ^2 affects the success probability with fixed λ when we apply the Gaussian distributed phase noise $\delta\beta = \mathcal{N}(\mu = 0.05, \sigma^2)$. In Fig. 3, we apply Poisson and uniform distributed noise instead of Gaussian distribution. Simulation results support that our algorithm has the best performance in phase noise environment.

References

[1] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th ACM STOC*, pages 212–219, 1996.

[2] M. A. Nielsen and I. Chuang. Quantum computation and quantum information. *American Association of Physics Teachers*, 2002.

[3] T. Roy, L. Jiang, and D. I. Schuster. Deterministic Grover search with a restricted oracle. *Physical Review Research*, 26(4):L022013, 2022.

[4] N. Shenvi, K. R. Brown, and K. B. Whaley. Effects of a random noisy oracle on search algorithm complexity. *Physical Review A*, 5(68):052313, 2003.

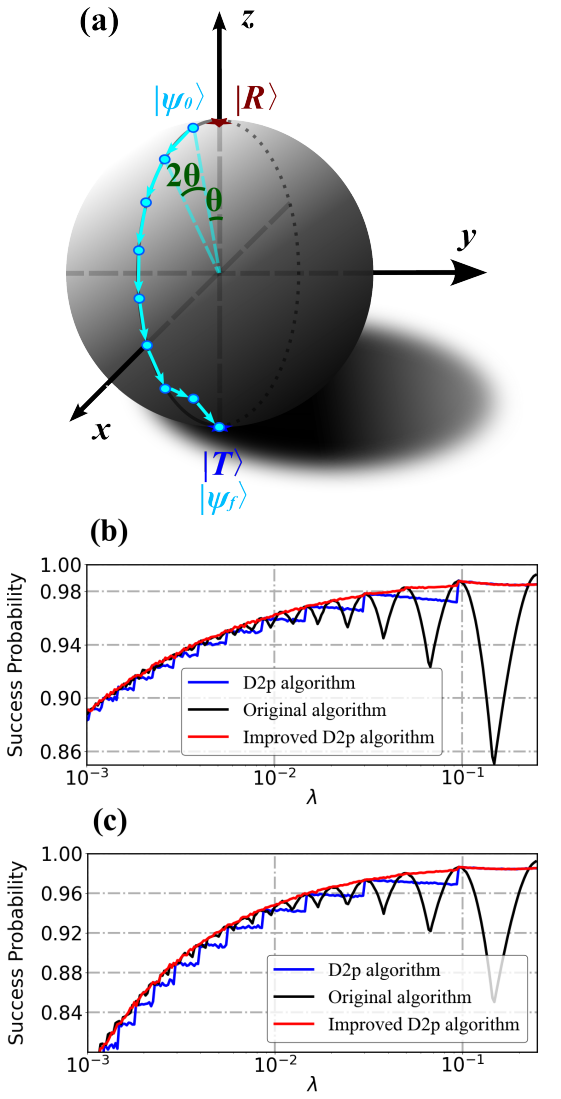


Figure 1: (a) Illustration for our improved D2p Grover's algorithm. First, we follow the original Grover's algorithm to rotate initial state $|\psi_0\rangle$ for $k-2 = \lceil k_0 \rceil - 2$ steps. Then we design two particular steps to lead the final state $|\psi_f\rangle$ to exactly coincide with target state, i.e., the success probability is 100% in noiseless environment. (b) Define $\lambda = M/N$ where M and N are the amount of target states and total states respectively. We apply the same Gaussian distributed phase noise $\delta\beta = \mathcal{N}(\mu = 0, \sigma^2 = 0.04)$ to original Grover's algorithm, D2p protocol and our improved D2p algorithm. Ten thousand samples are averaged for the data. (c) All works are same to (b) but with the distribution $\mathcal{N}(\mu = 0.05, \sigma^2 = 0.04)$.

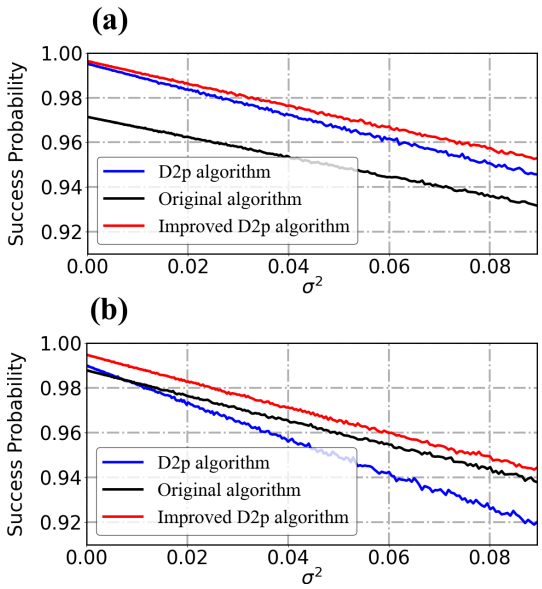


Figure 2: (a) Define $\lambda = M/N$ where M and N are the amount of target states and total states respectively. We apply the same Gaussian distributed phase noise $\delta\beta = \mathcal{N}(\mu = 0.05, \sigma^2)$ to original Grover's algorithm, D2p protocol and our improved D2p algorithm with fixed value $\lambda = 0.040$. We collect their success probability under different variation parameter σ^2. Ten thousand samples are averaged for the data. (b) All are the same to (a) but $\lambda = 0.027$.

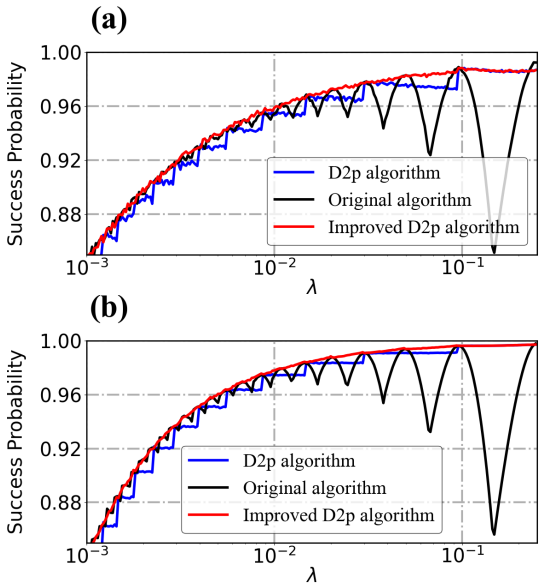


Figure 3: (a) Define $\lambda = M/N$ where M and N are the amount of target states and total states respectively. We apply the same Poisson distributed phase noise $\delta\beta = \mathcal{P}(0.04)$ to original Grover's algorithm, D2p protocol and our improved D2p algorithm. We collect their success probability with different λ. Ten thousand samples are averaged for the data. (b) The distribution of noise is changed to uniform $\delta\beta = \mathcal{U}(-0.1, 0.2)$. All other conditions are the same to (a).

Post-selection in noisy Gaussian boson sampling: part is better than whole

Tian-Yu Yang[1] * Yi-Xin Shen[1] † Zhou-Kai Cao[1] ‡ Xiang-Bin Wang[1 2 3 4 5] §

[1] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China*

[2] *Jinan Institute of Quantum technology, SAICT, Jinan 250101, China*

[3] *Shanghai 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*

[4] *Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China*

[5] *Frontier Science Center for Quantum Information, Beijing, China*

Abstract. Gaussian boson sampling (GBS) plays a central role in verifying quantum computing advantage. Due to technical limitations, the outcomes of GBS devices are influenced severely by photon loss. We present an efficient and practical method to reduce the negative effect caused by photon loss. With no hardware modification, our method takes the data post-selection process that discards low-quality data according to our criterion to improve the performance of the final computational results. Our post-selection method can turn a GBS experiment that would otherwise fail in a "non-classicality test" into one that can pass that test.

Keywords: Quantum advantage, Boson sampling, Error mitigation

The potential speed-up of quantum algorithms over their classical counterparts makes quantum computation a hot topic nowadays. In the past few years, people have witnessed fast development of quantum computing technologies. One of the central issues these years is to demonstrate the quantum advantage. Towards this goal, Gaussian Boson sampling (GBS) is proposed [1]. It is a variant of boson sampling problem proposed by Aaronson and Arkhipov [2] and is designed to facilitate the implementation of the original boson sampling problem without changing the problem's computational complexity.

Recent years, great progress has been made in GBS experiments [3, 4]. However, as the quantum devices are imperfect, errors occur frequently which may ruin the quantum advantage result.

In this work, we focus on error mitigation in the GBS problem. In a GBS device, one of the main error sources is photon loss. We present an efficient method to mitigate photon loss in GBS devices with no need for hardware modification. The main idea of our method is to take a classical data post-selection process, which follows an insight into the similarity among different sets of input quantum states. We first prove that a lossy GBS process can be mapped to another lossy GBS process under certain conditions. Then we give our post-selection method based on this relation. Some numerical results about the performance of our method is given in figure 1. Those numerical results are observed based on the analytical formulas in our main test. Figure 1 shows that our post-selection method is efficient.

*yty19@mails.tsinghua.edu.cn

†shen-yx21@mails.tsinghua.edu.cn

‡caozk21@mails.tsinghua.edu.cn

§xbwang@mail.tsinghua.edu.cn

We also use a "non-classicality test" [5] to test the performance of our post-selection method. This "non-classicality test" is widely used in GBS experiments as a reference to check whether quantum advantage might exist [3, 4]. Numerical results in figure 2 show that the post-selection method can turn a GBS experiment that would otherwise fail in the "non-classicality test" into one that can pass that test. This example, i.e., the post-selection method can help the GBS experiment to surpass the "non-classicality test", shows the potential value of the post-selection method in enhancing the quantum advantage results of the GBS experiment. Besides, by improving the transmission rate, the post-selection method is also beneficial for increasing circuit depth, which is another issue in recent GBS experiments [6].

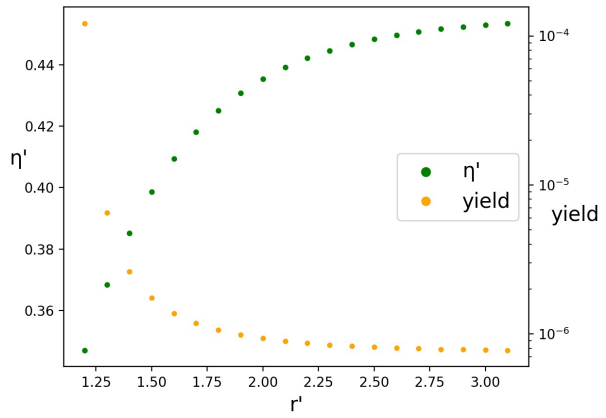
References

[1] Hamilton, Craig S. and Kruse, Regina and Sansoni, Linda and Barkhofen, Sonja and Silberhorn, Christine and Jex, Igor. Gaussian Boson Sampling. Physical review letters, 119(17), 170501, 2017.

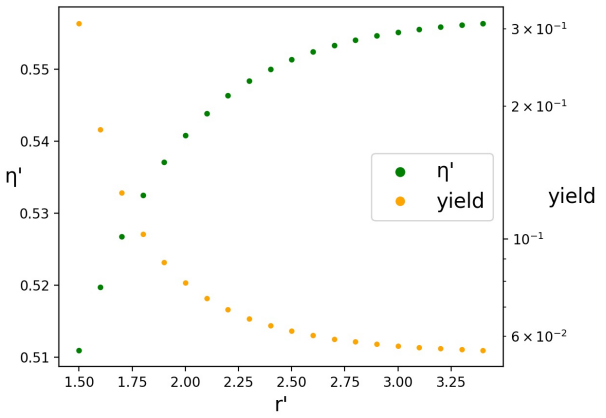
[2] Aaronson, Scott and Arkhipov, Alex. The Computational Complexity of Linear Optics. In Proceedings of the forty-third annual ACM symposium on Theory of computing, pages 333-342, 2011.

[3] Zhong, Han-Sen and Deng, Yu-Hao and Qin, Jian, et, al. Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light. Physical review letters, 127(18), 180502, 2021.

[4] Madsen, Lars S. and Laudenbach, Fabian and Askarani, Mohsen Falamarzi, et,al. Quantum computational advantage with a programmable photonic processor. Nature, 606(7912), 75-81, 2022.

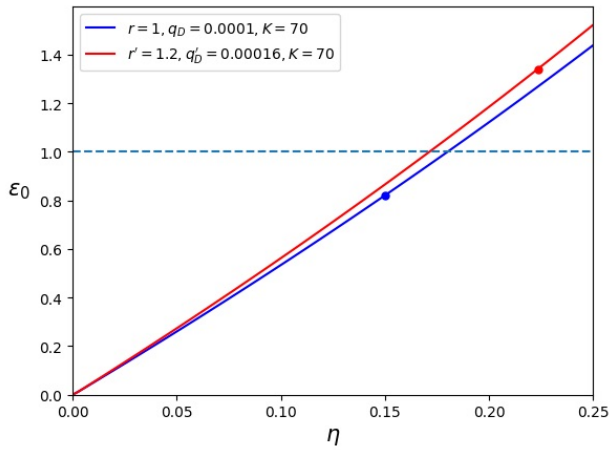


(a) $r = 1.1$, $K = 216$, $\eta = 0.32$, $N_0 = 219$

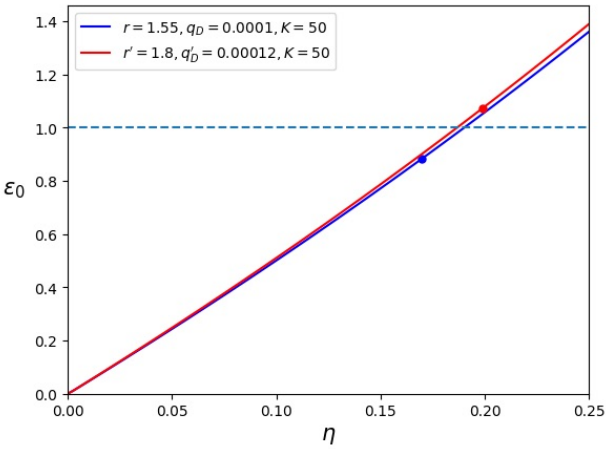


(b) $r = 1.4$, $K = 50$, $\eta = 0.5$, $N_0 = 113$

Figure 1: Performance of the post-selection method. r is input squeezing strength. r' is the target squeezing strength to be simulated. K is the number of input single-mode squeezed states. N_0 is cut-off photon number. η is the overall transmission rate. We use the results of Gaussian boson sampling devices with input squeezing strength r to simulate that of r' by the post-selection method of protocol 1. Red points correspond to η' which is the effective transmission rate in final samples. Orange points correspond to yield which is the percentage of preserved outputs.



(a) $r = 1$, $r' = 1.2$, $K = 70$, $q_D = 0.0001$, $N_0 = 40$, $y = 0.00017$.



(b) $r = 1.55$, $r' = 1.8$, $K = 50$, $q_D = 0.0001$, $N_0 = 100$, $y = 0.00038$.

Figure 2: Simulation errors of the classical algorithm given in [5] for different experimental parameters. The horizontal axis corresponds to the transmission rate η of the sampling process. The vertical axis corresponds to the error upper bound ε_0 of the classical simulation algorithm. When the error upper bound ε_0 on the vertical axis exceeds 1 (dashed line in the figure), the classical simulation algorithm fails. The blue lines show the simulation error upper bound of the classical algorithm for corresponding lossy Gaussian boson sampling experiments. The red lines show the simulation error upper bound of the classical algorithm for corresponding lossy Gaussian boson sampling sampling experiments after a post-selection process. The input squeezing strength is r. The target squeezing strength is r'. The number of input single-mode squeezed states is K. The dark count rate is q_D. The effective dark count rate after the post selection process is q'_D. The cut-off photon number is N_0. The yield is y. The blue points correspond to the error upper bound ε_0 of the classical simulation algorithm for simulating Gaussian boson sampling experiments with transmission rate η. The red points correspond to the error upper bound ε'_0 of the classical simulation algorithm for simulating the GBS experiments after a post-selection process

.

[5] Qi, Haoyu and Brod, Daniel J. and Quesada, Nicolás, et, al. Regimes of Classical Simulability for Noisy Gaussian Boson Sampling. Physical review letters, 124(10), 100502, 2020.

[6] Oh, Changhun and Lim, Youngrong and Fefferman, Bill, et, al. Classical Simulation of Boson Sampling Based on Graph Structure. Physical Review Letters, 128(19), 190501, 2022.

A Appendix

The technical version of this work will be present in following pages.

Trotter error analysis under decoherence in digital quantum simulation

Seong-Yeop Lim[1 2] Sangjin Lee[1] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Korea*
[2] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Korea*

Abstract. Digital quantum simulation (DQS) allows to simulate the time evolution of any Hamiltonian approximately, which finds wide applications for quantum chemistry, many-body and strongly correlated systems and so on. For a long time simulation, the evolution can be divided into a finite number of Trotter step, which unavoidably causes errors. While in an ideal case the Trotter error can be arbitrarily reduced by sufficiently increasing the Trotter number, the total errors may increase by getting higher number of the Trotter steps due to physical errors induced by the interaction between the system and environment and control imperfections. In this work, we analyze the total errors of digital quantum simulation taking into account both the effect of number of trotter steps and physical errors. Our results will be useful to optimize Trotterization and develop a mitigation strategy against the total error in implementing practical digital quantum simulators.

Keywords: Digital quantum simulation, Trotter errors, Decoherence

1 Introduction

Deeper understanding of quantum dynamics can be realized by simulating corresponding quantum systems. However, simulating quantum dynamics with a classical computer is difficult because the number of parameters and calculations to mimic the evolution of quantum system grows exponentially with system size. One of the best way to simulate quantum dynamics is to use quantum device called a quantum simulator. Quantum simulation has been realized with several platforms such as ultra-cold gases, superconducting circuits, trapped ions and photons. It finds wide applications in various fields of physics such as condensed matter physics, general quantum gauge theory, quantum chemistry.

In digital quantum simulation (DQS), the time evolution of Hamiltonian can be simulated by dividing the evolution by Trotterization [1]. Since the effective Hamiltonian is not exactly the same with the original Hamiltonian, digital quantum simulation by Trotterization yields Hamiltonian error, called Trotter error. If there are no physical errors, Trotter error can be arbitrary reduced if the Trotter number r is getting larger enough. On the other hand, in realistic simulations, physical errors caused by decoherence and gating errors may also affect the performance significantly. The effect of decoherence grows as the simulating time increases. The gating errors become larger as the number of gate grows. As the Trotter steps determines both the total simulation time and the number of implemented gates [2], increasing the number of Trotter steps would not be an optimal solution to suppress errors in practical digital quantum simulations. In this circumstance, we study and analyze the total errors in digital quantum simulation taking into account not only the Trotter steps but also realistic physical errors. Our work will be useful to optimize the Trotterization in digital quantum simulation and to devise a scheme for mitigating both Trotter and Physical errors.

*swleego@gmail.com

2 Trotter error bound

The target system Hamiltonian H is decomposed into L elements $H = \sum_{j=1}^{L} H_j$, and total Hamiltonian evolution time, t, is divided into r steps. Each evolution of a decomposed Hamiltonian for short time interval t/r, $\{e^{-iH_j t/r}\}_j$, are realized in terms of quantum gates depending on simulation platforms. Then, the simulation is governed by effective Hamiltonian $\tilde{H}$ rather than the original system Hamiltonian H and the effective Hamiltonian $\tilde{H}$ is defined as

$$e^{-i\tilde{H}t/r} = \prod_{j=1}^{L} e^{-iH_j t/r}. \tag{1}$$

The analytic form of the effective Hamiltonian can be derived by using Baker-Campbell-Hausdorff(BCH) formula

$$\tilde{H} = H - \frac{i}{2}\sum_{\nu=\mu+1}^{L}\sum_{\mu=1}^{L}[H_\nu, H_\mu](t/r) + O(t^2/r^2). \tag{2}$$

By expanding the Hamiltonian time evolution operator, a leading order term of the Trotter error is

$$\left\| e^{-iHt} - e^{-i\tilde{H}t} \right\| \leq \left\| -\frac{it^2}{2r}\sum_{\mu<\nu}^{L}[H_\nu, H_\mu] + O(t^3/r^2) \right\|. \tag{3}$$

3 Physical error model

In practice, quantum simulators experience various effects of physical errors such as decoherence and imperfect controls. We now intend to investigate the physical errors in Trotterization and investigate their accumulation by changing the Trotter number r.

Following a previous work by Knee *et al.* [3], we first consider the physical errors that are not correlated with the Trotter error. As a paradigmatic example of physical errors, we can consider the depolarization quantum channel, which turns an arbitrary density matrix ρ into

a totally mixed state with probability p, represented by

$$\mathcal{E}^{DEPOL}(\rho) = (1-p)\rho + p\frac{I}{d}, \tag{4}$$

where d is a dimension of the Hilbert space. Thus we can write the total simulating channel as

$$\mathcal{E} = \bigcirc_{j=1}^{r} \mathcal{E}^{DEPOL} \circ \mathcal{V}, \tag{5}$$

where $\mathcal{V}$ indicates one Trotter step evolution and $\bigcirc$ denotes the concatenation of channels. Note that it is assumed here that there is no correlation between the Trotter steps and the depolarization noise. Therefore, we can find that the accumulated error from depolarizing channel grows linearly with the Trotter number r. A bound of the total error D_{DEPOL} can then be calculated as [3]

$$D_{DEPOL} \leq (1-p)\mathcal{A}\frac{t^2}{2r} + rp(2 - \frac{2}{d^2}), \tag{6}$$

where

$$\mathcal{A} \propto \left\| \sum_{\mu<\nu} [H_\nu, H_\mu] \right\|. \tag{7}$$

Likewise for all the other physical error model that is uncorrelated with the Trotter error, one can find that the total error has the form

$$\frac{C}{r} + Dr, \tag{8}$$

with constants C and D which characterize the physical error model. We can then find the optimal Trotter number as $r_{opt} = \sqrt{C/D}$.

4 Analysis of nontrivial correlated error

Now, let us consider a decoherence error model that are correlated with the Trotter error. In such a model, the form of the total error of DQS may differ from Eq.(5). Under the assumption of time independent depolarization error model, the total error shows asymptotically linear growth as r after a certain Trotter number r_{opt}. On the other hand, for a decoherence model that are dependent on time, the corresponding quantum channel is also dependent on time. We thus consider realistic decoherence model correlated with the Trotter errors, resulting in a total error model nontrivially dependent on the Trotter numbers r as

$$\frac{C(r)}{r} + D(r)r, \tag{9}$$

where $C(r)$ and $D(r)$ are not constant anymore but nontrivially vary with r. In such a complicated error model including higher-order terms, the error bound can be also calculated by numerical optimization with Eq. (9). We consider some paradigmatic decoherence models. When analyzing the noise, we consider characteristic properties of decoherence models such as a spectral profile. When calculating the bound of the total error, we also consider interference of errors [4, 5] to get a more realistic result.

In this work, we establish a total error model accounting both the physical and Trotter errors as well as their correlations. We can then arrive at the optimal Trotter number r_{opt} by numerical optimization with Eq. (9). We expect that our result will be useful to optimize Trotterization in DQS and develop an efficient tools to mitigate the total error in developing practical digital quantum simulators.

References

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

[2] Andrew M Childs and Yuan Su. Nearly optimal lattice simulation by product formulas. *Phys. Rev. Lett.*, 123(5):050503, 2019.

[3] George C. Knee and William J. Munro. Optimal trotterization in universal quantum simulators under faulty control. *Phys. Rev. A*, 91:052327, May 2015.

[4] Minh C. Tran, Su-Kuan Chu, Yuan Su, Andrew M. Childs, and Alexey V. Gorshkov. Destructive error interference in product-formula lattice simulation. *Phys. Rev. Lett.*, 124:220502, Jun 2020.

[5] David Layden. First-order trotter error from a second-order perspective. *Phys. Rev. Lett.*, 128(21):210501, 2022.

Causal asymmetry of input-output processes

Spiros Kechrimparis[1] [*] Mile Gu[2 3 4] [†] Hyukjoon Kwon[1] [‡]

[1]*School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, South Korea*
[2]*Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, 637371, Singapore.*
[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore.*
[4]*MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, 117543, Singapore.*

Abstract. Given a pair of stochastic processes, in general it is more efficient, in terms of memory, to employ one in order to produce the other than to reproduce the outputs of the processes from scratch. In addition, *causal asymmetry* will be present, that is, the memory costs of mapping one process to the other and vice versa will in general be different. We show that this causal asymmetry is often inconsistent between classical and quantum models and in a certain sense this inconsistency can increase without a bound. In other words, classical theory might suggest that it costs less to produce the first process given the second while quantum theory might suggest the opposite.

Keywords: Causal asymmetry, stochastic processes, input-output processes, memory resources, quantum models

1 Introduction

Stochastic processes are mathematical models to explain phenomena that vary in a random manner, and find application in a wide range of areas including physics, biology, computer science, and economics. Given a pair of such processes one can consider the memory cost of producing one from the other. As an illustrative example, let us consider two streams of data, $d_{\mathcal{A}}$ = "...01010101..." and $d_{\mathcal{B}}$ = "...01230123...", which may be obtained from outcomes of measurements at discrete time steps on two physical systems with a periodic structure. To produce sequence $d_{\mathcal{A}}$ and $d_{\mathcal{B}}$ from scratch, we need to have access to memories of 1 and 2 bits respectively: in both cases we need to remember the previous output and the two alphabets contain 2 and 4 symbols, respectively. On the other hand, if we have access to one of the two sequences, we could do better in reproducing the other. To obtain sequence $d_{\mathcal{B}}$ from $d_{\mathcal{A}}$ we need only 1 bit of memory by mapping every block of observed "01" to either "01" or "23" sequentially and by remembering the last output. Producing $d_{\mathcal{A}}$ from $d_{\mathcal{B}}$ is even easier without incurring a memory cost: all we have to do is substitute every observed "2" with a "0" and every "3" with a "1". Thus, producing $d_{\mathcal{A}}$ from $d_{\mathcal{B}}$ incurs no memory cost, sequence $d_{\mathcal{A}}$ comes for *free* given that we possess sequence $d_{\mathcal{B}}$.

The aforementioned scenario which involves *input-output processes* or *channels*, maps between two stochastic processes, indicates the presence of *causal asymmetry*: when memory is viewed as a resource, it may be cheaper to produce one of the processes given access to the other than the other way around. Causal asymmetry has been identified in a number of different contexts. For example, in the context of outcomes from a single process, it was shown that the cost of prediction and retrodiction are in general different [1, 2]. That is, the memory cost of predicting future outputs or retrodicting past outputs are not the same, even though this causal asymmetry appears to be lifted when a quantum memory is employed [3]. In the general setting of input-output processes, we also find that the memory costs of producing $\mathcal{B}$ from $\mathcal{A}$ and vice versa are not equal. What is, however, more surprising is that causal asymmetry can not even be assigned a consistent positive or negative value between different theories. In other words, the classical and quantum memory costs of the two maps may assume different ordering.

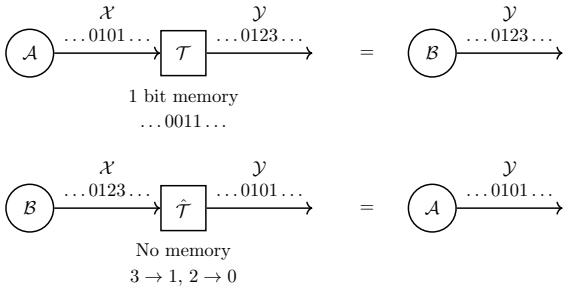


Figure 1: Mapping two processes $\mathcal{A}$ and $\mathcal{B}$ to each other by emplying a memory and using one of them as input.

2 Preliminaries

The information theoretic study of minimal causal models of stochastic processes as well as input-output processes, is the focus of *Computational Mechanics* [4, 5, 6]. A major discovery of the field is that provably memory-optimal descriptions of processes can be systematically constructed, from which information theoretic quantities can be deduced.

Consider an input-output process that accepts as input a stochastic processes over an input alphabet $\mathcal{X}$ and outputs stochastic processes over an output alphabet $\mathcal{Y}$. By grouping joint pasts of inputs and outputs that lead to statistically indistinguishable future

[*] skechrimparis@gmail.com
[†] mgu@quantumcomplexity.org
[‡] hjkwon@kias.re.kr

predictions, one can obtain the channel's equivalence classes of pasts, which are referred to as *causal states*. Having obtained the causal states, transitions between them are described through a set of transition matrices $\mathcal{T} \equiv \{T^{(y|x)}\}_{x\in\mathcal{X},y\in\mathcal{Y}}$ with elements explicitly given by $T_{ij}^{(y|x)} = \Pr(Y_t = y, S_{t+1} = s_j | X_t = x, S_t = s_i)$, representing the probability of transitioning from causal state s_i to state s_j while emitting the symbol y, upon receiving input symbol x. Note that the transition matrices are labelled by conditional symbols, output for a given input. The causal states and the transitions between them lead to the minimal presentation of an input-output process, referred to as the *ϵ-transducer*, which is formally defined as the tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{S}, \mathcal{T})$ consisting of the input and output alphabets, the set of causal states and the conditional transitions probabilities. Given an input process $\mathcal{A}$, the ϵ-transducer's causal states are driven to a unique distribution, the *stationary distribution*, which we denote by $\pi_{\mathcal{A}}$. For example, $\pi_{\mathcal{A},i}$ denotes the probability of being at state s_i when driven by the input process $\mathcal{A}$. The classical memory necessary on average to effect the given channel is given by the *statistical complexity*, defined as the entropy of the distribution over causal states, $C_{\mathcal{A}} = H(\pi_{\mathcal{A}}) = -\sum_i \pi_{\mathcal{A},i} \log \pi_{\mathcal{A},i}$.

By employing quantum mechanics, however, we can do better. We can reduce the complexity by mapping the causal states of the ϵ-transducer to quantum states, designing appropriate measurements that extract the emissions and prepare the next state in a way that is indistinguishable from the classical model. The quantum causal states can always be taken to be pure states [7], and the quantum complexity is defined as the von Neumann entropy $Q_{\mathcal{A}} = S(\rho_{\mathcal{A}})$ of the average state of the quantum memory, $\rho_{\mathcal{A}} = \sum_i \pi_{\mathcal{A},i} |s_i\rangle\langle s_i|$, with $|s_i\rangle\langle s_i|$ denoting the quantum state representing the classical causal state s_i. A quantum model is at least as efficient as the best classical model, that is $Q_{\mathcal{A}} \leq C_{\mathcal{A}}$ [7, 8]. In the limit where the quantum causal states become orthogonal, we recover the classical complexity $C_{\mathcal{A}}$, while a strict inequality $Q_{\mathcal{A}} < C_{\mathcal{A}}$ holds for quantum models whose causal states have some non zero overlaps.

3 Results

Consider the following causation scenario. We have two Markovian processes $\mathcal{A}$ and $\mathcal{B}_n$ and the minimal mapping, $\mathcal{T}_n$, from $\mathcal{A}$ to $\mathcal{B}_n$ and analogously the minimal mapping from processes $\mathcal{B}_n$ to process $\mathcal{A}$, denoted by $\hat{\mathcal{T}}_n$. We show, by constructing an explicit example, that the difference of the classical complexities, $C_{\mathcal{A}\to\mathcal{B}_n} - C_{\mathcal{B}_n\to\mathcal{A}}$, of the two mappings can grow without bound, suggesting that mapping $\mathcal{A}$ to $\mathcal{B}_n$ is classically increasingly harder with n, while the difference of the quantum complexities, $Q_{\mathcal{A}\to\mathcal{B}_n} - Q_{\mathcal{B}_n\to\mathcal{A}}$, is upper bounded by a certain negative value, implying the opposite statement.

Specifically, let $\mathcal{A}$ denote the stochastic process that is shown in Fig. 2. It consists of an alphabet of three symbols and two internal states, r_0 and r_1, the first of which is synchronised to whenever a 0 is emitted while the second whenever one observes a 1 or 2. Moreover, at state r_0, there is 50% chance that either a 1 or 2 is emitted, while at state r_1, there is 50% chance that either a 0 or 1 is output.

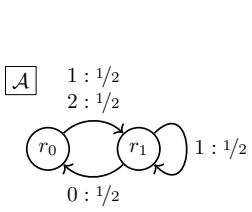


Figure 2: Process $\mathcal{A}$

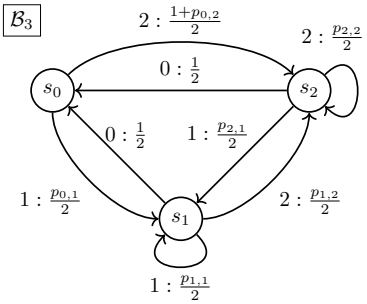


Figure 3: Process $\mathcal{B}_3$

Consider also the family of stochastic processes, $\mathcal{B}_n$, labeled by an index $n \in \mathbb{N}$ with $n \geq 3$, each of which consists of n causal states, $s_0 \ldots, s_{n-1}$, and n outputs, $y \in \mathcal{Y} = \{0, \ldots, n-1\}$ with the following properties: (i) an emission of symbol y_j leads to a transition to the state of the same index, s_j, (ii) from states $s_1, \ldots, s_{n-1}$, a transition with output $y_j \neq 0$ can occur with probability $p_{s_i y_j}/2$, while with probability $1/2$ if $y = 0$,(iii) from state s_0, a transition with output $y_j \neq 0, 2$ can occur with probability $p_{s_i y_j}/2$, while with outputs $y = 0, 2$ with probability 0 and $1+p_{s_0 y_2}/2$, respectively. Moreover, the probabilities p_{s_i,y_j} of emitting a certain symbol are all assumed to be numerically close to the value $1/n-1$ but different from each other. The case with $n = 3$ is shown in Fig. 3.

A family of input-output processes that maps process $\mathcal{A}$ to the family $\mathcal{B}_n$ with minimal classical complexity is given by the ϵ-transducers $\mathcal{T}_n$ that consist of n states, $\Sigma = \{\sigma_i\}_{i=0\ldots n-1}$, accept a 3-symbol input alphabet $\mathcal{X} = 0, 1, 2$ and output from an n symbol alphabet $\mathcal{Y} = 0, \ldots, n-1$. The ϵ-transducers leave inputs 0 and 2 intact but modify input 1 so that it correctly reproduces the probabilities of the target output $\mathcal{B}_n$. The ϵ-transducer with $n = 3$ is shown in Fig. 4. Similarly, the channel that maps $\mathcal{B}_n$ to $\mathcal{A}$ keeps intact the emissions of symbol 0 but has to erase all the probabilities associated with the remaining $n-1$ outputs. We denote this with $\hat{\mathcal{T}}_n$. The case with $n = 3$ is shown in Fig. 5.

Turning to the classical and quantum memory costs of the two maps, we first derive the classical complexity of the map from $\mathcal{A}$ to $\mathcal{B}_n$ and find that it grows logarithmically with n and thus it is unbounded. On the other hand, the ϵ-transducers that map $\mathcal{B}_n$ to $\mathcal{A}$ can be shown to have a classical complexity of $C_{\mathcal{B}_n\to\mathcal{A}} = \log(27/4)/\log(8) \approx 0.918$ independent of n. It follows that the difference of the two complexities $C_{\mathcal{A}\to\mathcal{B}_n} - C_{\mathcal{B}_n\to\mathcal{A}} \sim \log n$, that is, it grows as the logarithm of n. In other words, mapping process $\mathcal{A}$ to $\mathcal{B}_n$ is increasingly costly in terms of memory, when a classical memory is employed.

We now turn to the quantum complexity, $Q_{\mathcal{A}\to\mathcal{B}_n}$. We explicitly construct the following quantum models [7, 3] where the classical causal states are encoded to quantum

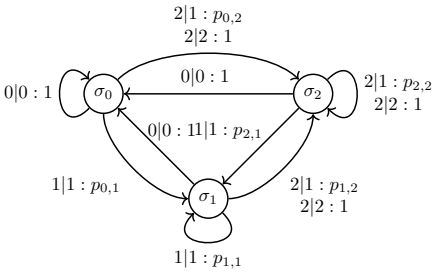


Figure 4: The ϵ-transducer $\mathcal{T}_3$ from the family $\mathcal{T}_n$.

states as $|s_i\rangle = \otimes_x |s_i^x\rangle$, with

$$|s_i^x\rangle = \sum_k \sum_y \sqrt{T_{ik}^{(y|x)}} |y\rangle|k\rangle \,, \tag{1}$$

The ϵ-transducers $\mathcal{T}_n$ are such that for all inputs $x \neq 1$ we have that $|s_i^x\rangle = |x\rangle|x\rangle$ independent of the state index i. Meanwhile, it is easy to see that $|s_i^1\rangle = \sum_{j\neq 0} \sqrt{p_{i,j}}|j\rangle|j\rangle$. As a result, the overlap between quantum causal states is given by $\langle s_i|s_j\rangle = \sum_{k\neq 1} \sqrt{p_{i,k}\, p_{j,k}}$. The quantum complexity is the von Neumann entropy of the average state of the quantum memory, $\rho = \sum_i \varphi_i |s_i\rangle\langle s_i|$ where φ_i denotes the $i-$th element of the stationary distribution of the ϵ-transducer $\mathcal{T}_n$ when driven by the input $\mathcal{A}$. It is known that state ρ and the Gram matrix of overlaps, with elements $G_{i,j} = \sqrt{\varphi_i \varphi_j}\langle s_i|s_j\rangle$, have the same non-zero eigenvalues [9]. Thus, they have the same von Neuman entropy. From this fact and the freedom to choose all probabilities $p_{i,j}$ to be arbitrarily close to each other (but not equal), we have that $G_{i,j} \approx \sqrt{\varphi_i \varphi_j}$. Under this assumption, $G \approx vv^\top$, where we defined $v^\top = (\sqrt{\varphi_1}, \ldots, \sqrt{\varphi_n})$, and thus approximately the Gram matrix has one eigenvalue equal to 1 and all others equal to 0. It follows that the quantum complexity in the limit where all the $p_{i,j}$ are the same becomes 0. If they are not exactly equal but sufficiently close, the quantum complexity can be made arbitrarily small. A precise statement is that given a small perturbation of the probabilities around the value $1/n-1$ so that $p_{ij} = \frac{1}{n-1} + \delta_{ij}$, with $|\delta_{ij}| \leq \delta$ for some small $\delta > 0$, the optimal quantum complexity is bounded as

$$Q^{\text{upper}}_{\mathcal{A}\to\mathcal{B}_n}(\delta) \geq Q_{\mathcal{A}\to\mathcal{B}_n} \geq 0 \,, \tag{2}$$

where $Q^{\text{upper}}_{\mathcal{A}\to\mathcal{B}_n}(\delta)$ can be made arbitrarily small by an appropriate choice of δ.

Turning to the quantum complexity of the map from B_n to $\mathcal{A}$, the situation is more intricate. We have to consider all possible classical maps and then show that the complexity of all possible quantum models is bounded. Specifically, we show that the optimal quantum complexity is bounded from below and above according to the inequality

$$Q^{\text{upper}}_{\mathcal{B}_n\to\mathcal{A}} \geq Q_{\mathcal{B}_n\to\mathcal{A}} \geq 0.55 \,, \tag{3}$$

where $Q^{\text{upper}}_{\mathcal{B}_n\to\mathcal{A}}$ depends on the value of n; it takes the value 0.682 for $n = 3$ and approaches the classical complexity of 0.918 with increasing values of n.

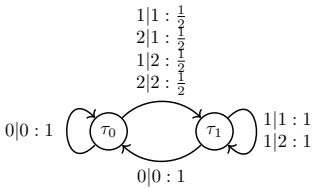


Figure 5: The ϵ-transducer $\hat{\mathcal{T}}_n$ that maps process $\mathcal{B}_n$ to process $\mathcal{A}$ in the case of $n = 3$.

Using Eqs. (2), (3), we obtain the following bounds on the difference of the quantum complexities of optimal quantum models

$$Q^{\text{upper}}_{\mathcal{A}\to\mathcal{B}_n}(\delta) - 0.55 \geq Q^{\text{opt}}_{\mathcal{A}\to\mathcal{B}_n} - Q^{\text{opt}}_{\mathcal{B}_n\to\mathcal{A}} \geq -Q^{\text{upper}}_{\mathcal{B}_n\to\mathcal{A}} \,. \tag{4}$$

On the left hand side and for any n, there always exists a range of value of δ that make this difference negative. This implies that mapping processes $\mathcal{B}_n$ to $\mathcal{A}$ is harder, when a quantum memory is employed.

In Fig. 6 we have plotted the difference of classical and quantum complexities, $C_{\mathcal{A}\to\mathcal{B}_n} - C_{\mathcal{B}_n\to\mathcal{A}}$ and $Q_{\mathcal{A}\to\mathcal{B}_n} - Q_{\mathcal{B}_n\to\mathcal{A}}$, for $n = 3, \ldots, 200$ and $\delta = 10^{-4}$. We see that the difference of the quantum complexities approaches a finite negative value while that of the classical ones grows logarithmically with n.

In summary, given the minimal maps between two stochastic processes, $\mathcal{A}$ and $\mathcal{B}$, we have demonstrated that not only causal asymmetry may be present, but it can be also inconsistent between different theories. In other words, the difference is not only of quantitative nature but also qualitative in that different theories may assign different ordering of the complexities: classical theory may suggest that is harder to map $\mathcal{A}$ to $\mathcal{B}$ and at the same time quantum theory may suggest the opposite, mapping $\mathcal{B}$ to $\mathcal{A}$ requires more memory resources.

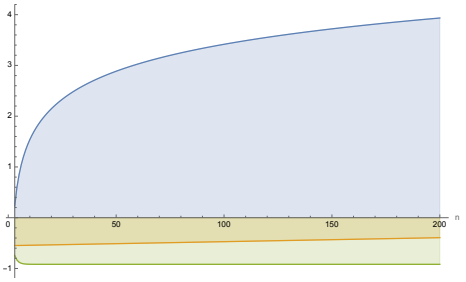


Figure 6: The difference of classical and quantum complexities of the ϵ-transducers that map $\mathcal{A}$ to $\mathcal{B}_n$ and vice versa. In blue we show the values of $C_{\mathcal{A}\to\mathcal{B}_n} - C_{\mathcal{B}_n\to\mathcal{A}}$, while the values of $Q_{\mathcal{A}\to\mathcal{B}_n} - Q_{\mathcal{B}_n\to\mathcal{A}}$ lie in-between the green and orange curves.

References

[1] J. P. Crutchfield, C. J. Ellison, J. R. Mahoney, Phys. Rev. Lett., **9**, 094101 (2009).

[2] C.J. Ellison, J.R. Mahoney, J.P. Crutchfield, J. Stat. Phys **136**, 1005–1034 (2009).

[3] J. Thompson, A. J. P. Garner, J. R. Mahoney, J. P. Crutchfield, V. Vedral, M. Gu, Phys. Rev. X **8**, 031013 (2018).

[4] J. P. Crutchfield, Nature Phys., **8(1)**:17-24 (2012).

[5] J. P. Crutchfield, K. Young, Phys. Rev. Lett., **63**,105 (1989).

[6] N. Barnett, J. P. Crutchfield, J. Stat. Phys. **161**, 404–451 (2015).

[7] T.J. Elliott, M. Gu, A. J. P. Garner, J. Thompson, Phys. Rev. X **12**, 011007 (2022).

[8] J. Thompson, A. J. P. Garner, V. Vedral, M. Gu, npj Quantum Inf **3**, 6 (2017).

[9] R. Jozsa, J. Schlienz, Phys. Rev. A **62**, 012301 (2000).

Port Based Entanglement Teleportation

Ha Eum Kim[1] * Kabgyun Jeong[2 3] †

[1] *Department of Physics, Korea University, Seoul 02841, Korea*
[2] *Research Institute of Mathematics, Seoul National University, Seoul 08826, Korea*
[3] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*

Abstract. Port-based teleportation(PBT) is a teleportation protocol that employs a number of Bell pairs and a joint measurement to enact an approximate input-ouput identity channel. In this work, we fully characterise the PBT protocol in terms of depolarising noise on resource states using the invariant of the resource and measurement has. We extend our description to the amplitude damping noise. Finally, we calculate the entanglement teleportation of PBT. We found that the measure of quantum entanglement teleported by PBT increases inversely with the number of ports. This property holds even when the resource states are affected by the environment.

Keywords: Port based teleportation, entanglement teleportation, noisy channel

1 Introduction

Quantum teleportation, introduced by Bennett et al. [1], is a seminal process for transmitting unknown quantum states over long distances without physically sending the quantum system itself. It relies on the utilization of distributed entanglement to transfer quantum information from a sender to a remote receiver. A variant of quantum teleportation, known as port-based teleportation (PBT), has been proposed as an efficient alternative approach [2, 3, 4]. In PBT, receiver is not required to do recovery operation at the end of the protocol, instead he selects a port based on classical information associated with the sender's measurement outcome. The unique features of PBT enable its applications in various quantum information processing tasks, such as instantaneous non-local quantum computation [6], quantum-channel discrimination [7], and quantum telecloning protocols [8, 9].

Entanglement in quantum information refers to the phenomenon where two or more quantum systems become correlated in such a way that the state of one system cannot be described independently of the others, contrasting with classical correlations where the state of each system can be determined separately. In the context of quantum networks, entanglement serves as a crucial resource for enabling various quantum communication protocols, including quantum teleportation, which allows for the transfer of unknown quantum states between distant network nodes, thereby facilitating the distribution and manipulation of quantum information in a scalable and secure manner.

Entanglement teleportation, introduced by Lee et al. [5], is to transmit the entanglement initially prepared over remote place. Research has been conducted to investigate the effects of noisy quantum channels on entanglement teleportation, exploring strategies to mitigate the detrimental impact of noise and enhance the fidelity and reliability of entanglement transfer in realistic quantum communication scenarios.

In this study, we aim to investigate the entanglement teleportation using the PBT protocol under the influence of a noisy quantum channel. We found that the measure of quantum entanglement teleported by PBT increases inversely with the number of ports. This result is invariant under influences of a noisy qunatum channel to resource state.

2 Port-based Teleportation Channel

In the PBT protocol, the sender and receiver share N entangled resource states with each other. The sender measures the partition of the resource states it holds between the states it wants to send and the states of the resource through the square-root measurement. After the measurement, the sender communicates to the receiver which port it should select. In this protocol, the receiver does not need to perform any quantum operations.

We investigate the PBT channel using the invariant property that POVM measurement and resource state have.

2.1 Maximally Entangled State

We investigate the property of the teleportation channel using invariant operation on maximally entangled state. As the state is invariant under twirling by single qubit arbitrary unitary operator and its conjugation to the other qubit, this implies that the resource state and POVM measurement, which are constructed by the state, are also invariant under the twirling and the teleportation channel is a depolarizing channel. The channel can be describe with the entanglement fidelity of PBT F_0 as

$$\frac{4}{3}(1-F_0)\frac{\hat{I}}{2}+\frac{1}{3}(4F_0-1)\hat{\rho}, \tag{1}$$

*hekim007@korea.ac.kr
†kgjeong6@snu.ac.kr

where $\hat{\rho}$ is the state sender want to teleport and $\hat{I}$ is identity operator.

We also considered for the case when the resource states are effected by the noise. We assume that every sites are separated each other and equally influenced by the same environment.

2.2 Deporalized Resource State

We first analysed the teleportation channel when the resource states are equivalently depolarized due to the noise. This noise doesn't break the invariant under the twirling that resource states have. So The teleportation channel can also be describe with the entanglement fidelity F_0 as

$$\frac{4}{3}(1-F_0)\frac{\hat{I}}{2}+\frac{1}{3}(4F_0-1)(\mathcal{D}\cdot\mathcal{D})(\hat{\rho}), \tag{2}$$

where $\mathcal{D}$ is the depolarizing channel to a single site. The limited number of port made the teleportation channel be depolarizing channel independent to the depolarizing noise on the resource states. The noise on the single site of the resource states effected to the state teleported to be twice.

2.3 Amplitude Damped Resource State

We secondly investigated the case when the each resource states site are effected by amplitude damping. Different with the maximally entangled resource state and depolarized resource state, the invariant partially broke down. Fortunately, the resource state is invariant by the twirling of every z axis rotation operators. This implies that the teleportation channel is a amplitude damping channel.

This channel is depolarized with same order as resource state we saw above. At the small amplitude damping noise, We saw that the noise is approximately doubly effected at the teleported state as we saw for teleportation with deporalized resource state.

3 Entanglement Teleportation

With the port-based teleportation channels we calculated above section, we investigate the entanglement teleportation on PBT.

Lee et al. [5] calculated the measure of entanglement for the standard teleportation

$$\max\left[0,-\frac{1}{2}+\left(\frac{1+2\mathcal{N}_{\text{dep}}}{3}\right)^2\left(\mathcal{M}_0+\frac{1}{2}\right)\right], \tag{3}$$

where $\mathcal{N}_{\text{dep}}$ is the measure of entanglement for resource state and $\mathcal{M}_0$ is the measure of entanglement for prepared entangled state.

We investigate that the measure of entanglement for PBT with maximally entangled preshared state is

$$\max\left[0,-\frac{1}{2}+\frac{4F_0-1}{3}\left(\mathcal{M}_0+\frac{1}{2}\right)\right]. \tag{4}$$

The measure of entanglement for PBT with depolarized preshared state is

$$\max\left[0,-\frac{1}{2}+\frac{4F_0-1}{3}\left(\frac{1+2\mathcal{N}_{\text{dep}}}{3}\right)^2\left(\mathcal{M}_0+\frac{1}{2}\right)\right]. \tag{5}$$

In the asymptotic limit of number of ports goes infinite, same as $F_0\to 1$, equation (4) and (5) are same as (3). As entanglement fidelity becomes

$$F_0\to 1-\frac{3}{4N} \tag{6}$$

for $N\to\infty$, the positive measure of entanglement can be written as

$$-\frac{1}{2}+\left(1-\frac{1}{N}\right)\left(\frac{1+2\mathcal{N}_{\text{dep}}}{3}\right)^2\left(\mathcal{M}_0+\frac{1}{2}\right) \tag{7}$$

using number of ports N. We conclude that the measure of quantum entanglement teleported by PBT increases inversely with the number of ports. This result consists for weakly amplitude damped at the resource states.

4 Acknowledgments

This work was supported by Creation of the Quantum Information Science R&D Ecosystem (Grant No. NRF-2023R1A2C1005588) through the National Research Foundation of Korea (NRF) funded by the Korean government (Ministry of Science and ICT), and by the National Research Foundation of Korea (NRF) through a grant funded by the Ministry of Science and ICT (NRF-2022M3H3A1098237), the Ministry of Education (NRF-2021R1I1A1A01042199), and Korea Institute of Science and Technology Information (P23031).

References

[1] C. H. Bennett. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70(13), 1895, 1993.

[2] S. Ishizaka. Asymptotic teleportation scheme as a universal programmable quantum processor. Phys. Rev. Lett. 101(24), 240501, 2008.

[3] S. Ishizaka. Quantum teleportation scheme by selecting one of multiple output ports. Phys. Rev. A. 79(4), 042306, 2009.

[4] K. Jeong. Generalization of port-based teleportation and controlled teleportation capability. Phys. Rev. A. 102(1), 012414, 2020.

[5] J. Lee. Entanglement Teleportation via Werner States. Phys. Rev. Lett. 84(18), 4236, 2000.

[6] S. Beigi. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New J. Phys. 13(9), 093036, 2011.

[7] S. Pirandola. Fundamental limits to quantum channel discrimination. *npj Quantum Inf.* 5(1), 50, 2019.

[8] M. Murao. Quantum telecloning and multiparticle entanglement. Phys. Rev. A. 59(1), 156, 1999.

[9] G. Prettico. Superactivation, unlockability, and secrecy distribution of bound information. Phys. Rev. A. 83(4), 042336, 2011.

[10] V. Vedral. Quantifying entanglement. Phys. Rev. Lett. 78(12), 2275, 1997.

[11] A. Peres. Separability criterion for density matrices. Phys. Rev. Lett. 77(8), 1413, 1996.

Discrete and continuous variable hybrid quantum computation using single photon and cat code

Jaehak Lee[1 2] Nuri Kang[1 3] Seung-Woo Lee[1 *]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Korea*
[2] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Republic of Korea*
[3] *Department of Physics, Korea University, Seoul 02841, South Korea*

Abstract. We introduce a scheme of discrete variable (DV) and continuous variable (CV) hybrid quantum computation based on single photon and cat-code. We define the hybrid logical basis of qubits by taking the advantages of both DV and CV photonic qubits. Near-deterministic Bell measurements on hybrid qubits enable efficient implementation of logical universal gate operations by employing the gate teleportation scheme. Photon loss can be detected and corrected during the teleportation process due to the loss of single photon or the parity change in the cat-code. Our scheme outperforms previous proposals of photonic quantum computation in fault-tolerance analysis.

Keywords: Photonic hybrid quantum computation, Quantum error correction, Bosonic code

1 Hybrid quantum computation

In realistic situations, qubits encounter errors due to imperfect operations and interaction with environments. Quantum error correction (QEC) has been developed to provide systematic ways for protecting encoded information from unavoidable errors. Error correction codes have been developed both for discrete-variable (DV) and continuous-variable (CV) systems. In CV approach, various error correction codes have been proposed for a bosonic system in an infinite-dimensional Hilbert space such as GKP, binary and cat codes. The cat-code is designed against photon loss by encoding a qubit in the cat state with even parity [1, 2]. A single photon loss causes the change of parity and thus can be detected by a parity measurement. One of the major defects of the cat code is additional errors originated from the non-orthogonality between logical basis states. This also makes it difficult to implement gate operations such as Z gate with linear optical elements.

To solve the problems, we define hybrid qubits by combining DV and CV photonic qubits. While in the previous study of hybrid qubits [3] single photons and coherent states are employed as DV and CV qubits, respectively, we here incorporate the error-correcting feature of cat codes into the CV part. The logical basis is given by [4]

$$\left\{|0_L\rangle = |+\rangle|\mathcal{C}_\alpha^+\rangle, |1_L\rangle = |-\rangle|\mathcal{C}_{i\alpha}^+\rangle\right\}, \tag{1}$$

where the first mode $|\pm\rangle$ represents the polarization of single photon state and the second mode represents even cat states $|\mathcal{C}_\alpha^+\rangle = \mathcal{N}_\mathcal{C}^+(|\alpha\rangle + |-\alpha\rangle)$ with the normalization factor $\mathcal{N}_\mathcal{C}^+ \equiv 1/\sqrt{2(1+e^{-2\alpha^2})}$. The logical basis states become orthogonal due to the DV qubit and single qubit rotations can be done with simple linear optical elements. The Pauli X operation can be implemented by applying bit flip operations on both CV and DV qubits, using a polarization rotator acting as $|+\rangle \leftrightarrow |-\rangle$ and a $\frac{\pi}{2}$ phase shifter acting as $|\mathcal{C}_\alpha^+\rangle \leftrightarrow |\mathcal{C}_{i\alpha}^+\rangle$. The arbitrary rotation along Z axis, Z_θ, can be implemented by a θ phase shifter applied only on the DV qubit as $|+\rangle \to |+\rangle, |-\rangle \to e^{i\theta}|-\rangle$.

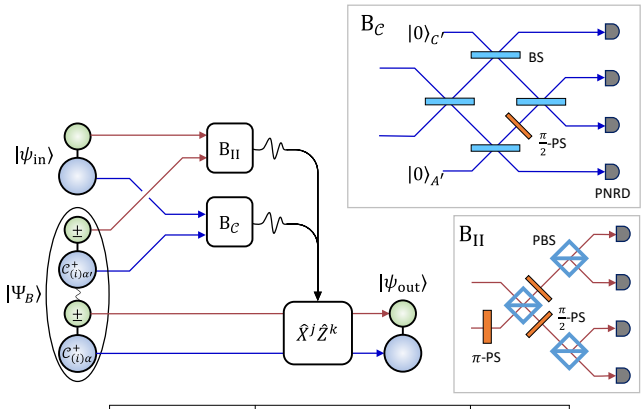
Another technical challenge in the cat code is the realization of parity measurement without disturbing the information encoded in the qubit. Recently, schemes for photon loss correction have been proposed in a telecorrection manner [5, 6]. A single photon loss is detected during the Bell measurement and automatically corrected at the output of teleportation. In our hybrid quantum computation, we devise a hybrid Bell-state measurement (HBSM) which is performed by type II fusion operation of DV qubits and cat-code Bell measurement of CV qubits. Because the success probability of HBSM is close to unity, it enables near-deterministic gate teleportation of H and CZ gates for universal quantum computation. Further, due to the error-correcting feature of cat code, a photon loss is automatically corrected during every teleportation.

We evaluate the performance of quantum computation based on our hybrid qubit. We analyze the fault-tolerance using the simulation with the concatenation of outer error correction codes and show that the performance can be significantly improved [7].

2 Teleportation

The teleportation circuit for hybrid qubits is described in Fig. 1. For HBSM, we perform Bell measurements of DV qubits and CV qubits simultaneously. For DV qubits, we employ type II fusion operation $\mathrm{B_{II}}$ which distinguishes only two types of Bell states with success probability 1/2. For CV qubits, we employ the cat-code Bell measurement $\mathrm{B}_\mathcal{C}$ introduced in Ref. [5]. $\mathrm{B}_\mathcal{C}$ is implemented using linear optical elements and four photon-number-resolving (PNR) detectors. Using the counting statistics of PNR detectors, one can determine which of four Bell states has been measured. In some cases, one cannot perfectly distinguish Bell states, where the failure probability is approximately given by $p_f(\alpha) \approx 2e^{-\alpha^2/2}$. HBSM succeeds if either $\mathrm{B_{II}}$ or $\mathrm{B}_\mathcal{C}$ succeds, and thus the total failure probability $P_f = \frac{1}{2}p_f(\alpha)$, rapidly decays to

*swleego@gmail.com



$B_{\mathcal{C}}$	B_{II}	Operation
$\|\Psi_{\mathcal{C}}^+\rangle$: $j=0,k=0$ $\|\Psi_{\mathcal{C}}^-\rangle$: $j=0,k=1$ $\|\Phi_{\mathcal{C}}^+\rangle$: $j=1,k=0$ $\|\Phi_{\mathcal{C}}^-\rangle$: $j=1,k=1$	(H,H), (H,V), (V,H), (V,V) : Flip k ($0 \leftrightarrow 1$)	$\hat{X}^j\hat{Z}^k$
	Failure: No flip	
Failure	(H,V), (V,H): $j=0,k=1$ (H,H), (V,V): $j=1,k=1$	
	Failure	Failure

Figure 1: The teleportation of hybrid qubits. Green circles and blue circles represent polarization qubits and cat-code qubits, respectively. Bell measurements B_{II} and $B_{\mathcal{C}}$ are performed on the input qubit and the one part of entangled channel. Implementations of B_{II} and $B_{\mathcal{C}}$ are shown in gray boxes. Measurement outcomes are used to determine Pauli operations to be applied on the output qubit as summarized in the table.

0 for large α. Once the measurement outcomes are determined, the teleportation is accomplished by applying Pauli operations on the output qubit, which is summarized in the table of Fig. 1.

The gate teleportation can be accomplished by using appropriate entangled channel. For instance, the Hadamard gate H can be performed using the resource state $|\Phi_H\rangle \propto |0_L,0_L\rangle + |0_L,1_L\rangle + |1_L,0_L\rangle - |1_L,1_L\rangle$ and the CZ gate can be performed with two teleportation circuits using $|\Phi_{CZ}\rangle \propto |0_L,0_L,0_L,0_L\rangle + |0_L,0_L,1_L,1_L\rangle + |1_L,1_L,0_L,0_L\rangle - |1_L,1_L,1_L,1_L\rangle$. The resource states can be generated by merging DV entangled pairs $|H,H\rangle + |V,V\rangle$ and hybrid entangled states $|H\rangle|\mathcal{C}_\alpha^+\rangle + |V\rangle|\mathcal{C}_{i\alpha}^+\rangle$ using $B_{\mathcal{C}}$ or type I fusion operation B_{I}. A hybrid entangled state can be generated by a cross-Kerr interaction between a single photon and an even cat state.

3 Photon loss correction

In ideal case of $B_{\mathcal{C}}$, the total number detected by PNR detectors should be even since the cat code is encoded in the even photon-number space. If a photon is lost from CV qubit, the state is changed to odd cat state, modelled as $\hat{a}|\mathcal{C}_\alpha^+\rangle \propto |\mathcal{C}_\alpha^-\rangle$. In this case, the total number of photon detected by PNR detectors becoms odd, which informs us that a photon loss has been occurred. Despite that, one can determine the Bell state before loss from the photon counting statistics. Since the output port of the entangled channel is prepared in the logical code space, the qubit is recovered to the original input state

(a) `STEANE` code

Logical encoding	Optimal α	Loss threshold
DV+coherent [3]	1.24	0.00029
DV+cat [*this work*]	2.97	0.00116

(b) Topological code

Logical encoding	Optimal α	Loss threshold
DV+coherent [8]	1.66	0.0022
DV+cat [*this work*]	3.45	0.0221

Table 1: Loss threshold for (a) `STEANE` and (b) topological code. We find the optimal encoding amplitude α which yields the highest loss threshold. Note that we recalculate the result of [8] under the same error model for fair comparison.

once the teleportation succeeds. Remarkably, in every teleportation, the photon loss correction is automatically implemented.

If two or more photons are lost on CV qubit, a logical Z error occurs because the teleportation can correct only single photon loss. If DV photon is lost, it is considered as a dephasing error. We denote q as the total Z error rate due to photon loss.

4 Fault-tolerant quantum computation

In our error model, important parameters are the failure probability P_f of HBSM and the Z error rate q, which are given as functions of the loss rate η and the encoding amplitude α. The failure probability P_f is high for small α while q becomes high for large α. Therefore, it is important to take appropriate value of α to obtain high loss threshold.

To investigate the loss threshold for our hybrid qubits, we perform the simulation using two kinds of outer error correction codes: `STEANE` and `topological` error correction code. The result is summarized in Table 1. It is shown that the loss threshold is significantly improved although the cat-code qubit requires twice larger encoding amplitude than that of the coherent-state qubit. For `STEANE` code, the loss threshold is improved by a factor of 4. In the topological error correction, the loss threshold is improved almost by an order of magnitude by employing cat code. The loss threshold of 2.21% is, to the best of our knowledge, the highest threshold for CV encoding of optical qubits [7].

References

[1] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, Hardware-Efficient Autonomous Quantum Memory Protection, Phys. Rev. Lett. **111**, 120501 (2013).

[2] M. Bergmann and P. van Loock, Quantum error correction against photon loss using multicomponent cat states, Phys. Rev. A 94, 042332 (2016).

[3] S.-W. Lee and H. Jeong, Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits, Phys. Rev. A **87**, 022326 (2013).

[4] J. Lee *et al.*, to be submitted (2023).

[5] D. Su, I. Dhand, and T. C. Ralph, Universal quantum computation with optical four-component cat qubits, Phys. Rev. A **106**, 042614 (2022).

[6] J. Hastrup and U. L. Andersen, All-optical cat-code quantum error correction, Phys. Rev. Research **4**, 043065 (2022).

[7] N. Kang *et al.* to be submitted (2023).

[8] S. Omkar, Y. S. Teo, and H. Jeong, Resource-Efficient Topological Fault-Tolerant Quantum Computation with Hybrid Entanglement of Light, Phys. Rev. Lett. **125**, 060501 (2020).

Modeling and physically interpreting dissipative dynamics of a charge qubit-atom hybrid system under the Born-Markov limit

Min Namkung[1] * Jeongsoo Kang[2] † Younghun Kwon[2] ‡

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, Korea*
[2] *Department of Applied Physics, Center for Bionano Intelligence Education and Research, Hanyang University, Ansan, Republic of Korea*

Abstract. In this extended abstract, we describe a dissipative dynamics of the *charge qubit-atom hybrid model* in the Born-Markov limit. Specifically, we focus on the relation between the spectral density of the Boson bath and the dissipation effect on the charge qubit-atom hybrid model. We analytically show that the relaxation and the dephasing noises affects both Josephson junction and the gate capacitor of the model when the spectral density is a *genuine-nonlinear function*. We further numerically show that the nonlinearity of the spectral density results in the rapid destruction of the entanglement in the model.

Keywords: Superconducting circuit, Dissipative dynamics, Master equation, Born-Markov limit, Spectral density, Entanglement

1 Introduction

For several decades, it has been shown that a quantum computer is superior to a classical one in solving certain computational tasks including data search [1, 2], integer factorization [3], and quantum chemistry simulation [4]. For this reasons, realization of the quantum computer is an important feature of the quantum technology. Among several candidates for implementing the novel super computer [5, 6, 7], superconducting circuit has been considered as the most promising one [8]. The superconducting circuit-based quantum computer has advantage of the high-speed computation ability. Also, since a qubit composed of the superconducting circuit is a macroscopic system, the quantum computer composed of the superconducting qubits is flexibly designed and easily tunable [9].

However, the macroscopic scale implies the short coherence time of the superconducting qubit [13, 14]. One way for improving the coherence time of the superconducting qubit is the hybridization with a two-level atom qubit [9, 14, 15, 16]. The *charge qubit-atom hybrid model* [9], which is composed of a charge qubit [10, 11, 12] and a two-level Rydberg atom strongly coupled to each other, is the one example of the hybrid model. It was shown that this model can perform high-speed CNOT operation [9], when it is not exposed to the noise.

In this extended abstract, we describe a dissipative dynamics of the charge qubit-atom hybrid model in terms of the master equation [17, 18, 19, 20]. Specifically, we consider that one Boson bath is interacting with the Josephson junction of the charge qubit, and the other one is interacting with the gate capacitor. In the Born-Markov limit [17], we verify the relation between the spectral density and the dissipation effect on the charge qubit-atom hybrid model. We analytically show that, when the the spectral density is a *nearly linear function*, we can leave the first-order term of the master equation and neglect the high order terms. We note that each Boson bath is separately interacting with the Josephson junction and the gate capacitor, respectively. Meanwhile, in case that the spectral density is a *genuinely nonlinear function*, we need to leave the second-order term of the master equation. This means that both Boson baths are simultaneously interacting with the Josephson junction and the gate capacitor. We further numerically show the dependence of the spectral density and the entanglement. In our case study, the concurrence [21] does not decrease under the certain value in case the the spectral density is nearly linear, but rapidly vanishes in case of the nonlinear spectral density.

The technical details about this extended abstract are presented in J. Opt. Soc. Am. B 39, pp. 2362-2377 (2022).

2 Structure of dissipative dynamics

Here, we propose the structure of the dissipative dynamics for describing noisy charge qubit-atom hybrid model. We begin this by describing the charge qubit-atom hybrid model interacting with Boson bath, and then discuss the methodology to model the dissipative dynamics in terms of the master equation under the Born-Markov limit [17].

2.1 Description of noisy model

We first briefly review the structure of the ideal charge qubit-atom hybrid model. In this model, a two-level Rydberg atom is positioned inside the gate capacitor of the charge qubit. Thus, the two-level Rydberg atom and the charge qubit are interacting each other via the electric field generated inside the gate capacitor. This ideal charge qubit-atom hybrid model is described as the system Hamiltonian [9]

$$\hat{H}_S = \hat{H}_C + \hat{H}_A, \tag{1}$$

where $\hat{H}_C$ and $\hat{H}_A$ are Hamiltonians of the charge qubit and the two-level Rydberg atom, respectively. It is noted

*mnamkung@kist.re.kr
†js.kang1202@gmail.com
‡yyhkwon@hanyang.ac.kr

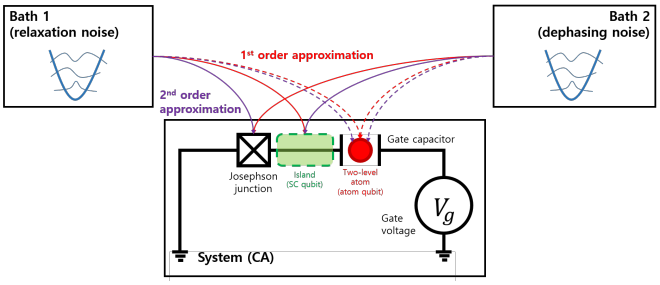


Figure 1: Effect of first- and second-order approximations in charge qubit-atom hybrid model.

that the interaction terms are absorbed in $\hat{H}_C$ and $\hat{H}_A$ of Eq. (1), which means that the charge qubit and the two-level Rydberg atom are strongly interacting each other. Thus, both $\hat{H}_C$ and $\hat{H}_A$ in Eq. (1) are defined on the composite Hilbert space of the charge qubit and two-level Rydberg atom systems.

In our model illustrated as Figure 1, we consider that the Boson bath 1 is interacting with the Josephson junction and the Boson bath 2 is with the gate capacitor. We first describe both two Boson baths as the environment Hamiltonian

$$\hat{H}_S = \hat{H}_{E1} \otimes \hat{\mathbb{I}}^{(e_2)} + \hat{\mathbb{I}}^{(e_1)} \otimes \hat{H}_{E2}, \tag{2}$$

where $\hat{H}_{E1}$ and $\hat{H}_{E2}$ are Hamiltonians of the Boson bath 1 and 2, respectively, and $\hat{\mathbb{I}}^{(e_i)}$ is the identity operator on the Hilbert space of the i-th Boson bath system. Now, we describe the interaction between two Boson baths and the charge qubit-atom hybrid model as the interaction Hamiltonian

$$\hat{H}_I = \hat{\sigma}_x^{(c)} \otimes \hat{\mathbb{I}}^{(a)} \otimes \hat{X}^{(e_1)} \otimes \hat{\mathbb{I}}^{(e_2)} + \hat{\sigma}_z^{(c)} \otimes \hat{\mathbb{I}}^{(a)} \otimes \hat{\mathbb{I}}^{(e_1)} \otimes \hat{X}^{(e_2)}, \tag{3}$$

where $\hat{\mathbb{I}}^{(a)}$ is the identity operator on the Hilbert space of the two-level Rydberg atom, $\hat{X}^{(e_i)}$ is the operator composed of position operators of particles in the i-th Boson bath, and $\hat{\sigma}_x^{(c)}$ and $\hat{\sigma}_z^{(c)}$ are Pauli x and z operators on the charge qubit, respectively. In Eq. (3), $\hat{\sigma}_x^{(c)}$ represents the situation that the number of Cooper pairs accumulated inside the island is changed due to the unexpected current, which can be understood as the *relaxation noise*. $\hat{\sigma}_z^{(c)}$ represents the situation that the Cooper pairs are unexpectedly accumulated between the Josephson capacitor, which can be understood as the *dephasing noise*.

Combining Eqs. (1), (2), and (3), we describe the charge qubit-atom hybrid model interacting with two Boson baths as the entire Hamiltonian

$$\hat{H} = \hat{H}_S + \hat{H}_E + \hat{H}_I. \tag{4}$$

We note that the dissipative dynamics of the charge qubit-atom hybrid begins from describing time evolution of the system and environment states in terms of the Liouville-von Neumann equation with Eq. (4). This will be further discussed in the next subsection.

2.2 Modeling dissipative dynamics

The dissipative dynamics of a quantum system is exactly described in terms of the non-Markovian master equation [23, 24]. However, without certain approximation, the master equation is not efficiently solved because of the convolution terms therein [18]. To avoid the inefficiency, we consider the Born-Markov approximation in which the environment is memoryless and has large scale compared to the charge qubit-atom hybrid model.

We further assume that the density operator of the environment $\hat{\rho}_E$ is express as the thermal state because of the thermal equilibrium [17]. Then, we can apply the method in Ref. [22] to describe the noisy charge qubit-atom hybrid model in terms of the master equation. Since the Hamiltonian in Eq. (4) has complicated form, the interaction picture of $\hat{\sigma}_x^{(c)}$ and $\hat{\sigma}_z^{(c)}$ in Eq. (3) takes the form of infinite series. Thus, we describe the dissipative dynamics as the Born-Markov master equation including infinite series,

$$\begin{aligned}
\frac{d}{dt}\hat{\rho}_S(t) = &-\frac{i}{\hbar}[\hat{H}_S, \hat{\rho}_S(t)] \\
&+ \frac{iC_j\gamma_1\Omega}{\hbar}\sum_{n=0}^{\infty}\frac{n!}{\Omega^n}\left[\hat{A}_1, \left\{\xi_n[\hat{A}_1], \hat{\rho}_S(t)\right\}\right] \\
&- \frac{C_j\gamma_1\omega_0}{\hbar}\sum_{n=0}^{\infty}\frac{n!}{\Omega^n}\left[\hat{A}_1, \left[\xi_n[\hat{A}_1], \hat{\rho}_S(t)\right]\right] \\
&+ \frac{iC_g\gamma_2\Omega}{\hbar}\sum_{n=0}^{\infty}\frac{n!}{\Omega^n}\left[\hat{A}_2, \left\{\xi_n[\hat{A}_2], \hat{\rho}_S(t)\right\}\right] \\
&- \frac{C_g\gamma_2\omega_0}{\hbar}\sum_{n=0}^{\infty}\frac{n!}{\Omega^n}\left[\hat{A}_2, \left[\xi_n[\hat{A}_2], \hat{\rho}_S(t)\right]\right],
\end{aligned} \tag{5}$$

with the interaction strength γ_i with respect to the i-th Boson bath, the resonant frequency of the charge qubit ω_0 [20, 22], and $\hat{A}_1 = \hat{\sigma}_x^{(c)} \otimes \hat{\mathbb{I}}^{(a)}$ and $\hat{A}_2 = \hat{\sigma}_z^{(c)} \otimes \hat{\mathbb{I}}^{(a)}$. In the above master equation, coefficient $\xi[\hat{A}_i]$ is the coefficient in the interaction picture [17, 22] of $\hat{A}_i$.

3 Analytical result

In this section, we discuss the analytical results about the relation between the property of the spectral density in Eq. (6) and the dissipative dynamics.

We note that the dissipation on the charge qubit-atom hybrid model occurred by the infinite number of the particles in the i-th Boson bath can be effectively described in terms of the spectral density having the form of the Lorentz-Drude cutoff function [17],

$$J_i(\omega) = \gamma_i \frac{\omega\Omega^2}{\omega^2 + \Omega^2} \tag{6}$$

with the cutoff frequency Ω. If Ω is sufficiently large compared to ω, then the spectral density in Eq. (6) is approximated as

$$J_i(\omega) \approx \gamma_i\omega. \tag{7}$$

In this case, we call the spectral density as *nearly linear*. If Ω is not sufficiently large, Eq. (6) is not approximated as a linear function. In this case, we call it as *genuine-nonlinear*.

Now, we relate the property of the spectral density in Eq. (6) discussed above and the dissipative dynamics

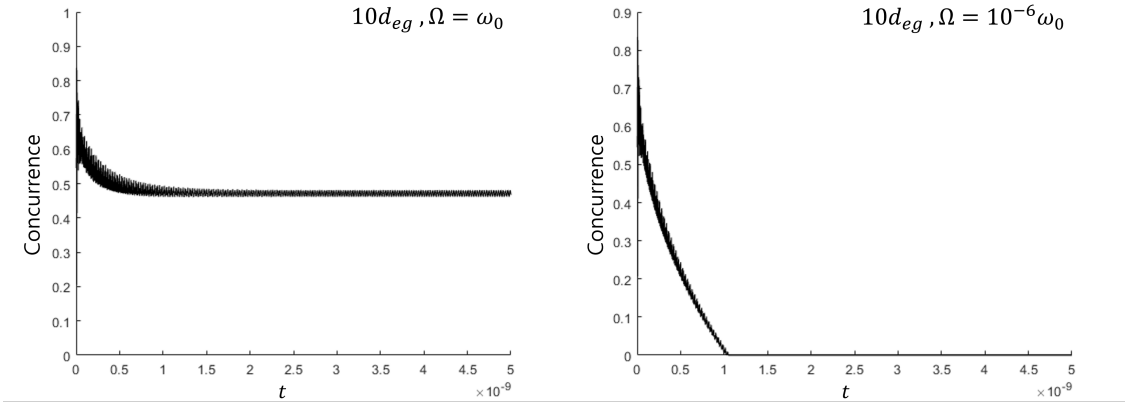


Figure 2: Concurrence of charge qubit-atom hybrid model. Here, the cutoff frequency is considered as $\Omega = \omega_0$ or $\Omega = 10^{-6}\omega_0$ with the resonant frequency ω_0.

described in Eq. (5), with respect to the scale of Ω. In case of $\Omega \gg \omega$, the high-order terms of Ω^{-1} in Eq. (5) can be neglected. Thus, Eq. (5) is approximated as

$$\begin{aligned}\frac{d}{dt}\hat{\rho}_S(t) = &-\frac{i}{\hbar}[\hat{H}_S, \hat{\rho}_S(t)] \\ &+ \frac{iC_j\gamma_1\Omega}{\hbar}\sum_{n=0,1}\frac{n!}{\Omega^n}\left[\hat{A}_1, \left\{\xi_n[\hat{A}_1], \hat{\rho}_S(t)\right\}\right] \\ &- \frac{C_j\gamma_1\omega_0}{\hbar}\sum_{n=0,1}\frac{n!}{\Omega^n}\left[\hat{A}_1, \left[\xi_n[\hat{A}_1], \hat{\rho}_S(t)\right]\right] \\ &+ \frac{iC_g\gamma_2\Omega}{\hbar}\sum_{n=0,1}\frac{n!}{\Omega^n}\left[\hat{A}_2, \left\{\xi_n[\hat{A}_2], \hat{\rho}_S(t)\right\}\right] \\ &- \frac{C_g\gamma_2\omega_0}{\hbar}\sum_{n=0,1}\frac{n!}{\Omega^n}\left[\hat{A}_2, \left[\xi_n[\hat{A}_2], \hat{\rho}_S(t)\right]\right], \quad (8)\end{aligned}$$

From the form of the above approximated master equation, we observe that the Boson bath 1 and 2 affect the gate capacitor (or island, equivalently) and the Josephson junction, respectively (see Figure 1). We further note that the above master equation can be simplified by diagonalizing the two corresponding Kossakowski matrices κ_1 and κ_2. Since these matrices are degenerate, the master equation in Eq. (8) has one approximated Lindblad form [25]. This means that, as the spectral density in Eq. (6) is linear, the dissipative dynamics described in terms of the Lindblad form is stable.

When Ω is not sufficiently large compared with ω, the second-order term of Ω^{-1} in Eq. (5) can affect the dissipative dynamics of the interested system [22]. In this case, we observe that the Boson bath 1 and 2 simultaneously affect the gate capacitor (or island, equivalently) and the Josephson junction. Furthermore, the Kossakowski matrices of the second-order master equation are degenerate. In other words, the approximated Lindblad form is not unique. This means that the dissipative dynamics is not stable.

4 Numerical result

We further numerally investigate the relation between the spectral density and the entanglement dynamics.

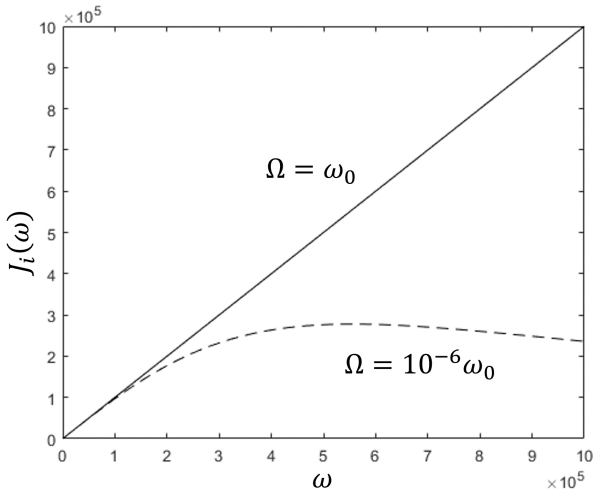


Figure 3: Concurrence of charge qubit-atom hybrid model. Here, the cutoff frequency is considered as $\Omega = \omega_0$ or $\Omega = 10^{-6}\omega_0$ with the resonant frequency ω_0.

Here, we consider the charge qubit-atom hybrid model with parameters in Ref. [9]. We first solve the 1st-order Lindblad equation [26] approximated from Eq. (5) using 4th Runge-Kutta method. Then, we evaluate the concurrence for each time from the solution.

We illustrate the entanglement dynamics as Figure 2. Here, we consider that the cutoff frequency Ω in the spectral density of Eq. (6) is equal to the resonant frequency ω_0 or $10^{-6}\omega_0$. We observe from Figure 2 that the concurrence does not decrease below 0.5 when $\Omega = \omega_0$, but rapidly decreases to zero when $\Omega = 10^{-6}\omega_0$.

We further illustrate the spectral density as Figure 3. When $\Omega = \omega_0$, we observe that the spectral density is approximated as a linear function. Meanwhile, when $\Omega = 10^{-6}\omega_0$, the spectral density is a genuine-nonlinear function. From Figure 3 together with Figure 2, we observe that the entanglement is preserved against the dissipation effect of Figure 1 when the spectral density is a nearly-linear function, but rapidly vanishes when the spectral density is a genuine-nonlinear function.

Acknowledgement

This work(J.K and Y.K) is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF2022R1F1A1064459) and Creation of the Quantum Information Science R&D Ecosystem (Grant No. 2022M3H3A106307411) through the National Research Foundation of Korea (NRF) funded by the Korean government (Ministry of Science and ICT. M.N. acknowledges support from the National Research Foundation of Korea (NRF) grant funded by the Korean government (Ministry of Science and ICT) (NRF2020M3E4A1080088).

References

[1] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th ACM STOC*, pages 212–219, 1996.

[2] J. Bae and Y. Kwon. Maximum speedup in quantum search. International Journal of Theoretical Physics **42**, pp. 2069-2074 (2002).

[3] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Comp.*, 26(5):1484–1509, 1997.

[4] P. J. O'Malley *et al.* Scalable quantum simulation of molecular energies. Physical Review X **6**, 031007 (2016).

[5] J. I. Cirac and P. Zoller. Quantum Computation with Cold Trapped Ions. Physical Review Letter **74**, 4091 (1995).

[6] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. Physical Review A **57**, 120 (1998).

[7] T. Xin *et al.* Nuclear magnetic resonance for quantum computing: Techniques and recent achievements. Chinese Physics B **27**, 020308 (2018).

[8] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver. A quantum engineer's guide to superconducting qubits. Applied Physical Reviews **6**, 021318 (2019).

[9] D. Yu, M. M.Valado, C. Hufnagel, L. C. Kwek, L. Amico, and R. Dumke. Charge qubit-atom hybrid. Physical Review A **93**, 042329 (2016).

[10] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-Cooper-pair box. Nature **398**, pp. 78-788 (1999).

[11] Y. A. Pashkin, O. Astafiev, T. Yamamoto, Y. Nakamura, and J. S. Tsai. Josephson charge qubits: a brief review. Quantum Information Processing **8**, pp. 55-80 (2009).

[12] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, and M. H. Devoret. Quantum coherence with a single Cooper pair. Physica Scripta **1998**, 165 (1998).

[13] Y. Makhlin, G. Schon, and A. Shnirman. Quantum-state engineering with Josephson-junction devices. Review Modern Physics **73**, 357 (2001).

[14] Z.-L. Xiang, S. Ashhab, J. Q. You, and F. Nori. Hybrid quantum circuits: Superconducting circuits interacting with other quantum systems. Review Modern Physics **85**, 623 (2013).

[15] D. Yu, A. Landra, M. M. Valado, C. Hufnagel, L. C. Kwek, L. Amico, and R. Dumke. Superconducting resonator and Rydberg atom hybrid system in the strong coupling regime. Physical Review A **94**, 062301 (2016).

[16] D. Yu, L. C. Kwek, L. Amico, and R. Dumke. Superconducting qubit-resonator-atom hybrid system. Quantum Science and Technology **2**, 035005 (2017).

[17] M. A. Schlosshauer. Decoherence and the Quantum-to-Classical Transition. *Springer*, 2007.

[18] H.-P. Breuer and F. Petruccione. The Theory of Open Quantum Systems. *Oxford University Press*, 2007.

[19] U. Swiss. Quantum Dissipative Systems. *World Scientific*, 2012.

[20] A. M. Zagoskin. Quantum Engineering: Theory and Design of Quantum Coherent Structures. *Cambridge University Press*, 2011.

[21] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. Physical Review Letter **80**, 2245 (1998).

[22] S. N. A. Duffus et al. Some implications of superconducting quantum interference to the application of master equations in engineering quantum technologies. Physical Review B **94**, 064518 (2016).

[23] S. Nakajima. On quantum theory of transport phenomena: steady diffusion. Prgress on Theoretical Physics **20**, pp. 948-959 (1958).

[24] R. Zwanzig. Ensemble method in the theory of irreversibility. Journal of Chemical Physics **33**, pp. 1338-1341 (1960).

[25] G. Lindblad. On the generators of quantum dynamical semigroups. Communication of Mathematical Physics **48**, pp. 119-130 (1976).

[26] We note that the solution of the Lindblad equation is always the density operator [27].

[27] A. Livas and S. F. Huelga. Open Quantum Systems. *Springer*, 2012.

Bound on local minimum-error discrimination of bipartite quantum states

Donghoon Ha[1] Jeong San Kim[1] *

[1] *Department of Applied Mathematics and Institute of Natural Sciences, Kyung Hee University, Yongin 17104, Republic of Korea*

Abstract. We consider the optimal discrimination of bipartite quantum states and provide an upper bound for the maximum success probability of optimal local discrimination. We also provide a necessary and sufficient condition for a measurement to realize the upper bound. We further establish a necessary and sufficient condition for this upper bound to be saturated. Finally, we illustrate our results using an example.

Keywords: minimum-error discrimination, bipartite quantum states, upper bound

Quantum state discrimination is one of the fundamental tasks in quantum information processing [1–3]. In discriminating orthogonal quantum states, there is always a measurement of perfect discrimination. On the other hand, non-orthogonal quantum states cannot be perfectly discriminated by means of any measurement. For this reason, there has been a huge amount of research effort focused on finding good state-discriminating strategies [4].

In discriminating multiparty quantum states, it is known that some optimal state discrimination cannot be realized only by *local operations and classical communication* (LOCC) [5–8]. To characterize the limitation of LOCC discrimination, many studies have been contributed to optimal local discrimination of multiparty quantum states [9–15]. Nevertheless, due to the difficulty of mathematical characterization for LOCC, it is still a hard task to realize optimal local discrimination.

One efficient way to handle this difficulty is to investigate possible upper bounds for the maximum success probability of optimal local discrimination. Moreover, establishing good conditions on measurements realizing such upper bounds is also important for a better understanding of optimal local discrimination.

Here, we consider bipartite quantum state discrimination and provide an upper bound for the maximum success probability of optimal local discrimination [16]. We also provide a necessary and sufficient condition for a measurement to realize the upper bound. Moreover, we establish a necessary and sufficient condition for this upper bound to be saturated; it is equal to the maximum success probability of optimal local discrimination. Finally, we illustrate our results using an example [16].

Let us consider the situation of discriminating n *bipartite* quantum states $\rho_1, \ldots, \rho_n$ in which the state ρ_i is prepared with the probability η_i. We denote this situation as an ensemble,

$$\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n. \tag{1}$$

We use $p_{\mathrm{G}}(\mathcal{E})$ to denote the optimal success probability in the *minimum-error discrimination* [17–19] of $\mathcal{E}$.

$$p_{\mathrm{G}}(\mathcal{E}) = \max_{\text{Measurement}} \sum_{i=1}^n \eta_i \mathrm{Tr}(\rho_i M_i), \tag{2}$$

where the maximum is taken over all possible measurement. The measurements providing the optimal success probability $p_{\mathrm{G}}(\mathcal{E})$ can be verified from the following conditions [18–21]:

$$\sum_{j=1}^n \eta_j \rho_j M_j - \eta_i \rho_i \succeq 0 \ \forall i = 1, \ldots, n, \tag{3a}$$

$$M_i(\eta_i \rho_i - \eta_j \rho_j) M_j = 0 \ \forall i, j = 1, \ldots, n. \tag{3b}$$

Note that Condition (3a) is a necessary and sufficient condition for a measurement $\{M_i\}_{i=1}^n$ to realize $p_{\mathrm{G}}(\mathcal{E})$, whereas Condition (3b) is a necessary but not sufficient condition for a measurement $\{M_i\}_{i=1}^n$ to provide $p_{\mathrm{G}}(\mathcal{E})$.

Definition 1 *A Hermitian operator E on $\mathcal{H}$ is called* positive-partial-transpose*(PPT) if its partial transposition, denoted E^{PT}, is positive semidefinite [22–24]. Similarly, we say that a set of Hermitian operators $\{E_i\}_i$ is PPT if E_i is PPT for all i.*

When the available measurements are limited to PPT measurements, we denote the maximum success probability by

$$p_{\mathrm{PPT}}(\mathcal{E}) = \max_{\substack{\mathrm{PPT} \\ \text{measurement}}} \sum_{i=1}^n \eta_i \mathrm{Tr}(\rho_i M_i). \tag{4}$$

We denote by $p_{\mathrm{L}}(\mathcal{E})$ the maximum of success probability that can be obtained by using LOCC measurements; that is,

$$p_{\mathrm{L}}(\mathcal{E}) = \max_{\substack{\mathrm{LOCC} \\ \text{measurement}}} \sum_{i=1}^n \eta_i \mathrm{Tr}(\rho_i M_i). \tag{5}$$

From the definitions of $p_{\mathrm{G}}(\mathcal{E})$ and $p_{\mathrm{PPT}}(\mathcal{E})$, $p_{\mathrm{G}}(\mathcal{E})$ is obviously an upper bound of $p_{\mathrm{PPT}}(\mathcal{E})$. Moreover, $p_{\mathrm{L}}(\mathcal{E})$ is a lower bound of $p_{\mathrm{PPT}}(\mathcal{E})$ because all LOCC measurements are PPT [25]. Thus, we have

$$p_{\mathrm{L}}(\mathcal{E}) \leqslant p_{\mathrm{PPT}}(\mathcal{E}) \leqslant p_{\mathrm{G}}(\mathcal{E}). \tag{6}$$

*freddie1@khu.ac.kr

We also note that $p_{\rm L}(\mathcal{E}) = p_{\rm PPT}(\mathcal{E})$ if and only if there exists a LOCC measurement realizing $p_{\rm PPT}(\mathcal{E})$ since both $p_{\rm PPT}(\mathcal{E})$ and $p_{\rm L}(\mathcal{E})$ have the same objective function for maximization.

Definition 2 *For a given ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$, let us consider the maximum quantity*

$$q_{\rm G}(\mathcal{E}) = \max_{\text{Measurement}} \sum_{i=1}^n \eta_i {\rm Tr}(\rho_i^{\rm PT} M_i) \tag{7}$$

over all possible measurements.

The following lemma shows that $q_{\rm G}(\mathcal{E})$ in Eq. (7) is an upper bound of $p_{\rm PPT}(\mathcal{E})$:

Lemma 3 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$,*

$$p_{\rm PPT}(\mathcal{E}) \leqslant q_{\rm G}(\mathcal{E}), \tag{8}$$

where the equality holds if and only if there exists a PPT measurement providing $q_{\rm G}(\mathcal{E})$.

Corollary 4 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$,*

$$p_{\rm L}(\mathcal{E}) = q_{\rm G}(\mathcal{E}) \tag{9}$$

if and only if there exists a LOCC measurement $\{M_i\}_{i=1}^n$ satisfying

$$\sum_{i=1}^n \eta_i \, {\rm Tr}(\rho_i M_i) = q_{\rm G}(\mathcal{E}). \tag{10}$$

For a given state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$, the following theorem provides a necessary and sufficient condition on a measurement $\{M_i\}_{i=1}^n$ to realize $q_{\rm G}(\mathcal{E})$ in Eq. (7).

Theorem 5 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$ and a measurement $\{M_i\}_{i=1}^n$,*

$$\sum_{i=1}^n \eta_i \, {\rm Tr}(\rho_i^{\rm PT} M_i) = q_{\rm G}(\mathcal{E}) \tag{11}$$

if and only if

$$\sum_{j=1}^n \eta_j \rho_j^{\rm PT} M_j - \eta_i \rho_i^{\rm PT} \succeq 0 \ \forall i = 1, \ldots, n. \tag{12}$$

Moreover, if Eq. (11) holds, then

$$M_i(\eta_i \rho_i^{\rm PT} - \eta_j \rho_j^{\rm PT}) M_j = 0 \ \forall i, j = 1, \ldots, n. \tag{13}$$

From Corollary 4 and Theorem 5, we have the following corollary.

Corollary 6 *For a bipartite quantum state ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_{i=1}^n$,*

$$p_{\rm L}(\mathcal{E}) = q_{\rm G}(\mathcal{E}) \tag{14}$$

if and only if there exists a LOCC measurement $\{M_i\}_{i=1}^n$ satisfying

$$\sum_{j=1}^n \eta_j \rho_j^{\rm PT} M_j^{\rm PT} - \eta_i \rho_i^{\rm PT} \succeq 0 \ \forall i = 1, \ldots, n. \tag{15}$$

In this case, Eq. (10) holds.

Example 1 *For any integer $d \geqslant 2$, let us consider the two-qudit state ensemble $\mathcal{E} = \{\eta_{i,j}^{(k)}, \rho_{i,j}^{(k)}\}_{i,j,k}$ consisting of $2d(d-1)$ states with equal prior probability,*

$$\eta_{i,j}^{(k)} = \frac{1}{2d(d-1)}, \ \rho_{i,j}^{(k)} = \lambda |\Psi_{i,j}^{(k)}\rangle\langle\Psi_{i,j}^{(k)}| + (1-\lambda)\sigma,$$
$$i, j \in \{0, 1, \ldots, d-1\} \text{ with } i < j, \ k = 1, 2, 3, 4, \tag{16}$$

where $0 < \lambda \leqslant 1$, σ is an arbitrary two-qudit state, and

$$\begin{aligned}
|\Psi_{i,j}^{(1)}\rangle &= \frac{1}{\sqrt{2}}(|i\rangle \otimes |i\rangle + |j\rangle \otimes |j\rangle), \\
|\Psi_{i,j}^{(2)}\rangle &= \frac{1}{\sqrt{2}}(|i\rangle \otimes |i\rangle - |j\rangle \otimes |j\rangle), \\
|\Psi_{i,j}^{(3)}\rangle &= \frac{1}{\sqrt{2}}(|i\rangle \otimes |j\rangle + |j\rangle \otimes |i\rangle), \\
|\Psi_{i,j}^{(4)}\rangle &= \frac{1}{\sqrt{2}}(|i\rangle \otimes |j\rangle - |j\rangle \otimes |i\rangle).
\end{aligned} \tag{17}$$

For a measurement $\{M_{i,j}^{(k)}\}_{i,j,k}$ with

$$\begin{aligned}
M_{i,j}^{(1)} &= \frac{1}{d-1}|\Psi_{i,j}^{(1)}\rangle\langle\Psi_{i,j}^{(1)}|, \ M_{i,j}^{(3)} = |\Psi_{i,j}^{(3)}\rangle\langle\Psi_{i,j}^{(3)}|, \\
M_{i,j}^{(2)} &= \frac{1}{d-1}|\Psi_{i,j}^{(2)}\rangle\langle\Psi_{i,j}^{(2)}|, \ M_{i,j}^{(4)} = |\Psi_{i,j}^{(4)}\rangle\langle\Psi_{i,j}^{(4)}|,
\end{aligned} \tag{18}$$

Condition (3a) holds, that is,

$$\begin{aligned}
&\sum_{i',j',k'} \eta_{i',j'}^{(k')} \rho_{i',j'}^{(k')} M_{i',j'}^{(k')} - \eta_{i,j}^{(k)} \rho_{i,j}^{(k)} \\
=&\frac{\lambda}{2d(d-1)}\left(\mathbb{1} - |\Psi_{i,j}^{(k)}\rangle\langle\Psi_{i,j}^{(k)}|\right) \succeq 0, \ \forall i, j, k.
\end{aligned} \tag{19}$$

Therefore, the optimal success probability $p_{\rm G}(\mathcal{E})$ is

$$p_{\rm G}(\mathcal{E}) = \sum_{i,j,k} \eta_{i,j}^{(k)} {\rm Tr}(\rho_{i,j}^{(k)} M_{i,j}^{(k)}) = \frac{1 + \lambda(d^2-1)}{2d(d-1)}. \tag{20}$$

For a measurement $\{M_{i,j}^{(k)}\}_{i,j,k}$ with

$$\begin{aligned}
M_{i,j}^{(1)} &= \frac{1}{d-1}|i\rangle\langle i| \otimes |i\rangle\langle i|, \ M_{i,j}^{(3)} = |i\rangle\langle i| \otimes |j\rangle\langle j|, \\
M_{i,j}^{(2)} &= \frac{1}{d-1}|j\rangle\langle j| \otimes |j\rangle\langle j|, \ M_{i,j}^{(4)} = |j\rangle\langle j| \otimes |i\rangle\langle i|.
\end{aligned} \tag{21}$$

Condition (15) holds, that is,

$$\begin{aligned}
&\sum_{i',j',k'} \eta_{i',j'}^{(k')} \rho_{i',j'}^{(k')\ {\rm PT}} M_{i',j'}^{(k')\ {\rm PT}} - \eta_{i,j}^{(k)} \rho_{i,j}^{(k)\ {\rm PT}} \\
=&\frac{\lambda}{4d(d-1)}\left(\mathbb{1} - \mathbb{1}_{i,j} + 2|\Psi_{i,j}^{(5-k)}\rangle\langle\Psi_{i,j}^{(5-k)}|\right) \succeq 0 \ \forall i, j, k,
\end{aligned} \tag{22}$$

where

$$\mathbb{1}_{i,j} = (|i\rangle\langle i| + |j\rangle\langle j|) \otimes (|i\rangle\langle i| + |j\rangle\langle j|). \tag{23}$$

Moreover, the measurement $\{M_{i,j}^{(k)}\}_{i,j,k}$ in Eq. (21) is a LOCC measurement since it can be implemented by performing the same local measurement $\{|l\rangle\langle l|\}_{l=0}^{d-1}$ on two subsystems. Thus, Corollary 6 and Eq. (20) lead us to

$$\begin{aligned}
p_{\rm L}(\mathcal{E}) &= q_{\rm G}(\mathcal{E}) = \sum_{i,j,k} \eta_{i,j}^{(k)} {\rm Tr}(\rho_{i,j}^{(k)} M_{i,j}^{(k)}) \\
&= \frac{2 + \lambda(d^2-2)}{4d(d-1)} = p_{\rm G}(\mathcal{E}) - \frac{\lambda d}{4(d-1)}.
\end{aligned} \tag{24}$$

In the case of $d = 2$, Eqs. (20) and (24) coincide with the existing results in Ref. [15].

We note that finding $p_{\rm G}(\mathcal{E})$ or $q_{\rm G}(\mathcal{E})$ in discriminating separable quantum states can be useful in studying the nonlocal phenomenon of separable quantum states, namely *nonlocality without entanglement*(NLWE) [5, 6]. For the minimum-error discrimination of a separable state ensemble $\{\eta_i, \rho_i\}_{i=1}^n$, NLWE occurs if the guessing probability $p_{\rm G}(\mathcal{E})$ cannot be achieved only by LOCC, that is, $p_{\rm L}(\mathcal{E}) < p_{\rm G}(\mathcal{E})$. From Lemma 3 and Inequality (6), $q_{\rm G}(\mathcal{E}) < p_{\rm G}(\mathcal{E})$ implies $p_{\rm L}(\mathcal{E}) < p_{\rm G}(\mathcal{E})$, therefore the occurrence of NLWE. Moreover, even if $q_{\rm G}(\mathcal{E}) > p_{\rm G}(\mathcal{E})$, we can show the NLWE phenomenon in terms of $\{\eta_i, \rho_i^{\rm PT}\}_{i=1}^n$ because the partial transposition of any separable state is another separable state and the roles of $p_{\rm G}(\mathcal{E})$ and $q_{\rm G}(\mathcal{E})$ are interchanged for the minimum-error discrimination of $\{\eta_i, \rho_i^{\rm PT}\}_{i=1}^n$.

It is an interesting future work to investigate good conditions of optimal local discrimination in multiparty quantum systems having more than two parties. It is also natural to ask if our results are still valid for other optimal discrimination strategies other than minimum-error discrimination.

References

[1] A. Chefles. Quantum state discrimination. *Contemp. Phys.* 41: 401, 2000.

[2] S. M. Barnett and S. Croke. Quantum state discrimination. *Adv. Opt. Photon.* 1: 238, 2009.

[3] J. A. Bergou. Discrimination of quantum states. *J. Mod. Opt.* 57: 160, 2010.

[4] J. Bae and L.-C. Kwek. Quantum state discrimination and its applications. *J. Phys. A: Math. Theor.* 48: 083001, 2015.

[5] A. Peres and W. K. Wootters. Optimal detection of quantum information. *Phys. Rev. Lett.* 66: 1119, 1991.

[6] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin and W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A* 59: 1070, 1999.

[7] R. Duan, Y. Feng, Z. Ji and M. Ying. Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication. *Phys. Rev. Lett.* 98: 230502, 2007.

[8] E. Chitambar and M.-H. Hsieh. Revisiting the optimal detection of quantum information. *Phys. Rev. A* 88: 020302(R), 2013.

[9] S. Ghosh, G. Kar, A. Roy, A. Sen(De) and U. Sen. Distinguishability of Bell states. *Phys. Rev. Lett.* 87: 277902, 2001.

[10] J. Walgate and L. Hardy. Nonlocality, asymmetry, and distinguishing bipartite states. *Phys. Rev. Lett.* 89: 147901, 2002.

[11] H. Fan. Distinguishability and indistinguishability by local operations and classical communication. *Phys. Rev. Lett.* 92: 177905, 2004.

[12] R. Duan, Y. Feng, Y. Xin and M. Ying. Distinguishability of quantum states by separable operations. *IEEE Trans. Inf. Theory* 55: 1320, 2009.

[13] E. Chitambar, R. Duan and M.-H. Hsieh. When do local operations and classical communication suffice for two-qubit state discrimination? *IEEE Trans. Inf. Theory* 60: 1549, 2014.

[14] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous and N. Yu. Limitations on separable measurements by convex optimization. *IEEE Trans. Inf. Theory* 61: 3593, 2015.

[15] S. Bandyopadhyay and V. Russo. Entanglement cost of discriminating noisy Bell states by local operations and classical communication. *Phys. Rev. A* 104: 032429, 2021.

[16] D. Ha and J.S. Kim. Bound on local minimum-error discrimination of bipartite quantum states. *Phys. Rev. A* 105: 032421, 2022.

[17] C. W. Helstrom. Quantum detection and estimation theory. *J. Stat. Phys.* 1: 231, 1969.

[18] A. S. Holevo. Remarks on Optimal Quantum Measurements. *Probl. Peredachi Inf.* 10: 51, 1974.

[19] H. Yuen, R. Kennedy and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theory* 21: 125, 1975.

[20] S. M. Barnett and S. Croke. On the conditions for discrimination between quantum states with minimum error. *J. Phys. A: Math. and Theor.* 42: 062001, 2009.

[21] J. Bae. Structure of minimum-error quantum state discrimination. *New J. Phys.* 15: 073037, 2013.

[22] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.* 77: 1413, 1996.

[23] M. Horodecki, P. Horodecki and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* 223: 1, 1996.

[24] PPT property does not depend on the choice of basis or the subsystem to be transposed. For simplicity, we consider the standard basis and the second subsystem throughout this paper.

[25] E. Chitambar, D. Leung, L. Mančinska, M. Ozols and A. Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Commun. Math. Phys.* 328: 303, 2014.

Continuous-Variable Nonclassicality Detection under Coarse-Grained Measurement

Chan Roh[1] * Young-Do Yoon[1] † Jiyong Park[2] ‡ Young-Sik Ra[1] §

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*
[2] *School of Basic Sciences, Hanbat National University, Daejeon 34158, Korea*

Abstract. We experimentally detect the nonclassicality of continuous-variable quantum states under coarse-grained measurement. Furthermore, we show that the coarse-grained measurement generally outperforms the ideal fine-grained measurement in nonclassicality detection.

Keywords: continuous-variable quantum information, nonclassicality, coarse-grained detection

A continuous-variable (CV) quantum state of light is a fundamental quantum resource for quantum information technologies. For example, a single mode CV quantum state can make quantum enhancement in quantum parameter estimation [1] and quantum key distribution [2]. Moreover, a single mode quantum state is utilized to construct quantum entanglement [3]. To exploit the experimentally generated CV quantum state for quantum information technologies in practice, it is essential to confirm the nonclassicality of the state.

The nonclassicality can be detected by performing quantum state tomography (QST), but QST needs informationally complete measurements and a complicated reconstruction process [4]. Otherwise, high-order moments [5] or a characteristic function method [6] can be used to detect nonclassicality with only a single quadrature measurement. These methods however require substantial data to achieve sufficient statistical significance. Even worse, all of these methods face *false-positive* detection of nonclassicality under *coarse-grained measurement* [7], where nearby measurement outcomes are grouped as a single bin and produce the same result. Coarse graining commonly occurs in realistic quantum measurement, so reliable nonclassicality criteria compatible with coarse-grained measurement is essential in real experiments.

In this work [8], we present experiments that reliably detect the nonclassicality of quantum states under coarse-grained homodyne detection. Furthermore, our method with coarse-grained effect detects the nonclassicality more efficiently than the well-known normally ordered moments method [5] even with fine-grained homodyne detection.

Our nonclassicality test considers a single-quadrature probability distribution $P(x)$ of a quantum state. A nonclassicality test can be conducted by noticing that the probability distribution of any classical state cannot have a narrower structure than a coherent state because any classical state can be expressed as a statistical sum of coherent states. $R(s) = P(s)P(-s)e^{s^2}/P(0)^2$ allows us to compare the width of the probability distribution of a given state with a coherent state. Specifically, $R < 1$ implies that the probability distribution has a narrower structure than a coherent state, i.e., the state is nonclassical [9]. This test can be adapted for coarse-grained measurement:

$$\mathcal{R} = \frac{C_d C_{-d}}{C_0^2} e^{\sigma^2 d^2}. \tag{1}$$

C_m represents the count of measurement outcomes in a range of $[(m-1/2)\sigma, (m+1/2)\sigma]$ with a bin size σ. $\mathcal{R} < 1$ certifies the nonclassicality of a given CV state. This test uses counts of three bins from coarse-grained data, so we call this nonclassicality test a *three-bin test*.

We experimentally demonstrate the three-bin test on squeezed vacuum states with various phase diffusions. Our experimental setup is shown in Fig. 1. We use a 2-mm-thick BiBO crystal for type-I spontaneous parametric down-conversion in the synchronously pumped optical parametric oscillator (SPOPO). SPOPO generates squeezed light in the below-threshold condition, and we add the Gaussian phase noise. We measure the $\hat{x}$ (squeezing) quadrature data of phase-diffused squeezed vacuum by homodyne detection.

Fig. 2 (a) shows the three-bin test conducted using the coarse-grained $\hat{x}$ quadrature data obtained by the experiment. The hatched three bins are selected, obtaining the $\mathcal{R} = 0.62 \pm 0.05 < 1$, where $d = 3$ and $\sigma = 0.5$. This result implies that the three-bin test detects nonclassicality of phase-diffused squeezed vacuum. To optimize this three-bin test, we fix d, and change σ to check the effect of bin size. In Fig. 2 (b), $\mathcal{R} = 0.60 \pm 0.05 < 1$ at $\sigma = 0.55$ gives the smallest $\mathcal{R}$ value, where the bin size is optimized for the $d = 3$ case. We also check the performance of the three-bin test compared with the conven-

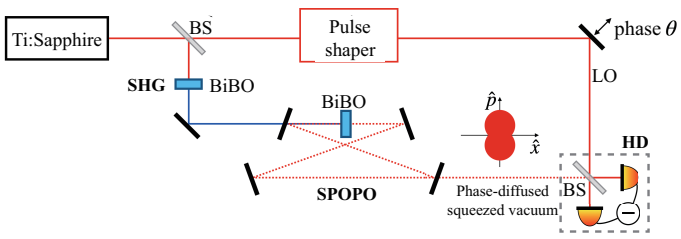


Figure 1: Experiment setup.

*croh@kaist.ac.kr
†yoon_yd@kaist.ac.kr
‡jiyong.park@hanbat.ac.kr
§youngsikra@gmail.com

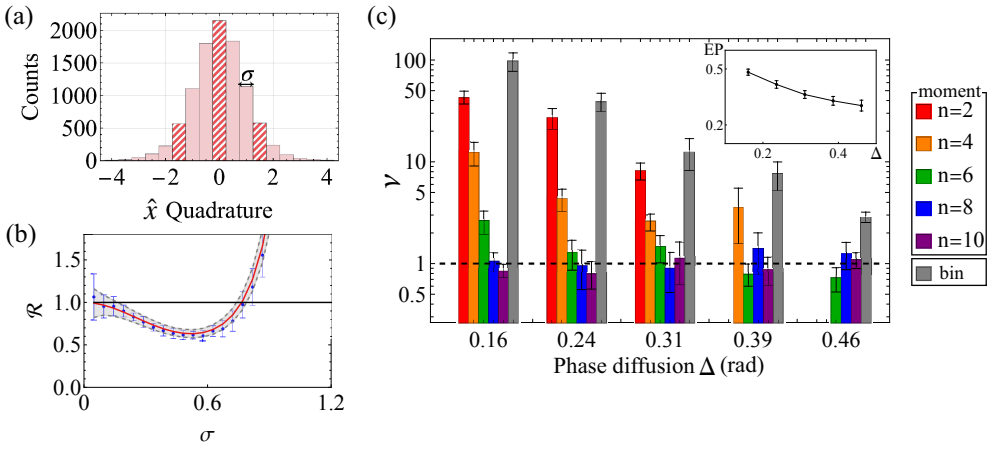


Figure 2: (a) Three-bin test with coarse-grained quadrature data of the phase-diffused squeezed vacuum. (b) Effect of the bin size on three-bin test. (c) Performance comparison between the moment method (moment) and three-bin test (bin).

tional higher-order moment method. A violation degree $\mathcal{V}$ is defined as the ratio between the distance from the classical limit and its standard deviation on each method. A positive $\mathcal{V}$ shows the detection of nonclassicality, and the larger positive $\mathcal{V}$ denotes the strong statistical significance of nonclassicality detection. In Fig. 2 (c), the three-bin test always outperforms the moment method with fine-graining detection. Moreover, the three-bin test reliably detects nonclassicality in the range of phase diffusion shown in Fig. 2 (c), while the high-order moments method cannot detect nonclassicality at large phase diffusion.

In conclusion, we have experimentally demonstrated reliable CV nonclassicality detection under coarse-grained measurement. Our three-bin test employs coarse-grained data to directly investigate the width of the phase-space structure, so there is no false detection of the nonclassicality under coarse-grained measurement. We have tested phase-diffused squeezed vacuum to compare the three-bin test with conventional high-order moments criteria, and the former outperformed the latter in the robustness under phase diffusion and the statistical significance. Our results strongly suggest that systematic and rigorous approaches to coarse-graining models may provide fundamental and practical tools in quantum information technologies.

References

[1] C. Oh, C. Lee, C. Rockstuhl, H. Jeong, J. Kim, H. Nha, and S.-Y. Lee, Optimal Gaussian measurements for phase estimation in single-mode Gaussian metrology, *npj Quantum Inf.* **5**, 10 (2019).

[2] I. Derkach, V. C. Usenki, and R. Filip, Squeezing-enhanced quantum key distribution over atmospheric channels, *New J. Phys.* **22**, 053006 (2020).

[3] J. K. Asbóth, J. Calsamiglia, and H. Ritsch, Computable measure of nonclassicality for light, *Phys. Rev. Lett.* **94**, 173602 (2005).

[4] A. I. Lvovsky and M. G. Raymer, Continuous-variable optical quantum-state tomography, *Rev. Mod. Phys.* **81**, 299 (2009).

[5] G. S. Agarwal, Nonclassical characteristics of the marginals for the radiation field, *Opt. Commun.* **95**, 109 (1993).

[6] W. Vogel, Nonclassical states: an observable criterion, *Phys. Rev. Lett.* **84**, 1849 (2000).

[7] J. Schneeloch, P. B. Dixon, G. A. Howland, C. J. Broadbent, and J. C. Howell, Violation of continuous-variable Einstein-Podolsky-Rosen steering with discrete measurements, *Phys. Rev. Lett.* **110**, 130407 (2013).

[8] C. Roh, Y.-D Yoon, J. Park, and Y.-S. Ra, Continuous-Variable Nonclassicality Detection under Coarse-Grained Measurement, *arXiv preprint* arXiv:2212.14343 (2022).

[9] J. Park, J. Lee, H. Nha, Verifying single-mode nonclassicality beyond negativity in phase space, *Phys. Rev. Res.* **3**, 043116 (2021).

Scalable Quantum Computation of Highly Excited Eigenstates with Spectral Transforms

Shao-Hen Chiew[1,2] and Leong-Chuan Kwek[2,3,4,5]

[1] *Department of Physics, Faculty of Science National University of Singapore Blk S12 Level 2, Science Drive 3 Singapore 117551*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3] *MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3654, Singapore*
[4] *National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore*
[5] *Quantum Science and Engineering Centre (QSec), Nanyang Technological University, Singapore*

We propose a natural application of Quantum Linear Systems Problem (QLSP) solvers such as the HHL algorithm to efficiently prepare highly excited interior eigenstates of physical Hamiltonians in a variational manner. This is enabled by the efficient computation of inverse expectation values, taking advantage of the QLSP solvers' exponentially better scaling in problem size without concealing exponentially costly pre/post-processing steps that usually accompanies it. We detail implementations of this scheme for both fault-tolerant and near-term quantum computers, analyse their efficiency and implementability, and discuss applications and simulation results in many-body physics and quantum chemistry that demonstrate its superior effectiveness and scalability over existing approaches.

Introduction.— The study of the spectral properties of physical systems plays a central role in physics, chemistry, and materials, and constitutes a leading candidate for quantum computers to display an advantage over classical approaches [1–6]. While the study of ground states with quantum computers has been an active area of research, excited states have received comparatively less attention due to its greater complexity and intractability [7, 8]. Despite recent developments to solve for excited states with near-term quantum computers [9–15], most existing approaches explore a limited number of eigenstates close to the ground state, lacking scalability for highly excited states.

Nonetheless, the development of theoretical and computational methods to study excited states remain crucial for a plethora of reasons, from the understanding of the ergodic-localization phase transition of disordered many-body systems [16–18], the calculation of reaction rates and binding energies of molecules [19, 20] and photochemistry [21], to an understanding of biological processes such as photosynthesis [22] and human vision [23]. Classically, when analytical or approximative treatments are inadequate, one resorts to large scale computational approaches such as Lanczos methods combined with spectral transforms [18] and machine learning methods [8], but they are ultimately hampered by demanding memory and time requirements that scale exponentially with system size.

The application of quantum computers to linear algebraic tasks constitutes another promising avenue with wide-reaching applications. Among them is the solution of linear systems of equations and its quantum variant, the Quantum Linear Systems Problem (QLSP), which, given input matrix A and quantum state $|b\rangle$ seeks the preparation of a quantum state $|x\rangle$ that solves the linear system $A|x\rangle = |b\rangle$ (up to a normalization factor, which we hide in the main text). An efficient solution for the QLSP on quantum computers was first proposed by Harrow, Hassidim and Lloyd [24], which yielded an exponential improvement in the scaling in input matrix dimension over the best general classical algorithm known. Since then, a flurry of work have resulted in improved algorithms with better scalings [25–28]. The development of variational QLSP solvers that are feasible in near-term devices have also been proposed and tested on current quantum computers [29–32].

However, the exponential improvement over classical solvers comes with several important caveats that prevents straightforward application [33]. Besides requiring A to be sparse and well-conditioned, QLSP solvers output a quantum state, only allowing efficient access to its statistical quantities. Access to the wavefunction amplitudes that it encodes require further processing, which may scale as the exponentially many number of amplitudes if complete information is desired. The encoding of the entries of $\vec{b}$ as amplitudes of a quantum state $|b\rangle$ is also non-trivial, facing the same complexity for unstructured inputs. Any application of QLSP solvers must therefore conform to these potentially limiting requirements to truly harness the exponential improvement, of which there are limited instances [34–37]. Indeed, the search for such applications constitutes an interesting and difficult problem in itself.

In this work, we propose a framework with which QLSP solvers can naturally be applied to solve for highly excited states of physical and chemical systems with both near-term and fault-tolerant quantum computers. Inspired by variational algorithms and classical diagonalization techniques based on spectral transformations, this algorithms prepares arbitrary excited eigenstates of Hamiltonians in a variational manner, which is enabled by the efficient computation and optimization of inverse expectation values on quantum computers. Our main insight is in realizing that QLSP solvers can be utilized in a natural manner when its inputs are taken to be Hamiltonians and quantum states corresponding to physical systems. The resulting procedure then leverages the efficient

representation of physical quantum states on quantum computers and the exponential speedup of QLSP solvers, without concealing exponentially costly processing steps that appear in classical linear algebraic applications.

Moreover, this procedure does not suffer from resource limitations plaguing existing iterative near-term quantum approaches for the preparation of excited eigenstates, most of which require exponentially many circuit executions with increasing system size when targeting high-energy states. Instead, our algorithm targets arbitrary eigenstates directly with an efficiency that depends mainly on the local density of states (LDOS) near the target, potentially enabling applications in near-term devices.

Our work is structured as follows. We begin with a description of the algorithm in an implementation-independent manner. We then detail the fault-tolerant and near-term implementations of the algorithm, followed by analyses of their complexities and implementational costs. Next, we discuss promising applications of the procedure in many-body physics and chemistry, supplemented with illustrative numerical results when solving for the interior eigenstates of molecular and lattice Hamiltonians. We refer the reader to the appendices for details throughout the text.

The algorithm.— We begin by outlining the algorithm and its features in an implementation-independent manner. To prepare a target eigenstate $|\lambda_k\rangle$ of H with energy λ_k, we first require a shift $\sigma \in \mathbb{R}$ chosen in $(\lambda_{k-1}, \lambda_{k+1})$, and an easily preparable quantum state denoted $|0\rangle^{\otimes n}$. The description of the algorithm is then as follows:

1. **Variational state preparation** : Prepare a parametrised input state $|b(\theta)\rangle$ with a unitary ansatz $U(\theta)\,|0\rangle^{\otimes n} = |b(\theta)\rangle$.

2. **Inverse expectation estimation** : Compute an approximation to $C(\theta) = \langle b(\theta)|\,(H-\sigma\mathbb{1})^{-1}\,|b(\theta)\rangle$:

   (a) **Solution of the QLSP of $H-\sigma\mathbb{1}$ and $|b(\theta)\rangle$** : Obtain the quantum state $|\tilde{x}(\theta)\rangle \approx (H-\sigma\mathbb{1})^{-1}\,|b(\theta)\rangle$ by solving the QLSP $(H-\sigma\mathbb{1})\,|x(\theta)\rangle = |b(\theta)\rangle$ with a quantum computer, with σ chosen in $(\lambda_{k-1}, \lambda_{k+1})$.

   (b) **Expectation estimation** : Compute the expectation value of $H-\sigma\mathbb{1}$ on the output state $|\tilde{x}(\theta)\rangle$, which approximates $\langle b(\theta)|\,(H-\sigma\mathbb{1})^{-1}\,|b(\theta)\rangle$.

3. **Classical optimiser feedback** : Using $C(\theta)$ as a cost function to be optimized (maximized if σ in $(\lambda_{k-1}, \lambda_k)$, minimized if σ in $(\lambda_k, \lambda_{k+1})$), use an iterative classical optimiser to determine the next set of parameters θ'.

4. **Optimise over variational parameters until convergence** : Repeat steps 1 and 2 with updated parameters until the classical optimizer converges, yielding optimal parameters θ^*. Finally, repeat step 1 with θ^* to prepare an approximation of $|\lambda_k\rangle$. The final optimized parameters are stored efficiently in classical memory.

By variationally preparing a quantum state with optimal shift-inverted energy, the target eigenstate is obtained, because extremal eigenstates of the shift-inverted Hamiltonian $(H-\sigma\mathbb{1})^{-1}$ correspond precisely to the target excited eigenstate of the original Hamiltonian H. This procedure heavily penalises eigenstates near the target by either repelling or shifting them to the other end of the transformed spectrum, which is a reason it outperforms simpler methods such as spectral folding/shift-squaring [9, 11] which further concentrate neighboring eigenstates. Arbitrary eigenstates can also be targeted as long as an estimate of its energy is known, circumventing the limitations of existing iterative variational algorithms that are ill-adapted for highly excited eigenstates (Surveyed in Appendix. (E 2)).

A key step in this procedure is the estimation of the expectation value of an inverted Hermitian operator $\langle H^{-1}\rangle$ - we refer to this as *inverse expectation estimation*. This is enabled through the solution of a QLSP (Step 2.a) and the measurement of H on the output (Step 2.b), for $H\,|x\rangle = |b\rangle$ implies:

$$\langle b|\,H^{-1}\,|b\rangle = \langle x|\,H^{\dagger}H^{-1}H\,|x\rangle = \langle x|\,H\,|x\rangle \qquad (1)$$

due to the self-adjointness of H. Depending on the resources required for the implementation of the QLSP solver and expectation estimation subroutines, the algorithm can either be classified as requiring fault-tolerance or feasible in near-term devices, which we detail in the following sections. For the former case, we describe an efficient implementation with the HHL algorithm with runtime that scales polylogarithmically with the dimension N of the input matrix and polynomially with its condition number κ, sparsity s and LDOS near the target eigenstate.

Secondly, the QLSP's input state $|b\rangle$ possesses structure that can be exploited, in that it should ultimately correspond to eigenstates of physical systems. This means that $U(\theta)$ can be chosen in a physically motivated manner with efficient implementations such as the adaptive [38, 39] or unitary coupled-cluster type [40, 41] ansatzes for chemistry and the Hamiltonian Variational Ansatz for lattice models [42]. Ongoing studies to avoid the appearance of barren plateaus that limit trainability, such as the usage of motivated initialization strategies and ansatzes will also play important roles in keeping $U(\theta)$ efficient [43, 44].

Therefore, by representing quantum states directly on a quantum computer, and solving QLSPs with quantum algorithms with exponentially improved scalings in matrix dimension and at most polynomial deteriorations in other parameters, this procedure likely outperforms classical implementations of shift-invert diagonalization. For these reasons, we argue that our algorithm involves QLSP solvers in a natural manner that bypasses their usual caveats (elaborated in Appendix. (B)).

Fault-tolerant implementation.— With access to fault-tolerant quantum computers, both expectation estimation and QLSP, and hence inverse expectation estimation can be performed efficiently with quantum algorithms at each iteration of the optimisation loop. In this section, we choose the QLSP solver to be the well-studied HHL algorithm for concreteness, adopting similar assumptions as HHL [24] (c.f. Appendix. (A 1) for review, notations, and assumptions). In principle, algorithms with improved scalings can be used.

The solution of the QLSP is the most demanding subroutine of the procedure, involving long coherent evolution of a quantum state with a circuit shown in Fig. (2). To adapt it for shift-inversion, we modify the eigenvalue inversion part (consisting of a $R_y(\theta)$ Pauli rotation controlled by qubits of the eigenvalue register with $\theta = \arccos(C/\tilde{\lambda})$) by choosing $\theta = \arccos(C/(\tilde{\lambda} - \sigma))$, resulting in the transformation:

$$\sum_j \beta_j \left|\tilde{\lambda_j}\right\rangle |u_j\rangle |0\rangle \to \sum_j \beta_j \sqrt{1 - \frac{C^2}{(\tilde{\lambda_j} - \sigma)^2}} \left|\tilde{\lambda_j}\right\rangle |u_j\rangle |0\rangle + \beta_j \frac{C}{\tilde{\lambda_j} - \sigma} \left|\tilde{\lambda_j}\right\rangle |u_j\rangle |1\rangle . \tag{2}$$

Post-selecting the '1' states of the ancilla qubit and normalizing then yields:

$$\sum_j \frac{\beta_j}{\tilde{\lambda_j} - \sigma} \left|\tilde{\lambda_j}\right\rangle |0\rangle^m |1\rangle \equiv |\tilde{x}'\rangle |0\rangle^m |1\rangle , \tag{3}$$

where $|\tilde{x}'\rangle$ is an approximation to the solution $|x'\rangle$ of:

$$(H - \sigma \mathbb{1}) |x'\rangle = |b\rangle . \tag{4}$$

The choice of the constant C must also be modified accordingly to satisfy unitarity while at the same time remaining large to maximise the probability of obtaining the outcome '1'. This results in the choice:

$$C = \min_i \{|\lambda_i - \sigma|\} = \min\{|\lambda_k - \sigma|, |\lambda_{k+1} - \sigma|, |\lambda_{k-1} - \sigma|\}. \tag{5}$$

Finally, as our goal is to transform λ_k to the end of the spectrum, we choose σ to be between λ_k and λ_{k+1} (or between λ_{k-1} and λ_k), but not too close to either values to keep C as large as possible. This implies that the LDOS near λ_k will impact the success probability of the algorithm, similar to how input matrices with large condition numbers affect the HHL algorithm. Amplitude amplification is expected to improve the success probability by a quadratic factor. This also means that the resulting complexity does not depend directly on the position of the target eigenstate in the spectrum, but rather on the local spectral properties around the target eigenstate. This allows the algorithm to be executed successfully as long as the LDOS is not too high around the target eigenstate.

Finally, the expectation value $\langle\tilde{x}| (H - \sigma\mathbb{1}) |\tilde{x}\rangle$ at each iteration of the optimisation can be computed with QPE-based techniques [45], operator averaging, or with the SWAP test since $\langle x| A |x\rangle \propto \langle x|b\rangle\langle b|x\rangle$.

Error and complexity of the fault-tolerant implementation.— Firstly, we remark that the only effect of modifying the HHL algorithm to introduce a shift σ is to change the success probability to depend on the LDOS near the shift (Eq. (5)); QPE is still performed on H, which has eigenvalues $\lambda_1, ..., \lambda_N$ between $1/\kappa$ and 1.

Denote by $\langle\psi|M|\psi\rangle_{est}$ the estimated value of $\langle\psi|M|\psi\rangle$. An upper bound for the error in the expectation value estimated from the output of the QLSP algorithm ϵ can be split into:

$$\begin{aligned} \epsilon &= |\langle\tilde{x}|M|\tilde{x}\rangle_{est} - \langle x|M|x\rangle| \\ &\leq |\langle\tilde{x}|M|\tilde{x}\rangle_{est} - \langle\tilde{x}|M|\tilde{x}\rangle| + |\langle\tilde{x}|M|\tilde{x}\rangle - \langle x|M|x\rangle| \\ &\equiv \epsilon_{exp} + \epsilon_{HHL}, \end{aligned} \tag{6}$$

with $\epsilon_{exp} \equiv |\langle\tilde{x}|M|\tilde{x}\rangle_{est} - \langle\tilde{x}|M|\tilde{x}\rangle|$ the error from the imprecise estimation of the expectation value of M on the state $|\tilde{x}\rangle$, and $\epsilon_{HHL} \equiv |\langle\tilde{x}|M|\tilde{x}\rangle - \langle x|M|x\rangle|$ the error from the imprecise output of the HHL algorithm.

For ϵ_{HHL}, we derive an upper bound for it to be $O(\|M\|_\infty \frac{\kappa}{t_0})$, where $\|M\|_\infty$ is the largest eigenvalue of M, and $t_0 \leq t$ where t is the time that appears in e^{iHt} for QPE (Appendix. (C)). As the observable M to be measured is always taken to be equal to the input of the QLSP solver $H - \sigma\mathbb{1}$, and σ is always chosen between the largest and smallest eigenvalues of H, the shifted operator have eigenvalues in $[1/\kappa - 1, 1 - 1/\kappa]$, which results in $O((\kappa - 1)/t_0)$. This implies that an error of $\leq \epsilon_{HHL}$ will require taking $t_0 = (\kappa - 1)/\epsilon_{HHL}$. Since the depth required by QPE (within HHL) scales as $O(\log(N)s^2 t_0)$ (or $O(\log(N)s^2(\kappa - 1)/\epsilon_{HHL})$ in terms of ϵ_{HHL}), while the preparation of $|b(\theta)\rangle$ is assumed to scale as $O(\text{polylog}N)$ with the choice of an efficient variational ansatz $U(\theta)$, the resulting circuit depth to prepare $|\tilde{x}\rangle$ is $O(\log(N)s^2(\kappa - 1)/\epsilon_{HHL} + \text{polylog}(N))$. Additionally, $O(p^2)$ repetitions are required to successfully post-select the shift-inverted quantum state, where $p = \min\{|\lambda_k - \sigma|, |\lambda_{k+1} - \sigma|, |\lambda_{k-1} - \sigma|\}$, which can be reduced to $O(p)$ by amplitude amplification.

For ϵ_{exp}, expectation estimation of $\langle H\rangle$ by QPE-based methods contributes $O(1/\epsilon_{exp})$ additional operations, while operator averaging contributes at most $O(M/\epsilon_{exp}^2)$ repetitions where M is the number of terms in H.

For the number of qubits, an ancillary qubit plus $n = \log(N)$ qubits to encode $|b\rangle$ are always required. Imposing that the target eigenstate's energy must be distinguishable from its neighbors, we find that the size of the eigenvalue register also scales efficiently as $m = O(-\log(\delta_k))$, where $\delta_k \equiv \min\{|\lambda_k - \lambda_{k-1}|, |\lambda_k - \lambda_{k+1}|\}$ is the smallest spectral gap between the target eigenstate $|\lambda_k\rangle$ and its neighbors (elaborated in Appendix. (C)).

Near-term implementation.— We describe how the algorithm can be implemented in a completely variational manner that does not require fault-tolerance, and is thus executable on near-term devices. An example we use to illustrate this is the VQLS [29], a variational QLSP solver

requiring circuit depths and repetitions that scale only polynomially in the number of qubits, and a constant or linear number of ancillary qubits. Using VQLS as the QLSP solver in Step 2.a of the algorithm in conjunction with operator averaging for expectation estimation in Step 2.b, inverse expectation estimation can therefore in principle be performed on near-term quantum computers.

Again, solution of the QLSP is the most demanding. Given an input matrix H which can be decomposed as a linear combination of L unitary matrices with complex coefficients $H = \sum_{i=1}^{L} c_i U_i$ and quantum state $|b\rangle$, VQLS solves the QLSP in a variational manner by minimising the cost function $C_{VQLS}(\phi) = |\langle b|H|x(\phi)\rangle|^2$ with the ansatz $V(\phi)$, where $H|x(\phi)\rangle = V(\phi)|0...0\rangle$. In our context, the Hamiltonian H can naturally be decomposed as a linear combination of unitaries [46, 47], while $|b\rangle$ corresponds to the variational state $|b(\theta)\rangle$ (prepared with $U(\theta)$) with which the shift-inverted energy $C(\theta)$ is minimised.

Finally, the estimation of the expectation value $\langle\tilde{x}|(H - \sigma\mathbb{1})|\tilde{x}\rangle$ during the classical optimization loop over θ can be performed by operator averaging, a standard approach for near-term algorithms [9].

Analysis of the near-term implementation.— The time complexity of the near-term implementation depends on the whether both the computation and optimisation of the outer ($C(\theta)$) and inner ($C_{VQLS}(\phi)$) loops can be performed efficiently.

For the outer loop, the computation of $C(\theta)$ with operator averaging incurs no additional circuit depth, at the expense of repetitions that scale as $O(M/\epsilon^2)$, where M is the number of terms in H. Heavy parallelization and recent developments such as efficient term grouping strategies [48–50] and QPE-based enhancements [51] are expected to improve this scaling. For the inner loop, the cost of computing $C_{VQLS}(\phi)$ depends on the choices of $U(\theta)$ and $V(\phi)$. Denoting their depths as D_U and D_V respectively, its computation with the Hadamard test requires $O(L^2)$ circuits of depth $\propto 2D_U + D_V$ to be executed at each iteration of the classical optimisation over θ. If D_U and D_V can be taken to scale efficiently in n, each circuit execution is efficient.

This brings us to trainability. The issue for $U(\theta)$ was discussed earlier. For $V(\phi)$, numerical results [29] for a particular ansatz choice with D_V that scales linearly with n indicate scaling of the runtime of VQLS in problem size, condition number, and error that is efficient and comparable with known optimal bounds [24]. This provides positive indications on the trainability of $C_{VQLS}(\phi)$, although the issue is subtler [32, 52] and requires further study of the VQLS, which is beyond the scope of our discussion. Nonetheless, we expect physically motivated choices of $V(\phi)$ to be crucial, an example being the ADAPT-VQE ansatz that have been shown to circumvent the barren plateau problem in certain situations [38, 39].

Applications.— Problems arising from chemistry and many-body physics satisfy the criteria of the algorithm, and are natural candidates that can exploit the speedup offered by QLSP solvers. Namely, their Hamiltonians generally admit sparse representations, inputs to the QLSP solver can be prepared with physically motivated ansatzes that exploit the target eigenstate's structure without the need to read from a classical vector, and only statistical quantities such as expectation values need to be extracted from the QLSP solver's output, without the need for complete tomography. The output of the algorithm is then a small set of real numbers θ^* that allows efficient preparation of the target quantum state, from which meaningful physical quantities can be extracted.

In the context of *ab initio* methods in chemistry and materials, our algorithm allows a primary output – the quantum state itself – to be obtained, which can then be probed for useful quantities such as dipole moments, partial charges, absorption spectra and so on. This is traditionally a difficult task in large scale even for pioneering machine learning methods [8], and is important for a variety of applications as discussed in the introduction. We refer the reader to a related classical algorithm that exploits shift-inversion – known as the Harmonic Davidson method [53] – for its numerous applications. As an illustration, Fig. (1) shows numerical simulations of our algorithm applied to prepare highly excited ($k = 500^{th}$) eigenstates of a 10-qubit molecular Hamiltonian – the Lithium Hydride (LiH) molecule in the STO-3G basis – at different bond lengths to recover its potential energy surface, compared against spectral folding, another existing variational algorithm. We consistently obtain superior results across all types of problems considered, described in Appendix. (D 1).

Many-body quantum systems constitute another natural candidate due to the exponential scaling of classical resources needed to simulate larger systems. In particular, many-body localised (MBL) systems have recently become a subject of interest in our context [16, 17], due to the presence of a mobility edge in energy, resulting in the MBL-ergodic transition occurring at different critical disorders for different energies [54]. A detailed understanding of this dynamical phase transition therefore entails a study of the entire spectrum instead of only the ground state, requiring the preparation and study of highly excited eigenstates. In fact, classical shift-invert diagonalisation constitute the state-of-the-art, but is ultimately limited by exponentially demanding memory requirements to less than $\sim$ 26 spins [18]. Since QLSP solvers outperform existing iterative classical solvers, we expect our algorithm to also perform well in this context, potentially allowing the study of higher-dimensional lattices in the near-term. This is explored and verified in Appendix. (D 1 b).

Discussion and outlook.— Immediate implementation of the near-term variant of the algorithm will likely be difficult for molecular Hamiltonians of classically intractable sizes due to the number of terms that generically scale as $O(n^4)$ [50], leading to a large number of

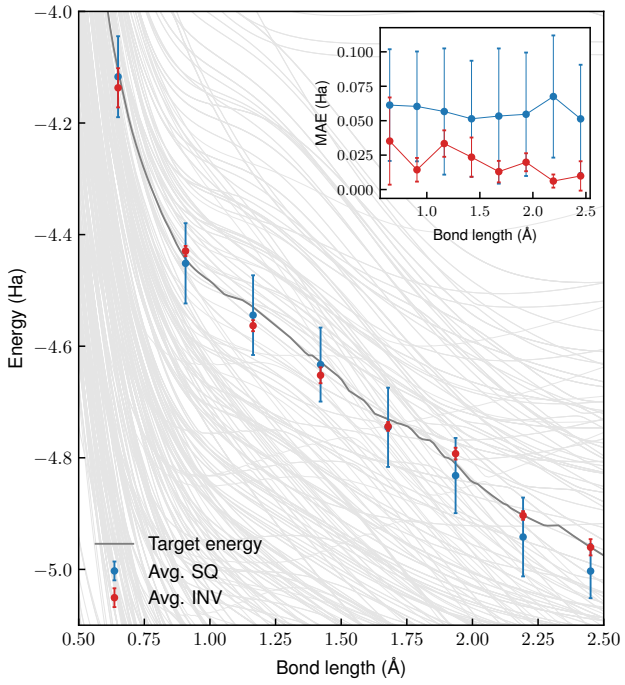


Figure 1: Energy spectrum of LiH computed with the shift-inversion algorithm (blue) and the spectral folding/shift-squaring algorithm (red), compared to ED results (dark grey line). An eigenstate near the middle of the spectrum ($k = 500$) is targeted at all bond lengths. Exact potential energy surfaces for other energies are also shown (light grey lines). Each datapoint is obtained by averaging 100 runs of the algorithm with randomly chosen initial parameters, and standard deviations are indicated by vertical error bars. The ansatz of Fig. (3) with 12 layers and the SLSQP/BFGS optimizers are used. Inset shows Mean Absolute Error (MAE) from exact results, with errors bars indicating standard deviations. We observe better accuracy and consistent converges with shift-inversion.

circuits needed for VQLS. Ongoing studies such as the incorporation of adaptive ansatzes, term grouping strategies, and measurement optimisation will severely reduce this requirement. On the other hand, lattice models such as the disordered Heisenberg model which exhibits MBL appear within reach : the cost of expectation estimation is reduced to a constant scaling after qubit-wise-commutation grouping, while the number of terms scale only as $O(nD)$, where D is the lattice dimensionality.

A potential impediment is the dependence on the LDOS near the target, a limitation also shared by classical spectral transformation techniques [18, 55]. While this is not problematic for systems such as Anderson localised models [56] and certain electronic structure problems [57], systems that exhibit exponential concentration of the LDOS at certain energies may prohibit efficient implementation. To weaken this dependence beyond amplitude amplification, pre-conditioners and filter functions – which are also crucial techniques in state-of-the-art classical methods [18] – will be important. Alternatively, the algorithm can be used as a warm-starting subroutine that prepares a quantum state with high overlap with the target eigenstate, which is then taken as the input of other algorithms such as QPE or filtering algorithms [58], in the same spirit as adiabatic inspired state initialisations for ground state searches. Similarly for the near-term implementation, rough initial outputs can be refined with additional variational circuits that approximate excitation operators [11] or variance-minimisation techniques [15]. Finally, we note that characteristics beyond the energy can be exploited to overcome the exponentially concentrating DOS, an idea that has been exploited in DMRG-based approaches for MBL where large differences in spatial properties of neighboring excited eigenstates allow them to be resolved despite being exponentially close in energy [59, 60].

In practice, prior information on the spectrum may also be required to select a suitable shift σ and normalise H. Well-studied strategies in the context of chemistry such as efficient approximations of the LDOS near the target [61, 62] and iterative approaches [63] can be applied for shift selection, while standard VQE can be used to obtain extremal eigenvalues to normalize H.

Summarising, we have proposed an algorithm that can efficiently prepare highly excited states of physical and chemical Hamiltonians, which exploits the efficiency QLSP of solvers while avoiding its usual caveats. Demonstrations in existing devices also appear attainable, especially for lattice models. We believe that the practical relevance of our algorithm provides compelling motivations to improve on existing QLSP solvers and other aspects of the algorithm.

Acknowledgments.— We thank Chee-Kong Lee, Liang Shi, and Patrick Rebentrost for useful discussions. LCK and SHC thank the Ministry of Education, Singapore and the National Research Foundation Singapore for their support.

[1] B. Bauer, S. Bravyi, M. Motta, and G. K.-L. Chan, "Quantum algorithms for quantum chemistry and quantum materials science," *Chemical Reviews*, vol. 120, no. 22, pp. 12685–12717, 2020.

[2] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, "The theory of variational hybrid quantum-classical algorithms," *New Journal of Physics*, vol. 18, no. 2, p. 023023, 2016.

[3] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[4] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, *et al.*, "Variational quantum algorithms," *Nature Reviews Physics*, vol. 3, no. 9, pp. 625–644, 2021.

[5] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke, *et al.*, "Noisy intermediate-scale quantum (nisq) algorithms," *arXiv preprint arXiv:2101.08448*, 2021.

[6] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, "Quantum certification and benchmarking," *Nature Reviews Physics*, vol. 2, no. 7, pp. 382–390, 2020.

[7] L. González, D. Escudero, and L. Serrano-Andrés, "Progress and challenges in the calculation of electronic excited states," *ChemPhysChem*, vol. 13, no. 1, pp. 28–51, 2012.

[8] J. Westermayr and P. Marquetand, "Machine learning for electronically excited states of molecules," *Chemical Reviews*, vol. 121, no. 16, pp. 9873–9926, 2020.

[9] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'brien, "A variational eigenvalue solver on a photonic quantum processor," *Nature communications*, vol. 5, no. 1, pp. 1–7, 2014.

[10] J. R. McClean, M. E. Kimchi-Schwartz, J. Carter, and W. A. De Jong, "Hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states," *Physical Review A*, vol. 95, no. 4, p. 042308, 2017.

[11] R. Santagati, J. Wang, A. A. Gentile, S. Paesani, N. Wiebe, J. R. McClean, S. Morley-Short, P. J. Shadbolt, D. Bonneau, J. W. Silverstone, *et al.*, "Witnessing eigenstates for quantum simulation of hamiltonian spectra," *Science advances*, vol. 4, no. 1, p. eaap9646, 2018.

[12] R. M. Parrish, E. G. Hohenstein, P. L. McMahon, and T. J. Martínez, "Quantum computation of electronic transitions using a variational quantum eigensolver," *Physical review letters*, vol. 122, no. 23, p. 230401, 2019.

[13] O. Higgott, D. Wang, and S. Brierley, "Variational quantum computation of excited states," vol. 3, p. 156.

[14] K. M. Nakanishi, K. Mitarai, and K. Fujii, "Subspace-search variational quantum eigensolver for excited states," *Physical Review Research*, vol. 1, no. 3, p. 033062, 2019.

[15] F. Zhang, N. Gomes, Y. Yao, P. P. Orth, and T. Iadecola, "Adaptive variational quantum eigensolvers for highly excited states," *Physical Review B*, vol. 104, no. 7, p. 075159, 2021.

[16] B. Bauer and C. Nayak, "Analyzing many-body localization with a quantum computer," *Physical Review X*, vol. 4, no. 4, p. 041021, 2014.

[17] J. Smith, A. Lee, P. Richerme, B. Neyenhuis, P. W. Hess, P. Hauke, M. Heyl, D. A. Huse, and C. Monroe, "Many-body localization in a quantum simulator with programmable random disorder," *Nature Physics*, vol. 12, no. 10, pp. 907–911, 2016.

[18] F. Pietracaprina, N. Macé, D. J. Luitz, and F. Alet, "Shift-invert diagonalization of large many-body localizing spin chains," *SciPost Physics*, vol. 5, no. 5, p. 045, 2018.

[19] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, "Elucidating reaction mechanisms on quantum computers," *Proceedings of the national academy of sciences*, vol. 114, no. 29, pp. 7555–7560, 2017.

[20] Y. Cao, J. Romero, J. P. Olson, M. Degroote, P. D. Johnson, M. Kieferová, I. D. Kivlichan, T. Menke, B. Peropadre, N. P. Sawaya, *et al.*, "Quantum chemistry in the age of quantum computing," *Chemical reviews*, vol. 119, no. 19, pp. 10856–10915, 2019.

[21] R. Lindh and L. González, *Quantum Chemistry and Dynamics of Excited States: Methods and Applications*. John Wiley & Sons, 2020.

[22] G. Cerullo, D. Polli, G. Lanzani, S. De Silvestri, H. Hashimoto, and R. J. Cogdell, "Photosynthetic light harvesting by carotenoids: detection of an intermediate excited state," *science*, vol. 298, no. 5602, pp. 2395–2398, 2002.

[23] J. Herbst, K. Heyne, and R. Diller, "Femtosecond infrared spectroscopy of bacteriorhodopsin chromophore isomerization," *Science*, vol. 297, no. 5582, pp. 822–825, 2002.

[24] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Physical review letters*, vol. 103, no. 15, p. 150502, 2009.

[25] D. W. Berry, A. M. Childs, and R. Kothari, "Hamiltonian simulation with nearly optimal dependence on all parameters," in *2015 IEEE 56th annual symposium on foundations of computer science*, pp. 792–809, IEEE, 2015.

[26] A. M. Childs, R. Kothari, and R. D. Somma, "Quantum algorithm for systems of linear equations with exponentially improved dependence on precision," *SIAM Journal on Computing*, vol. 46, no. 6, pp. 1920–1950, 2017.

[27] G. H. Low and I. L. Chuang, "Optimal hamiltonian simulation by quantum signal processing," *Physical review letters*, vol. 118, no. 1, p. 010501, 2017.

[28] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pp. 193–204, 2019.

[29] C. Bravo-Prieto, R. LaRose, M. Cerezo, Y. Subasi, L. Cincio, and P. J. Coles, "Variational quantum linear solver," *arXiv preprint arXiv:1909.05820*, 2019.

[30] R. Yalovetzky, P. Minssen, D. Herman, and M. Pistoia, "Nisq-hhl: Portfolio optimization for near-term quantum hardware," *arXiv preprint arXiv:2110.15958*, 2021.

[31] X. Xu, S. C. Benjamin, and X. Yuan, "Variational circuit compiler for quantum error correction," *Physical Review Applied*, vol. 15, no. 3, p. 034068, 2021.

[32] H.-Y. Huang, K. Bharti, and P. Rebentrost, "Near-term quantum algorithms for linear systems of equations with regression loss functions," *New Journal of Physics*, vol. 23, no. 11, p. 113021, 2021.

[33] S. Aaronson, "Read the fine print," *Nature Physics*, vol. 11, no. 4, pp. 291–293, 2015.

[34] N. Wiebe, D. Braun, and S. Lloyd, "Quantum algorithm for data fitting," *Physical review letters*, vol. 109, no. 5, p. 050505, 2012.

[35] B. D. Clader, B. C. Jacobs, and C. R. Sprouse, "Preconditioned quantum linear system algorithm," *Physical review letters*, vol. 110, no. 25, p. 250504, 2013.

[36] G. Wang, "Efficient quantum algorithms for analyzing large sparse electrical networks," *Quantum Information & Computation*, vol. 17, no. 11-12, pp. 987–1026, 2017.

[37] A. N. Chowdhury and R. D. Somma, "Quantum algo-

rithms for gibbs sampling and hitting-time estimation," *arXiv preprint arXiv:1603.02940*, 2016.

[38] H. R. Grimsley, S. E. Economou, E. Barnes, and N. J. Mayhall, "An adaptive variational algorithm for exact molecular simulations on a quantum computer," *Nature communications*, vol. 10, no. 1, pp. 1–9, 2019.

[39] H. L. Tang, V. Shkolnikov, G. S. Barron, H. R. Grimsley, N. J. Mayhall, E. Barnes, and S. E. Economou, "qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor," *PRX Quantum*, vol. 2, no. 2, p. 020310, 2021.

[40] J. Lee, W. J. Huggins, M. Head-Gordon, and K. B. Whaley, "Generalized unitary coupled cluster wave functions for quantum computation," *Journal of chemical theory and computation*, vol. 15, no. 1, pp. 311–324, 2018.

[41] G. Greene-Diniz and D. Muñoz Ramo, "Generalized unitary coupled cluster excitations for multireference molecular states optimized by the variational quantum eigensolver," *International Journal of Quantum Chemistry*, vol. 121, no. 4, p. e26352, 2021.

[42] D. Wecker, M. B. Hastings, and M. Troyer, "Progress towards practical quantum variational algorithms," *Physical Review A*, vol. 92, no. 4, p. 042303, 2015.

[43] E. Grant, L. Wossnig, M. Ostaszewski, and M. Benedetti, "An initialization strategy for addressing barren plateaus in parametrized quantum circuits," *Quantum*, vol. 3, p. 214, 2019.

[44] H. R. Grimsley, G. S. Barron, E. Barnes, S. E. Economou, and N. J. Mayhall, "Adapt-vqe is insensitive to rough parameter landscapes and barren plateaus," *arXiv preprint arXiv:2204.07179*, 2022.

[45] E. Knill, G. Ortiz, and R. D. Somma, "Optimal quantum measurements of expectation values of observables," *Physical Review A*, vol. 75, no. 1, p. 012328, 2007.

[46] A. F. Izmaylov, T.-C. Yen, R. A. Lang, and V. Verteletskyi, "Unitary partitioning approach to the measurement problem in the variational quantum eigensolver method," *Journal of chemical theory and computation*, vol. 16, no. 1, pp. 190–195, 2019.

[47] A. Ralli, P. J. Love, A. Tranter, and P. V. Coveney, "Implementation of measurement reduction for the variational quantum eigensolver," *Physical Review Research*, vol. 3, no. 3, p. 033195, 2021.

[48] A. Arrasmith, L. Cincio, R. D. Somma, and P. J. Coles, "Operator sampling for shot-frugal optimization in variational algorithms," *arXiv preprint arXiv:2004.06252*, 2020.

[49] W. J. Huggins, J. R. McClean, N. C. Rubin, Z. Jiang, N. Wiebe, K. B. Whaley, and R. Babbush, "Efficient and noise resilient measurements for quantum chemistry on near-term quantum computers," *npj Quantum Information*, vol. 7, no. 1, pp. 1–9, 2021.

[50] J. Tilly, H. Chen, S. Cao, D. Picozzi, K. Setia, Y. Li, E. Grant, L. Wossnig, I. Rungger, G. H. Booth, *et al.*, "The variational quantum eigensolver: a review of methods and best practices," *Physics Reports*, vol. 986, pp. 1–128, 2022.

[51] D. Wang, O. Higgott, and S. Brierley, "Accelerated variational quantum eigensolver," *Physical review letters*, vol. 122, no. 14, p. 140504, 2019.

[52] R. D. Somma and Y. Subaşı, "Complexity of quantum state verification in the quantum linear systems problem," *PRX Quantum*, vol. 2, no. 1, p. 010315, 2021.

[53] G. L. Sleijpen, A. G. Booten, D. R. Fokkema, and H. A. Van der Vorst, "Jacobi-davidson type methods for generalized eigenproblems and polynomial eigenproblems," *BIT Numerical Mathematics*, vol. 36, no. 3, pp. 595–633, 1996.

[54] D. A. Abanin, E. Altman, I. Bloch, and M. Serbyn, "Many-body localization, thermalization, and entanglement," *Reviews of Modern Physics*, vol. 91, no. 2, p. 021001, 2019.

[55] P. Sierant, M. Lewenstein, and J. Zakrzewski, "Polynomially filtered exact diagonalization approach to many-body localization," *Physical Review Letters*, vol. 125, no. 15, p. 156601, 2020.

[56] U. Elsner, V. Mehrmann, F. Milde, R. A. Römer, and M. Schreiber, "The anderson model of localization: a challenge for modern eigenvalue methods," *SIAM Journal on Scientific Computing*, vol. 20, no. 6, pp. 2089–2102, 1999.

[57] M. Keçeli, H. Zhang, P. Zapol, D. A. Dixon, and A. F. Wagner, "Shift-and-invert parallel spectral transformation eigensolver: Massively parallel performance for density-functional based tight-binding," *Journal of computational chemistry*, vol. 37, no. 4, pp. 448–459, 2016.

[58] L. Lin and Y. Tong, "Optimal polynomial based quantum eigenstate filtering with application to solving quantum linear systems," *Quantum*, vol. 4, p. 361, 2020.

[59] V. Khemani, F. Pollmann, and S. L. Sondhi, "Obtaining highly excited eigenstates of many-body localized hamiltonians by the density matrix renormalization group approach," *Physical review letters*, vol. 116, no. 24, p. 247204, 2016.

[60] X. Yu, D. Pekker, and B. K. Clark, "Finding matrix product state representations of highly excited eigenstates of many-body localized hamiltonians," *Physical review letters*, vol. 118, no. 1, p. 017201, 2017.

[61] M. Keçeli, F. Corsetti, C. Campos, J. E. Roman, H. Zhang, Á. Vázquez-Mayagoitia, P. Zapol, and A. F. Wagner, "Siesta-sips: Massively parallel spectrum-slicing eigensolver for an ab initio molecular dynamics package," 2018.

[62] D. B. Williams-Young, P. G. Beckman, and C. Yang, "A shift selection strategy for parallel shift-invert spectrum slicing in symmetric self-consistent eigenvalue computation," *ACM Transactions on Mathematical Software (TOMS)*, vol. 46, no. 4, pp. 1–31, 2020.

[63] J. J. Dorando, J. Hachmann, and G. K.-L. Chan, "Targeted excited state algorithms," *The Journal of chemical physics*, vol. 127, no. 8, p. 084109, 2007.

[64] A. C. Vazquez, R. Hiptmair, and S. Woerner, "Enhancing the quantum linear systems algorithm using richardson extrapolation," *ACM Transactions on Quantum Computing*, vol. 3, no. 1, pp. 1–37, 2022.

[65] M. Mottonen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, "Transformation of quantum states using uniformly controlled rotations," *arXiv preprint quant-ph/0407010*, 2004.

[66] G. Aleksandrowicz, T. Alexander, P. Barkoutsos, L. Bello, Y. Ben-Haim, D. Bucher, F. J. Cabrera-Hernández, J. Carballo-Franquis, A. Chen, C.-F. Chen, *et al.*, "Qiskit: An open-source framework for quantum computing," *Accessed on: Mar*, vol. 16, 2019.

[67] A. Pieper, M. Kreutzer, A. Alvermann, M. Galgon, H. Fehske, G. Hager, B. Lang, and G. Wellein, "High-performance implementation of chebyshev filter diago-

nalization for interior eigenvalue computations," *Journal of Computational Physics*, vol. 325, pp. 226–243, 2016.
[68] T. Sakurai and H. Sugiura, "A projection method for generalized eigenvalue problems using numerical integration," *Journal of computational and applied mathematics*, vol. 159, no. 1, pp. 119–128, 2003.
[69] E. Polizzi, "Density-matrix-based algorithm for solving eigenvalue problems," *Physical Review B*, vol. 79, no. 11, p. 115112, 2009.
[70] J. Dolbeault and M. J. Esteban, "Variational methods in relativistic quantum mechanics."
[71] R. N. Hill and C. Krauthauser, "A solution to the problem of variational collapse for the one-particle dirac equation," vol. 72, no. 14, pp. 2151–2154.
[72] F. Fillion-Gourdeau, S. MacLean, and R. Laflamme, "Algorithm for the solution of the dirac equation on digital quantum computers," vol. 95, no. 4, p. 042343.
[73] K. Hagino and Y. Tanimura, "Iterative solution of a dirac equation with inverse hamiltonian method," vol. 82, no. 5, p. 057301.
[74] Y. Tanimura, K. Hagino, and P. Ring, "Application of the inverse hamiltonian method to hartree-fock-bogoliubov calculations," *Physical Review C*, vol. 88, no. 1, p. 017301, 2013.
[75] S. Endo, I. Kurata, and Y. O. Nakagawa, "Calculation of the green's function on near-term quantum computers," *Physical Review Research*, vol. 2, no. 3, p. 033281, 2020.

Quantum Neural Networks for Quantum Mutual Information Estimation

Myeongjin Shin[1] * Junseo Lee[2 3] † Kabgyun Jeong[4 5] ‡

[1] *School of Computing, KAIST, Daejeon 34141, Korea*
[2] *School of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, Korea*
[3] *Quantum Security R&D, Norma Inc., Seoul 04799, Korea*
[4] *Research Institute of Mathematics, Seoul National University, Seoul 08826, Korea*
[5] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*

Abstract. This paper introduces QMINE (Quantum Mutual Information Neural Estimation), a method for estimating von Neumann entropy and quantum mutual information. QMINE utilizes a quantum neural network to minimize a loss function that determines von Neumann entropy, leveraging the advantages of quantum data processing and the efficiency of quantum neural networks compared to classical counterparts. To create the loss function, we propose the Quantum Donsker-Varadhan Representation (QDVR), a quantum version of the Donsker-Varadhan representation. By applying the parameter shift rule on parametrized quantum circuits, QMINE can be implemented and optimized. Experimental results validate the effectiveness of QDVR and demonstrate the performance of QMINE in estimating quantum mutual information.

Keywords: Quantum Mutual Information, Von Neumann entropy, Quantum neural network, Quantum Donsker-Varadhan Representation, Parameter shift rule

1 Introduction

In this paper, a method called QMINE (Quantum Mutual Information Neural Estimation) is introduced for determining the von Neumann entropy and quantum mutual information. QMINE utilizes a quantum neural network to minimize a loss function that evaluates the von Neumann entropy. To estimate the von Neumann entropy, a quantum version of the Donsker-Varadhan representation, known as the Quantum Donsker-Varadhan Representation (QDVR), is proposed to generate an appropriate loss function. QMINE offers a potential advantage in estimating von Neumann entropy using only $O(\mathrm{poly}(r), \mathrm{poly}(\frac{1}{\varepsilon}))$ copies of the quantum state, which is advantageous in terms of computational resources. However, the challenging barren plateau problem and the development of efficient quantum training methods need to be further investigated to fully harness this potential.

2 Quantum Donsker-Varadhan Representation (QDVR)

The Quantum Donsker-Varadhan Representation (QDVR) is a mathematical framework that allows quantum neural networks to estimate von Neumann entropy. It is a quantum adaptation of the classical Donsker-Varadhan Representation, focusing specifically on quantum entropy instead of relative entropy. QDVR is essentially a modified version of the Gibbs variational principle, which operates on density matrices. While the classical Donsker-Varadhan Representation was used in MINE [1] to estimate classical mutual information with classical neural networks, a quantum version of this representation is suitable for estimating quantum mutual information. By estimating the von Neumann entropies of specific density matrices, such as $S(\rho_A)$, $S(\rho_B)$, and $S(\rho_{AB})$, the quantum mutual information $I(A:B)$ can be determined. Furthermore, there exists a variational formula for von Neumann entropy.

Proposition 1 (QDVR) *Let $f : H^{d\times d} \to \mathbb{R}$ be a function defined on d-dimensional Hermitian matrices, and let ρ be an r-rank density matrix.*

$$g(T) = \mathrm{Tr}(c\rho T) - \log(\mathrm{Tr}(e^{cT})),\ \textit{where}\ c \geq 2rn + r\log\left(\frac{1}{\varepsilon}\right) \tag{1}$$

Then,

$$|S(\rho) - \inf(g(T))| < \varepsilon \tag{2}$$

for d-dimensional r-rank density matrices T.

3 Von Neumann Entropy Estimation with Quantum Neural Networks

We will now describe the process of estimating von Neumann entropy using quantum neural networks, specifically focusing on parametrized quantum circuits as an example. Our methodology draws inspiration from the work of Liu et al. [2], which employs variational autoregressive networks and quantum circuits to address quantum statistical mechanics problems. Let's begin by assigning specific values to the variables in T. We define t as a set of real numbers, $\{t_i | t_i \in \mathbb{R}\}$, and $|\psi_i\rangle$ as complex vectors in $\mathbb{C}^d$. Additionally, we assume the rank of ρ is denoted as r, and we define $T = \sum_{i=1}^{r} t_i |\psi_i\rangle\langle\psi_i|$.

Consequently, the function $g(T)$ takes the form $g(T) = -c\sum_{i=1}^{r} t_i \langle\psi_i|\rho|\psi_i\rangle + \log\left(d - r + \sum_{i=1}^{r} e^{ct_i}\right)$. To introduce a unitary operator U that transforms $|\psi_i\rangle$ to $|i\rangle$, we represent this unitary operator using a set of parameters θ as $U(\theta)$.

*hanwoolmj@kaist.ac.kr
†js_lee@norma.co.kr
‡kgjeong6@snu.ac.kr

$$g(T) = -c\sum_{i=1}^{r} t_i \langle i|U(\theta)\rho U^\dagger(\theta)|i\rangle + \log\left(d - r + \sum_{i=1}^{r} e^{ct_i}\right) \tag{3}$$

By considering $U(\theta)$ as a quantum neural network with ρ as its input, we can compute the network's output by evaluating $U(\theta)\rho U^\dagger(\theta)$. To calculate $g(T)$ accurately with an error less than ε, we must measure the output of the quantum neural network approximately $O\left(\frac{\mathrm{Var}(ct_i)^2}{\varepsilon^2}\right) = O\left(\frac{c^2}{\varepsilon^2}\right)$ times.

Our objective is now to optimize the parameters to find the maximum value of $g(T)$. As an example, let's consider a parametrized quantum circuit [3] with Pauli gates as the quantum neural network $U(\theta) = \prod_{i=1}^{k} U(\theta_i)$, where $U(\theta_i) = e^{-i\frac{\theta_i}{2}P_i}$. By applying the parameter shift rule [4], we can observe that

$$\nabla_\theta g(t,\theta) = \frac{1}{2}\left[g\left(t,\theta+\frac{\pi}{2}\right) - g\left(t,\theta-\frac{\pi}{2}\right)\right] \tag{4}$$

$$\frac{\partial g(t,\theta)}{\partial t_i} = -c\langle i|U(\theta)\rho U^\dagger(\theta)|i\rangle + \frac{ce^{ct_i}}{d-r+\sum_{i=1}^{r} e^{ct_i}} \tag{5}$$

To satisfy the conditions $t_i \geq 0$ and $\sum_{i=1}^{r} t_i = 1$, we can choose $t_i = \left(\prod_{j=1}^{i-1}\sin^2\varphi_j\right)\left(\cos^2\varphi_j\right)$. By performing gradient descent on φ_j and θ_i, we can optimize the quantum circuit. Calculating the gradient requires $O\left(\frac{c^2}{\varepsilon^2} \times (\text{number of parameters in the QNN})\right)$ copies of ρ. Thus, to obtain $\inf(g(T))$ and estimate $S(\rho)$ with an error less than ε, we need

$$O\left(\frac{1}{\varepsilon^2}\left(r^2n^2 + r^2\log^2\left(\frac{1}{\varepsilon}\right)\right)n_{\text{params}}n_{\text{train}}\right)$$

copies of ρ.

Using analytic gradient measurements in convex loss functions requires $O\left(\frac{n^3}{\epsilon^2}\right)$ copies of ρ to converge to a solution that is $O(\epsilon)$ close to the optimum [5]. Although situations involving parametrized quantum circuits often feature non-convex loss functions, many algorithms still utilize them and achieve quantum speed-ups. We expect that employing parametrized quantum circuits with analytic gradient measurements in QMINE will lead to a quantum speed-up. Furthermore, estimating the von Neumann entropy using $O(\text{poly}(r))$ copies of ρ is feasible. In future research, we will explore the relationships between n_{train}, n_{params}, and the approach's performance. The key idea is that we have transformed the problem of estimating quantum mutual information into a quantum neural network problem.

4 Numerical Simulations

We validate the performance of QMINE in estimating the quantum mutual information of randomly generated density matrices through numerical simulations of a quantum circuit. Our objective is to demonstrate that QMINE can estimate the quantum mutual information with a high degree of accuracy. Additionally, we conduct an analysis of the rank and trainable parameters, along with simulations to support the results obtained from QDVR.

4.1 Rank Analysis

In accordance with QDVR, we establish that if the rank of the density matrix ρ is denoted as r, setting the rank of the parameter matrix T to r is sufficient. Hence, our aim is to find the optimal T that provides an accurate estimation of the von Neumann entropy. To investigate the influence of the rank, we experiment with different ranks of T, denoting $r = \text{rank}(\rho)$ and $k = \text{rank}(T)$. In this analysis, we simulate a scenario with $N = 5$, $D = 30$, $r = 8$, and $c \leq 80$, where N represents the number of qubits, D denotes the circuit depth, r signifies the rank of the density matrix, and c is calculated using QDVR (for more details, refer to the supplementary material). The results depicted in Figure 1 illustrate that when $k \geq r$, QMINE converges to the correct value, while for $k < r$, it converges with a high error. This phenomenon is observed consistently in other cases as well, thereby supporting QDVR's assertion that the rank of the optimal solution T is r. Given that convergence is faster when $k = r$ compared to when $k > r$, it is advisable to utilize QMINE with $k = r$. Please refer to Figure 1 for the results.

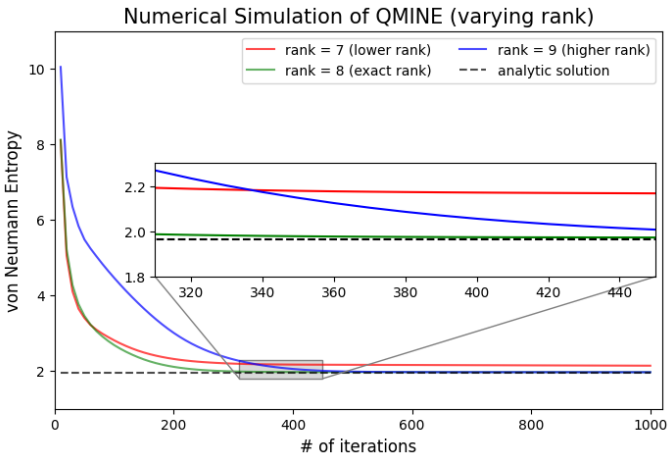


Figure 1: The green curve represents QMINE with the exact rank, displaying the best performance with rapid convergence and low error. The red curve represents QMINE with a lower rank, which exhibits high error during convergence. Finally, the blue curve represents QMINE with a higher rank, converging with low error but at a slower pace.

4.2 Analysis of the Number of Trainable Parameters in the Quantum Circuit

To assess the performance of QMINE, we analyze the impact of varying the depth of the quantum circuit. Our simulations involve $N = 5$, $D = 30$, $r = k = 8$, and

$c \leq 80$. The experimental findings confirm that as the circuit depth increases and the number of parameters grows, the estimation accuracy of QMINE improves. Figure 2 illustrates the results, indicating that a circuit depth of 20 achieves optimal performance. It converges quickly with a lower error compared to a depth of 30, which, although yielding a similar error, takes longer to converge. These results highlight the significance of selecting an appropriate circuit depth (corresponding to the number of parameters) in QMINE. The complexity of copying the density matrix is determined by the number of parameters (n_{params}) and the number of training iterations (n_{train}). Thus, when applying QMINE in various scenarios, choosing the suitable circuit depth becomes crucial. We intend to further investigate this aspect in future research. Please refer to Figure 2 for the results.

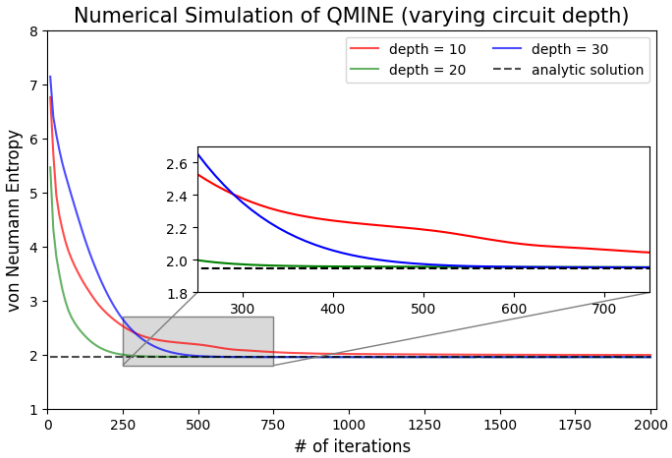


Figure 2: The graph displays different performance outcomes illustrated by three lines. The green line represents a circuit depth of 20 with 400 parameters, which showed the most favorable performance. It rapidly converged with a minimal error. In contrast, the red line represents a depth of 10 with 200 parameters, which converged with a high error. The blue line corresponds to a depth of 30 with 600 parameters, achieving a low error but requiring a longer convergence time.

4.3 Estimating Quantum Mutual Information

We estimate the quantum mutual information of a randomly generated density matrix using simulations with $N = 4$ qubits. For each tested random density matrix, we achieve an error rate ranging from 0.1% to 1%. Supplementary Information B provides additional details. Please refer to Figure 3 for the results.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) through a grant funded by the Ministry of Science and ICT (NRF-2020M3E4A1077861, NRF-2022M3H3A1098237) and the Ministry of Education (NRF-2021R1I1A1A01042199).

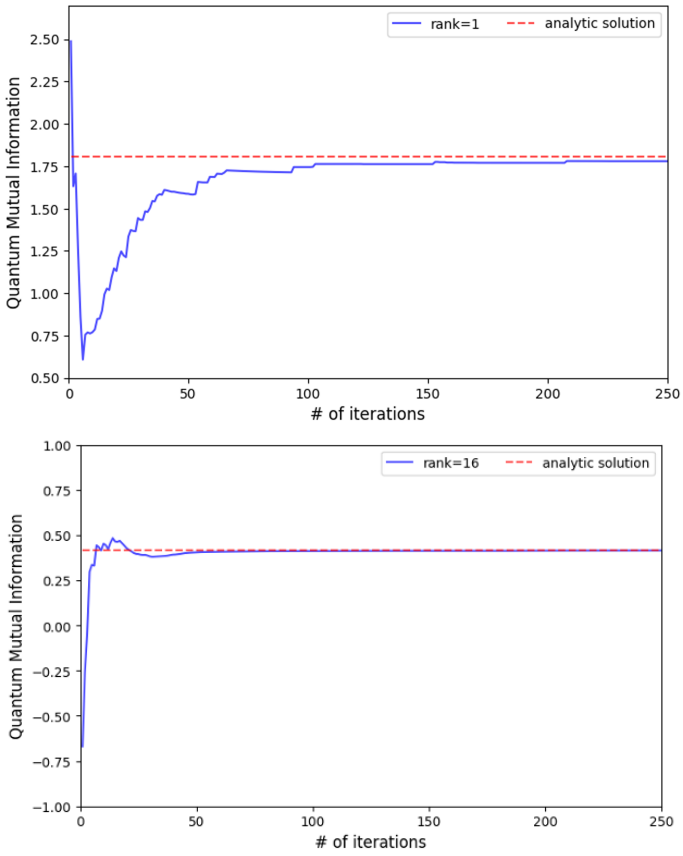


Figure 3: Estimation results of the quantum mutual information for a random density matrix.

References

[1] M. I. Belghazi, A. Baratin, S. Rajeswar, S. Ozair, Y. Bengio, A. Courville, and R. D. Hjelm, "Mine: mutual information neural estimation," *arXiv preprint arXiv:1801.04062*, 2018.

[2] J.-G. Liu, L. Mao, P. Zhang, and L. Wang, "Solving quantum statistical mechanics with variational autoregressive networks and quantum circuits," *Machine Learning: Science and Technology*, vol. 2, no. 2, p. 025011, 2021.

[3] M. Benedetti, E. Lloyd, S. Sack, and M. Fiorentini, "Parameterized quantum circuits as machine learning models," *Quantum Science and Technology*, vol. 4, no. 4, p. 043001, 2019.

[4] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, "Quantum circuit learning," *Physical Review A*, vol. 98, no. 3, p. 032309, 2018.

[5] A. W. Harrow and J. C. Napp, "Low-depth gradient measurements can improve convergence in variational hybrid quantum-classical algorithms," *Physical Review Letters*, vol. 126, no. 14, p. 140502, 2021.

Efficiency of Virtual Purification in Quantum Metrology

Hyukgun Kwon[1] Changhun Oh[2] Youngrong Lim[3] Hyunseok Jeong[1] *
Liang Jiang[2]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Republic of Korea*
[2] *Pritzker School of Molecular Engineering, University of Chicago, Chicago, Illinois 60637, USA*
[3] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*

Abstract. Recently, there has been a study applying the celebrated error mitigation technique, the "Virtual-Purification" (VPEM) to quantum metrology and successfully reduce the bias caused by noise, for particular estimation tasks. Beyond the specific tasks, we study factors determining the efficacy of the VPEM on general quantum estimation schemes. We find that the closeness between the dominant eigenvector of a noisy state and the ideal quantum probe (without noise) determines the mitigatable bias. Next, we show that one should carefully choose the reference point of a target parameter. Otherwise, even if the dominant eigenvector and the ideal quantum probe are close enough, the bias of the mitigated case could be larger than the non-mitigated one. Finally, we study the error-mitigated phase estimation scheme in optical systems, under various noises.

Keywords: Quantum Error Mitigation, Quantum Metrology, Bosonic system

1 Introduction

Recently there has been research applying Virtual-Purification (VPEM) to quantum metrology to reduce bias caused by unknown noise [4]. However, while Ref. [4] presented a framework of VPEM for quantum metrology and provided examples in which VPEM effectively reduces a bias, the general applicability of VPEM to quantum metrology has not been fully understood. In this work, we study when VPEM can effectively reduce the bias caused by an unknown noise. In particular, we identify two crucial factors that determine whether VPEM can reduce bias. The first one is how close the dominant eigenvector of a noisy state and the (noiseless) ideal state are. More specifically, the closeness decides the achievable amount of reduced bias. The second one is the reference point of a parameter that we want to estimate. Assuming that the unknown parameter to be estimated is small (often called local parameter estimation), the reference point is the one around which the unknown parameter varies. In local parameter estimation, we show that one has to carefully choose the reference point that gives the smallest bias before applying VPEM to quantum parameter estimation. Otherwise, even if the expectation values of $\hat{A}$ over the ideal quantum probe and the dominant eigenvector are the same, the bias of the mitigated case could be larger than the non-mitigated case. We emphasize that a strategy of choosing a reference point is a unique feature of quantum metrology that has not been considered in the previous studies.

2 Results

All the detailed caculations and results are in Ref. [1].

*h.jeong37@gmail.com

2.1 The dominant eigenvector $|\psi\rangle$

We consider local parameter estimation where unknown parameter ϕ is assumed to be small and varies around a reference point ϕ_0 . We analyze how the bias changes when we apply VPEM to local parameter estimation. More specifically, we inspect what will be the leading order of the bias in terms of the noise strength Δ when we apply VPEM. First, we inspect the bias of the non-mitigated case. If we exploit a non-mitigated quantum probe which corresponds to an error state $\hat{\rho}_{\mathrm{e}}(\phi+\phi_0)$ to estimate the parameter ϕ, the corresponding bias is

$$B_{\mathrm{e}}(\phi,\phi_0,\Delta)=\sum_{k=1}^{n-1}\left[f_k(\phi_0)+\phi\frac{\partial f_k(\phi)}{\partial\phi}\Big|_{\phi=\phi_0}\right]\Delta^k+O(\Delta^n). \tag{1}$$

Here the derivative over ϕ comes from the linear regression since we consider small ϕ and we express the bias using Taylor's series in terms of noise strength Δ. We find that all the coefficients, f_k's, come from the difference between the ideal state and the error state. In other words, all the f_k's depend on the difference between (i) the expectation value of $\hat{A}$ over the dominant eigenvector and the ideal state, (ii) the eigenvalues of the error state and 1 (we note that the eigenvalue of the ideal state is 1), and (iii) the expectation value of $\hat{A}$ over the rest of the eigenvectors and the ideal state. Next, the bias of mitigated case is

$$B_{\mathrm{mit}}(\phi,\phi_0,\Delta)=\sum_{k=1}^{n-1}\left[a_k(\phi_0)+\phi\frac{\partial a_k(\phi)}{\partial\phi}\Big|_{\phi=\phi_0}\right]\Delta^k+O(\Delta^n). \tag{2}$$

The coefficients of the mitigated case a_k's show stark contrast to the non-mitigated case. We find that a_k's only depends on the difference between the expectation value of $\hat{A}$ over the dominant eigenvector $|\psi\rangle$ and the ideal state. Therefore, the difference between the

dominant eigenvector and the ideal state dictates the leading order in Δ of the bias while other components in (ii) and (iii) are suppressed by VPEM. As a consequence, if $|\psi\rangle = |\psi_{\rm id}\rangle$, while $B_{\rm e} = O(\Delta)$, which clearly shows that in the small regime of Δ, the bias can be reduced by applying VPEM. However, if the dominant eigenvector and the ideal state are not close enough, we emphasize that VPEM cannot even guarantee the constant factor reduction of the bias even for small noise [1].

2.2 Reference point of the parameter

We emphasize that according to Eqs. (1) and (2), the bias of both error and mitigation case consist of zeroth and the first order of ϕ. In addition, both biases are a function of the reference point ϕ_0. Therefore, we can alleviate the bias by choosing a reference point that minimizes the zeroth order of ϕ of the bias. We call the reference point as *optimal reference point* and denote it as $\phi_0^{\rm opt}$. We note that the optimal reference point of error and mitigation case could be different in general and denote them as $\phi_{0,\rm e}^{\rm opt}$ and $\phi_{0,\rm mit}^{\rm opt}$.

Without appropriate reference point, even if the dominant eigenvector and ideal state are identical, $(B_{\rm mit})^2$ can be larger than $(B_{\rm e})^2$ because of an inadequate reference point instead of the failure of error mitigation. Therefore, one should consider a reference point when adopting VPEM to quantum metrology, unlike expectation value estimation [2, 3].

In general, the optimal reference point depends on noise strength, $\phi_0^{\rm opt} = \phi_0^{\rm opt}(\Delta)$. Although choosing an optimal reference point seems not feasible for an unknown noise, we can still apply our method to some situations. Let us assume that we know the type of occurring noise during the estimation, but, we do not know the noise strength Δ. First, when the optimal point does not depend on Δ, one can choose the optimal point regardless of noise strength. When the optimal point depends on Δ, a possible choice of the reference point is to use some prior knowledge in such as way that

$$\phi_0^{\rm opt} = \arg\min_{\phi_0} \int_{\Delta_1}^{\Delta_2} p(\Delta) B(\phi = 0, \phi_0, \Delta)^2 d\Delta, \qquad (3)$$

as a reference point that minimizes the zeroth order of bias in the average sense. Here $p(\Delta)$ is the prior distribution of noise strength Δ and the bias B $(\phi_0^{\rm opt})$ stands for $B_{\rm e/mit}$ $(\phi_{0,\rm e/mit}^{\rm opt})$. When the optimal point does not rapidly change as Δ, the above choice can be sufficient.

2.3 Phase Estimation in optical system

We inspect phase estimation in optical systems with several quantum probes and different kinds of noises.

2.3.1 N00N state-photon loss

N00N state as a quantum probe in the presence of the photon loss, we find that the dominant eigenvector is equal to the ideal state and the optimal reference point does not depend on a noise strength. Fig. 1 exhibits simulation results of bias errors with the N00N state in the presence of photon loss. They show that under the optimal reference point, VPEM can always effectively reduce the bias regardless of noise strength and the value of ϕ. In addition, if one does not carefully choose a reference point, an error case could have a smaller bias than a mitigation case even though the dominant eigenvector and the ideal state are the same.

2.3.2 Squeezed and coherent state-photon loss

Squeezed and coherent state entangled by a beam-splitter as a quantum probe in the presence of the photon loss, we find that dominant eigenvector are different from the ideal state and the optimal reference point depends on noise strength. Fig. 2 shows the non-effectiveness of VPEM-based quantum metrology as implied by our analysis because of the difference between the dominant eigenvector and the ideal state. For the most of the regions of ϕ, $B_{\rm e}(\phi, \phi_{0,\rm e}^{\rm opt}, \Delta)^2$ and $B_{\rm mit}(\phi, \phi_{0,\rm mit}^{\rm opt}, \Delta)^2$ are similar in magnitudes.

2.3.3 Squeezed and coherent state-Additive Gaussian noise

We consider squeezed and coherent state entangled by a beam-splitter as a quantum probe. For pedagogical purposes, we consider an additive Gaussian noise, which might not be directly relevant to experiments. We assume that Gaussian noise occurs only on the mode of the coherent state. Furthermore, we assume that Δ_x and Δ_p that are the standard deviations of the Gaussian noise are

$$\Delta_x = \sqrt{\frac{\Delta}{2}} e^{-r}, \quad \Delta_p = \sqrt{\frac{\Delta}{2}} e^{r} \qquad (4)$$

where r is a squeezing parameter and Δ is a noise strength. In this case, we find that the dominant eigenvector is equal to the ideal state but the optimal reference point depends on a noise strength. Fig. 3, shows the validity of the averaged optimal reference point defined in Eq. (3). We find that under the averaged optimal reference point, VPEM can always effectively reduce the bias regardless of noise strength and the value of ϕ.

References

[1] H. Kwon *et al.*, Efficacy of virtual purification-based error mitigation on quantum metrology arXiv: 2303.15838, (2023).

[2] B.Koczor, Exponential Error Suppression for Near-Term Quantum Devices, Phys. Rev. X. **11**, 031057 (2021).

[3] W. J. Huggins *et al.*, Virtual Distillation for Quantum Error Mitigation, Phys. Rev. X. **11**, 041036 (2021).

[4] K. Yamamoto *et al.*, Error-mitigated quantum metrology via virtual purification, Phys. Rev. Lett. **129**, 250503 (2022).

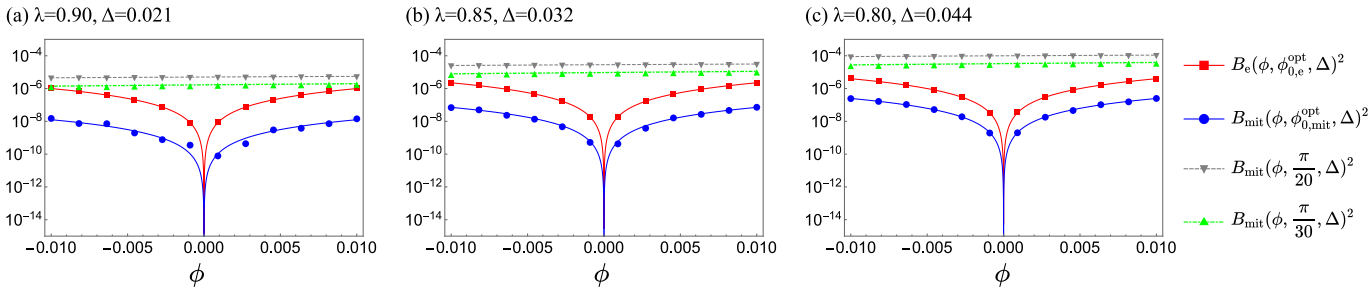


Figure 1: (a)-(c) Simulations of bias (with log scale) exploiting N00N state ($N = 5$) as a quantum probe in the presence of photon loss with different noise strengths. We use $N_s = 10^7$ numbers of samples. Solid, dashed, and dot-dashed lines are theoretical values of the bias errors.

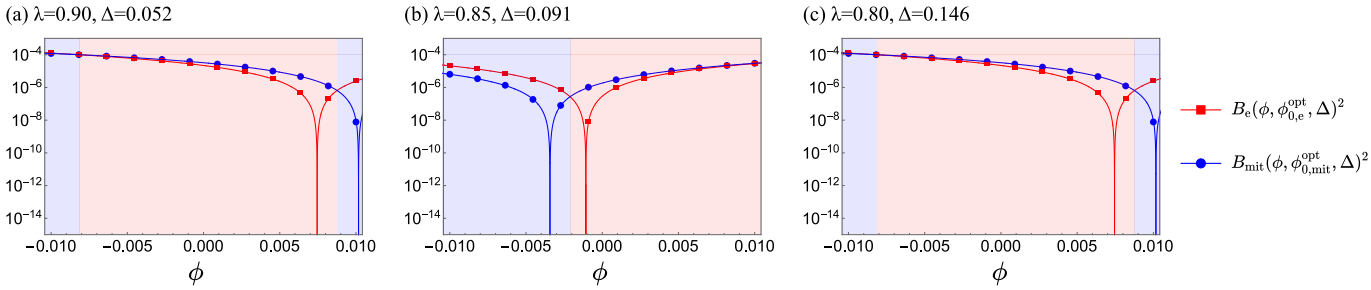


Figure 2: (a)-(c) Simulations of bias (with log scale) using the coherent state ($N_c = 2.5$) and squeezed vacuum state ($N_r = 2.5$) in the presence of photon loss with different noise strengths. Other features of the figure are the same as Fig. 1.

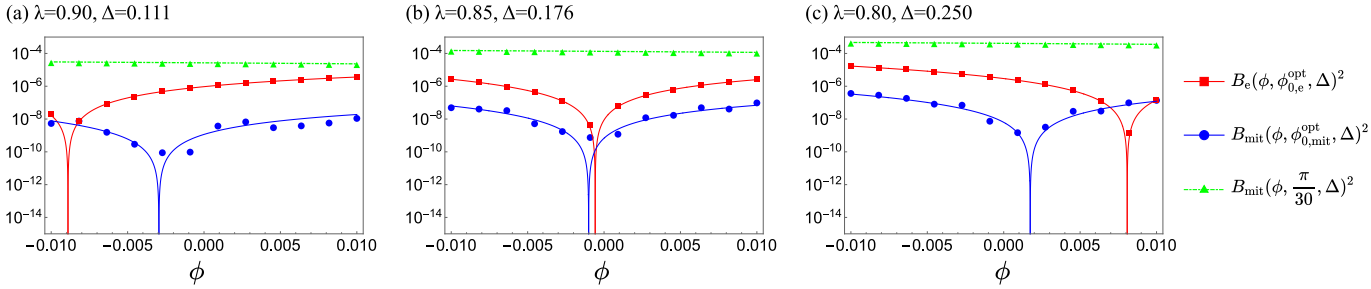


Figure 3: (a)-(c) Simulations of bias (with log scale) using the coherent state ($N_c = 2.5$) and squeezed vacuum state ($N_r = 2.5$) in the presence of additive Gaussian noise with different noise strengths. Other features of the figure are the same as Fig. 1.

Scalable quantum measurement error mitigation via conditional independence and transfer learning

ChangWon Lee[1] * Daniel K. Park[1 2] †

[1] *Department of Statistics and Data Science, Yonsei University, Seoul, 03722, Republic of Korea*
[2] *Department of Applied Statistics, Yonsei University, Seoul 03722, Republic of Korea*

Abstract. Mitigating measurement errors in quantum systems without relying on quantum error correction is crucial for the practical development of quantum technology. Deep learning-based quantum measurement error mitigation has exhibited advantages over the linear inversion method due to its capability to correct non-linear noise. However, scalability remains a challenge for both methods. In this study, we propose a scalable quantum measurement error mitigation method that leverages the conditional independence of distant qubits and incorporates transfer learning techniques. By leveraging the conditional independence assumption, we achieve an exponential reduction in the size of neural networks used for error mitigation. Additionally, incorporating transfer learning provides a constant speedup. We validate the effectiveness of our approach through experiments conducted on IBM's 7-qubit and 13-qubit systems, demonstrating excellent error mitigation performance and highlighting the efficiency of our method.

Keywords: Quantum error mitigation, deep learning, conditional independence, transfer learning

1 Introduction

The susceptibility of quantum computing to noise and imperfections poses a significant challenge, limiting its ability to surpass classical capabilities in solving real-world problems. While the theory of quantum error correction (QEC) and fault-tolerance holds the promise of scalable quantum computation, building a fault-tolerant quantum computer remains a long-term endeavor. Quantum error mitigation (QEM) refers to a set of techniques that reduces the impact of errors on the outcomes of quantum computations, as opposed to completely removing it as done in QEC. QEM is crucial for practical quantum computation, especially in the Noisy Intermediate-Scale Quantum (NISQ) era [1], as it maximizes the utilization of limited quantum resources and expands the capacity of quantum systems for solving real-world problems.

Measurement is an essential operation in quantum computing, but is prone to errors. In certain quantum devices, measurement errors can severely damage the overall computation. For instance, IBM Quantum devices typically exhibit measurement error rates on the order of 1%, with some cases reaching as high as 40%. Several methods have been proposed to mitigate measurement errors [2–6], but their complexity scales exponentially with the number of qubits, imposing limitations on both scalability and practicality.

In this paper, we present a scalable deep learning-based method for quantum measurement error mitigation (QMEM). Our method leverages the concepts of conditional independence and transfer learning [7] to significantly improve the efficiency compared to previous methods. Conditional independence assumes that the impact of measurement cross-talk between distant qubits is negligible. By incorporating this assumption, we are able to exponentially reduce the size of neural networks used for QMEM. Transfer learning assumes the existence of an error component that is shared across all qubits. This assumption facilitates a constant factor reduction in training time by effectively leveraging pre-trained models. To validate our approach, we conducted proof-of-principle experiments on IBM quantum devices with 7 and 13 qubits. The results demonstrate that the underlying assumptions hold and affirm the effectiveness of our QMEM method in reducing measurement errors.

2 Background

Many experimental setups for both the quantum circuit model and quantum annealing use projective measurement in the computational basis to perform readout of a quantum state. Moreover, positive operator-valued measurements can be realized through the projective measurement with ancillary qubits [8, 9]. Therefore, our primary focus is the development of error mitigation techniques to enhance the projective measurement in the computational basis. An ideal measurement on n qubits results in the probability distribution, which can be represented as a vector $\boldsymbol{p} = \{p_1, p_2, ..., p_{2^n}\}$. However, the observed probability distribution in experiments deviate from $\boldsymbol{p}$ due to measurement errors. We denote the observed probability as $\hat{p}_i$ and the error map as $\mathcal{N}$ such that $\hat{\boldsymbol{p}} = \mathcal{N}(\boldsymbol{p})$. The goal of QMEM is to minimize the loss function, $D(\boldsymbol{p}, \hat{\boldsymbol{p}})$ where D is some distance measure.

The linear inversion method (LI-QMEM) assumes a noise model $\mathcal{N}(\boldsymbol{p}) = \boldsymbol{\Lambda}\boldsymbol{p}$ and aims to reconstruct the noise matrix $\boldsymbol{\Lambda}$ through tomography. It produces an error-mitigated probability vector $\tilde{\boldsymbol{p}} = \boldsymbol{\Lambda}^{-1}\hat{\boldsymbol{p}}$ [2–4]. In contrast, QMEM can be performed by training a deep neural network $\mathcal{F}$ to approximate the inverse noise function $\mathcal{N}^{-1}$ [5, 6]. The trained neural network produces an error-mitigated probability vector $\tilde{\boldsymbol{p}} = \mathcal{F}(\hat{\boldsymbol{p}}) \approx \mathcal{N}^{-1}(\hat{\boldsymbol{p}}) = \boldsymbol{p}$. This approach, referred to as NN-QMEM, is capable of correcting non-linear errors, which is not possible with LI-QMEM [6]. However, both LI-QMEM

*changwonlee@yonsei.ac.kr
†dkd.park@yonsei.ac.kr

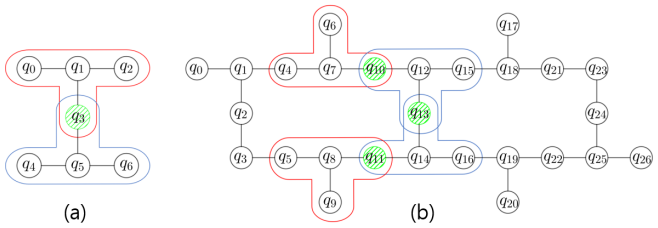


Figure 1: Connectivity of the quantum devices used in this paper. (a) is 7qubit quantum device (b) is 27qubit quantum device.

and NN-QMEM suffer from scalability limitations as the memory and computation time grow exponentially with the number of qubits. Recent estimations suggest that the current classical computational resources can only handle NN-QMEM for quantum systems of up to 16 qubits [6].

3 Main results

3.1 Theoretical Framework

In NN-QMEM, the size of the neural network can be exponentially reduced by leveraging the concept of conditional independence. The definition of conditional independence is as follows. Consider random variables X, Y and Z. We say that X and Y are conditionally independent given Z if the joint probability of X and Y given Z can be expressed as $p(X,Y|Z) = p(X|Z)p(Y|Z)$. As an example, consider a 7 qubit system with q_i denotes an i^{th} qubit. Suppose that the set of qubits $A = \{q_0, q_1, q_2\}$ and $B = \{q_4, q_5, q_6\}$ are connected only through $C = \{q_3\}$ as illustrated in Fig. 1 (a). Then assuming conditional independence of subsystems A and B given C, the joint probability distribution can be written as

$$p(A,B,C) = p(A,B|C)p(C) = p(A|C)p(B|C)p(C).$$

To learn how to correct for the full joint probability $p(A,B,C)$ via deep learning, the number of input nodes of the neural network must grow exponentially with the number of qubits. Typically, the total number of nodes grows linearly with the number of input nodes, and the number of parameters grows quadratically. On the other hand, under the conditional independence assumptions, one needs three machine learning models that correct for $p(A|C)$, $p(B|C)$, and $p(C)$ independently. In this example, the number of input nodes for $p(A|C)$ and $p(B|C)$ is 2^3, and is 2^1 for $p(C)$. Thus the total number of parameters to be trained is proportional to $2((2^3)^2 + (2^3)^2) + (2^1)^2 = 260$, whereas for the full model requires it to be proportional to $(2^7)^2 = 16384$. Reduced parameter count in neural networks implies less training data is needed for convergence. Therefore, by leveraging the conditional independence assumption, the overall training time can be significantly decreased. Additionally, smaller networks lead to faster inference runtimes. Hereinafter, we refer to as the qubit corresponding to C as the conditional qubit.

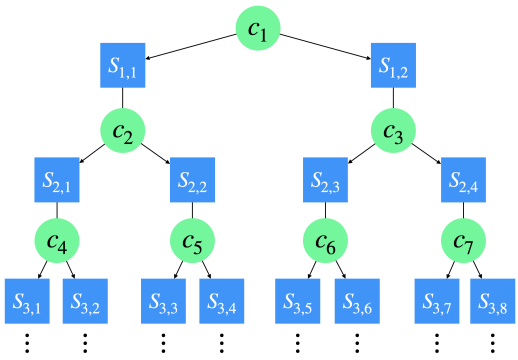


Figure 2: Partitioning of qubits according to the conditional independence assumption.

The general idea of partitioning the given quantum system according to the conditional independence is illustrated in Fig. 2. In the figure, $S_{i,j}$ means the j^{th} subsystem at a partition level i, and c_i means the qubit that bridges the two subsystems partitioned under the assumption that the subsystems are independent given the state of c_i. The partitioning continues until the subsystems in the leaf nodes have a small number of qubits (e.g. less than 10). If, for example, the partitioning ends at level 3 in Fig. 2, then we need eight independent neural networks, one for each leaf node, to correct for a conditional probability distribution $p(S_{3,i}|c_j c_k c_l)$, $i = 1, \ldots, 8$ and jkl indicates the set of indices of conditional qubits that connects the leaf and the root. The conditional probability distributions have to be corrected for all computational basis states of the conditional qubits $c_j c_k c_l$, but the number of conditional qubits grows with the depth of the tree, which grows logarithmically with the number of total qubits. Therefore, the number of neural networks to be trained independently grows linearly with the number of total qubits, and the size of each neural network is constant. This constitutes an efficient QMEM method that is exponentially faster than previous methods that aim to correct for the full joint probability distribution model without conditional independence, for which the size of the neural network or the size of the linear response matrix grows exponentially with the number of qubits.

Transfer learning can further reduce the training runtime by leveraging pre-trained neural networks. Instead of training a new neural network from scratch on a new dataset, transfer learning involves using parameters from a pre-trained network on a reference dataset that shares some similarities with the new dataset. Typically, the lower layers representing low-level features are kept frozen, while only the upper layers are trained. This eliminates the need to learn low-level features again, resulting in faster convergence and reduced training time. For example, in our case, the neural networks for $S_{3,i}$, $i > 1$, can utilize the parameters of the initial layers from the neural network trained on $S_{3,1}$, and only fine-tune the remaining layers specifically for each subsystem $S_{3,i}$ with $i > 1$.

3.2 Experimental Results

The first set of experiments were conducted on the 7-qubit IBM quantum devices, ibmq_jakarta and ibm_lagos, to compare the performance of our QMEM with LI-QMEM and NN-QMEM. For each device, we generated 7,500 data and split them into 6,000 for training and 1,500 for testing. To compare the performance of different QMEM methods, we used mean square error (MSE),

$$D_{MSE} = \frac{1}{2^n} \sum_{i=0}^{2^n-1} |\tilde{p}_i - p_i|^2$$

where p_i and $\tilde{p}_i$ are the i^{th} elements of the ideal and the mitigated probability distributions, respectively.

We report MSE for the probability distributions obtained with (1) no error mitigation ($\hat{\boldsymbol{p}}$), (2) LI-QMEM ($\tilde{\boldsymbol{p}}_{\text{LI}}$) (3) NN-QMEM ($\tilde{\boldsymbol{p}}_{\text{NN}}$) (4) our method using conditional independence ($\tilde{\boldsymbol{p}}_{\text{CI}}$), which we call CI-QMEM, and (5) our method using conditional independence and transfer learning ($\tilde{\boldsymbol{p}}_{\text{CI+Transfer}}$), which we call CITL-QMEM. First, we compare the cases (1) to (4) with respect to the number of training data. The results are shown in Fig. 3.

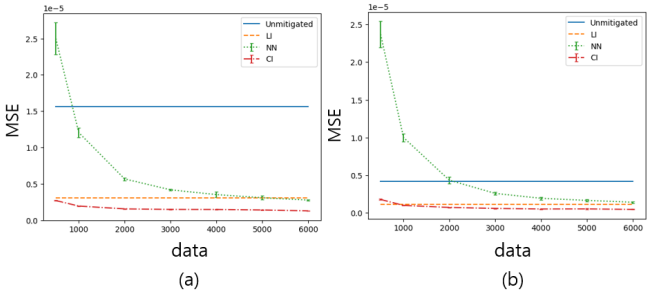


Figure 3: Experimental results showing the mean square error with respect to the ideal probability distribution as a function of the number of training data. The results are obtained by executing the experiments on (a) ibmq_jakarta and (b) ibm_lagos.

The experimental results indicate that CI-QMEM achieves substantial error mitigation using less data compared to NN-QMEM. While NN-QMEM employs 1,805,568 parameters, CI-QMEM achieves even better performance with only 29,484 parameters. These findings highlight the efficiency of training time achieved through a significant reduction in the number of parameters, while maintaining robust performance. Furthermore, by employing transfer learning, the number of parameters in CITL-QMEM was further reduced to 15,644. Figure 4 visually illustrates the effectiveness of transfer learning in reducing errors.

Finally, we performed QMEM on 13 qubits, selected from 27-qubit quantum devices, ibmq_mumbai and ibmq_kolkata. For each device, we generated 6,000 data and split them into 5,000 for training and 1,000 for testing. The partitioning of the 13-qubit system is shown in Fig. 1 (b), and the results are shown in Fig. 5.

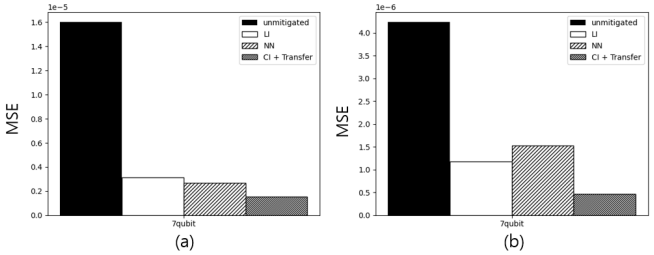


Figure 4: Seven-qubit QMEM results on (a) ibmq_jakarta and (b) ibm_lagos.

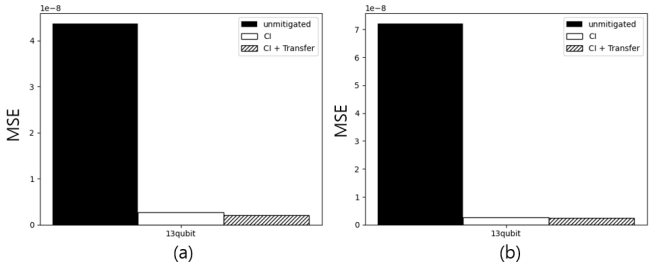


Figure 5: Thirteen-qubit QMEM results n (a) ibmq_mumbai and (b) ibmq_kolkata.

Our method significantly reduces errors on the 13-qubit system. Note that LI-QMEM requires 8192 data and NN-QMEM requires 7 billion parameters, while our method is trained with much less data and parameters.

4 Conclusions

This work presents a scalable quantum measurement error mitigation method, overcoming the limitations of existing methods. By harnessing conditional independence and transfer learning, we achieve exponential reductions in neural network size while preserving excellent error-mitigation capabilities. Our method not only reduces neural network size and the number of parameters to optimize but also significantly decreases the amount of data required to train a neural network. Experimental results on 7-qubit and 13-qubit systems validate the efficiency and effectiveness of our method in mitigating measurement errors.

References

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

[2] Yanzhu Chen, Maziar Farahzad, Shinjae Yoo, and Tzu-Chieh Wei. Detector tomography on ibm quantum computers and mitigation of an imperfect measurement. *Phys. Rev. A*, 100:052315, Nov 2019.

[3] Filip B. Maciejewski, Zoltán Zimborás, and Michał Oszmaniec. Mitigation of readout noise in near-term quantum devices by classical post-processing based on detector tomography. *Quantum*, 4:257, April 2020.

[4] Hyeokjea Kwon and Joonwoo Bae. A hybrid quantum-classical approach to mitigating measure-

ment errors in quantum algorithms. *IEEE Transactions on Computers*, 70(9):1401–1411, 2021.

[5] Benjamin Lienhard, Antti Vepsäläinen, Luke C.G. Govia, Cole R. Hoffer, Jack Y. Qiu, Diego Ristè, Matthew Ware, David Kim, Roni Winik, Alexander Melville, Bethany Niedzielski, Jonilyn Yoder, Guilhem J. Ribeill, Thomas A. Ohki, Hari K. Krovi, Terry P. Orlando, Simon Gustavsson, and William D. Oliver. Deep-neural-network discrimination of multiplexed superconducting-qubit states. *Phys. Rev. Applied*, 17:014024, Jan 2022.

[6] Jihye Kim, Byungdu Oh, Yonuk Chong, Euyheon Hwang, and Daniel K Park. Quantum readout error mitigation via deep learning. *New Journal of Physics*, 24(7):073009, 2022.

[7] Sinno Jialin Pan and Qiang Yang. A survey on transfer learning. *IEEE Transactions on knowledge and data engineering*, 22(10):1345–1359, 2010.

[8] Yordan S. Yordanov and Crispin H. W. Barnes. Implementation of a general single-qubit positive operator-valued measure on a circuit-based quantum computer. *Phys. Rev. A*, 100:062317, Dec 2019.

[9] Dongkeun Lee, Kyunghyun Baek, Joonsuk Huh, and Daniel K Park. Variational quantum state discriminator for supervised machine learning. *arXiv preprint arXiv:2303.03588*, 2023.

Quantum Common-Interest Games, Replicator Dynamics, and the Separability Problem

Wayne Lin[1] * Georgios Piliouras[1] † Ryann Sim[1] ‡ Antonios Varvitsiotis[1] §

[1] *Singapore University of Technology and Design, Singapore*

Abstract. Gamification is a machine learning technique that reframes optimization problems as games, allowing for the design of robust, implementable, and parallelizable algorithms. In this work we introduce quantum common-interest games (QCIG) for studying the Best Separable State (BSS) problem and establish equivalence between KKT points of a BSS instance and Nash equilibria of its corresponding QCIG. For learning in QCIGs, we introduce non-commutative extensions of (continuous-time) replicator dynamics and (discrete-time) Baum-Eagon and linear multiplicative weights updates and show that the utility strictly increases along trajectories. We corroborate our results through simulations, finding that our continuous-time dynamic empirically converges to Nash equilibria.

Keywords: Quantum game theory, separability, Best Separable State problem, replicator dynamics, Baum-Eagon dynamics, Matrix Multiplicative Weights Update

1 Introduction

The framework of gamification has recently emerged as a prominent trend in the field of machine learning, offering a novel approach to solving optimization problems. By reimagining these problems as games, it is possible to design distributed and decentralized algorithms that are robust and easily parallelizable. A notable application of this approach are the constrained min-max optimization problems that underlie Generative Adversarial Networks (GANs), which are known to be computationally challenging [10]. However, by framing them as competitive games between two players, simple decentralized algorithms have been developed, showcasing practical effectiveness and convergence towards appropriate solution concepts. Furthermore, gamification has showcased success in addressing other optimization problems in machine learning such as Principal Component Analysis [13] and Nonnegative Matrix Factorization [34]. While the most well-known achievements are based on zero-sum games [8, 9, 29, 33], the current focus is increasingly shifting towards the more challenging domain of cooperative settings [4, 27, 35], where all agents share the same goals and try to optimize the same function.

In this work, we leverage the gamification paradigm to address the Best Separable State problem (BSS), which corresponds to linear optimization over the convex hull of bipartite product states $\rho \otimes \sigma$, i.e.,

$$\max\{\mathrm{Tr}(R(\rho \otimes \sigma)) : \rho \in D(\mathcal{A}), \sigma \in D(\mathcal{B})\}. \qquad \text{(BSS)}$$

where R is a fixed Hermitian matrix. The BSS problem is a crucial challenge in quantum information theory that is closely tied to entanglement detection [15, 22, 16, 14]. To apply the gamification approach to the BSS problem, we model a BSS instance as a quantum common-interest game and bridge the gap between optimization and game theory by establishing equivalence between KKT points of a BSS instance and Nash equilibria of its corresponding game. Quantum games, which allow players access to quantum resources, are a natural extension of the classical game theory framework, see e.g. [11, 7, 17, 39]. In the simplest possible setup, two players (Alice and Bob) control quantum registers $\mathcal{A}$ and $\mathcal{B}$ and their strategies are density matrices acting on $\mathcal{A}$ and $\mathcal{B}$ respectively. Upon playing strategy profile (ρ, σ) each player i receives a bilinear utility $u_i(\rho, \sigma) = \mathrm{Tr}(R_i(\rho \otimes \sigma))$, where R_i is a Hermitian matrix. Quantum common-interest games, which are introduced and studied in this work, involve two players who jointly aim to maximize a shared bilinear utility function $u(\rho, \sigma) = \mathrm{Tr}(R(\rho \otimes \sigma))$.

We study quantum potential games under the paradigm of learning in games, where equilibration arises as the outcome of each agent implementing a strategy revision mechanism that relies on past interactions. Because of the equivalence between KKT points of a BSS instance and Nash equilibria of the corresponding game, learning dynamics for the quantum common-interest game give rise to decentralized algorithms for the BSS problem that are robust, easily implementable, and parallelizable algorithms.

Our results. In Section 3 we introduce quantum common-interest games. We show that any BSS instance can be interpreted as a quantum common-interest game where KKT points corresponds to Nash equilibria. In Sections 4 and 5 we study continuous and discrete-time dynamics respectively for learning in a quantum common-interest game. We show that if players update their states according to any of our dynamics, the utility is strictly increasing, limit points are fixed points, and interior fixed points are Nash equilibria. Finally, we perform extensive experiments to assess the performance of our dynamics. We demonstrate that our continuous-time dynamics empirically converges to Nash equilibria, while our discrete-time dynamics perform well ($\approx 0.97\mathrm{OPT}$) on the BSS problem.

*wayne_lin@mymail.sutd.edu.sg
†georgios@sutd.edu.sg
‡ryann_sim@mymail.sutd.edu.sg
§antonios@sutd.edu.sg

2 Preliminaries and related work

Classical games and learning dynamics. Natural first-order learning dynamics converge to various notions of equilibria in classes of classical games, see e.g. [20, 18, 28]. A well-studied first-order continuous-time dynamic are the replicator dynamics. For a two player CIG where players select simplex vectors x, y and receive common payoff $x^\top Ay$, the replicator dynamics (written only for the x-player) are given by:

$$\dot{x}_i = x_i((Ay)_i - x^\top Ay). \tag{REP}$$

see e.g. [36, 20, 6, 38]. In terms of properties, replicator dynamics converge to Nash equilibria in CIGs [20, 28] and are a gradient flow with respect to the Shahshahani metric $\langle v, w\rangle_x = \sum_i \frac{1}{x_i} v_i w_i$ [32].

There are three related discrete-time dynamics, the latter two of which have an adjustable stepsize $\epsilon > 0$:

$$x_i \leftarrow x_i \frac{(Ay)_i}{x^\top Ay}, \tag{BE}$$

$$x_i \leftarrow x_i \frac{1 + \epsilon(Ay)_i}{\sum_i x_i(1 + \epsilon(Ay)_i)}, \tag{lin-MWU}$$

$$x_i \leftarrow x_i \frac{\exp(\epsilon(Ay)_i)}{\sum_i x_i \exp(\epsilon(Ay)_i)}. \tag{exp-MWU}$$

These discrete-time dynamics are referred to respectively as the *Baum-Eagon update* [5], the *linear multiplicative weights update*, and the *exponential multiplicative weights update*, see e.g., [19, 2, 31, 12]. The utility function $x^\top Ay$ under both BE and lin-MWU is non-decreasing [5], and the limit points of lin-MWU are Nash equilibria [31].

Quantum games and learning dynamics. The majority of the literature on quantum games investigates the potential advantages of using quantum strategies over classical ones. To this end, researchers have developed quantum versions of well-known games such as the Prisoner's Dilemma and Matching Pennies [11]. In addition, an increasing amount of research has focused on studying quantum notions of equilibria, i.e., states that remain stable against unilateral player deviations [39], determine their tractability [7], and structural charactreizations of equilibrium sets [21]. Beyond the analysis of specific games, various attempts have been made to establish more general theories of quantum games that aim to unify the existing works, e.g., [17, 7].

In contrast, there are relatively few works that investigate learning in quantum games. Most existing results focus on the zero-sum regime, where players select density matrices ρ and σ and receive a bilinear utility $u_i(\rho, \sigma) = \mathrm{Tr}(R_i(\rho \otimes \sigma))$, subject to the constraint that $u_1(\rho, \sigma) + u_2(\rho, \sigma) = 0$. The payoffs can also be expressed explicitly as bilinear functions $u_i(\rho, \sigma) = \langle \rho, \Phi_i(\sigma)\rangle$, where R_i represents the Choi matrix of the superoperator Φ_i. In the zero-sum setting, the Matrix Multiplicative Weights Update (written only from the perspective of the ρ player) is given by:

$$\rho(t+1) \leftarrow \exp\left(\epsilon \sum_{\tau=1}^{t} \Phi(\sigma(\tau))\right), \tag{MMWU}$$

and converges (in the time-average sense) to Nash equilibria in quantum zero-sum games [25]. MMWU was first introduced for online optimization over the set of density matrices [2, 26, 37] MMWU has found many other applications: important examples include solving SDPs [3], proving that QIP=PSPACE [23], finding balanced separators [30], and spectral sparsification [1].

Recently, [24] introduced the exponential quantum replicator dynamics (exp-QREP), a (continuous-time) quantum analogue of an exponential expression of the replicator dynamics, given by:

$$\frac{d\rho}{dt} = \frac{d}{dt}\left(\frac{\exp(A)}{\mathrm{Tr}(\exp(A))}\right), \quad A(t) = \int_0^t \Phi(\sigma(\tau))d\tau. \tag{exp-QREP}$$

3 Quantum CIGs and the BSS

We define a two-player Quantum Common-Interest Game (CIG) between Alice and Bob, who have access to quantum registers $\mathcal{H}_1 = \mathcal{A}$ and $\mathcal{H}_2 = \mathcal{B}$ respectively, as one in which Alice selects a density matrix $\rho \in D(\mathcal{A})$, Bob selects a density matrix
$sigma \in D(\mathcal{B})$, and they both obtain common utilty

$$u(\rho, \sigma) = \mathrm{Tr}(R(\rho \otimes \sigma)) = \left\langle \rho, \Phi(\sigma^\top \right\rangle$$

for some Hermitian operator R. (R and Φ are related via the Choi isomorphism.)

We can define Alice's *best response set* to Bob's strategy $\sigma \in D(\mathcal{B})$ by $\mathrm{BR}_{\mathcal{A}}(\sigma) = \{\rho \in D(\mathcal{A}) : u(\rho, \sigma) \geq u(\rho', \sigma)\ \forall\ \rho' \in D(\mathcal{A})\}$, and analogously for Bob. The *Nash equilibria* (NE) of the game are the strategy profiles $(\rho, \sigma) \in D(\mathcal{A}) \times D(\mathcal{B})$ such that Alice's and Bob's strategies are best responses to each other, i.e.

$$u(\rho, \sigma) \geq u(\rho', \sigma)\ \forall\ \rho' \in D(\mathcal{A})$$

and

$$u(\rho, \sigma) \geq u(\rho, \sigma')\ \forall\ \sigma' \in D(\mathcal{B}).$$

Lastly, a Nash equilibrium (ρ, σ) is called *interior* if both ρ and σ are positive definite.

Relation between quantum CIGs and the BSS problem. In a quantum CIG, Alice and Bob try to jointly maximize their common utility function $u(\rho, \sigma) = \langle \rho, \Phi(\sigma)\rangle$. Analogous to the classical case, there is a strong connection among the NE of the game and the underlying BSS optimization problem. Recall that the BSS problem corresponds to maximizing a linear function over the set of separable states, i.e.,

Theorem 1 *The Nash equilibria of a two-player quantum common-interest game with common utility function $u(\rho, \sigma) = \langle \rho, \Phi(\sigma)\rangle$ correspond to the KKT points of BSS.*

For a classical game, if (x, y) is a Nash equilibrium, every pure strategy that is played by Alice with positive probability is a best response to y, i.e., for each i with $x_i > 0$ we have $(Ay)_i = x^T Ay$, and similarly for Bob. We have the analogous statement for quantum CIGs:

Theorem 2 *Let (ρ, σ) be a Nash equilibrium of a two-player quantum CIG with common utility $u(\rho, \sigma) = \langle \rho, \Phi(\sigma) \rangle$. If $\rho \succ 0$, we have that $\Phi(\sigma) = \langle \rho, \Phi(\sigma) \rangle \mathbb{1}_{\mathcal{B}}$, i.e., for any $\rho' \in D(\mathcal{A})$ we have $\rho' \in \mathrm{BR}_{\mathcal{A}}(\sigma)$. Similarly, if (ρ, σ) is a Nash equilibrium and $\sigma \succ 0$, then $\Phi^\dagger(\rho) = \langle \rho, \Phi(\sigma) \rangle \mathbb{1}_{\mathcal{A}}$.*

With the connection between Nash equilibria and KKT points established, and motivated by the well-known classical result that 'natural' learning dynamics converge to Nash equilibria in classical CIGs, in the next section we propose a non-commutative extension of one such family of gradient flow dynamics and study their theoretical convergence properties.

4 Continuous-time dynamics

We define the *linear quantum replicator dynamics*

$$\begin{aligned} \frac{\mathrm{d}\rho}{\mathrm{d}t} &= \rho^{1/2}\Big[\Phi(\sigma) - \langle \rho, \Phi(\sigma) \rangle \mathbb{1}_{\mathcal{A}}\Big]\rho^{1/2}, \\ \frac{\mathrm{d}\sigma}{\mathrm{d}t} &= \sigma^{1/2}\Big[\Phi^\dagger(\rho) - \langle \rho, \Phi(\sigma) \rangle \mathbb{1}_{\mathcal{B}}\Big]\sigma^{1/2}, \end{aligned} \tag{lin-QREP}$$

which were obtained as a normalized gradient flow of the utility with respect to the *quantum Shahshani metric*

$$\langle A, B \rangle_\rho := \mathrm{Tr}\Big[\rho^{-\frac{1}{2}} A \rho^{-\frac{1}{2}} B\Big]$$

which we define on the PSD manifold. We have the following results:

Theorem 3 *Consider a quantum CIG with utility function $u(\rho, \sigma) = \langle \rho, \Phi(\sigma) \rangle$ where $\rho \in D(\mathcal{A}), \sigma \in D(\mathcal{B})$. The lin-QREP dynamics define a gradient flow of the utility function $u(\rho, \sigma)$ on the product manifold $D(\mathcal{A}) \times D(\mathcal{B})$ imbued with the quantum Shahshahani metric. Moreover, the utility $u(\rho, \sigma)$ is strictly increasing along the trajectories of the lin-QREP dynamics.*

Corollary 4 *The set of ω-limit points of a trajectory $\{\rho(t), \sigma(t)\}_{t \geq 0}$ of the lin-QREP dynamics is a compact, connected set of fixed points of the dynamics that all attain the same utility.*

Theorem 5 *For a quantum CIG with common utility function $u(\rho, \sigma) = \langle \rho, \Phi(\sigma) \rangle$ where $\rho \in D(\mathcal{A}), \sigma \in D(\mathcal{B})$, we have the following two properties relating interior fixed points and ω-limit points of the lin-QREP dynamics with Nash equilibria of the game:*

(1) The set of interior fixed points of the lin-QREP dynamics is equivalent to the set of interior Nash equilibria.

(2) The interior ω-limits of any trajectory of the lin-QREP dynamics are Nash equilbria.

5 Discrete-time dynamics

We introduce the *Matrix Baum-Eagon update*

$$\begin{aligned} \rho^{new} &\leftarrow \frac{1}{\langle \rho, \Phi(\sigma) \rangle} \rho^{1/2} \Phi(\sigma) \rho^{1/2}, \\ \sigma^{new} &\leftarrow \frac{1}{\langle \rho^{new}, \Phi(\sigma) \rangle} \sigma^{1/2} \Phi^\dagger(\rho^{new}) \sigma^{1/2} \end{aligned} \tag{Matrix BE}$$

and the *Linear Matrix Multiplicative Weights Update*

$$\begin{aligned} \rho^{new} &\leftarrow \frac{\rho^{1/2}[\mathbb{1}_{\mathcal{A}} + \epsilon \Phi(\sigma)]\rho^{1/2}}{1 + \epsilon \langle \rho, \Phi(\sigma) \rangle}, \\ \sigma^{new} &\leftarrow \frac{\sigma^{1/2}[\mathbb{1}_{\mathcal{B}} + \epsilon \Phi^\dagger(\rho)]\sigma^{1/2}}{1 + \epsilon \langle \sigma, \Phi^\dagger(\rho) \rangle}. \end{aligned} \tag{lin-MMWU}$$

for an adjustable stepsize $\epsilon > 0$. Matrix BE and lin-MMWU are non-commutative extensions of BE and lin-MWU respectively, and the former is a special case of the latter in the limit $\epsilon \to \infty$. We have the following results:

Theorem 6 *For any quantum CIG with a positive definite game operator R, the common utility $u(\rho, \sigma) = \langle R, \rho \otimes \sigma \rangle = \langle \rho, \Phi(\sigma) \rangle$, is strictly increasing along the trajectories of Matrix BE or lin-MMWU, except when at a fixed point.*

Corollary 7 *The set of limit points of an orbit $\{(\rho(t), \sigma(t))\}_{t \in \mathbb{N}}$ of Matrix BE or lin-MMWU is a compact, connected set of fixed points.*

Theorem 8 *The set of fixed points of the discrete-time update rules Matrix BE and lin-MMWU are equal to the set of fixed points of the continuous-time gradient flow lin-QREP.*

6 Full paper

A full paper with proofs and experiments can be found on the arXiv at `https://arxiv.org/abs/2302.04789`.

References

[1] Z. Allen-Zhu, Z. Liao, and L. Orecchia. Spectral sparsification and regret minimization beyond matrix multiplicative updates. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 237–245, 2015.

[2] S. Arora, E. Hazan, and S. Kale. The multiplicative weights update method: a meta-algorithm and applications. *Theory of computing*, 8(1):121–164, 2012.

[3] S. Arora and S. Kale. A combinatorial, primal-dual approach to semidefinite programs. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 227–236, 2007.

[4] N. Bard, J. N. Foerster, S. Chandar, N. Burch, M. Lanctot, H. F. Song, E. Parisotto, V. Dumoulin, S. Moitra, E. Hughes, et al. The hanabi challenge: A new frontier for ai research. *Artificial Intelligence*, 280:103216, 2020.

[5] L. E. Baum and J. A. Eagon. An inequality with applications to statistical estimation for probabilistic functions of markov processes and to a model for ecology. *Bulletin of the American Mathematical Society*, 73(3):360–363, 1967.

[6] I. M. Bomze. Lotka-Volterra equation and replicator dynamics: a two-dimensional classification. *Biological cybernetics*, 48(3):201–211, 1983.

[7] J. Bostanci and J. Watrous. Quantum game theory and the complexity of approximating quantum nash equilibria. *Quantum*, 6:882, 2022.

[8] A. Dafoe, Y. Bachrach, G. Hadfield, E. Horvitz, K. Larson, and T. Graepel. Cooperative ai: machines must learn to find common ground. *Nature*, 2021.

[9] A. Dafoe, E. Hughes, Y. Bachrach, T. Collins, K. R. McKee, J. Z. Leibo, K. Larson, and T. Graepel. Open problems in cooperative ai. *arXiv preprint arXiv:2012.08630*, 2020.

[10] C. Daskalakis, S. Skoulakis, and M. Zampetakis. The complexity of constrained min-max optimization. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1466–1478, 2021.

[11] J. Eisert, M. Wilkens, and M. Lewenstein. Quantum games and quantum strategies. *Physical Review Letters*, 83(15):3077, 1999.

[12] Y. Freund and R. E. Schapire. A decision-theoretic generalization of on-line learning and an application to boosting. *Journal of computer and system sciences*, 55(1):119–139, 1997.

[13] I. Gemp, B. McWilliams, C. Vernade, and T. Graepel. Eigengame: PCA as a nash equilibrium. *arXiv preprint arXiv:2010.00554*, 2020.

[14] S. Gharibian. Strong NP-hardness of the quantum separability problem. *arXiv preprint arXiv:0810.4507*, 2008.

[15] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2. Springer Science & Business Media, 2012.

[16] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 10–19, 2003.

[17] G. Gutoski and J. Watrous. Toward a general theory of quantum games. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574, 2007.

[18] J. Hofbauer and W. H. Sandholm. On the global convergence of stochastic fictitious play. *Econometrica*, 70(6):2265–2294, 2002.

[19] J. Hofbauer and K. Sigmund. Evolutionary game dynamics. *Bulletin of the American mathematical society*, 40(4):479–519, 2003.

[20] J. Hofbauer, K. Sigmund, et al. *Evolutionary games and population dynamics*. Cambridge university press, 1998.

[21] C. Ickstadt, T. Theobald, and E. Tsigaridas. Semidefinite games. *arXiv preprint arXiv:2202.12035*, 2022.

[22] L. M. Ioannou. Computational complexity of the quantum separability problem. *arXiv preprint quant-ph/0603199*, 2006.

[23] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP=PSPACE. *Journal of the ACM (JACM)*, 58(6):1–27, 2011.

[24] R. Jain, G. Piliouras, and R. Sim. Matrix multiplicative weights updates in quantum zero-sum games: Conservation laws & recurrence. *arXiv preprint arXiv:2211.01681*, 2022.

[25] R. Jain and J. Watrous. Parallel approximation of non-interactive zero-sum quantum games. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 243–253. IEEE, 2009.

[26] S. Kale. *Efficient algorithms using the multiplicative weights update method*. Princeton University, 2007.

[27] H. Kitano, M. Asada, Y. Kuniyoshi, I. Noda, E. Osawa, and H. Matsubara. Robocup: A challenge problem for ai. *AI magazine*, 18(1):73–73, 1997.

[28] R. Kleinberg, G. Piliouras, and É. Tardos. Multiplicative updates outperform generic no-regret learning in congestion games. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 533–542, 2009.

[29] M. Moravčík, M. Schmid, N. Burch, V. Lisỳ, D. Morrill, N. Bard, T. Davis, K. Waugh, M. Johanson, and M. Bowling. Deepstack: Expert-level artificial intelligence in heads-up no-limit poker. *Science*, 356(6337):508–513, 2017.

[30] L. Orecchia, S. Sachdeva, and N. K. Vishnoi. Approximating the exponential, the Lanczos method and an O(m)-time spectral algorithm for balanced separator. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 1141–1160, 2012.

[31] G. Palaiopanos, I. Panageas, and G. Piliouras. Multiplicative weights update with constant step-size in congestion games: Convergence, limit cycles and chaos. *Advances in Neural Information Processing Systems*, 30, 2017.

[32] S. Shahshahani. *A new mathematical framework for the study of linkage and selection*. American Mathematical Soc., 1979.

[33] D. Silver, A. Huang, C. J. Maddison, A. Guez, L. Sifre, G. Van Den Driessche, J. Schrittwieser, I. Antonoglou, V. Panneershelvam, M. Lanctot, et al. Mastering the game of go with deep neural networks and tree search. *nature*, 529(7587):484–489, 2016.

[34] S. H. Singh. A Non-Negative Matrix Factorization game. *arXiv preprint arXiv:2104.05069*, 2021.

[35] P. Stone, G. Kaminka, S. Kraus, and J. Rosenschein. Ad hoc autonomous agent teams: Collaboration without pre-coordination. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 24, pages 1504–1509, 2010.

[36] P. D. Taylor and L. B. Jonker. Evolutionary stable strategies and game dynamics. *Mathematical biosciences*, 40(1-2):145–156, 1978.

[37] K. Tsuda, G. Rätsch, and M. K. Warmuth. Matrix exponentiated gradient updates for on-line learning and Bregman projection. *Journal of Machine Learning Research*, 6(Jun):995–1018, 2005.

[38] J. W. Weibull. *Evolutionary game theory*. MIT press, 1997.

[39] S. Zhang. Quantum strategic game theory. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 39–59, 2012.

Cost of the Fault-Tolerant Quantum Circuits

Yongsoo Hwang
Electronics and Telecommunications Research Institute, Daejon, 34129, Republic of Korea

Abstract. To realize fault-tolerant quantum computing, we need fault-tolerant quantum circuits of theoretically verified quantum protocols. Unlike topological codes, for concatenated codes, we have to find the fault-tolerant quantum circuits separately from the protocols. To resolve the geometric locality, the circuit must contain the qubit moves not revealed in the protocols. In this presentation, we analyze the cost by those qubit moves and discuss how to reduce it in theory.

Keywords: fault-tolerant quantum circuit, concatenated code

1 Introduction

Topological codes represented by surface code [1] and color code [2] have been paid attention for the last years due to a high threshold around $O(10^{-2})$ and local gate composition. On the other hand, concatenated codes have been less studied due to high hurdle for implementation. However, we believe some concatenated codes such as [[23,1,7]] Golay code [3, 4] are still important and can play significant role in implementing FTQC. For example, from the fixed code length, it is possible to build a syndrome lookup table, which makes an instant error decoding.

To implement FTQC based on concatenated codes, we have to generate quantum circuits that preserve *fault tolerance* and *locality*. To date, manually obtained circuits have been proposed for well-known small-sized codes [5, 6, 7]. Since they are optimized for a target case including a specific qubit layout, it can not be directly applied to other cases, in particular large codes.

The authors proposed a quantum circuit mapping algorithm suited for fault-tolerant quantum protocol [8]. They enumerated the requirements for the circuits of universal fault-tolerant quantum computing and implemented their idea with heuristic quantum circuit mapping algorithm.

In this presentation, we analyze the cost of the circuits of fault-tolerant quantum protocols based on the products of the fault-tolerant quantum circuit mapping algorithm described in Ref. [8].

2 Non-FT Circuit versus FT Circuit

The quantum circuit mapping on computational algorithms focuses on associating physical qubits and algorithm qubits with respect to the physical qubit connectivity. However, the circuit mapping on fault-tolerant quantum protocols has to check the type of the quantum state physical qubits hold because we have to block spreading quantum errors to data qubits. In this regard, the fault-tolerant quantum circuit produced by the circuit mapper specialized for the fault-tolerant protocols includes more SWAP gates and therefore has more faulty locations. Fig. 1 shows a reason why the FT circuit may need more SWAP gates.

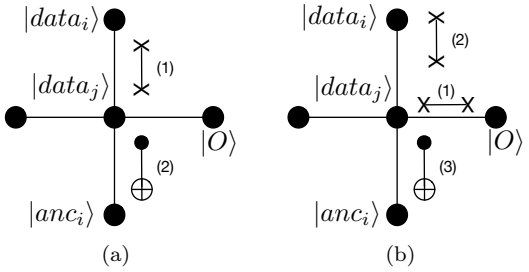


Figure 1: Qubit move to execute CNOT $|data_i\rangle, |anc_i\rangle$. Since both qubits are not located in neighbor, any qubit should be moved first. (a) Non-FT move including the noisy SWAP gate between data qubits $|data_i\rangle$ and $|data_j\rangle$. (b) FT move not including the noisy SWAP gate between data qubits. Note that $|O\rangle$ indicates a dummy qubit not carrying an important information.

Here we compare fault-tolerant circuit with large locations and non-fault-tolerant circuit with small locations in terms of the threshold and the yield of fault-tolerant preparation of logical basis state. From the results, we claim that the theoretical fault-tolerance of a protocol does not guarantee its fault-tolerant execution. We need a fault-tolerant quantum circuit.

3 FT Circuit on large qubit connectivity

In general, by taking a quantum chip having a larger qubit-connectivity, it becomes possible to make a quantum circuit of less depth. So far, most of the quantum circuits of fault-tolerant protocols implemented on 2-dimensional rectangular lattice [5, 6, 7]. In this presentation, we applied the quantum chips having larger connectivity than the conventional architectures for developing the fault-tolerant circuits (see Fig. 2). In particular, this work for the first time show the fault-tolerant quantum circuit working on 3-dimensional cube lattice. Table 1 compares the depths of the fault-tolerant quantum circuits of [[7,1,3]] Steane code on the various qubit architectures. As the connectivity increases, the depth is decreased even though the degree is not so large.

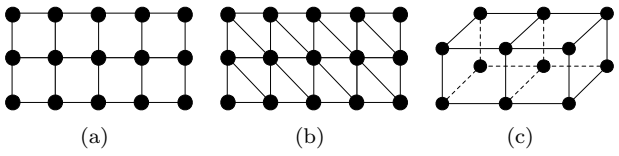


Figure 2: Qubit Connectivities: (a) 2D Rectangular Lattice, (b) 2D Triangular Lattice, and (c) 3D Cube Lattice

Table 1: Circuit Depth of FT Syndrome Measurement of [[7,1,3]] Steane code on Diverse Qubit Connectivities

Q-Chip Architecture	2D Rect. (5 X 7)	2D Tri. (5 X 7)	3D Cube (3 X 3 X 4)
Circuit Depth	35 [8]	34	32

4 Discussion

We say that for implementing fault-tolerant quantum computing, we need the quantum circuits that are executable in the fault-tolerant way, besides the protocols having the fault-tolerance. The topological code that is inherently composed of local gates and therefore the fault-tolerant protocol for the code is directly executable on a quantum device. However, for concatenated code, we have find such circuits separately.

To find a full set of quantum circuits for universal fault-tolerant quantum computing, we developed an algorithmic method and here we analyzed several cases. Since the method is heuristic, the results shown here may not be so remarkable. But, the method can be applied any target situation of concatenated code and the topological code cases for a certain non-trivial quantum chip architecture.

References

[1] Kitaev, A. Y. Fault-tolerant quantum computation by anyons. *Annals of Physics* **303**, 2 – 30 (2003-01).

[2] Bombín, H. & Martin-Delgado, M. A. Topological Quantum Distillation. *Physical Review Letters* **97**, 180501 – 4 (2006).

[3] Paetzick, A. & Reichardt, B. W. Fault-Tolerant Ancilla Preparation and Noise Threshold Lower Bounds for the 23-Qubit Golay Code. *Quantum Information and Computation* **12**, 1034–1080 (2012).

[4] Cross, A. W., Divincenzo, D. P. & Terhal, B. M. A comparative code study for quantum fault tolerance. *Quantum Information and Computation* **9**, 541–572 (2009).

[5] Svore, K. M., DiVincenzo, D. P. & Terhal, B. M. Noise Threshold for a Fault-Tolerant Two-Dimensional Lattice Architecture. *Quantum Information and Computation* **7**, 297–318 (2007).

[6] Spedalieri, F. M. & Roychowdhury, V. P. Latency in local, two-dimensional, fault-tolerant quantum computing. *Quantum Information & Computation* **9**, 666–682 (2009). 0805.4213.

[7] Lai, C.-Y., Paz, G., Suchara, M. & Brun, T. A. Performance and Error Analysis of Knill's Postselection Scheme in a Two-Dimensional Architecture. *Quantum Information & Computation* **14**, 807–822 (2014). 1305.5657.

[8] Hwang, Y. Fault-tolerant circuit synthesis for universal fault-tolerant quantum computing. *arXiv* (2022). 2206.02691.

Subsystem decompositions of quantum circuits and processes with indefinite causal order

Julian Wechs[1] * Ognyan Oreshkov[1] †

[1] *QuIC, Ecole Polytechnique de Bruxelles, C.P. 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*

Abstract. It has been found that one can conceive of processes where multiple parties locally perform quantum operations, but where the causal order between the parties is no longer well-defined. A central question is which of these processes have an operational interpretation or physical realisation, and, more particularly, whether and how indefinite causal order could be realised within standard physics. It has been shown that certain causally indefinite processes can take place as part of standard quantum mechanical evolutions, described by acyclic quantum circuits, if the latter are described with respect to an alternative choice of quantum subsystems which can be delocalised in time. In this contribution, we provide a general framework to describe such transformations between different subsystem decompositions of quantum circuits. On this basis, we then analyse transformations between different causal perspectives in the *quantum switch*, which turn out to be inequivalent from the subsystem perspective we developed.

Keywords: Quantum causality, Indefinite causal order, Process matrix framework, Causal (non)separability, Time-delocalised quantum subsystems

This submission is based on Ref. [1], as well as follow-up work in progress.

1 Introduction and context

Recently, there has been significant interest in the question of what quantum theory implies for our understanding of causality, and what new types of causal relations can emerge in the presence of quantum effects. In particular, it has been found that one can theoretically conceive of situations where the causal order between quantum operations is no longer well-defined. Such indefinite causal order arises in the *process matrix framework* [2], where one assumes separate parties that locally abide by the laws of quantum theory, but that are not embedded into any a priori causal structure, and one studies the most general correlations that these parties can establish. Through this general top-down approach, on the one hand, one recovers standard quantum scenarios such as measurements on multipartite quantum states, or quantum circuits in which the parties apply their operations in a fixed causal order. On the other hand, one also finds so-called *causally nonseparable processes*, in which the parties cannot be assigned a well-defined causal order (see e.g. Refs.[2, 3, 4, 5, 6, 7]).

The operational meaning or physical realisability of these causally nonseparable processes is one of the central questions in the field. In particular, a central open problem is which of these processes are realisable in standard physics, without resorting to exotic physical effects or new physical regimes such as quantum gravity. A framework to formally pose and investigate this question is that of *time-delocalised quantum subsystems* [1, 8]. Namely, certain indefinite causal order processes can be shown to take place as part of standard quantum mechanical time evolutions, described by acyclic quantum circuits, if the latter are described with respect to an alternative choice of quantum systems. These alternative systems are delocalised over several of the standard, "time-local" systems in the circuit which are associated to different times.

Such realisations on time-delocalised systems notably exist for indefinite causal order processes that are based on coherent control of the order of operations [8, 9] (in particular, for the *quantum switch* [3, 10], a paradigmatic, widely studied example of a causally nonseparable process). Recently, it has been shown that a larger class of tripartite processes, that of *tripartite processes with a unitary extension* [11], also has realisations on time-delocalised subsystems [1]. This class includes some exotic examples that violate so-called *causal inequalities* (see e.g. [2, 4, 5, 6, 12, 13]), and that require new ways of time-delocalising quantum operations, beyond those achievable by coherent control of causal orders.

In this submission, we provide a general framework to describe different subsystem decompositions of quantum circuits. For a given quantum circuit, we consider the tensor product of all its operations, which defines a quantum operation acting on the joint Hilbert space of all systems in the circuit. An alternative subsystem decomposition of the circuit is then defined by an alternative tensor factorisation of this joint Hilbert space. Our formulation provides a convenient and concise way to formalise the notion that certain processes with indefinite causal order have a realisation on time-delocalised subsystems. Namely, the situations described in the process matrix formalism can be understood as particular instances of cyclic quantum circuits, and having a realisation on time-delocalised subsystems means that these cyclic quantum circuits can be transformed into standard, acyclic circuits through a subsystem transformation of the type we define here. For the known examples of causally indefinite processes on time-delocalised systems, this construction requires considering a "fine-grained" or "extended" process matrix picture—that is, the cyclic circuits that get transformed into acyclic ones involve additional systems, over which one needs to compose to recover the process matrix

*julian.wechs@ulb.be
†ognyan.oreshkov@ulb.be

situation [1]. This fact has implications for the question of whether one can transform between different temporal circuits that realise the quantum switch, and which describe different "causal perspectives" in which one of the operations is respectively localised in time. From the subsystem perspective we develop, these causal perspectives turn out to be inequivalent, because the respective "fine-grained" or "extended" cyclic circuits including the additional systems are different in the two cases. This raises the question of whether the framework can be extended or modified to account for such transformations between causal perspectives.

2 Subsystem decompositions of quantum circuits

Quantum experiments can be abstractly described in terms of a *quantum circuit*, that is, a collection of quantum operations (pictorially represented by "boxes") that are composed through quantum systems (pictorially represented by "wires"), see Fig. 1 for an example.

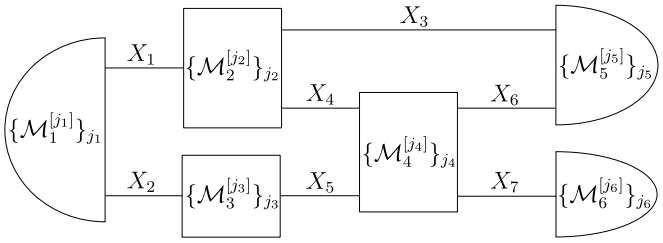


Figure 1: An example of a quantum circuit. Here, we have an acyclic circuit consisting of operations $\{\mathcal{M}_1^{[j_1]}\}_{j_1}$, ..., $\{\mathcal{M}_6^{[j_6]}\}_{j_6}$, which are composed over quantum systems X_1, ..., X_7.

The quantum operations are, in the most general case, *quantum instruments*, that is, collections of completely positive (CP) maps, each associated to a measurement outcome, whose sum is a completely positive and trace-preserving map. For a circuit with no open wires, the composition of all operations corresponds to the joint probability of the measurement outcomes [14, 15].

In Fig. 2, we illustrate the general idea of how to transform between alternative subsystem descriptions of one and the same quantum circuit. For that purpose, we "unfold" the circuit as on the left-hand side in Fig. 2—that is, we consider the tensor product of all operations in the circuit, which defines a quantum operation $\{\mathcal{M}^{[j_1,\ldots,j_N]}\}_{(j_1,\ldots,j_N)}$, with $\mathcal{M}^{[j_1,\ldots,j_N]} := \mathcal{M}_1^{[j_1]} \otimes \cdots \otimes \mathcal{M}_N^{[j_N]}$, that acts on all systems in the circuit. The composition over all systems is obtained by feeding the output of this operation back into its input. In general, the decomposition of a quantum system into subsystems is defined by a tensor factor decomposition of the corresponding Hilbert space. Here, an alternative subsystem decomposition of the circuit is thus most generally defined by an isomorphism J which defines another tensor factorisation of the joint Hilbert space of all systems, and which acts on the input and output Hilbert space of the operation describing the quantum circuit (cf. the middle of Fig. 2). This defines the description of the circuit with respect to the new systems (cf. the right-hand side of Fig. 2) which is given by an quantum instrument $\{\mathcal{N}^{[j_1,\ldots,j_N]}\}_{(j_1,\ldots,j_N)}$ with CP maps $\mathcal{N}^{[j_1,\ldots,j_N]} = J \circ \mathcal{M}^{[j_1,\ldots,j_N]} \circ J^{-1}$. With respect to an arbitrary subsystem decomposition, a standard, temporally ordered circuit can contain cycles [1, 8].

3 Application to indefinite causal order processes

Quantum processes with indefinite causal order are formally described in the *process matrix framework* [2]. There, one considers parties that locally perform quantum instruments, but that are not a priori embedded into any global causal order. The object which connects the parties is the *process matrix*, which formally describes a channel that takes the output systems of the parties back to their input systems. A quantum process can thus be understood as a cyclic quantum circuit, in which the (variable) local operations performed by the parties are composed in a cyclic manner with the (fixed) channel corresponding to the process matrix, see Fig. 3.

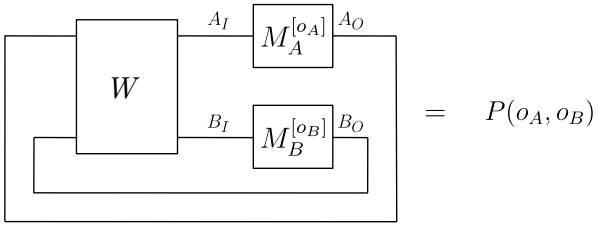


Figure 3: In the process matrix framework, the local operations performed by the parties are composed with the process matrix, which defines a channel from the output systems of the parties back to their input systems, in a circuit with a cycle.

Certain processes with indefinite causal order have realisations on time-delocalised systems [1, 8]. That is, one can find a standard, acyclic quantum circuit (with "variable" operations, depending on the local operations that the parties are to apply), which precisely corresponds to the cyclic circuit considered in the process matrix framework when described in terms of suitable alternative subsystems. This is, in particular, the case for unitary extensions of bipartite [8] and tripartite [1] processes.

Our general formulation of subsystem decompositions of quantum circuits allows us to formalise this idea in a simpler and more concise way. Namely, a given cyclic circuit is realisable on time-delocalised subsystems precisely if there exists a circuit transformation of the type we described in Sec. 2, which maps it back to a standard, acyclic quantum circuit.

For the examples of indefinite causal order processes that have been shown so far to have realisations on time-delocalised subsystems, it is however necessary to embed them into a larger circuit, i.e., one needs to consider some "fine-grained" process matrix picture, from which

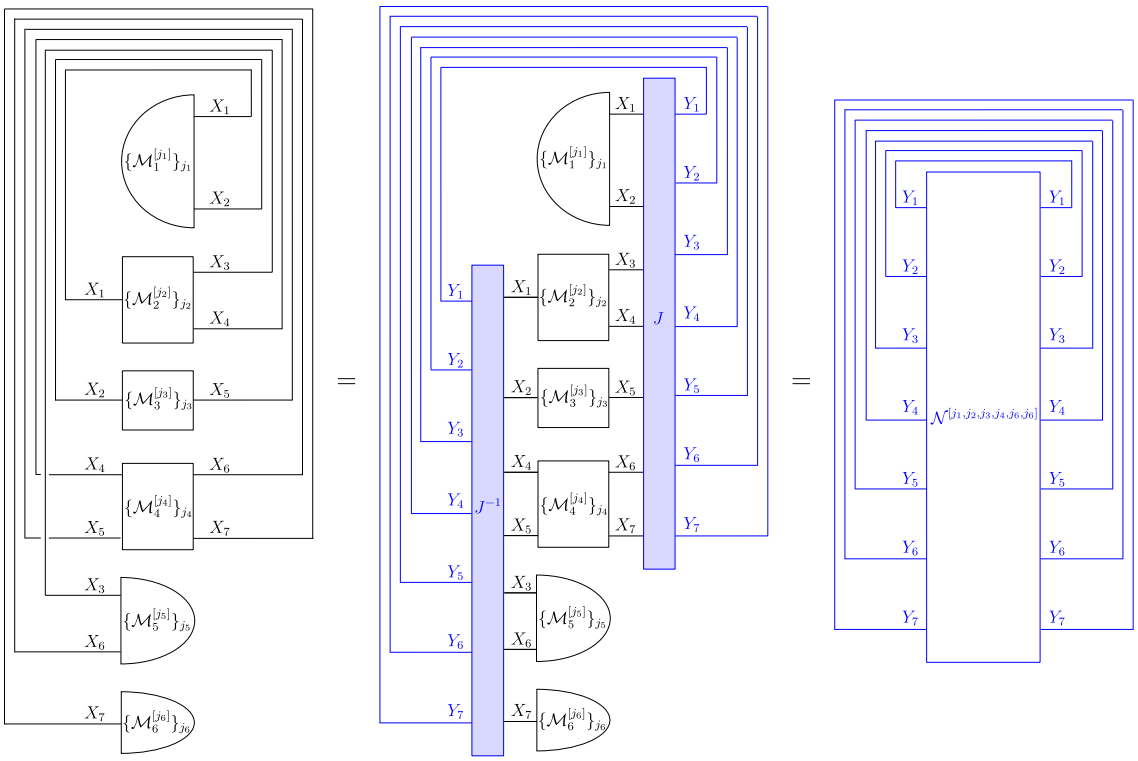


Figure 2: General prescription to change the subsystem decomposition of a quantum circuit. The circuit is "unfolded" as on the left-hand side, i.e., one considers a quantum operation consisting of all boxes in the circuit, which acts on the joint Hilbert space of all systems in the circuit. Another subsystem decomposition of the same circuit is defined in terms of an isomorphism J which acts on the joint Hilbert space of all systems in the circuit, and defines a new factorisation thereof.

the cyclic circuit consisting of the process matrix and the local operations can be recovered by partially composing over certain of the subsystems [1, 8].

4 Transformations between "causal perspectives" in the quantum switch

The *quantum switch* [3, 10] is a paradigmatic example of a causally nonseparable process, in which two parties Alice and Bob apply their operations in an order that is controlled coherently. This process can be realised on time-delocalised systems in different ways—that is, there are several temporal circuits that one can associate to the quantum switch via the correspondence described in the previous section. In particular, one can realise the quantum switch through the two temporal circuits shown in Fig. 4. In Fig. 4(a), we have a temporal circuit in which the operation U_A associated to Alice occurs at a definite time, while the operation U_B, associated to Bob, occurs either before it or after it, depending on the state of the control system, which is initialised in the "global past". In Fig. 4(b), the situation is reversed, and Bob's operation occurs at a definite time. The two temporal circuits can be interpreted as describing the "causal perspectives" [16] associated to the two parties Alice and Bob, respectively. Each circuit describes a situation where one respective operation is "temporally localised", while the other operation is delocalised around it.

One may wonder whether it is possible to find a transformation between subsystem decompositions that directly relates the circuit in Fig. 4(a) to the circuit in Fig. 4(b). Interestingly, it turns out that in our framework, such a subsystem transformation between the two "causal perspectives" does not exist—although the two temporal circuit both realise the quantum switch, the "fine-grained" process matrix picture which one obtains in the two cases is not the same, and one can show that there is no isomorphism between subsystem descriptions of the two circuits that relates them. This raises the question of whether and how the framework could be modified to account for transformations between different causal perspectives, e.g. by considering a continuous version.

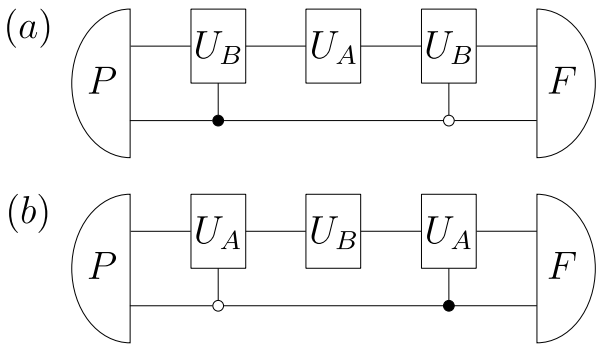


Figure 4: Two temporal circuits for the quantum switch, which describe the "causal perspectives" of Alice and Bob, respectively.

References

[1] J. Wechs, C. Branciard, and O. Oreshkov. Existence of processes violating causal inequalities on time-delocalised subsystems. *Nat Commun 14, 1471*, 2023.

[2] O. Oreshkov, F. Costa, Č. Brukner. Quantum correlations with no causal order. *Nat Commun 3*, 1092, 2012.

[3] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, Č. Brukner. Witnessing causal nonseparability. *New J. Phys. 17, 102001*, 2015.

[4] O. Oreshkov, C. Giarmiatzi. Causal and causally separable processes. *New J. Phys. 18, 093020*, 2016.

[5] C. Branciard, M. Araújo, A. Feix, F. Costa, Č. Brukner. The simplest causal inequalities and their violation. *New J. Phys. 18 013008*, 2016.

[6] A. A. Abbott, C. Giarmatzi, F. Costa, and C. Branciard. Multipartite causal correlations: Polytopes and inequalities. *Phys. Rev. A 94, 032131*, 2016.

[7] J. Wechs, A. A. Abbott, and C. Branciard. On the definition and characterisation of multipartite causal (non)separability. *New J. Phys. 21 013027*, 2019.

[8] O. Oreshkov. Time-delocalized quantum subsystems and operations: on the existence of processes with indefinite causal structure in quantum mechanics. *Quantum 3, 206*, 2019.

[9] J. Wechs, H. Dourdent, A. A. Abbott, and C. Branciard. Quantum circuits with classical versus quantum control of causal order. *PRX Quantum 2, 030335*, 2021.

[10] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron. Quantum computations without definite causal structure. *Phys. Rev. A 88, 022318*, 2013.

[11] M. Araújo, A. Feix, M. Navascués, Č. Brukner. A purification postulate for quantum mechanics with indefinite causal order. *Quantum 1, 10*, 2017.

[12] Ä. Baumeler, A. Feix, and S. Wolf. Maximal incompatibility of locally classical behavior and global causal order in multi-party scenarios. *Phys. Rev. A 90, 042106*, 2014.

[13] Ä. Baumeler, and S. Wolf. The space of logically consistent classical processes without causal order. *New. J. Phys. 18, 013036*, 2016.

[14] L. Hardy. Operational structures as a foundation for probabilistic theories. Perimeter Institute Recorded Seminar Archive http://pirsa. org/09060015/, 2009.

[15] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Probabilistic theories with purification. *Phys. Rev. A 81, 062348*, 2010.

[16] P. A. Guérin, and Č. Brukner. Observer-dependent locality of quantum events. *New J. Phys. 20, 103031*, 2018.

Coreset Selection for Quantum Learning Algorithms *

Yiming Huang[1] Huiyuan Wang[2] Yuxuan Du[3] Xiao Yuan[1]

[1] *Department of Computer Science, Center on Frontiers of Computing Studies, Peking University, Beijing 100871, China*

[2] *Peterhouse, Univeristy of Cambridge, CB2 1RD Cambridge, Cambridgeshire, U.K.*

[3] *JD Explore Academy, Beijing 101111, China.*

Abstract. Quantum machine learning (QML) is a promising approach for leveraging quantum advantages in the noisy intermediate-scale quantum (NISQ) era. However, practical challenges remain in handling massive data sets. To tackle this, we propose coreset selection, which reduces training data size while maintaining competitive performance for quantum learning algorithms. We formalize coreset selection as a k-set cover problem and analyze the generalization performance of quantum learning models trained on coreset. We apply the proposed method to three quantum learning tasks including synthetic data classification, quantum correlation classification, and quantum compiling. The numerical results obtained in this study provide evidence that models trained on coreset outperform those trained using random sampling. The coreset not only enhances the performance of quantum learning models but also accelerates the training time, addressing a critical concern in the context of NISQ devices.

Keywords: quantum machine learning, coreset, quantum kernels, variational quantum algorithm

1 Introduction

Classical machine learning models have achieved remarkable success across diverse fields, benefiting from vast amounts of data [15] [10] [12]. To leverage the potential of quantum computing in solving learning problems, quantum machine learning (QML) has gained significant attention, spanning from theoretical exploration to practical applications [3] [6] [5]. In certain scenarios, QML has demonstrated quantum advantages over classical counterparts, such as enhanced performance on challenging synthetic data or improved effective dimensionality [1] [14] [18]. Data is essential in both classical and quantum settings. In classical models, abundant data enables better training and higher accuracy, given sufficient capacity and expressivity. However, in the context of noisy intermediate-scale quantum (NISQ) machines, increased data volume poses challenges for storage, access, and analysis. Effective loading of enormous amounts of data from classical to quantum presents a significant challenge. Thus, QML models hardly show their true power under the limits in practical terms. In terms of feature engineering, it often applies the kernel trick to encode classical samples into quantum-enhanced feature space. The advantage is the capability of capturing the intractable complex patterns that classical methods are hard to handle. However, the complexity of estimating the quantum kernel matrix is still $O(n^2)$, where n is the training set size which is computationally infeasible when dealing with large data sets. Besides, when considering training efficiency, the quantum learning model, such as a quantum neural network (QNN), trained on a large data set naturally takes a long time to converge.

2 Overview of main results

Here we devise a generic method that can construct a reduced data set yielding competitive performance with the original training data set for most QML models. More precisely, we propose a coreset-based method to distill a handcraft dataset from the original dataset in the preprocessing procedure. We further analyze the comparable generalization performance of QNN and quantum kernel learning when they are optimized under the original dataset and the coreset. Numerical simulations on synthetic data, identification of non-classical correlations in quantum states, and quantum circuit compilation confirm the effectiveness of our proposal.

In the remainder of this section, we first introduce the basic knowledge of coreset and generalization error, followed by presenting the proposed coreset selection algorithm and exhibiting the corresponding generalization error of QNNs and quantum kernels.

Coreset The coreset selection, originally developed in computational geometry, provides a framework for approximating various measures of point sets by identifying a small subset [2]. This concept has been extended to practical coreset approaches that assist in tackling computationally challenging problems in machine learning [4] [11]. The underlying idea is to find a representative subset of the data that allows a learning model trained on this subset to achieve competitive performance compared to models trained on the entire data set. For example, the coreset method for support vector machines utilizes the minimum enclosing ball (MEB) algorithm to approximate the solution [19], while approaches for k-Means and k-Median clustering aim to compute a weighted subset of points with an acceptable approximation error [13].

Performance Analysis of Learning Models The goal of the supervised learning algorithm is to find a hypothesis $f : \mathcal{X} \to \mathcal{Y}$ with parameters $\boldsymbol{w}$ such that the true risk R on given data is minimized, $R = \mathbb{E}_{\boldsymbol{x},y}[l((f, \boldsymbol{x}, y))]$, where $l(\cdot)$ is the function that measures the degree of fit between the output of hypothesis $f(\boldsymbol{x})$ and ground

*See the attached file for the technical version of the submission.

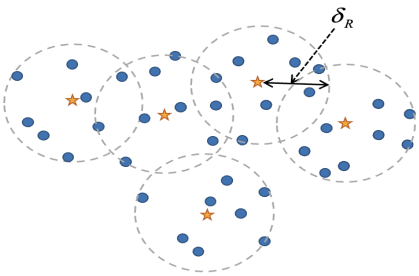


Figure 1: The illustration of k set cover problem. The red stars are the picked k points with δ_R radius covering the entire set. In the case shown in figure, there are 5 center data points $P_k \in \mathcal{D}, k \in [5]$ such that the maximum distance from any point in $\mathcal{D}$ to its closest center is minimized.

truth y. As it is impossible and necessary to access all the data, thus we employ the empirical risk $R_e = \frac{1}{S_t}\sum_{\boldsymbol{x}_i, y_i \in S_t} l(f, \boldsymbol{x}_i, y_i)$ on training data S_t to approximate instead. Since our aim is to explore the performance of the learning model with coreset selection, we analyze the following upper bound of the true risk R,

$$R \leq \underbrace{\|R - R_e\|}_{\text{generalization error}} + \underbrace{\|R_e - R_c\|}_{\text{coreset error}} + \underbrace{\|R_c\|}_{\text{training error}} . \quad (1)$$

Coreset Selection Algorithm Enhancing quantum learning models through coreset selection involves choosing a subset $\mathcal{S}_c$ of points $\boldsymbol{x}_j$ from the entire data set $\mathcal{S}_t$. The objective is to minimize the difference in average empirical loss between the entire data set and the selected subset. We regard coreset construction as a k set cover problem, where a few points with a radius of δ_R are chosen to cover the entire set. In practical terms, finding a subset that covers the entire data set is equivalent to solving a k-center problem. The goal is to identify k data points as centers $\mathcal{C}$, minimizing the maximum distance between any point $s \in \mathcal{S}_t$ and its nearest center. In other words, the aim is to select $\mathcal{C}$ such that the radius δ_R is minimized.

$$\mathcal{S}_c = \arg \min_{\mathcal{C} \subseteq \mathcal{S}_t, |\mathcal{C}|=k} \max_{\boldsymbol{x}_j \in \mathcal{S}_t} D(\boldsymbol{x}_j, \boldsymbol{x}_c) \quad (2)$$

where the $D(\boldsymbol{x}_i, \boldsymbol{x}_c) = \min_{\boldsymbol{x}_c \in \mathcal{C}} d(\boldsymbol{x}_i, \boldsymbol{x}_c)$ denotes the distance between point i to its closest center. Although it is an NP-Hard problem, there is a provable greedy algorithm that can efficiently get a 2-approximate solution, that is if $\mathcal{S}_c^*$ is the optimal solution of Eq. (2), it is proven to find a solution $\mathcal{S}_c$ such that $\delta_{\mathcal{C}}^* \leq \delta_{\mathcal{C}} \leq 2 \cdot \delta_{\mathcal{C}}^*$.

Generalization bounds with coreset Based on the aforementioned coreset construction strategy, we investigate the true risk of two mainstream quantum learning protocols, QNN and quantum kernel, built with coreset. These results give a rigorous analysis that combines the out-of-sample performance and coreset performance.

QNN We utilize the greedy algorithm to construct k-center coreset and feed it as the training data to QNN. In classification, QNN typically employs a parameterized quantum circuit (PQC) $U(\boldsymbol{\theta})$ that consists of a sequence of m fixed or gates parametrized quantum gates, generated by the Hermitian operator H_i and represented as $U(\theta_i) = \exp(-i\theta_i H_i)$, to evaluate state $|\boldsymbol{x}\rangle$ which encodes the training data $\boldsymbol{x}$. Then it estimates the expectation value of observable M as the output. According to the loss function $l(f_{\boldsymbol{\theta}}; \boldsymbol{x}, y) = \frac{1}{2}(\langle 0|U^\dagger(\boldsymbol{x})U^\dagger(\boldsymbol{\theta})MU(\boldsymbol{\theta})U(\boldsymbol{x})|0\rangle - y)^2$, QNN iteratively updates the parameters θ of PQC to minimize the empirical risk R_e. we assume the training loss $l(f_{\boldsymbol{\theta}}; \boldsymbol{x}_i, y_i)$ over coreset $\mathcal{S}_c$ is equal to zero. Thus, only the first two terms in Eq. (1) we need to consider which are generalization error and coreset error. Given N_t training data $\{\boldsymbol{x}_i, y_i\}_{i=1}^{N_t}$, Ref. [8] proved that the upper bound of the generalization error is $\|R - R_e\| \in \mathcal{O}(L\sqrt{\frac{m\log(m)}{N_t}} + L\sqrt{\frac{\log(1/\delta)}{N_t}})$.

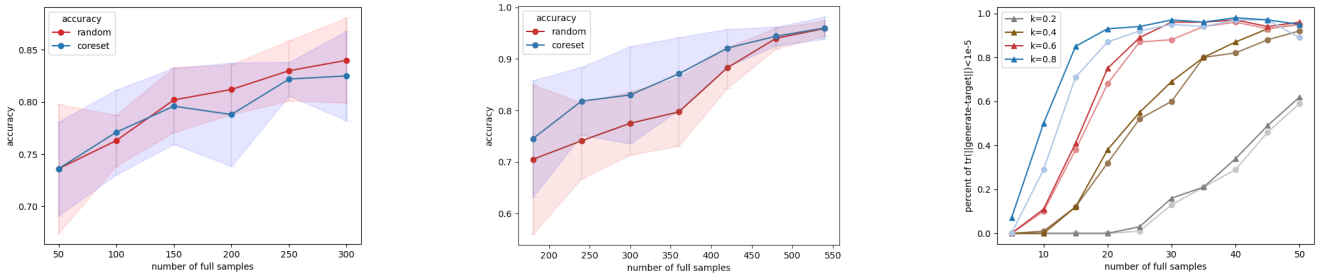
With regard to the coreset error, since we assume the training error over coreset is zero, the coreset error only leaves the term of the empirical error over the full data set, i.e. $\frac{1}{N_t}\sum_i l(f_\theta, \boldsymbol{x}_i, y_i)$. Thus, if we are able to give a bound of $\mathbb{E}_{\boldsymbol{x},y}[l(f_\theta; \boldsymbol{x}, y)]$, then the coreset error can be bounded. Assume there are λ_η-Lipshcitz continuous class-specific regression functions $\eta_c(\boldsymbol{x}) = p(y = c|\boldsymbol{x})$ for all class c, the loss $l(f_\theta, \cdot, y)$ is bounded by L, and we construct δ_c coreset to cover full data set, we have the following bound on coreset error, $\|R_e - R_c\| \in \mathcal{O}(\delta_c m\|M\|^2 + \delta_c\lambda_\eta L|c|)$. Combine the generalization error and coreset error together, we reach the bound for the true risk

$$R \in \mathcal{O}(L\sqrt{\frac{m\log(m)}{N_t}} + L\sqrt{\frac{\log(1/\delta)}{N_t}} + \delta_c m\|M\|^2 + \delta_c\lambda_\eta L|c|).$$

It provides valuable insights into sample complexity bounds. For any given $\varepsilon > 0$, we can ensure, with a high probability of success, that $R \leq \varepsilon$ require training data of size $N_t \in \mathcal{O}(\frac{m\log m}{\varepsilon^2 + \delta_c^2 m^2})$. Remarkably, this sample complexity scales effectively in a linear manner with the number of parameterized gates m. These results highlight the effectiveness and efficiency of our approach in achieving accurate and reliable results with a reasonable amount of training data.

Quantum Kernel Quantum kernels are kernel functions that utilize a quantum embedding from a real-valued vector $\boldsymbol{x} \in \mathbb{R}^d$ to a quantum state $U_{\boldsymbol{x}}|0\rangle$. From the quantum state, one can devise a kernel function $\kappa(\boldsymbol{x}, \boldsymbol{x}')$, mapping to a real value, representing the closeness of the two states in some high dimensional Hilbert space. The common choice of the quantum kernel function is $|\langle 0|U_{\boldsymbol{x}_i}^\dagger U_{\boldsymbol{x}_j}|0\rangle|^2$, though any other symmetric positive-definite functions are also valid candidates. Different forms of the quantum kernel correspond to different feature maps in Hilbert space, which could provide quantum advantage for classification tasks if designed properly [16].

Adopting a quantum-kernel-based hypothesis of the form $\langle \boldsymbol{w}, \phi(\boldsymbol{x})\rangle$ to predict the class label, either Support Vector Machine (SVM) or other relevant models can be applied to perform binary classification tasks on data distribution $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$, where $\mathcal{X}$ is the feature space bounded by Euclidean radius of r, and $\mathcal{Y}$ is label space with $y_i \in \{1, -1\}$. Given N_t number of training samples,



(a) classification by quantum kernel, (b) correlation classification by QNN, (c) compiling by QNN,

Figure 2: (a) and (b) demonstrate the performance of quantum kernel and QNN on classification over synthetic data and quantum correlation, respectively. The shaded area refers to the range of the test accuracy while the solid line represents the average accuracy. (c) The performance comparison between the different compression ratio of coreset on compiling task. The solid dark and light lines represent the models trained on the coreset and random samples. The vertical axis represents the percentage of states in the test set for which the trace distance to their corresponding targets is below 10^{-5}.

the parameters of the model could be optimized to $\boldsymbol{w}^*$. When exposing to the full distribution, the generalization error of the model would be bounded by [14], i.e.,

$$\|R - R_e\| \in \mathcal{O}(\sqrt{\frac{\sqrt{\langle \boldsymbol{w}^*, \boldsymbol{w}^* \rangle}}{N_t}} + \sqrt{\frac{\log(4/\delta)}{N_t}}).$$

If we utilize quantum kernel to encode each training point to a N_q qubit system and further condense these N_t samples to a coreset with fewer samples using k set cover selection with radius δ_c. The true risk of the model could be bounded by the following (assuming zero in-coreset error and up-to-quadratic terms in Hamiltonian):

$$R \in \mathcal{O}(\sqrt{\frac{\sqrt{\langle \boldsymbol{w}^*, \boldsymbol{w}^* \rangle}}{N_t}} + \sqrt{\frac{\log(4/\delta)}{N_t}} + \delta_c d^{2.5} N_q \max_j |w_j^*| r + \delta_c \lambda_\eta L |c|).$$

This result is in accordance with the general interpretation that a wider geometric margin, $1/||\boldsymbol{w}^*||_2$, means less generalization error. However, it should be noted that the optimized parameters in the bounds are not known prior to the optimization, at the data selection stage, which depends on the selected coreset, the form of the kernel function, and also the optimization objective [14].

3 Numerical Results

In this section, we employ the coreset selection method for three related learning tasks including 1) classification of synthetic data with quantum advantage. 2) classification of quantum correlations, and 3) quantum compiling. Here we mainly present the key results and defer the omitted details in the technical version.

Classification by Quantum Kernel We employ the coreset selection for a classifier with quantum kernel on the synthetic data set $\{\boldsymbol{x}_i, y_i\}_{i=1}^{N_t}$. The construction rule of the synthetic data set follows Ref. [14]. In Fig 2a, we compare the classification performance of coreset and random sampling as the data reduction strategy. Two methods exhibit similar performance, possibly due to the fact that the synthetic data is approximately evenly distributed. In which case, the geometrical uniformity guaranteed by the coreset approach is in no significant difference to the random sampling following the probabilistic distribution.

Correlation Classification by QNN We employ the quantum neural network combined with coreset selection in this learning task. We consider a family of quantum states characterized by parameters p and θ, defined as follows:

$$\rho_{AB}(p, \theta) = p|\psi_\theta\rangle\langle\psi_\theta| + (1-p)\frac{\mathbb{I}}{2} \otimes tr_A(|\psi_\theta\rangle\langle\psi_\theta|) \quad (3)$$

where the $p \in (0, 1)$, $\theta \in (0, 2\pi)$ and state $|\psi_\theta\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$. Fig.2b shows our numerical results. The numerical investigation demonstrates that the accuracy of the coreset overperforms the random sampling under different training samples under 40% compression ratio.

Quantum Compiling by QNN Compiling a unitary or algorithm into gate sequences is a challenging task for NISQ quantum devices, considering functionality, circuit connectivity, and hardware limitations. Recent advancements optimize the PQC to approximate the desired unitary [7, 9, 17]. Besides, there are some works also exploring how to generate few data for compiling [8, 20]. In this study, we apply a quantum neural network for tackling the compiling task. Training data consists of randomly chosen input states and their corresponding outputs when a target unitary U is applied, denoted as $\{|\psi_j\rangle, U|\psi_j\rangle\}_{j=1}^{N_t}$ for an n-qubit system. To approximate U, we minimize the empirical loss, which is the squared trace distance between the target states $U|\psi_j\rangle$ and the parametrized output states $U(\theta)|\psi_j\rangle$, using randomly sampled states in the Hilbert space. The numerical results of the compiling task, spanning a compression ratio range from 20% to 80%, are depicted in Fig. 2c.

References

[1] Amira Abbas, David Sutter, Christa Zoufal, Aurélien Lucchi, Alessio Figalli, and Stefan Woerner. The power of quantum neural networks. *Nature Computational Science*, 1(6):403–409, 2021. doi: 10.1038/s43588-021-00084-1.

[2] Pankaj K Agarwal, Sariel Har-Peled, Kasturi R Varadarajan, et al. Geometric approximation via coresets. *Combinatorial and computational geometry*, 52(1), 2005.

[3] Srinivasan Arunachalam and Ronald de Wolf. A survey of quantum learning theory. *ArXiv*, abs/1701.06806, 2017.

[4] Olivier Bachem, Mario Lucic, and Andreas Krause. Practical coreset constructions for machine learning. *arXiv preprint arXiv:1703.06476*, 2017.

[5] Marcello Benedetti, Erika Lloyd, and Stefan H. Sack. Parameterized quantum circuits as machine learning models. *ArXiv*, abs/1906.07682, 2019.

[6] Jacob D. Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549:195–202, 2017.

[7] M Bilkis, Marco Cerezo, Guillaume Verdon, Patrick J Coles, and Lukasz Cincio. A semi-agnostic ansatz with variable structure for quantum machine learning. *arXiv preprint arXiv:2103.06712*, 2021.

[8] Matthias C Caro, Hsin-Yuan Huang, M Cerezo, Kunal Sharma, Andrew Sornborger, Lukasz Cincio, and Patrick J Coles. Generalization in quantum machine learning from few training data. *arXiv preprint arXiv:2111.05292*, 2021.

[9] Matthias C Caro, Hsin-Yuan Huang, Marco Cerezo, Kunal Sharma, Andrew Sornborger, Lukasz Cincio, and Patrick J Coles. Generalization in quantum machine learning from few training data. *Nature communications*, 13(1):1–11, 2022.

[10] Jonas Degrave, Federico Felici, Jonas Buchli, Michael Neunert, Brendan D. Tracey, Francesco Carpanese, Timo Ewalds, Roland Hafner, Abbas Abdolmaleki, Diego de Las Casas, Craig Donner, Leslie Fritz, Cristian Galperti, Andrea Huber, James Keeling, Maria Tsimpoukelli, Jackie Kay, Antoine Merle, J-M. Moret, Seb Noury, Federico Pesamosca, David G. Pfau, Olivier Sauter, Cristian Sommariva, Stefano Coda, B. Duval, Ambrogio Fasoli, Pushmeet Kohli, Koray Kavukcuoglu, Demis Hassabis, and Martin A. Riedmiller. Magnetic control of tokamak plasmas through deep reinforcement learning. *Nature*, 602 7897:414–419, 2022.

[11] Dan Feldman. Introduction to core-sets: an updated survey. *arXiv preprint arXiv:2011.09384*, 2020.

[12] Ian J. Goodfellow, Yoshua Bengio, and Aaron C. Courville. Deep learning. *Nature*, 521:436–444, 2015.

[13] Sariel Har-Peled and Soham Mazumdar. On coresets for k-means and k-median clustering. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 291–300, 2004.

[14] Hsin-Yuan Huang, Mick Broughton, Masoud Mohseni, Ryan Babbush, Sergio Boixo, Hartmut Neven, and Jarrod R. McClean. Power of data in quantum machine learning. *Nature Communications*, 12, 2021. doi: 10.1038/s41467-021-22539-9.

[15] John M. Jumper, Richard Evans, Alexander Pritzel, Tim Green, Michael Figurnov, Olaf Ronneberger, Kathryn Tunyasuvunakool, Russ Bates, Augustin Zídek, Anna Potapenko, Alex Bridgland, Clemens Meyer, Simon A A Kohl, Andy Ballard, Andrew Cowie, Bernardino Romera-Paredes, Stanislav Nikolov, Rishub Jain, Jonas Adler, Trevor Back, Stig Petersen, David A. Reiman, Ellen Clancy, Michal Zielinski, Martin Steinegger, Michalina Pacholska, Tamas Berghammer, Sebastian Bodenstein, David Silver, Oriol Vinyals, Andrew W. Senior, Koray Kavukcuoglu, Pushmeet Kohli, and Demis Hassabis. Highly accurate protein structure prediction with alphafold. *Nature*, 596:583 – 589, 2021.

[16] Jonas Jäger and Roman V. Krems. Universal expressiveness of variational quantum classifiers and quantum kernels for support vector machines. *Nature Communications*, 14(1), feb 2023.

[17] Sumeet Khatri, Ryan LaRose, Alexander Poremba, Lukasz Cincio, Andrew T Sornborger, and Patrick J Coles. Quantum-assisted quantum compiling. *Quantum*, 3:140, 2019.

[18] Yunchao Liu, Srinivasan Arunachalam, and Kristan Temme. A rigorous and robust quantum speed-up in supervised machine learning. *ArXiv*, abs/2010.02174, 2021.

[19] Ivor W Tsang, James T Kwok, Pak-Ming Cheung, and Nello Cristianini. Core vector machines: Fast svm training on very large data sets. *Journal of Machine Learning Research*, 6(4), 2005.

[20] Zhan Yu, Xuanqiang Zhao, Benchi Zhao, and Xin Wang. Optimal quantum dataset for learning a unitary transformation. *Physical Review Applied*, 19(3): 034017, 2023.

Recovering quantum entanglement after its certification

Hyeon-Jin Kim[1] * Ji-Hyeok Jung[1] † Kyung-Jun Lee[1] ‡ Young-sik Ra[1] §

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*

Abstract. Entanglement is a crucial quantum resource with its versatile applications. For harnessing entanglement in practice, it is a prerequisite to certify the entanglement of a given quantum state. However, the certification process itself destroys the entanglement, thereby precluding further exploitation of the entanglement. Resolving this conflict, here we present a protocol that certifies the entanglement of a quantum state without complete destruction, and then, probabilistically recovers the original entanglement. Our results show how entanglement certification can be made compatible with subsequent quantum applications, and more importantly, be beneficial to sort entanglement for better performance in quantum technologies.

Keywords: Quantum measurement, Entanglement certification, Entanglement recovery

Entanglement, which distinguishes quantum physics from classical physics, has been a major source in the quantum application, such as quantum teleportation [1], quantum metrology [2], and quantum computation [3]. To ensure its functionality in quantum technology, entanglement certification should precede before the application. This entanglement certification can be classified into three different categories depending on the trust in the measurement devices of Alice and Bob. First, if both devices are trusted, one can certify the entanglement by performing quantum state tomography [4] or an entanglement witness test [5]. Second, when trusting only one device, a quantum steering test can be used [6], and finally, for no trust in both devices, a Bell nonlocality test can be used to certify entanglement [7]. However, these conventional certification tests destroy the original entanglement because they generally involve projective measurement to obtain information [8]. As a result, the state after the certification test is no longer applicable to further operations. Hence, the conventional certification protocols must assume that a quantum state under a certification test, which is in turn destroyed, is identical to an unmeasured quantum state used for quantum applications. Resolving this limitations, Can we make the entanglement certification be compatible with further quantum applications requiring entanglement?

Here we propose and demonstrate a solution to this question by avoiding the complete destruction of entanglement during the certification test from introducing non-projective measurements, i.e., weak measurements. Weak measurement prevents the complete destruction of the entanglement in the quantum state while extracting the sufficient information needed for certification. We have generalized widely-used entanglement certification tests (Entanglement witness, quantum (EPR) steering, Bell nonlocality) in entangled photonic qubit system by taking into account an intermediate measurement strength. After certification, we implement the reversal measurement for the disturbed state to restore its original entanglement. Through this reversal process, we can provide the fully recovered entangled state for subsequent quantum technological applications.

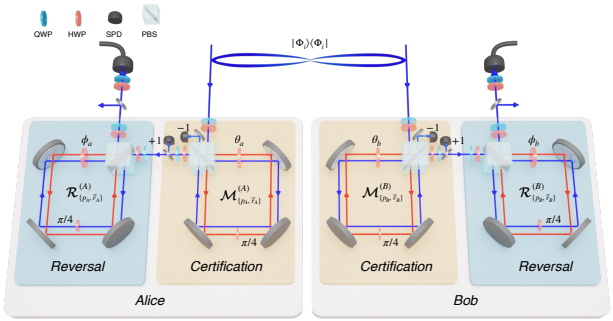


Figure 1: Experimental set-up for entanglement certification and its subsequent recovery

Figure 1 represents our experimental setup for demonstrating the entanglement certification and the subsequent recovery of the initial entanglement. The initial quantum state distributed to the two users is designed to target the Bell state $|\Phi_i\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$. To certify the generated state, users locally perform the weak measurement, which is implemented as the Sagnac interferometers, where the HWP angle θ_k controls the measurement strength as $p_k = |\cos 4\theta_k|$. The weak measurement is characterized as $\hat{M}^{(k)}_{\pm|\{p_k,\vec{r}_k\}} = \sqrt{(1\pm p_k)/2}\ \hat{\Pi}^{(k)}_{\pm|\vec{r}_k} + \sqrt{(1\mp p_k)/2}\,\hat{\Pi}^{(k)}_{\mp|\vec{r}_k}$, where $\hat{\Pi}^{(k)}_{\pm|\vec{r}_k} = \frac{1}{2}(\hat{I}^{(k)} \pm \vec{r}_k\cdot\vec{\hat{\sigma}}^{(k)})$ is the projection operator to the direction $\vec{r}_k$ ($\hat{I}$: an identity operator, $\vec{\sigma}$: Pauli operators $(\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)$), and the measurement strength p_k ranges from 0 (Identity operation) to 1 (projective measurement). To recover the disturbed state after the certification, we construct the reversal measurement operator; $\hat{R}^{(k)}_{\pm|\{q_k,\vec{s}_k\}} = \sqrt{(1\mp q_k)/2}\ \hat{\Pi}^{(k)}_{\pm|\vec{s}_k} + \sqrt{(1\pm q_k)/2}\ \hat{\Pi}^{(k)}_{\mp|\vec{s}_k}$, which is also implemented experimentally with Sagnac interferometers. Note that the recovered state $|\Psi_f\rangle = \sqrt{(1-p_A^2)(1-p_B^2)}|\Psi_i\rangle$ brings the normalization factor to the initial state, which can be interpreted as the success probability of the reverse operation, so-called reversibility ($R = \sqrt{(1-p_A^2)(1-p_B^2)}$).

*hjin.k@kaist.ac.kr
†jungjihyeok@kaist.ac.kr
‡kj_lee@kaist.ac.kr
§youngsikra@gmail.com

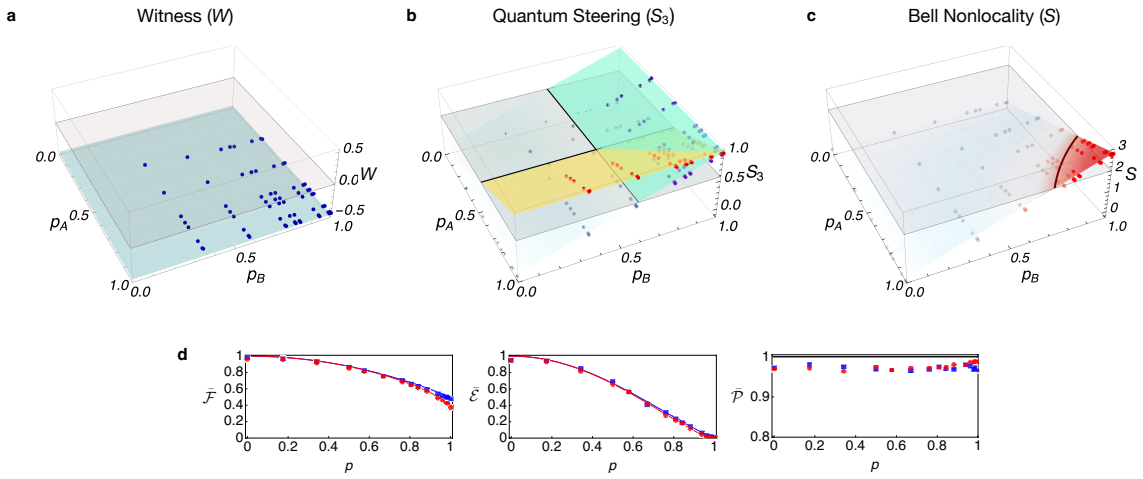


Figure 2: Entanglement certification by weak measurement

We implement three different entanglement certification tests; entanglement witness, steering, and Bell nonlocality. For witness (W), as in figure 2(a), we can always detect entanglement with non-vanishing measurement strength ($p_{a(b)}$: Alice's (Bob's) measurement strength) since we have the full knowledge of the weak measurement on the both sides. For quantum steering (S_3), only one side of the measurement device is known; therefore, it requires a measurement strength above a certain amount, $p_{a(b)} > \frac{1}{\sqrt{3}}$. One noticeable point for quantum steering is that two users individually achieve the steering condition (see figure 2(b)) by controlling the measurement strength separately; therefore, the steering can happen in one-way or both (two)-way. Lastly, the Bell nonlocality test (S), with no trust on both measurement devices, has the most stringent bound for measurement strength for certification; $p_{a,b} > \frac{1}{\sqrt{2}}$, corresponds to the red region in figure 2(c).

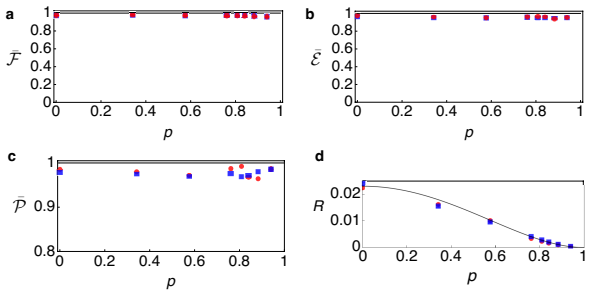


Figure 3: Recovery of the original quantum entanglement

In addition, we observe the fidelity and the entanglement of the quantum state after the certification. As expected, the fidelity and the entanglement decrease as the measurement strength increases, showing in figure 2(d). However, the purity is unaffected because the weak measurements do not introduce noise. The observed reduction of entanglement is attributed to the imbalance of probability amplitudes in the quantum state rather than generation of a mixed state, suggesting that appropriate quantum operations can recover the original entanglement.

To fully recover the entanglement disturbed during the certification, we implement the reversal measurement on the disturbed quantum state. We take the same measurement strength p for both users. Figure 3(a – c) shows the result of recovery: the final state exhibits near-unity values of fidelity, entanglement, and purity. The recovery process is probabilistic, where the reversibility (i.e., the success probability) R decreases as the measurement strength increases, as depicted in figure 3(d).

In summary, we propose and demonstrate a protocol that certifies the entanglement of a quantum state without fully destroying it, and then, recovers the original entanglement for subsequent quantum applications. Our protocol generalizes entanglement certification by incorporating non-destructive quantum measurements, which has been applied for various certification tests assuming different levels of trusts in the measurement devices. We have shown that our generalized protocol can successfully certify the entanglement by preserving useful entanglement, where the following reversal measurement fully recovers the original entanglement in a probabilistic way. From a practical perspective, our protocol is beneficial for enhancing the performance of quantum technologies by selecting high-quality entanglement from a realistic entanglement source. Our certification protocol may find broad applications in entanglement-based quantum technologies [2, 3, 10, 11, 12, 13], which is applicable to other quantum systems as well (e.g. superconductors [14] and trapped ions [15]).

References

[1] K. Tsurumoto *et. al.*, "Quantum teleportation-based state transfer of photon polarization into a carbon spin in diamond," Commun. Phys. **2**, 74, (2019).

[2] X. Guo *et. al.*, "Distributed quantum sensing in a continuous-variable entangled network," Nat. Phys. **3**, 281-284, (2020).

[3] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, "Deterministic multi-mode gates on a scalable photonic quantum computing platform," Nat. Phys. **17**, 1018-1023, (2021).

[4] James, DFV and Kwiat, Paul G and Munro, William J and White, AG, "Measurement of qubits," Phys. Rev. A **64**, 052312, (2001).

[5] Guhne, O and Hyllus, P and Bruß, D and Ekert, A and Lewenstein, M and Macchiavello, C and Sanpera, A, "Detection of entanglement with few local measurements," Phys. Rev. A **66**, 062305, (2002).

[6] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, "Experimental EPR-steering using Bell-local states," Nat. Phys. **6**, 845-849, (2010).

[7] B. Hensen *et. al.*, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," Nature **526**, 682-686, (2015).

[8] Y-W. Cho *et. al.*, "Emergence of the geometric phase from quantum measurement back-action," Nat. Phys. **15**, 665-670, (2019).

[9] M. Barbieri *et. al.*, "Detection of Entanglement with Polarized Photons: Experimental Realization of an Entanglement Witness," Phys. Rev. Lett. **91**, 227901, (2003).

[10] Ren, Ji-Gang *et. al.*, "Ground-to-satellite quantum teleportation," Nature **549**, 70–73, (2017).

[11] Darras, Tom *et. al.*, "A quantum-bit encoding converter," Nat. Photon. **17**, 165–170, (2023).

[12] Madsen, Lars S. *et. al.*, "Quantum computational advantage with a programmable photonic processor," Nature **606**, 75–81, (2022).

[13] Zhang, Wei *et. al.*, "A device-independent quantum key distribution system for distant users," Nature **607**, 687–691, (2022).

[14] White, T. C. *et. al.*, "Preserving entanglement during weak measurement demonstrated with a violation of the Bell–Leggett–Garg inequality," npj Quantum Inf. **2**, 15022, (2016).

[15] Pan, Yiming *et. al.*, "Weak-to-strong transition of quantum measurement in a trapped-ion system," Nat. Phys. **16**, 1206–1210, (2020).

The KQ-Cloud: A Cloud-based Service Framework for Quantum Computing Resources

Jieun Choi Inho Jeon Ji-Hoon Kang Hoon Ryu *

[1] *Korea Institute of Science and Technology Information, Daejeon 34141, Republic of Korea*

Abstract. The Republic of Korea (ROK) government recently has launched a national flagship project to develop a circuit-based full-stack quantum computer where the Korea Institute of Science and Technology Information (KISTI) leads the development of quantum software stack. Here, we introduce the cloud-based software framework that is currently being developed to serve the KISTI-powered emulating software, as well as the circuit-based quantum computer whose establishment is carried by the Korea Research Institute of Standards and Science (KRISS). With a web-based programming environment, our in-house framework provides a job submission interface for interactive & remote execution of user-defined tasks, enables users to monitor the status of jobs submitted to remote resources, and supports the functionality to visually check the results. Currently, the framework is connected to the emulator resource that can simulate up to 44 quantum bit (qubit) circuits with a parallel computing in the National 5^{th} supercomputer of ROK.

Keywords: Quantum software stack, Cloud-based service framework, Quantum emulator and Quantum Computer, High Performance Computing

1 Introduction

Quantum computing (QC) has witnessed remarkable progress in recent years, both in hardware platforms and software technologies, revolutionizing the landscape of computation and offering unprecedented potential for solving complex problems. On the hardware side, progress can be seen through an increase in the number of quantum bits (qubits) and the expansion of volume sizes. Recently, IBM announced the latest superconducting-based quantum processor of 433 qubits, whose quantum volume also exceeds that of the previous 127 qubit processor [1, 2]. On the software side, efforts are put to provide an user environment for developing and experimenting with algorithms and applications, and to overcome limited access to quantum computing systems. In particular, a cloud-based on-premise service model has been adopted to provide convenient access to quantum computers, enabling development and execution of quantum algorithms and applications in a cost-effective manner.

In this fierce competition for quantum computing technology, the Republic of Korea launched a national flagship project in June 2022 to develop a full-stack & gate-based 50-qubit quantum computer. This project involves collaborations among four institutions. Sungkyunkwan University (SKKU) and Ulsan National Institute of Science & Technology (UNIST) are responsible for fabricating superconducting-based Josephson junction arrays [3]. The Korea Research Institute of Standards and Science (KRISS) is in charge of designing qubit controls and integrating physical qubits into computing systems. The Korea Institute of Science and Technology Information (KISTI) focuses on developing software components required for programming circuits and public service of quantum computing resources.

This paper introduces a cloud-based software framework, designed to facilitate the development and programming of quantum algorithms and circuits. It enables interactive task submission and provides visual feedback on results, enhancing the user experience and promoting the adoption of quantum computing technologies. Additionally, to enable practical exploration of quantum computing, the framework incorporates an in-house scalable emulating software that can distribute simulation workload with a parallel computing into the classical high performance computing (HPC) resource.

*elec1020@kisti.re.kr (Corresponding Author)

2 KQ-Cloud: The KISTI Quantum computing cloud service framework

Figure 1 shows the architectural diagram of the KQ-Cloud service framework that we are developing to serve quantum computing resources. The KQ-Cloud consists of three software layers: (1) a hardware-level QC resources layer, (2) a QC service framework layer, and (3) a web-based interface layer through which users can access and program quantum computing resources. Each layer here communicates through a classical server that presents a set of application programming interfaces (APIs) that is developed to process requests from users and responses from resources.

The quantum resource layer: The KQ-Cloud is developed to serve two different QC resources: (1) The KRISS-driven superconductor-based quantum computer, and (2) the KISTI-driven software package that simulates large-scale quantum circuits with aids of a parallel computing in classical HPC systems and, particularly, the National 5^{th} supercomputer in Republic of Korea (the NURION system) [4]. A software component to be considered in the quantum resource layer for QC services is the Resource API server (marked with ④ in Figure 1), which receives requests for QC resources from the service framework, processes requests, and returns resource-generated responses to the service framework.

Figure 2(a) describes the actions according to the eight user resource identifiers (URIs) and corresponding

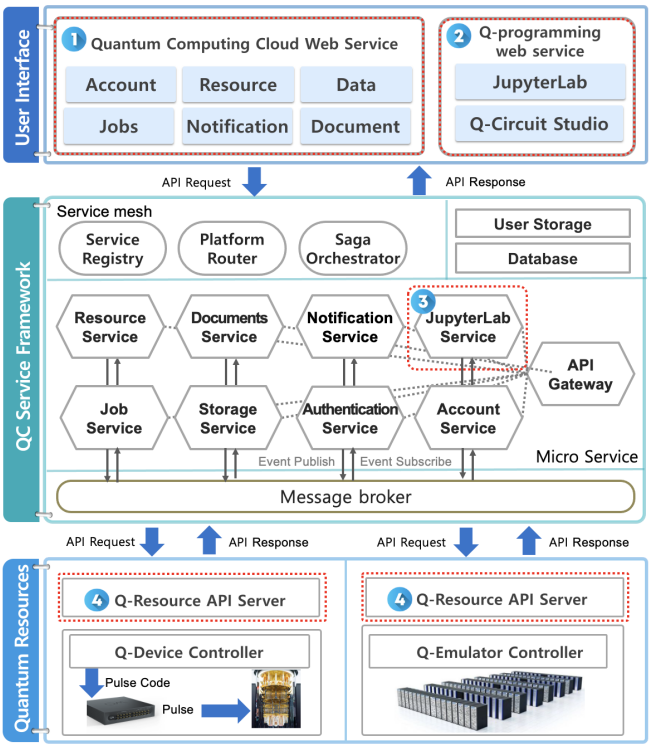


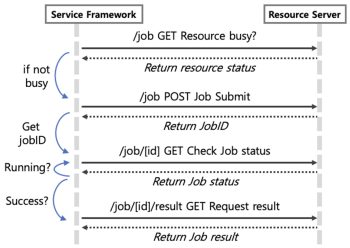
Figure 1: The KISTI Quantum (KQ) cloud consists of three software layers: Quantum computing (QC) resources, QC service framework and web-based user Interface. Each layer handles requests & responses for QC services through API-based communications. Note that we marked some of technical components with ①-④ for discussion in main texts.

RestAPI's provided by our resource API server. Figure 2(b) shows the communication process for a job submission between the service framework and the resource API server in order: (1) First, when the service framework checks whether the job manager of the backend QC resource selected through the GET/job method is busy, a response is returned. (2) If the job manager is not busy, a job is sent to the selected backend via the POST/job method, and the Resource API server returns an id for the task. (3) The service framework sends a Get/job[id] method request to check the progress of the job until the job is finished, and receives the job status as a response. (4) When the job status becomes 'success', *i.e.*, the job is successfully finished, the execution result of the job is delivered through a Get/job/[id]/result method.

The service framework layer: With aids of virtualization techniques, the service framework enables multiple users to access QC resources and run their applications with efficiency in the service overhead. The service framework is developed to flexibly incorporate the unique characteristics that QCs have against classical computing, such as the implementation platforms, the post processes of computational outputs, and etc. [5, 6, 7]. The KQ-Cloud adopts a microservices architecture and leverages the Kubernetes [8] to deploy service instances in

URI(Path)	Methods	Actions
/job	GET	Check job manager
/job	POST	Submit a job
/job/[id]	GET	Check the job status
/job/[id]	PUT	Cancel the job
/job/[id]	DELETE	Delete the job
/job/[id]/result	GET	Query the result of job
/resource	GET	Query the resource status
/resource	PUT	Change the status of resource

(a) RestAPI methods and actions for resource server



(b) Communication between framework & API server

Figure 2: (a) User resource identifiers (URIs), RestAPI methods and corresponding actions to handle quantum computing resources. (b) Communication flow between the service framework layer and the resource API server.

containers. It offers a total of eight backend service components: job, resource, storage, authentication, notification, documents, account, and JupyterLab services. To facilitate efficient communication between users and backend service components, we employ an API gateway that ensures proper routing of relevant service requests. Service components within the framework communicate through a message broker that is based on a publish-and-subscribe pattern for event-based interactions. A service mesh is also developed to enhance the speed of service discovery and routing process.

Throughout development of the KQ-Cloud, special attention has been given to meet the unique requirements of quantum computing services. In particular, the JupyterLab service utilizing JupyterLab Notebook (marked with ③ in Figure 1) places significant importance on preserving the users' working state, including their programming environment and data. Therefore, these services have been implemented to be compatible with Kubernetes' persistent volume (PV) and persistent volume claim (PVC) functionalities, which will ensure that user data and states are effectively stored and maintained.

The web-based user interface layer: Users can program and access QC resource through our web-based interface. Functionalities of the web portal are divided into two parts: one for cloud services and the other for circuit programming. The first part (marked with ① in Figure 1) provides an environment for six basic services: (1) account registration and management, (2) resource lookup, (3) user data management, (4) job submission, (5) notification, and (6) document delivery, similar to what traditional cloud systems do for classical computing. The second part (marked with ② in Figure 1) provides accesses to the JupyterLab-based programming environment. We also present a software development kit (SDK) so users can also interactively program circuits and check the results in the notebook.

Figure 3 depicts a series of processes in which users use the entire cloud-based service through our web portal. To access a programming environment, the user begins by logging into KQ-Cloud through a web browser. First, user initiate the process by creating a JupyterLab notebook (Step 1). Subsequently, a Python container,

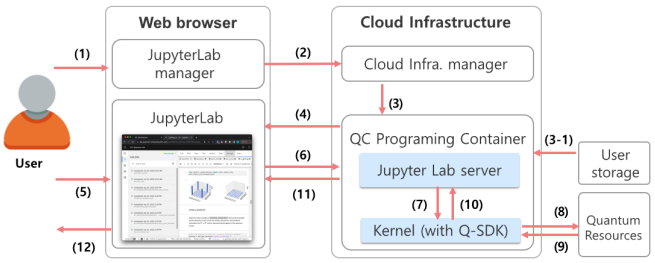


Figure 3: A conceptual illustration that shows the end-to-end workflow of the KQ-Cloud service framework

built on JupyterLab, is requested and generated, and the user is presented with the JupyterLab interface (Steps 2-4). Once the JupyterLab container is available, users can access it to develop quantum circuits and request execution (Steps 5-6). The JupyterLab server then executes the code and submits the job to QC resources (Steps 7-8). Upon the job completion, the result obtained from QC resources is transferred back to users (Steps 9-11). Finally, the user can examine the results through a visualization toolkit that is supported either directly by the SDK or by our in-house solution.

The quantum emulator: The SDK we present is based on the PennyLane package [9], and is used to program with both QC hardware and classical simulation software (*a.k.a.* quantum emulator). To drive scalable simulations of large quantum circuits in huge classical computing environments that normally consist of more than several hundred computing nodes, we parallelize the Pennylane-Lightning source code with the Message Passing Interface (MPI) [10]. Figure 4 shows the strong scalability tests that are conducted against 36-40 qubit random circuits in the NURION supercomputer [4], which confirms fairly nice parallel efficiency of large-scale quantum circuit simulations.

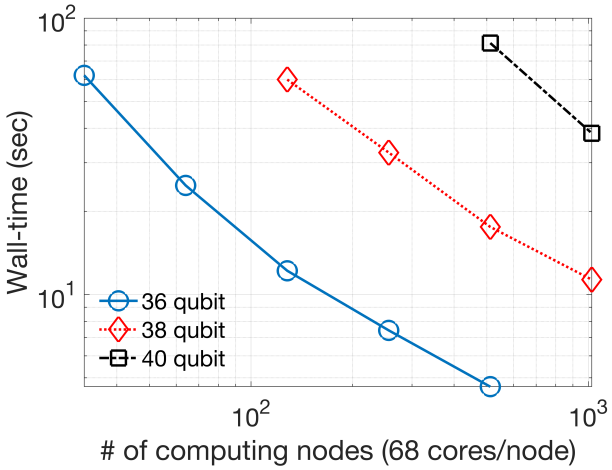


Figure 4: Strong scalability tested for parallel execution of 36-38 qubit random circuit simulations in the NURION supercomputer whose single computing node consists of 68 physical cores.

Acknowledgements This work has been carried out under support of the National Research Foundation of Korea (NRF-2022M3K2A1083890) funded by the Korea government (MSIP).

References

[1] O. Ezrattya. Perspective on superconducting qubit quantum computing In *The European Physical Journal A*, 59(5):94, 2023.

[2] S. A. Moses et al. A Race Track Trapped-Ion Quantum Processor In *arXiv preprint arXiv:2305.03828*, pages 1-24, 2023.

[3] G. Wendin and V. S. Shumeiko. Quantum bits with Josephson junctions In *Low Temperature Physics*, 33(9):724-744, 2007.

[4] The 5^{th} supercomputer of Korea (the NURION system), https://www.ksc.re.kr/eng/resource/nurion, access: 05, 2023.

[5] H. T. Nguyen et al. QFaaS: A Serverless Function-as-a-Service Framework for Quantum Computing In *arXiv preprint arXiv:2205.14845*, pages 1-35, 2022.

[6] M. Grossi, L. Crippa, A. Aita, G. Bartoli, V. Sammarco, E. Picca, N. Said, F. Tramonto, and F. Mattei. A Serverless Cloud Integration For Quantum Computing In *arXiv preprint arXiv:2107.02007*, pages 1-8, 2021.

[7] J. Garcia-Alonso, J. Rojo, D. Valencia, E. Moguel, J. Berrocal, and J. M. Murillo. Quantum Software as a Service Through a Quantum API Gateway In IEEE Internet Computing, 26(1):34-41, 2021.

[8] The Kubenetes software, https://kubernetes.io/, access: 05, 2023.

[9] The PennyLane SDK, https://pennylane.ai/, access: 05, 2023.

[10] The Message Passing Interface (MPI) standard, https://www.mcs.anl.gov/research/projects/mpi/, access: 05, 2023.

Quantum Similarity Testing with Convolutional Neural Networks

Ya-Dong Wu[1] Yan Zhu[1 * †] Ge Bai[2] Yuexuan Wang[3 4] Giulio Chiribella[1 5 6 ‡]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, 117543, Singapore*

[3] *AI Technology Lab, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[4] *College of Computer Science and Technology, Zhejiang University, Zhejiang Province, China*

[5] *Department of Computer Science, Parks Road, Oxford, OX1 3QD, United Kingdom*

[6] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

Abstract. Testing whether two uncharacterized quantum devices behave in the same way is crucial for benchmarking near-term quantum computers and quantum simulators, but has so far remained open for continuous-variable quantum systems. We develop a machine learning algorithm for comparing unknown continuous variable states using limited and noisy data. Our approach is based on a convolutional neural network that assesses the similarity of quantum states based on a lower-dimensional state representation built from measurement data. Our network can also be applied to the problem of comparing continuous variable states across different experimental platforms, with different sets of achievable measurements, and to the problem of experimentally testing whether two states are equivalent up to Gaussian unitary transformations.

Keywords: machine learning, neural network, quantum state characterization, continuous variable quantum information

1 Introduction

Comparing unknown quantum states based on experimental data [1, 2, 3, 4] is crucial for benchmarking quantum simulations and near-term quantum computers [5]. A natural approach in this context is to choose a trusted device as a reference standard, and to compare other devices to it. For example, the trusted device could be built and maintained by a quantum computing company, while the other devices could be owned by users in distant laboratories. One way to compare two unknown quantum devices is to estimate their overlap [6, 7, 8, 9, 1, 10, 11], which is also useful for tasks like quantum state discrimination and classification [12, 13, 14, 15]. Recently, Elben *et al.* proposed an approach named cross-platform verification [1], which uses only local Pauli measurements to experimentally estimate the overlap between two multiqubit states. This approach has been recently demonstrated on quantum systems with more than ten qubits [16]. An alternative approach to characterize quantum states from measurement data is provided by deep neural networks [17, 18, 19, 20, 21, 22, 23, 24, 25, 26], which can work with a smaller amount of data when the states under consideration belong to state families with sufficient structure, such as the family of ground states of the Ising model with different values of the couplings and of the magnetic field.

In this work, we develop a convolutional neural network for testing the similarity of quantum states drawn from a continuously-parametrized state family. For sufficiently regular families, our network manages to tell different states apart using noisy and incomplete measurement data, without requiring randomization over an exponentially large set of measurements, or correlations between measurements performed on different states. The network is trained with data from a fiducial set of quantum states sharing structural similarities with the states to be compared. After training, the network embeds the measurement data into a low-dimensional feature space in a way that reflects the similarity of quantum states. This low-dimensional state representation is then used by the network to decide whether the two given states are the same or not. Our approach is inspired by a classical technique for the recognition of human faces in blurred and incomplete images [27], a task that shares similarities with the task of comparing continuous-variable quantum states from finite-statistics approximations of their Wigner function.

2 Framework

Two experimenters, Alice and Bob, own two quantum devices producing copies of two unknown quantum states ρ and σ, respectively. Alice and Bob want to determine whether their devices prepare the same quantum state, that is, whether $\rho = \sigma$. To this purpose, they can only perform a limited set of quantum measurements, possibly different for Alice and Bob. The measurements can be chosen independently and randomly, but there is no need for Alice and Bob to sample them from the uniform distribution, or from any specific probability distribution. In general, the sets of performed measurements $\mathcal{S}_A$ and $\mathcal{S}_B$ need not be informationally complete.

Here we introduce a deep neural network that determines whether two unknown states are same or not, using limited and noisy data. We call our network StateNet, in analogy to FaceNet [27], a popular neural network for the

*Ya-Dong Wu and Yan Zhu contribute equally

†yzhu2@cs.hku.hk

‡giulio@cs.hku.hk

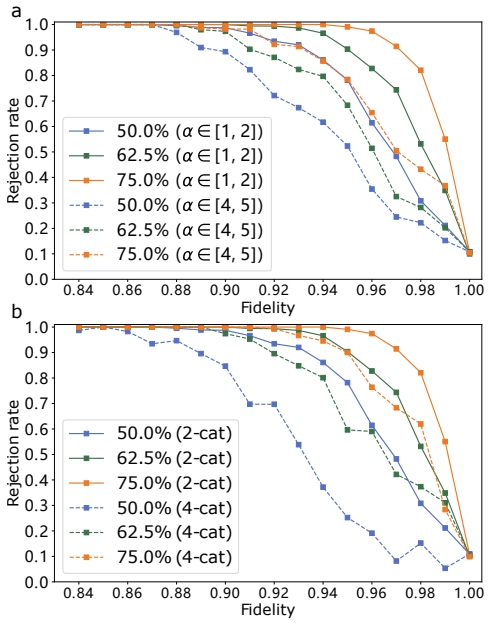


Figure 1: Rejection rate for cat states as a function of the fidelity. Three different scenarios are considered: 50%, 62.5% and 75% of 32×32 pixels are randomly selected as input to the neural network respectively. For all the scenarios, each pixel is an estimate of the Wigner function obtained from 300 measurement samples. In Fig.(a), solid lines are for cat states with $\alpha \in [1, 2]$ and dashed lines are for cat states with $\alpha \in [4, 5]$. In Fig.(b), solid lines are for four-component cat states and dashed lines are for two-component cat states.

identification of human faces. StateNet uses a convolutional neural network [28] to produce a low-dimensional representation of quantum states. For the training, we choose a set of fiducial states and provide the corresponding measurement data to the network. The training data can be generated by computer simulation, or by actual experiments, or by a combination of these two methods. Note that the training data need not be produced afresh; instead, one can use existing data from past simulations or past experiments. For each fiducial state τ, its measurement data set is fed into a deep neural network to produce a low-dimensional representation, given by a vector $\boldsymbol{r} \in \mathbb{R}^n$. The dimension n is a parameter of the network. Note that in general n can be much smaller than the dimension of the Hilbert spaces containing the fiducial states.

In the training phase, we optimize the parameters of the convolutional neural network with respect to a loss function, called triplet loss [27]. After the training is concluded, the network maps measurement data to vectors that reflect the similarity of quantum states. Quantum states are then compared by evaluating the Euclidean distance between the corresponding vectors. To decide whether two vectors correspond to the the same quantum state, the network uses a threshold value that balances between the false rejection rate and the false acceptance rate over a new set of unseen measurement data obtained from the fiducial states.

3 Testing the similarity of continuous variable states

A continuous-variable quantum state ρ is characterized by its Wigner function $W_\rho(\alpha)$ [29, 30]. An estimate of the value of $W_\rho(\alpha)$ at any phase-space point α can be achieved *e.g.* by measuring displaced parity operator, which is widely used for the characterization of quantum states in circuit quantum electrodynamics [31, 32, 33, 34]. Suppose that Alice (Bob) can estimate the Wigner function at a finite number of points, chosen at random from a square grid over the phase space. The set of all points on the grid corresponds to the set of achievable measurements $\mathcal{M}_A = \mathcal{M}_B =: \mathcal{M}$. Alice (Bob) randomly chooses a subset of points in the grid to perform measurements of the Wigner function, which is a subset $\mathcal{S}_A$ ($\mathcal{S}_B$) of $\mathcal{M}$. In general, the points chosen by Alice and Bob need not be the same. After a finite set of measurement runs, Alice (Bob) obtains a two-dimensional data image, where some pixels are missing and the value at each of the existing pixels is an estimate of the Wigner function at the associated phase-space point. As a result of the finite statistics, the image will generally be blurred.

We test our method on cat states [35, 36] $(|\alpha\rangle + |-\alpha\rangle)/\sqrt{2(1+\exp(-2|\alpha|^2))}$, where $|\alpha\rangle := D(\alpha)|0\rangle$ is a coherent state. We train StateNet using simulated measurement data from ideal cat states as well as noisy cat states with a fixed amount of thermal noise. After the training is concluded, we test the performance of StateNet in distinguishing between pairs of noisy cat states degraded by photon loss. For each pair of noisy cat states ρ and σ, we take ρ to play the role of the reference state, and make it close to its noiseless counterpart ρ_{ideal}, with fidelity 99%). On the other hand, we regard σ as the untrusted state that needs to be verified, and allow it to be generally noisier, allowing the fidelity with the trusted state ρ to range between 84% and 100%. To evaluate the performance of the network, we plot the rejection rate, namely the probability that the two states are judged to be different, as a function of their fidelity. The resulting plot is shown in Fig. 1.

Fig. 1(a) shows the performance of StateNet for noisy cat states with amplitudes $\alpha \in [1, 2]$ and $\alpha \in [4, 5]$. The numerical results indicate that, when the amplitude is increased without increasing the amount of measurement data, the prediction accuracy decreases. We also test how the performance of our neural network is affected by the states' complexity, as measured by their nonclassicality [37]. To this purpose, we consider cat-like states that are superposition of four coherent states instead of two. Fig. 1(b) demonstrates that the success rate of StateNet decreases as state complexity increases.

To test the ability of our network to cope with high-dimensional quantum states, we perform numerical experiments on noisy cat states with high amplitudes. Figure 2(b) illustrates the performances of StateNet for the comparison of two noisy cat states with amplitudes $\alpha \in [15, 16]$ (corresponding to an average number of photons between 225 and 256) using displaced parity measurement data on a 36×36 grid within $[-1.5, 1.5] \times [-1.5, 1.5]$

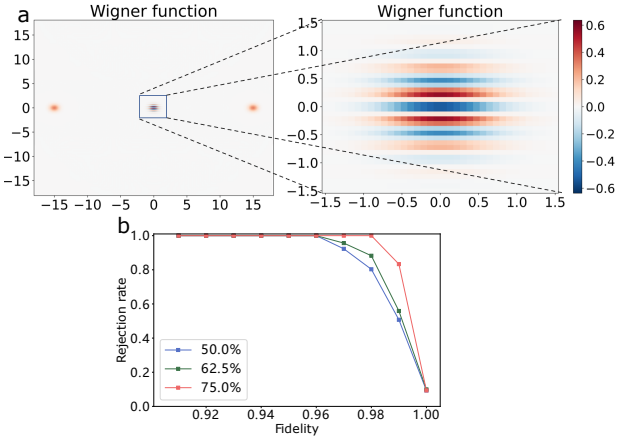


Figure 2: (a) Wigner function of a cat state with $\alpha = 16$, along with a inset figure of the Wigner function on a 36×36 fine grid within the region $[-1.5, 1.5] \times [-1.5, 1.5]$. (b) rejection rates against quantum fidelity when StateNet only utilizes 50%, 62.5%, 75% of the measurement data of the Wigner function on this 36×36 fine grid.

in phase space. Despite the limited amount of measurement data, StateNet achieves a relatively high success rate in this high amplitude scenario.

4 Verification of Equivalence up to Gaussian Unitary Operations.

A variant of StateNet can be used to decide whether two quantum states are the same up to a unitary transformation in a given set. A common example of unitary transformations are the Gaussian unitary transformations introduced by displacements, phase rotations and squeezing [38].

In the Wigner function representation, the combination of displacements, rotations, and squeezing corresponds to an affine transformation in phase space. We use StateNet for testing whether two data images generated from states of the form

$$|\phi_{\boldsymbol{\theta},\alpha}\rangle := \mathrm{SNAP}(\boldsymbol{\theta})\,|\alpha\rangle\,, \tag{1}$$

where $\mathrm{SNAP}(\boldsymbol{\theta}) := \sum_n \exp(\mathrm{i}\theta_n)\,|n\rangle\langle n|$ is a selective number-dependent arbitrary phase gate [33, 39], are equivalent up to an affine transformations. Fig. 3 shows examples of image data for equivalent as well as inequivalent quantum states. By balancing both the false rejection rate and the false acceptance rate, we obtain a distance threshold 0.4, which makes our model accept all pairs of equivalent states, and reject the inequivalent ones.

5 Similarity testing with two different sets of achievable measurements

Quantum information protocols have been implemented on a variety of experimental platforms, each involving different sets of feasible measurements. For instance, homodyne measurements are commonly used for

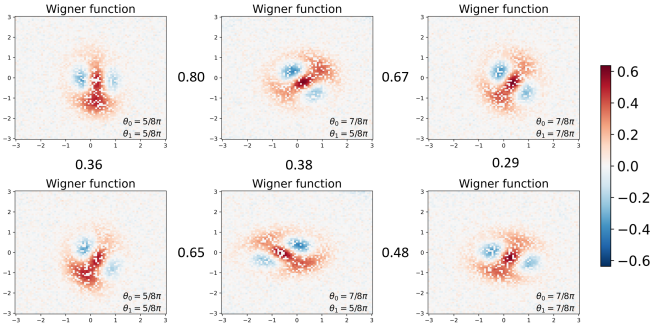


Figure 3: Verification of equivalence up to Gaussian unitary transformations. Each column contains a pair of data images of the same quantum state with different affine transformations. The three different columns correspond to three quantum states (1) with different values of θ_0 and θ_1 ($\theta_n = 0$ for $n \geq 2$). Each data image contains 4900 pixels randomly chosen from $81 \times 81 = 6561$ pixels, and the value at each pixel is an estimate of the Wigner function obtained from 500 measurement samples. The number between each pair of data images is the distance between their state representations produced by StateNet.

photonic systems [40], while displaced parity measurements are preferable in cavity quantum electrodynamics [33, 34]. Here we demonstrate that StateNet can test the similarity of quantum states realized on two different experimental platforms, with two different sets of accessible measurements.

We consider a scenario where Alice performs displaced parity measurements on state ρ, while Bob performs homodyne measurements on state σ. Given measurement data from these two essentially different types of measurements, Charlie aims to determine whether ρ equals to σ. To achieve this objective, we jointly train two neural networks, so that their measurement data from these two different types of measurements are mapped into a single representation space.

6 Similarity testing for multiqubit states

StateNet can also be adapted to the problem of testing the similarity of multiqubit states, such as the ground states of Ising model. We test its performance on pairs of 10-, 20-or 50-qubit states ρ and σ, where ρ represents an ideal ferromagnetic Ising ground state, and σ an untrusted Ising ground state with poor calibration of the coupling parameters. Alice (Bob) selects a subset of two-qubit nearest-neighbor Pauli measurements, and the measurement statistics is then input into StateNet. The results of our numerical experiments show that our approach can correctly identify whether two datasets are from the same ρ or different states ρ and σ with a probability of over 90% for 10 qubits. However, for 50 qubits, the success probability drops to 80% if the amount of measurement data is kept fixed.

A full technical version of this work can be found via the link https://arxiv.org/pdf/2211.01668.pdf.

References

[1] A. Elben, B. Vermersch, R. van Bijnen, C. Kokail, T. Brydges, C. Maier, M. K. Joshi, R. Blatt, C. F. Roos, and P. Zoller, "Cross-platform verification of intermediate scale quantum devices," *Phys. Rev. Lett.*, vol. 124, p. 010504, Jan 2020.

[2] S. Flammia, "Quantum computer crosscheck," *Physics*, vol. 13, p. 3, 2020.

[3] J. Carrasco, A. Elben, C. Kokail, B. Kraus, and P. Zoller, "Theoretical and experimental perspectives of quantum verification," *PRX Quantum*, vol. 2, p. 010102, Mar 2021.

[4] D. Zhu, Z.-P. Cian, C. Noel, A. Risinger, D. Biswas, L. Egan, Y. Zhu, A. M. Green, C. H. Alderete, N. H. Nguyen, *et al.*, "Cross-platform comparison of arbitrary quantum states," *Nat. Commun.*, vol. 13, p. 6620, 2022.

[5] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, "Quantum certification and benchmarking," *Nat. Rev. Phys.*, vol. 2, no. 7, p. 382, 2020.

[6] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Phys. Rev. Lett.*, vol. 87, p. 167902, Sep 2001.

[7] L. Cincio, Y. Subaşı, A. T. Sornborger, and P. J. Coles, "Learning the quantum algorithm for state overlap," *New J. Phys.*, vol. 20, no. 11, p. 113022, 2018.

[8] U. Chabaud, E. Diamanti, D. Markham, E. Kashefi, and A. Joux, "Optimal quantum-programmable projective measurement with linear optics," *Phys. Rev. A*, vol. 98, p. 062318, Dec 2018.

[9] M. Fanizza, M. Rosati, M. Skotiniotis, J. Calsamiglia, and V. Giovannetti, "Beyond the swap test: Optimal estimation of quantum state overlap," *Phys. Rev. Lett.*, vol. 124, p. 060503, Feb 2020.

[10] L. Guerini, R. Wiersema, J. F. Carrasquilla, and L. Aolita, "Quasiprobabilistic state-overlap estimator for nisq devices," *arXiv:2112.11618*, 2021.

[11] A. Anshu, Z. Landau, and Y. Liu, "Distributed quantum inner product estimation," in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, p. 44, 2022.

[12] C. W. Helstrom, "Quantum detection and estimation theory," *J. Stat. Phys.*, vol. 1, no. 2, p. 231, 1969.

[13] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, vol. 1. Springer Science & Business Media, 2011.

[14] M. Sasaki, A. Carlini, and R. Jozsa, "Quantum template matching," *Phys. Rev. A*, vol. 64, p. 022317, Jul 2001.

[15] V. Dunjko and H. J. Briegel, "Machine learning & artificial intelligence in the quantum domain: a review of recent progress," *Rep. Prog. Phys.*, vol. 81, no. 7, p. 074001, 2018.

[16] D. Zhu, Z. Cian, C. Noel, A. Risinger, D. Biswas, L. Egan, Y. Zhu, A. Green, C. H. Alderete, N. Nguyen, *et al.*, "Cross-platform comparison of arbitrary quantum states," *Nat. Commun.*, vol. 13, no. 1, p. 1, 2022.

[17] G. Torlai, G. Mazzola, J. Carrasquilla, M. Troyer, R. Melko, and G. Carleo, "Neural-network quantum state tomography," *Nat. Phys.*, vol. 14, no. 5, p. 447, 2018.

[18] G. Torlai and R. G. Melko, "Latent space purification via neural density operators," *Phys. Rev. Lett.*, vol. 120, p. 240503, Jun 2018.

[19] J. Carrasquilla, G. Torlai, R. G. Melko, and L. Aolita, "Reconstructing quantum states with generative models," *Nat. Mach. Intell.*, vol. 1, no. 3, p. 155, 2019.

[20] G. Torlai, B. Timar, E. P. L. van Nieuwenburg, H. Levine, A. Omran, A. Keesling, H. Bernien, M. Greiner, V. Vuletić, M. D. Lukin, R. G. Melko, and M. Endres, "Integrating neural networks with a quantum simulator for state reconstruction," *Phys. Rev. Lett.*, vol. 123, p. 230504, Dec 2019.

[21] E. S. Tiunov, V. Tiunova, A. E. Ulanov, A. Lvovsky, and A. K. Fedorov, "Experimental quantum homodyne tomography via machine learning," *Optica*, vol. 7, no. 5, p. 448, 2020.

[22] S. Ahmed, C. Sánchez Muñoz, F. Nori, and A. F. Kockum, "Quantum state tomography with conditional generative adversarial networks," *Phys. Rev. Lett.*, vol. 127, p. 140502, Sep 2021.

[23] A. W. R. Smith, J. Gray, and M. S. Kim, "Efficient quantum state sample tomography with basis-dependent neural networks," *PRX Quantum*, vol. 2, p. 020348, Jun 2021.

[24] T. Schmale, M. Reh, and M. Gärttner, "Efficient quantum state tomography with convolutional neural networks," *npj Quantum Inf.*, vol. 8, no. 1, p. 115, 2022.

[25] Y. Zhu, Y.-D. Wu, G. Bai, D.-S. Wang, Y. Wang, and G. Chiribella, "Flexible learning of quantum states with generative query neural networks," *Nat. Commun.*, vol. 13, no. 1, p. 6222, 2022.

[26] E. Fedotova, N. Kuznetsov, E. Tiunov, and A. Lvovsky, "Continuous-variable quantum tomography of high-amplitude states," *arXiv:2212.07406*, 2022.

[27] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *CVPR*, p. 815, 2015.

[28] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, p. 436, 2015.

[29] L. G. Lutterbach and L. Davidovich, "Method for direct measurement of the wigner function in cavity qed and ion traps," *Phys. Rev. Lett.*, vol. 78, p. 2547, Mar 1997.

[30] P. Bertet, A. Auffeves, P. Maioli, S. Osnaghi, T. Meunier, M. Brune, J. M. Raimond, and S. Haroche, "Direct measurement of the wigner function of a one-photon fock state in a cavity," *Phys. Rev. Lett.*, vol. 89, p. 200402, Oct 2002.

[31] B. Vlastakis, G. Kirchmair, Z. Leghtas, S. E. Nigg, L. Frunzio, S. M. Girvin, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, "Deterministically encoding quantum information using 100-photon schrödinger cat states," *Science*, vol. 342, no. 6158, p. 607, 2013.

[32] M. Kudra, M. Kervinen, I. Strandberg, S. Ahmed, M. Scigliuzzo, A. Osman, D. P. Lozano, M. O. Tholén, R. Borgani, D. B. Haviland, G. Ferrini, J. Bylander, A. F. Kockum, F. Quijandría, P. Delsing, and S. Gasparinetti, "Robust preparation of wigner-negative states with optimized snap-displacement sequences," *PRX Quantum*, vol. 3, p. 030301, Jul 2022.

[33] R. W. Heeres, B. Vlastakis, E. Holland, S. Krastanov, V. V. Albert, L. Frunzio, L. Jiang, and R. J. Schoelkopf, "Cavity state manipulation using photon-number selective phase gates," *Phys. Rev. Lett.*, vol. 115, p. 137002, Sep 2015.

[34] V. V. Sivak, A. Eickbusch, H. Liu, B. Royer, I. Tsioutsios, and M. H. Devoret, "Model-free quantum control with reinforcement learning," *Phys. Rev. X*, vol. 12, p. 011059, Mar 2022.

[35] B. Yurke and D. Stoler, "Generating quantum mechanical superpositions of macroscopically distinguishable states via amplitude dispersion," *Phys. Rev. Lett.*, vol. 57, p. 13, Jul 1986.

[36] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, "Dynamically protected cat-qubits: a new paradigm for universal quantum computation," *New J. Phys.*, vol. 16, no. 4, p. 045014, 2014.

[37] A. Kenfack and K. Życzkowski, "Negativity of the wigner function as an indicator of non-classicality," *J. Opt. B: Quantum Semiclass.*, vol. 6, no. 10, p. 396, 2004.

[38] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, p. 621, May 2012.

[39] T. Fösel, S. Krastanov, F. Marquardt, and L. Jiang, "Efficient cavity control with snap gates," *arXiv:2004.14256*, 2020.

[40] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," *Rev. Mod. Phys.*, vol. 81, p. 299, Mar 2009.

Investigating the Quantum Advantage of Variational Quantum Machine Learning Algorithms based on Parameterized Quantum Circuits from the Perspective of the Classical Machine Learning

Kyungmin Lee[1] * Hyeongjun Jeon[1] † Dongkyu Lee[2] ‡ Bongsang Kim[2] §
Taehyun Kim ¶[1 3 4 5 6]

[1] *Department of Computer Science and Engineering, Seoul National University, Seoul 08826, Republic of Korea*
[2] *Quantum AI Dept, AI Lab, CTO, LG Electronics, Seoul 06772, Republic of Korea*
[3] *Automation and System Research Institute, Seoul National University, Seoul 08826, Republic of Korea*
[4] *Inter-university Semiconductor Research Center, Seoul National University, Seoul 08826, Republic of Korea*
[5] *Institute of Computer Technology, Seoul National University, Seoul 08826, Republic of Korea*
[6] *Institute of Applied Physics, Seoul National University, Seoul 08826, Republic of Korea*

Abstract. In this study, we derive the general expression for variational quantum machine learning models based on parameterized quantum circuit, and we identify their inductive bias when they are applied to classical supervised machine learning tasks. Then we argue that a classical counterpart with similar capability can be easily constructed under such assumption. We also provide results of numerical experiments that support this claim.

Keywords: quantum machine learning, quantum advantage, variational quantum algorithm, parameterized quantum circuit

1 Introduction

Quantum machine learning (QML) is an emerging field that utilizes quantum computers for machine learning applications [1]. In recent years, with the development of quantum computing technology, variational quantum algorithms [2] drew much attention as a method that can give quantum advantage using noisy intermediate-scale quantum (NISQ) computer [3,4]. From the perspective of classical supervised machine learning (ML) tasks, there are two popular types of variational quantum machine learning (VQML) models, the variational quantum circuit (VQC) models [5–10] and the quantum kernel (QK) models [11–15]. However, still it is not clear whether the VQML models truly offer a quantum advantage compared to the other classical models in processing classical data, mainly because a lot of freedom in selecting the circuit structure of the VQML model makes it difficult to analyze how they handle classical data and how they can have better performance than its classical competitors. In addition, practical bench-marking results are not available on current NISQ quantum computer and therefore comparison of a quantum model with other classical models is limited [16]. Fundamentally, the notion of classical counterparts for VQML models is obscure, like a classical algorithm processing quantum data is not well-defined [17].

In this study, we will analyze how the VQML models process classical data, starting from the fact that any arbitrary quantum algorithms can be represented by universal gate set [18]. We will treat a set of single qubit rotation gates $R_{\sigma_x}, R_{\sigma_y}, R_{\sigma_z}$ and a two-qubit CNOT gate as a basic gate set. We utilize the Stokes representation [19] of a quantum state and figure out the real-valued matrix representation of these basic gates. Based on the representation, we construct general expression of the VQML models and clarify the conditions when these models can be suitably adopted. Finally, we suggest exmaples of classical counterparts for the VQML models and compare their performance on toy problems. Note that the VQML models may have various circuit structures and it requires a compilation process before it is run on a real quantum computer. This compilation process may convert the data or the model parameters, and therefore we consider the values of data and model parameters after the compilation since it is totally done on a classical computer.

2 Representation of basic gates

First, we consider a n-qubit quantum state $|\psi\rangle$ as 4^n-dimensional real vector $\boldsymbol{v}$ whose elements v_i are the Stokes parameters defined as follows:

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2^n} \sum_{i_1,i_2,\cdots,i_n=0}^{3} v_{i_1,i_2,\cdots,i_n} \left(\bigotimes_{k=1}^{n} \sigma_{i_k} \right),$$

where σ_0 is the identity matrix and $\sigma_{x,y,z} = \sigma_{1,2,3}$, the Pauli matrices. We denote v_i with $i = i_1 \times 4^{n-1} + i_2 \times 4^{n-2} + \cdots + i_n \times 4^0$. Now we obtain the real matrix representation of basic gates acting on $\boldsymbol{v}$. Note that we use the following equality to make CNOT gate representation on q_1 and q_2 qubits.

$$U_{\text{CNOT}}^{q_1 q_2} = e^{-i\frac{\pi}{4}} e^{-i\frac{\pi}{4}\left(Z_{q_1} X_{q_2}\right)} R_\sigma^{3_{q_1}} \left(-\frac{\pi}{2}\right) R_\sigma^{1_{q_2}} \left(-\frac{\pi}{2}\right)$$

*anfry15rudals@snu.ac.kr
†ijshj10@snu.ac.kr
‡dongkyu44.lee@lge.com
§bongsang.kim@lge.com
¶taehyun@snu.ac.kr

Note that $R_\sigma^{i_k}(\theta) = e^{-i\frac{\theta}{2}\sigma_{i_k}}$ is a single qubit gate acting on k-th qubit where $i_k \in \{1, 2, 3\}$. Figure 1 shows the graphical representations.

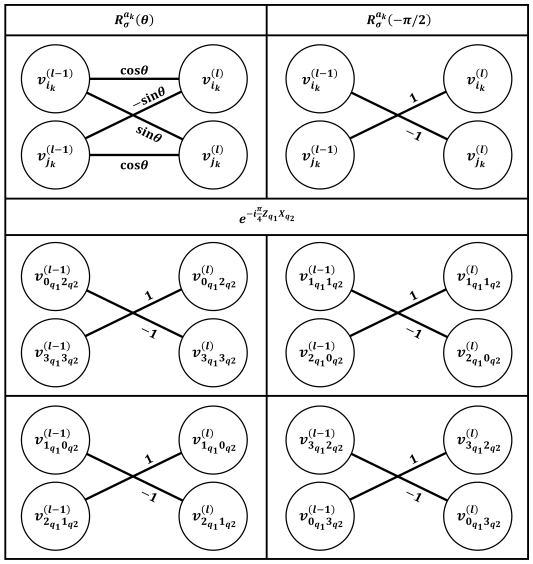


Figure 1: Graphical representation of single qubit gates and two-qubit gate. Note that we consider the single qubit gates acting on k-th qubit and $R_\sigma^{a_k} = e^{-i\frac{\theta}{2}\sigma_{a_k}}$. The two-qubit gate $e^{-i\frac{\pi}{4}Z_{q_1}X_{q_2}}$ acting on q_1, q_2 qubits is used to construct the CNOT gate.

3 Expression of VQML models

According to the result of the previous section, we can find that the final quantum state of VQML models has the following general form:

$$v_{\boldsymbol{i}\in\{0,1,2,3\}^n} = \sum_{\boldsymbol{k}\in\{0,1,2\}^d} c_{\boldsymbol{k}}^{\boldsymbol{i}} \prod_{j=1}^{d} g_{k_j}(\theta_j),$$

where the real vector $\boldsymbol{\theta}$ can be a data point or the model parameters or both and d is its dimension. Note that $c_{\boldsymbol{k}}^{\boldsymbol{i}} \in \{-1, 0, 1\}$ and $g_0(\theta) = 1$, $g_1(\theta) = \sin\theta$, and $g_2(\theta) = \cos\theta$. One may repeat the same circuit structure several times to enhance the capability of VQML models [20]. We can simply extend the above representation for this case:

$$v_{\boldsymbol{i}\in\{0,1,2,3\}^n} = \sum_{\substack{\boldsymbol{k}\in\{0,1,2\}^d \\ \boldsymbol{r}\in\{1,2,\cdots,l\}^d}} c_{\boldsymbol{k},\boldsymbol{r}}^{\boldsymbol{i}} \prod_{j=1}^{d} \left(g_{k_j}(\theta_j)\right)^{r_j}, \qquad (1)$$

According to this expression, we recognize that the VQML models require a knowledge of the important coefficients $c_{\boldsymbol{k},\boldsymbol{r}}^{\boldsymbol{i}}$ to have a good performance on supervised ML tasks. This can be considered as the inductive bias of VQML models, which raises the following question: Can a classical model be constructed under such condition, which can approximate the VQML models or even surpass their performance? We can think of two kinds of simple classical models which can be adopted instead of the VQML models.

3.1 Direct estimation model

When we have knowledge of crucial coefficients in (1), we can directly estimate it from data. Consider we have data point $\boldsymbol{x} \in [-\pi, \pi]^d$ and set $l = 1$. We assume that the data is properly pre-processed so that each data feature is independent of each other. From the orthogonal property of Fourier series, we can estimate the coefficients as follow:

$$\begin{aligned} c_{\boldsymbol{k}}^{\boldsymbol{i}} &= \int_{\boldsymbol{x}\in[-\pi,\pi]^d} f(\boldsymbol{x}) \left(\prod_{j=1}^{d} g_{k_j}(x_j)\right) d\boldsymbol{x} \\ &\approx \mathbb{E}_{(\boldsymbol{x},y)\in D}\left[y\left(\prod_{j=1}^{d} g_{k_j}(x_j)\right)\right] \end{aligned}$$

Of course this model can be used only when we need to evaluate small portion of $c_{\boldsymbol{k}}^{\boldsymbol{i}}$, since the number of coefficients grows exponentially as the dimension of data increases. This method assumes that each data feature is sampled from uniform distribution from $[-\pi, \pi]$. This assumption can be handled by using techniques like importance sampling, when we can infer the real distribution [21].

3.2 Classical kernel based model

The Dirichlet kernel is known to have the partial Fourier space as its reproducing kernel Hilbert space (RKHS) [22]. Consider a feature map of 1-dimensional data x.

$$\phi : x \to \left[e^{-ilx}, e^{-i(l-1)x}, \cdots, e^{ilx}\right], l \in \mathbb{N}$$

Then the inner product between $x^{(1)}$ and $x^{(2)}$ in this feature space can be computed as follows:

$$\phi^\dagger(x^{(1)})\phi(x^{(1)}) = \frac{sin\left((l+1/2)\Delta x\right)}{sin(\Delta x/2)} = D(\Delta x),$$

where $\Delta x = x^{(1)} - x^{(2)}$ and $D(\Delta x)$ is the Dirichlet kernel. It can be easily extended to d-dimensional data $\boldsymbol{x}$:

$$\phi^\dagger(\boldsymbol{x}^{(1)})\phi(\boldsymbol{x}^{(2)}) = \prod_{i=1}^{d} D(\Delta x_i).$$

A classical kernel method like kernel ridge regression (KRR) and kernel support vector machine (SVM) can be used with the Dirichlet kernel to approximate the output of VQML models.

4 Numerical experiments

We compare the outputs of VQML models and the classical models suggested in section 3 for toy examples. First, we sampled 2-dimensional data points $\boldsymbol{x} \in [-\pi, \pi]^2$ and generate the label based on values of a function $f(\boldsymbol{x})$ which has the form in equation (1) with $l = 3$. We randomly initialize the coefficients $c_{\boldsymbol{k},\boldsymbol{r}}^{\boldsymbol{i}}$ and then approximate the distribution of function values. In Figure 3, we present the distribution of the target function $f(\boldsymbol{x})$ and

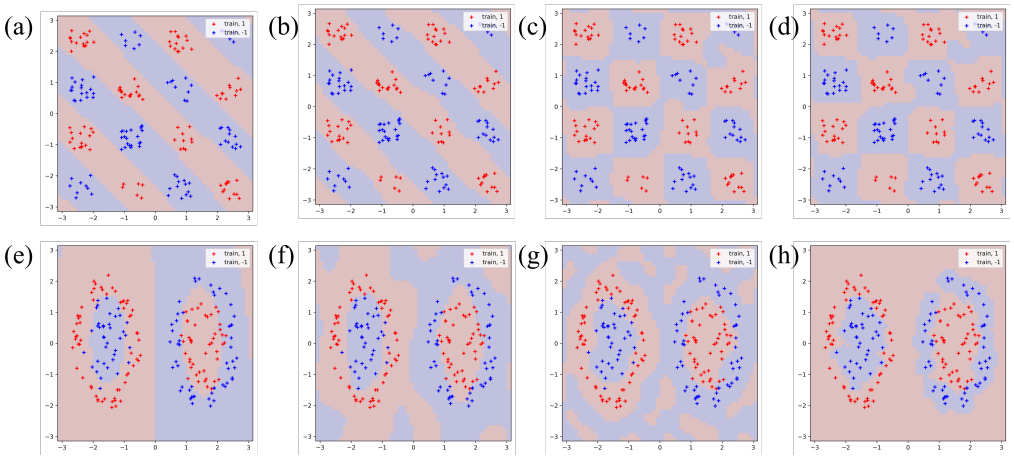


Figure 2: Outputs of models for (a)-(d) checkerboard and (e)-(h) symmetric donuts dataset. (a), (e) outputs of VQML model. (b), (c), (f), and (g) outputs of direct estimation model. (d), (h) outputs of kernel based SVM.

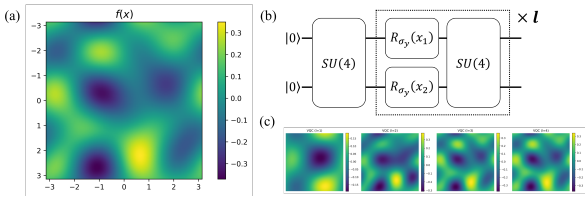


Figure 3: The distribution of target fucntion and VQC model output. (a) The function values for input $\boldsymbol{x} \in [-\pi, \pi]^2$. (b) The circuit structure used for VQC model. (c) The trained VQC model output for each number of layer l.

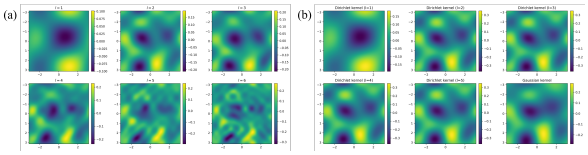


Figure 4: Output of classical models. (a) direct estimation model and (b) KRR model with the Dirichlet kernel.

the output of VQC model to approximate it. Figure 3 (b) shows the circuit structure used for VQC model and we trained it with different number of layers l. As the number of layer grows, the VQC model approximate $f(\boldsymbol{x})$ better. Note that $l = 3$ would be the least requirement for the VQC model to approximate $f(\boldsymbol{x})$ well, but the result shows that more than 3 layers are needed due to its limited capability.

We show the result of direct estimation model and the KRR model with Dirichlet kernel in Figure 4. As the estimated number of coefficients goes larger, the direct estimation model overfits to train data and becomes inefficient. KRR model utilizing the Dirichlet kernel approximates the target distribution well, without the necessity of estimating all the coefficients directly.

Next we aim to learn a synthetic data distribution shown in Figure 5. We apply a QK model suggested in Ref. [23] and its output for each dataset can be found in Figure 2 (a) and (e). It can separate the train data well but the output has much simpler form than the true distribution. For the direct estimation model, we first

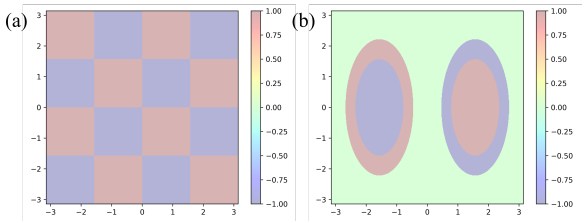


Figure 5: Distributions of synthetic datasets. (a) checkerboard and (b) symmetric donuts dataset.

estimated the largest 20 coefficients. The output is on Figure 2 (b) and (f). It has similar shape with the QK model for the input space. By estimating all coefficients, we could have more complex outputs which are more similar to the true ones. See Figure 2 (c) and (g). For the last, we applied SVM with the Dirichlet kernel. Again, the SVM could learn the target distribution well, without explicitly computing the coefficients. Figure 2 (d) and (h) shows the outputs of SVM.

5 Discussion

In this study, we showed explicit form of expression of the VQML models and argue that a classical counterpart can be constructed using the inductive bias which is necessary for the VQML models. We suggested two simple examples of classical model and showed that these classical models can surpass the performance of VQML models through numerical experiments with synthetic datasets. As Lee *et al.* [24] showed that the classical heuristics required for a quantum chemistry algorithm yield a question about the quantum advantage of such algorithm, the bias required for VQML models makes one to think of their potential quantum advantage. We identified the necessary conditions for VQML models and concluded that classical counterparts can be easily built under such kind of conditions. The results of our numerical experiments support our claim and demand a new approach of QML dealing with classical supervised ML tasks.

References

[1] J. Biamonte *et al.*, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[2] M. Cerezo *et al.*, "Variational quantum algorithms," *Nature Reviews Physics*, vol. 3, no. 9, pp. 625–644, 2021.

[3] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[4] K. Bharti *et al.*, "Noisy intermediate-scale quantum algorithms," *Reviews of Modern Physics*, vol. 94, no. 1, p. 015004, 2022.

[5] E. Farhi and H. Neven, "Classification with quantum neural networks on near term processors," *arXiv preprint arXiv:1802.06002*, 2018.

[6] M. Schuld *et al.*, "Circuit-centric quantum classifiers," *Physical Review A*, vol. 101, no. 3, p. 032308, 2020.

[7] K. Mitarai *et al.*, "Quantum circuit learning," *Physical Review A*, vol. 98, no. 3, p. 032309, 2018.

[8] M. Benedetti *et al.*, "Parameterized quantum circuits as machine learning models," *Quantum Science and Technology*, vol. 4, no. 4, p. 043001, 2019.

[9] A. Pérez-Salinas *et al.*, "Data re-uploading for a universal quantum classifier," *Quantum*, vol. 4, p. 226, 2020.

[10] T. Hur, L. Kim, and D. K. Park, "Quantum convolutional neural network for classical data classification," *Quantum Machine Intelligence*, vol. 4, no. 1, p. 3, 2022.

[11] H.-Y. Huang *et al.*, "Power of data in quantum machine learning," *Nature Communications*, vol. 12, no. 1, p. 2631, 2021.

[12] M. Schuld and N. Killoran, "Quantum machine learning in feature hilbert spaces," *Physical Review Letters*, vol. 122, no. 4, p. 040504, 2019.

[13] V. Havlíček *et al.*, "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, 2019.

[14] M. Schuld, M. Fingerhuth, and F. Petruccione, "Implementing a distance-based classifier with a quantum interference circuit," *Europhysics Letters*, vol. 119, no. 6, p. 60002, 2017.

[15] C. Blank *et al.*, "Quantum classifier with tailored quantum kernel," *npj Quantum Information*, vol. 6, no. 1, p. 41, 2020.

[16] M. Schuld and N. Killoran, "Is quantum advantage the right goal for quantum machine learning?," *PRX Quantum*, vol. 3, no. 3, p. 030101, 2022.

[17] E. Tang, "Quantum principal component analysis only achieves an exponential speedup because of its state preparation assumptions," *Physical Review Letters*, vol. 127, no. 6, p. 060503, 2021.

[18] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[19] D. F. James *et al.*, "Measurement of qubits," *Physical Review A*, vol. 64, no. 5, p. 052312, 2001.

[20] T. Haug *et al.*, "Capacity and quantum geometry of parametrized quantum circuits," *PRX Quantum*, vol. 2, no. 4, p. 040309, 2021.

[21] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[22] V. Vapnik, *The nature of statistical learning theory*. Springer, 1999.

[23] T. Hubregtsen *et al.*, "Training quantum embedding kernels on near-term quantum computers," *Physical Review A*, vol. 106, no. 4, p. 042431, 2022.

[24] S. Lee *et al.*, "Evaluating the evidence for exponential quantum advantage in ground-state quantum chemistry," *Nature Communications*, vol. 14, no. 1, p. 1952, 2023.

Effect of Scattering on Quantum Ghost Imaging and Ordinary Imaging

Yasushi Horiba[1] * Tiancheng Wang[1 2] † Tsuyoshi Sasaki Usuda[1] ‡

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, Aichi 480-1198, Japan.*
[2] *Faculty of Informatics, Kanagawa University, Kanagawa 221- 8686, Japan.*

Abstract. Scattered light is a inherent source of noise in X-ray imaging, and its influence can be mitigated by employing collimators. However, to compensate for the loss of light caused by collimators and obtain images of sufficient quality, it is necessary to increase the light intensity. Unfortunately, increasing the light intensity is undesirable for the human body due to the increased radiation exposure. In this study, we consider a quantum ghost imaging scheme to utilize the scattered light, which does not depend on collimators. We also demonstrate that this scheme can outperform the conventional approach.

Keywords: Quantum ghost imaging, Quantum entanglement, Scattering

1 Introduction

Quantum ghost imaging [1] is an application protocol of entanglement [2]. This protocol is much more robust against noise than conventional imaging techniques. It is expected to allow objects obscured by noise to be seen more clearly than with conventional technology. One of the common advantages of quantum measurement using light, including quantum ghost imaging, is that it is much more sensitive than conventional optical measurement when using light with extremely low energy. However, if the intensity of light in conventional optical measurements is increased, measurement with higher sensitivity than quantum measurements using weak light may be possible. Thus advantages of quantum measurements will disappear when we can use strong light.

Is there a case where we want to use the weakest possible light source for measurement? There are cases where there is a need to avoid damaging the object to be measured. For example, when measuring the human body with X-rays, there is a strong need to minimize the amount of exposure to radiation. In X-ray imaging in particular, scattered light is known to be a significant noise factor, and current technology uses collimators to remove scattered light. However, since collimators reduce the amount of light reaching the detector, it is necessary to increase the amount of light to obtain images of sufficient quality. Such an increase in light intensity is undesirable in human body measurements because it causes an increase in radiation exposure. Since scattering occurs when light is irradiated to an object, scattered light also contains information about the object. In addition, some studies have recently been conducted to increase measurement sensitivity by collecting information on the scattered light [3].

In this study, we focused on the fact that "scattering occurs when light is irradiated to an object". If quantum ghost imaging using two entangled lights is applied, the position of one light before it is refracted by scattering can be known by the position of the other light. This means that the information of the scattered light can be fully utilized.

In quantum ghost imaging, attenuation and other factors have been considered by various researchers, but the main theme of this study is to consider the effect of scattering. In this paper, we first treat a setup in which light randomly spreads around an object after passing through it as a simple model of scattering. Also we compare the characteristics of classical imaging and quantum ghost imaging through simulations. The object to be treated is simply an A-shaped shield (a setup similar to that in [4, 5]). As an evaluation method, first we are subjectively compare the obtained images and then we compute PSNR [6, 7] as an objective evaluation. PSNR is a measure of how close two images are and has often been used in the evaluation of quantum ghost imaging. The definition of PSNR is as follows:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{I_{\mathrm{MAX}}^2}{\mathrm{MSE}}\right), \tag{1}$$

where I_{MAX} is the maximum value of signal intensity and MSE is the mean squared error. In this paper, the intensity is assumed to be normalized and $I_{\mathrm{MAX}} = 1$.

2 Problem Setup

2.1 Quantum Ghost Imaging

Ghost imaging is a technique to create a two-dimensional image of the shape of an object by using two detectors with different roles and spatially correlated light. The two roles are to measure light intensity information and to measure light position information, respectively. Among ghost imaging techniques, those that use entanglement for correlation are called quantum ghost imaging. The schematic of quantum ghost imaging is shown in Fig.1. In Fig.1, D_A represents a detector without spatial resolution, D_B represents a detector with spatial resolution ($d \times d$ pixels), and C represents the correlator. An entangled photon pair consists of two modes: the modes A and B. The following explains the protocol:

(1) Two modes of a spatially entangled state are irradiated toward D_A and D_B, simultaneously.

(2) D_A detects the light and checks for the presence of an object at the corresponding coordinates.

*im231009@cis.aichi-pu.ac.jp
†wang@kanagawa-u.ac.jp
‡usuda@ist.aichi-pu.ac.jp

(3) Direct light from the light source at D_B to obtain information on the irradiated coordinates.

(4) The image is calculated by applying the information on the light intensity and coordinates obtained by the two detectors to a correlator.

While the mode A, where the object exists, is affected by noise, the mode B is an imaging technique that is less affected by noise due to the fact that it can obtain positional information by directly illuminating the detector and the fact that the image is obtained by the correlation process between the modes A and B.

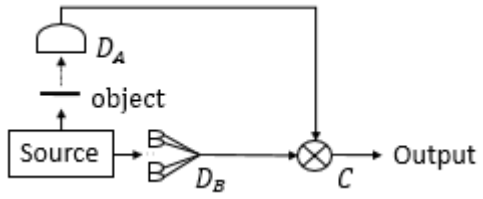


Figure 1: Schematic of quantum ghost imaging

2.2 Quantum State

The quantum state used in this study is an entangled state, defined by the following equation.

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |\Psi_i\rangle \,, \tag{2}$$

where

$$\begin{aligned} |\Psi_i\rangle \;\; = \;\; & |0_{\mathrm{L}}\rangle_{\mathrm{A}_1} |0_{\mathrm{L}}\rangle_{\mathrm{B}_1} \cdots \\ & |1_{\mathrm{L}}\rangle_{\mathrm{A}_i} |1_{\mathrm{L}}\rangle_{\mathrm{B}_i} \cdots |0_{\mathrm{L}}\rangle_{\mathrm{A}_N} |0_{\mathrm{L}}\rangle_{\mathrm{B}_N} \end{aligned} \tag{3}$$

is the product state of the modes A and B. Both the modes A and B consist of N points $A_1, \ldots, A_N$ and $B_1, \ldots, B_N$ corresponding to $N = d \times d$ pixels. In this study, $|0_{\mathrm{L}}\rangle$ is a photon number state with zero photons (vacuum state) and $|1_{\mathrm{L}}\rangle$ is a photon number state with a single photon. $|\Psi_i\rangle$ is defined as the product state of the quantum states at each point. The typical light source used for quantum ghost imaging is entangled light produced by spontaneous parametric down conversion (SPDC), and it was used in the world's first quantum ghost imaging experiment [1]. The state in Eq.(2) is in a sense an idealized version of the entangled state produced by SPDC; SPDC is a special case of parametric down conversion (PDC). Actually, PDC of X-rays has been considered since the 1960s [8, 9]. More recently, experiments on quantum ghost imaging using X-rays have also been performed [10].

2.3 Scattering

In this paper, as a simple model of scattering, we treat a setup in which light randomly spreads around an object after passing through it. The parameter s $(0 \leq s \leq 1)$ represents the fraction of light that spreads; when $s = 0$, it means that all light travels straight ahead; when $s = 0.5$, 50% of the light is scattered uniformly in the surroundings.

3 Results

Let k be the number of photons per pixel. For example, when $k = 10$, each pixel is irradiated 10 times, i.e., the total number of photon irradiations is $10 \times 100 = 1000$. The results of the simulation are shown below.

3.1 Output image

Fig.2 shows the output image by the quantum ghost imaging and Fig.3 shows that by an ordinary (classical) imaging. Here, a black point represents no photon is detected at the coordinate, whereas a white point represents at least a one photon is detected. In the ghost imaging, the shape of the shield A appears without the effect of scattering. In the classical imaging, the entire image is white due to the effect of scattering. Since the entire image is white in the classical case, to improve visibility, introduce a grey-scaled image instead of the black- and -white image. Fig.4 shows the grey-scaled image of the classical imaging. Here, the grey-level is determined by the number of detected photons. More precisely, we use a normalization with respect to the maximum number of detected photons. The image of shield A appears when the number of photon irradiations increases, but the number of irradiations must be increased significantly in order to clearly identify the shield as A. Even if the number of irradiations is greatly increased, the image of shield A becomes dim due to the effect of scattering.

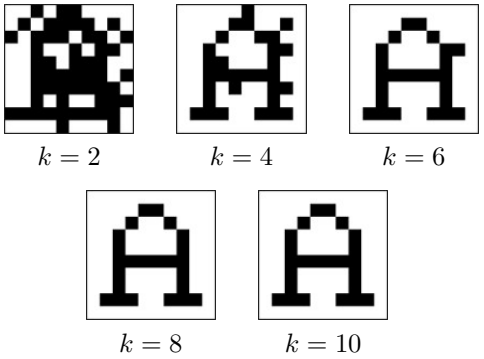


Figure 2: Output image of quantum ghost imaging

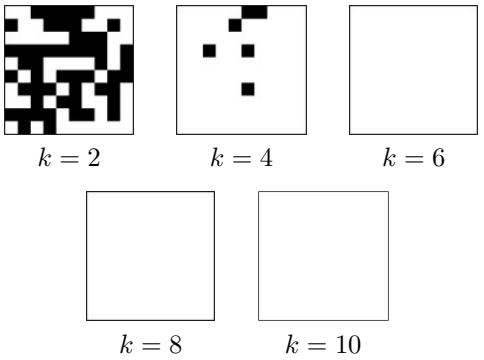


Figure 3: Output image of ordinary (classical) imaging

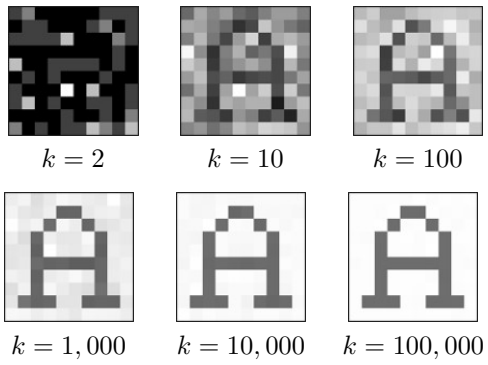


Figure 4: The grey-scaled (normalized) image of the classical imaging

3.2 PSNR

The PSNR is summarized in the graph shown in Fig.5. In classical imagings, the PSNR is strongly affected by scattering. As a result, when normalized to the maximum value, the PSNR reaches a certain value and no further improvement can be seen. In the quantum ghost imaging, the PSNR diverges because it coincides the original image. Fig.6 shows the dependence of the PSNR on the degree of scattering s. In the quantum ghost imaging, the effect of scattering is eliminated for any s, so the PSNR diverges and is not represented on the graph. In the classical imaging, except for the case of $s = 0$, the entire image is white and the PSNR is constant. In the grey-scaled case, the smaller the degree of scattering, the better the PSNR value, and the stronger the scattering, the worse the PSNR value.

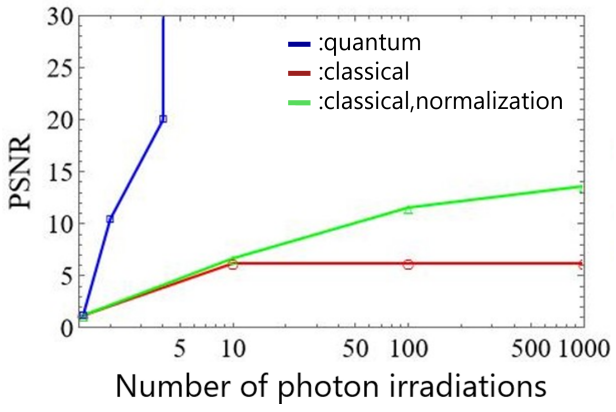


Figure 5: PSNR with respect to the number of photon irradiations

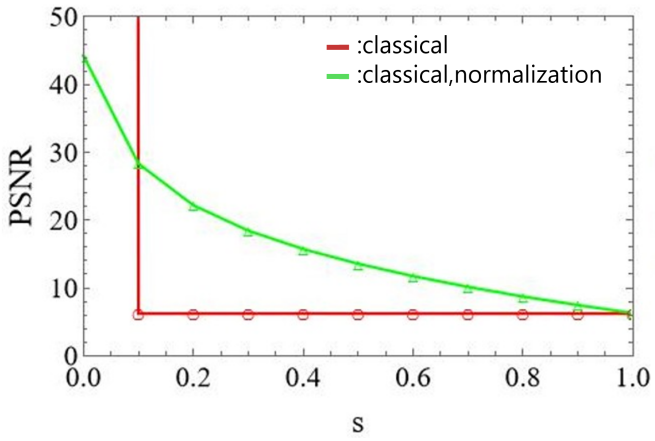


Figure 6: PSNR with respect to s when $k = 100,000$

4 Conclusion

We compared the performance of classical imaging and quantum ghost imaging under the influence of scattering. First, a simple model of scattering was considered and repeated irradiation simulations were performed. As a result, we found that classical imaging is greatly affected by scattering, and when the amount of scattering is large, a clear image cannot be obtained even if the number of irradiations is increased, whereas quantum ghost imaging is not affected by scattering, and the image becomes clearer as the number of irradiations is increased, regardless of the amount of scattering, based on examples of obtained images and PSNR.

Acknowledgments: This work has been supported in part by JSPS KAKENHI Grant Number 20H00581, 20K20397, 21K04064, 22K20437, and The Nitto Foundation.

References

[1] T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," Phys. Rev. **A52**, pp.R3429-R3432, (1995).

[2] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," Phys. Rev. **47**, pp.777-780, (1935).

[3] S. Ito and N. Toda, "Improvement of CT reconstruction using scattered X-rays," IEICE Trans. **E104.D**, no.8, pp.1378-1385, (2021).

[4] Y. Iwama, J. Yamauchi, T.Wang, and T. S. Usuda, "Dependence of performance of quantum ghost imaging with multiple position illumination on shape of ojects," Proc. of 2022 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, F6-7 (2021). (in Japanese)

[5] Y Takahashi, T. Wang, S Usami, and T. S. Usuda, "Characteristics of Quantum Ghost Imaging with

Multiple Positions Illumination," IEEJ Transactions on Erectronics on Electronics, Information and Systems **142**, no.8, pp.1933-1941, (2022).

[6] C. Zhang, S. Guo, J. Cao, J. Guan, and F. Gao, "Object reconstitution using pseudo-inverse for ghost imaging," Opt. Express **22**, pp.30063-30073, (2014).

[7] H. Huang, C. Zhou, T. Tian, D. Liu, and L. Song, "High-quality compressive ghost imaging," Opt. Commun. **412**, pp.60-65, (2018).

[8] I. Freund and B. F. Levine, "Parametric conversion of X rays," Phys. Rev. Lett. **23**, pp.854-857, (1969).

[9] P. Eisenberger and S. L. McCall, "X-ray parametric conversion," Phys. Rev. Lett. **26**, pp.684-688, (1971).

[10] D. Pelliccia, A. Rack, M. Scheel, V. Cantelli, and D. M. Paganin, "Experimental X-ray ghost imaging," Phys. Rev. Lett. **117**, 113902, (2016).