Asian
Quantum
Information
Science Conference **2019**

Abstract Booklet

Poster Day 1

August 19-23, 2019
Venue: KIAS, Seoul, Korea

Hosted by KIAS (Korea Institute for Advanced Study)

Edited by Shigeru Yamashita and Seung-Woo Lee

Posters

August 19, 2019 (Mon.) [Poster Session I]

Simultaneous cooling of coupled mechanical resonators in cavity optomechanics

Deng-Gao Lai[1] Fen Zou[1] Bang-Pin Hou[2] Yun-Feng Xiao[3] Jie-Qiao Liao[1] *

[1] *Key Laboratory of Low-Dimensional Quantum Structures and Quantum Control of Ministry of Education, Department of Physics and Synergetic Innovation Center for Quantum Effects and Applications, Hunan Normal University, Changsha 410081, China*

[2] *College of Physics and Electronic Engineering, Institute of Solid State Physics, Sichuan Normal University, Chengdu 610068, China*

[3] *State Key Laboratory for Mesoscopic Physics and School of Physics, Peking University, Collaborative Innovation Center of Quantum Matter, Beijing 100871, China*

Abstract. Quantum manipulation of coupled mechanical resonators has become an important research topic in optomechanics because these systems can be used to study the quantum coherence effects involving multiple mechanical modes. A prerequisite for observing macroscopic mechanical coherence is to cool the mechanical resonators to their ground state. Here we propose a theoretical scheme to cool two coupled mechanical resonators by introducing an optomechanical interface. The final mean phonon numbers are calculated exactly and the results show that the ground-state cooling is achievable in the resolved-sideband regime. By adiabatically eliminating the cavity field in the large-decay regime, we obtain the cooling limits, which show the smallest achievable phonon numbers and the parameter conditions under which the optimal cooling is achieved. Finally, the scheme is extended to the cooling of a chain of coupled mechanical resonators.

Keywords: resonators, phonon numbers, cooling limit

1 Model and Hamiltonian

We consider a three-mode optomechanical system, which is composed of one cavity mode and two mechanical modes, as illustrated in Fig. 1. The cavity-field mode is coupled to the first mechanical mode via the radiation-pressure coupling, and the two mechanical modes are coupled to each other via the so-called position-position interaction. To manipulate the optical and mechanical degrees of freedom, a proper driving field is applied to the optical cavity. The Hamiltonian of the system reads ($\hbar = 1$)

$$\begin{aligned} H &= \omega_c a^\dagger a + \sum_{l=1,2}\left(\frac{p_{xl}^2}{2m_l} + \frac{m_l\tilde{\omega}_l^2 x_l^2}{2}\right) - \lambda a^\dagger a x_1 \\ &\quad + \eta\left(x_1 - x_2\right)^2 + \Omega(a^\dagger e^{-i\omega_L t} + a e^{i\omega_L t}), \end{aligned} \tag{1}$$

where a and $a^\dagger$ are, respectively, the annihilation and creation operators of the cavity mode with the resonance frequency ω_c. The coordinate and momentum operators x_l and p_{xl} are introduced to describe the lth ($l = 1, 2$) mechanical resonator with mass m_l and resonance frequency $\tilde{\omega}_l$. The optomechanical coupling between the cavity field and the first mechanical mode is described by the λ term in Eq. (1), where $\lambda = \omega_c/L$ denotes the optomechanical force of a single photon, with L being the rest length of the optical cavity. The η term depicts the mechanical interaction between the two mechanical resonators. The parameters ω_L and Ω are, respectively, the optical driving frequency and driving amplitude, which is determined by the driving power via the relation $\Omega = \sqrt{2P_L\kappa/\omega_L}$, where P_L is the power of the driving laser, and κ is the decay rate of the cavity field.

*jqliao@hunnu.edu.cn

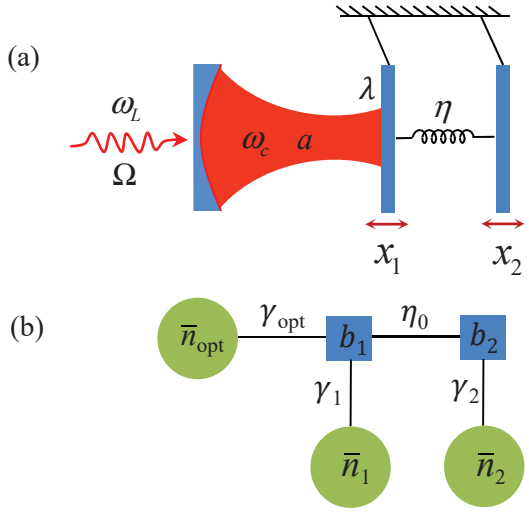


Figure 1: (a) Schematic of the three-mode optomechanical system. A single-mode cavity field with resonance frequency ω_c is coupled to an end mirror with resonance frequency $\tilde{\omega}_1$ via the radiation pressure coupling. The end mirror is coupled to another mechanical resonator with resonance frequency $\tilde{\omega}_2$ via the "position-position" interaction. (b) By adiabatically eliminating the cavity mode, the model (a) can be simplified as two mechanical modes b_1 and b_2 whose coupling strength is η_0. Each harmonic oscillator is also coupled to its own heat bath with initial phonon numbers $\bar{n}_1$ and $\bar{n}_2$ by decay rates γ_1 and γ_2. Additionally, the mode b_1 is coupled to an effective optical bath with the effective decay rate $\gamma_{\rm opt}$ and thermal occupation $\bar{n}_{\rm opt}$.

2 Ground state cooling and cooling limits

Mathematically, the final mean phonon numbers in the two mechanical resonators can be calculated by the rela-

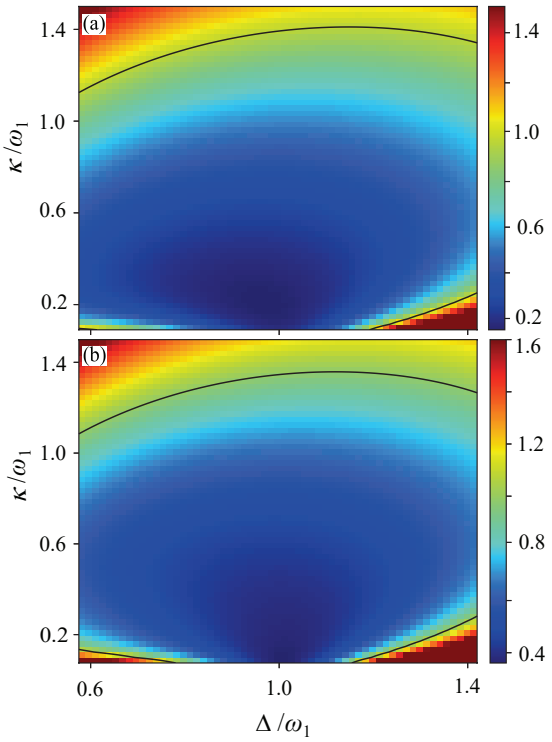


Figure 2: (Color online) The final mean phonon numbers (a) n_1^f and (b) n_2^f in the two mechanical resonators vs the effective driving detuning Δ/ω_1 and the decay rate κ/ω_1. The used parameters are given by $\omega_1/2\pi = \omega_2/2\pi = 10$ MHz, $\gamma_1/\omega_1 = \gamma_2/\omega_1 = 10^{-5}$, $\omega_c/\omega_1 = 2.817 \times 10^7$, $\eta_0/\omega_1 = 0.04$, $m_1 = m_2 = 250$ ng, $\bar{n}_1 = \bar{n}_2 = 1000$, $L = 0.5$ mm, $P_L = 50$ mW, and $\lambda = 1064$ nm. The black solid curves correspond to $n_1^f = n_2^f = 1$.

tion

$$n_l^f = \frac{1}{2}[\langle \delta q_l^2 \rangle + \langle \delta p_l^2 \rangle - 1], \tag{2}$$

where

$$\langle \delta q_l^2 \rangle = \frac{1}{2\pi}\int_{-\infty}^{\infty} S_{q_l}(\omega)d\omega, \qquad l = 1, 2, \tag{3a}$$

$$\langle \delta p_l^2 \rangle = \frac{1}{2\pi}\int_{-\infty}^{\infty} S_{p_l}(\omega)d\omega = \frac{1}{2\pi\omega_l^2}\int_{-\infty}^{\infty} \omega^2 S_{q_l}(\omega)d\omega. \tag{3b}$$

Here the fluctuation spectra of the position and momentum of the two mechanical oscillators are defined by

$$S_o(\omega) = \int_{-\infty}^{\infty} e^{-i\omega\tau}\langle \delta o(t+\tau)\delta o(t)\rangle_{\rm ss} d\tau, \tag{4}$$

for $o = q_{l=1,2}$ and $p_{l=1,2}$. The fluctuation spectrum can also be expressed in the frequency domain as

$$\langle \delta\tilde{o}(\omega)\delta\tilde{o}(\omega')\rangle_{\rm ss} = S_o(\omega)\delta(\omega+\omega'), \qquad (o = q_l, p_l). \tag{5}$$

In Fig. 2, we plot the final mean phonon numbers n_1^f and n_2^f as a function of the driving detuning Δ/ω_1 and the cavity-field decay rate κ/ω_1. When $\kappa/\omega_1 \ll 1$, the phonon sidebands can be resolved from the cavity emission spectrum, and this regime is called as the resolved-sideband limit. We can see that the two resonators can be cooled efficiently ($n_1^f, n_2^f \ll 1$) in the resolved-sideband limit and under the driving $\Delta/\omega_1 \sim 1$, which means that the ground-state cooling is achievable in this system. For a given value of the ratio κ/ω_1, the optimal driving detuning is given by $\Delta \approx \omega_1$. This is because the energy extraction efficiency between the cavity mode and the first mechanical mode should be maximum at $\Delta = \omega_1$, and the small deviation of the exact value of ω_1 in realistic simulations is caused by the counter RW term in the linearized interaction between the cavity mode and the first mechanical mode. Physically, the generation of an anti-Stokes photon will cool the mechanical oscillator by taking away a phonon from the mechanical resonator. For the optimal cooling detuning $\Delta \approx \omega_1$, the frequency ω_1 of the phonon exactly matches the driving detuning Δ and hence $\Delta/\omega_1 = 1$ corresponds to the optimal cooling. At the optimal driving $\Delta = \omega_1$, the final mean phonon numbers become worse with the increase of the ratio κ/ω_1.

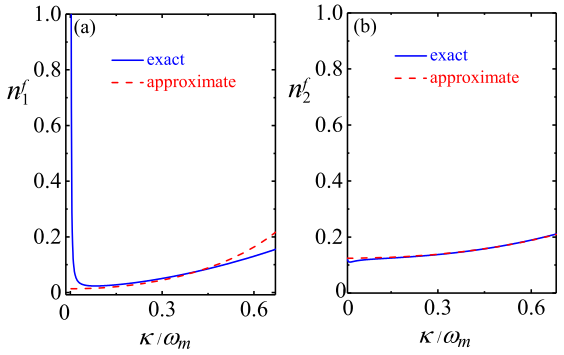


Figure 3: (Color online) Final mean phonon numbers (a) n_1^f and (b) n_2^f as a function of κ/ω_m. In addition, we take $\Delta = \omega_m$, $\gamma_1/\omega_m = \gamma_2/\omega_m = 10^{-6}$, and $\eta_0/\omega_1 = 0.02$. Other parameters are the same as those given in Fig. 2.

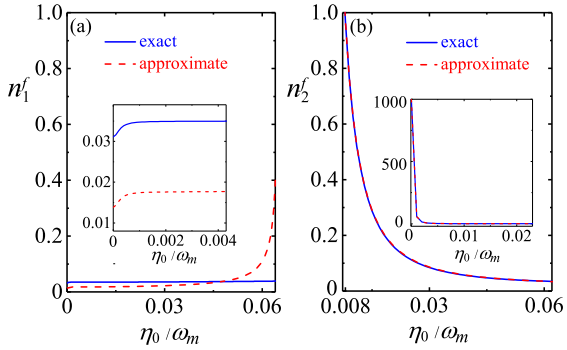


Figure 4: (Color online) Final mean phonon numbers (a) n_1^f and (b) n_2^f as a function of η_0/ω_m. The insets are zoom-in plots of the phonon numbers in a narrower range of η_0/ω_m. We take $\Delta = \omega_m$, $\kappa/\omega_1 = 0.2$, and $P_L = 70$ mW. Other parameters are the same as those given in Fig. 3.

Below, we derive the approximate cooling results in the bad-cavity regime such that compact expressions of the cooling limits can be obtained. This is achieved by elim-

inating adiabatically the cavity field in the large-decay regime ($\kappa \gg \tilde{G}$) and then calculating the final phonon numbers under the RWA ($\omega_{1,2} \gg \tilde{G}$). Thus, the approximate expressions of the final mean phonon numbers can be obtained as

$$n_1^f \approx \frac{\gamma_1 \bar{n}_1}{\Gamma_1} + \frac{\gamma_{\rm opt} n_{\rm opt} + \chi n_{1,\chi}}{\Gamma_1 - 4\chi}, \tag{6a}$$

$$n_2^f \approx \frac{\gamma_2 \bar{n}_2 + \chi n_{2,\chi}}{\chi + \gamma_2}, \tag{6b}$$

where $n_{\rm opt} = \kappa^2/4(\omega_m+\Delta)^2$, $n_{1,\chi} = \gamma_2\bar{n}_2(4\chi+\Gamma_1)/[(\Gamma_1+\gamma_2)(\chi+\gamma_2)]$, and $n_{2,\chi} = (\gamma_1\bar{n}_1+\gamma_2\bar{n}_2+\gamma_{\rm opt}n_{\rm opt})/(\Gamma_1+\gamma_2)$ with $\Gamma_1 = \gamma_1+\gamma_{\rm opt}$. We also introduce the effective decay rates $\gamma_{\rm opt} = 4|\tilde{G}|^2/\kappa$ and $\chi = 4\eta_0^2/(\gamma_1+\gamma_{\rm opt})$ corresponding to the optomechanical channel and the mechanical coupling channel, respectively. To evaluate the approximate cooling results, we compare the approximate results with the exact results. It shows that the approximate and exact phonon numbers coincide well with each other in $\kappa \approx 0.1\omega_m \sim 0.5\omega_m$ and $\eta_0 \approx 0 \sim 0.05\omega_m$. Figure 3(a) shows that difference between the approximate result and the exact result increases when $\kappa < 0.1\omega_m$. This is because the adiabatic elimination procedure only works under the condition $\kappa \gg \tilde{G}$. In Fig. 4(a), we see that the two results do not matched well for a large η_0 (for example $\eta_0/\omega_m > 0.05$ in our simulations). This phenomenon can be explained based on the parameter requirement of the system stability. In the case of $\Omega_1 \approx \omega_2$ and $\gamma_1 = \gamma_2$, the parameter condition is reduced to $\gamma_{\rm opt} > 4\chi$. Corresponding to Fig. 4(b), when $\eta_0/\omega_m > 0.05$, the stability condition $\gamma_{\rm opt} > 4\chi$ is violated.

3 Cooling of a chain of coupled mechanical resonators

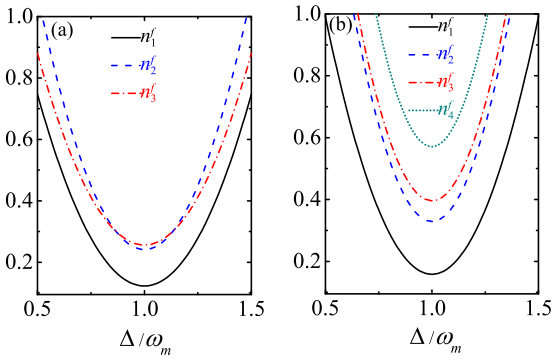


Figure 5: (Color online) Final mean phonon numbers in the mechanical resonators as a function of the effective driving detuning Δ when (a) $N = 3$ and (b) $N = 4$. Other parameters are given by $G/\omega_m = 0.2$, $\eta_0/\omega_m = 0.1$, $\kappa/\omega_m = 0.3$, $\gamma_m/\omega_m = 10^{-5}$, and $\bar{n} = 1000$.

In this section, we extend the optomechanical cooling means to the cooling of a coupled-mechanical-resonator chain. Without loss of generality, we assume that all the mechanical resonators are identical, having the same frequency, decay rate, and thermal occupation number. Meanwhile, the couplings between the mechanical resonators are much smaller than the mechanical frequency and hence the rotating-wave approximation is justified. In this case, the Hamiltonian of the system can be written in a frame rotating at the driving frequency as

$$\begin{aligned} H_I &= \Delta a^\dagger a + \omega_m \sum_{j=1}^{N} b_j^\dagger b_j - (G a^\dagger b_1 + G^\star b_1^\dagger a) \\ &\quad - \sum_{j=1}^{N-1} \eta_0 (b_j^\dagger b_{j+1} + b_{j+1}^\dagger b_j), \end{aligned} \tag{7}$$

where a ($a^\dagger$) and $b_{j=1-N}$ are the annihilation (creation) operators of the cavity mode and the jth resonator. The parameter Δ is the driving detuning after the linearization of the optomechanical coupling, G is the strength of the linearized optomechanical coupling, and ω_m and η_0 are the frequency of these resonators and the coupling strength between the neighboring mechanical resonators, respectively. To include the dissipations, we assume that the cavity is coupled to a vacuum bath and the mechanical resonators are coupled to independent heat baths at the same temperatures. Then the evolution of the system can be governed by the quantum master equation

$$\begin{aligned} \dot{\rho} &= i[\rho, H_I] + \frac{\kappa}{2}(2a\rho a^\dagger - a^\dagger a\rho - \rho a^\dagger a) \\ &\quad + \frac{\gamma_m}{2}(\bar{n}_m + 1)\sum_{j=1}^{N}(2b_j\rho b_j^\dagger - b_j^\dagger b_j\rho - \rho b_j^\dagger b_j) \\ &\quad + \frac{\gamma_m \bar{n}_m}{2}\sum_{j=1}^{N}(2b_j^\dagger \rho b_j - b_j b_j^\dagger \rho - \rho b_j b_j^\dagger), \end{aligned} \tag{8}$$

where ρ is the density matrix of the coupled cavity-resonator system, $\bar{n}_m$ is thermal phonon number of the heat baths of these mechanical resonators, κ and γ_m are the decay rates of the cavity mode and the mechanical resonators, respectively. To evaluate the cooling efficiency, we solve the steady-state solution of quantum master equation (8) and calculate the average occupation numbers in the cavity and these mechanical resonators. We see that the ground-state cooling is achievable and the final phonon numbers successively increase from n_1^f to n_N^f at the optimal effective detuning $\Delta = \omega_m$. The physical reason for this phenomenon is that the system is a cascade system and the vacuum bath of the optomechanical cavity provides the cooling reservoir to extract the thermal excitations in these mechanical resonators, which are thermally excited by their heat baths. After the linearization, the system is reduced to an array of coupled bosonic modes. Then the vacuum bath provides the cooling channel of the cavity, and the cavity provides the cooling channel of the first mechanical resonator. Successively, the former resonator provides the cooling channel for the next resonator. As a result, the cooling efficiency is higher for a mechanical oscillator which is closer to the cavity.

References

[1] D.-G. Lai, F. Zou, B.-P. Hou, Y.-F. Xiao, and J.-Q. Liao, Phys. Rev. A **98**, 023860 (2018).

Enhancement of few-photon optomechanical effects with cross-Kerr nonlinearity

Fen Zou[1] Li-Bao Fan[1] Jin-Feng Huang[1] * Jie-Qiao Liao[1] †

[1]*Key Laboratory of Low-Dimensional Quantum Structures and Quantum Control of Ministry of Education, Department of Physics and Synergetic Innovation Center for Quantum Effects and Applications, Hunan Normal University, Changsha 410081, China*

Abstract. Few-photon optomechanical effects are not only important physical evidences for understanding the radiation-pressure interaction between photons and mechanical oscillation, but also have wide potential applications in modern quantum technology. Here we study the few-photon optomechanical effects including photon blockade and generation of the Schrödinger cat states under the assistance of a cross-Kerr interaction, which is an inherent interaction accompanied the optomechanical coupling in a generalized optomechanical system. By exactly diagonalizing the generalized optomechanical Hamiltonian and calculating its unitary evolution operator, we find the physical mechanism of the enhancement of photon blockade and single-photon mechanical displacement.

Keywords: Cross-Kerr interaction, Photon blockade, Schrödinger cat states

1 Model and Hamiltonian

We consider a generalized optomechanical model, which is composed of a single-mode optical field and a mechanical mode [see Fig. 1(a)]. The Hamiltonian of the generalized optomechanical model reads ($\hbar = 1$)

$$\hat{H}_{\rm gom} = \omega_c \hat{a}^\dagger \hat{a} + \omega_M \hat{b}^\dagger \hat{b} - g_0 \hat{a}^\dagger \hat{a}(\hat{b}^\dagger + \hat{b}) - g_{\rm cK} \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b}, \quad (1)$$

where $\hat{a}$ ($\hat{a}^\dagger$) and $\hat{b}$ ($\hat{b}^\dagger$) are, respectively, the annihilation (creation) operators of the cavity mode and the mechanical mode, with the corresponding resonance frequencies ω_c and ω_M. The g_0 term denotes the optomechanical coupling between the cavity field and the mechanical mode, with the coupling strength g_0. The $g_{\rm cK}$ term describes the cross-Kerr interaction between the cavity field and the mechanical mode, with the coupling strength $g_{\rm cK}$.

To calculate the eigensystem of $\hat{H}_{\rm gom}$, we introduce a conditional displacement operator $\hat{D}(\hat{\xi}) = \exp[\hat{\xi}(\hat{b}^\dagger - \hat{b})]$, where the displacement amplitude $\hat{\xi}$ is a nonlinear function of the photon number operator $\hat{a}^\dagger \hat{a}$,

$$\hat{\xi} = \frac{g_0 \hat{a}^\dagger \hat{a}}{\omega_M - g_{\rm cK} \hat{a}^\dagger \hat{a}} = \sum_{m=0}^{\infty} \xi^{[m]} |m\rangle_a \, {}_a\langle m|, \quad (2)$$

with the m-photon induced mechanical displacement

$$\xi^{[m]} = \frac{m g_0}{\omega_M - m g_{\rm cK}}, \quad (3)$$

where we introduce the number states $|m\rangle_a$ ($m = 0, 1, 2, \cdots$) of the cavity mode. The Hamiltonian $\hat{H}_{\rm gom}$ can be diagonalized as follows,

$$\begin{aligned} \hat{\tilde{H}}_{\rm gom} &= \hat{D}^\dagger(\hat{\xi}) \hat{H}_{\rm gom} \hat{D}(\hat{\xi}) \\ &= \omega_c \hat{a}^\dagger \hat{a} + (\omega_M - g_{\rm cK} \hat{a}^\dagger \hat{a}) \hat{b}^\dagger \hat{b} - \hat{\delta}, \end{aligned} \quad (4)$$

where we introduce the optical nonlinearity as

*jfhuang@hunnu.edu.cn
†jqliao@hunnu.edu.cn

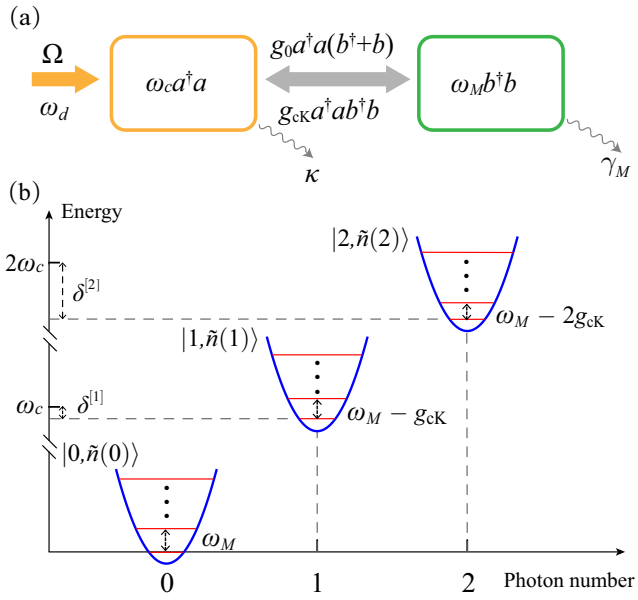


Figure 1: (Color online) (a) Schematic diagram of the generalized optomechanical model. (b) Diagram of the eigenenergy spectrum of the Hamiltonian $\hat{H}_{\rm gom}$ in the subspace associated with zero, one, and two photons.

$$\hat{\delta} = \frac{g_0^2 \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a}}{\omega_M - g_{\rm cK} \hat{a}^\dagger \hat{a}} = \sum_{m=0}^{\infty} \delta^{[m]} |m\rangle_a \, {}_a\langle m|, \quad (5)$$

with the m-photon energy shift

$$\delta^{[m]} = \frac{g_0^2 m^2}{\omega_M - m g_{\rm cK}}. \quad (6)$$

The eigensystem of the Hamiltonian $\hat{\tilde{H}}_{\rm gom}$ can be expressed as

$$\hat{\tilde{H}}_{\rm gom} |m\rangle_a |n\rangle_b = E_{m,n} |m\rangle_a |n\rangle_b, \quad (7)$$

where $|n\rangle_b$ ($n = 0, 1, 2, \cdots$) are number states of the mechanical mode. The corresponding eigenvalues are

$$E_{m,n} = m\omega_c + (\omega_M - m g_{\rm cK}) n - \delta^{[m]}. \quad (8)$$

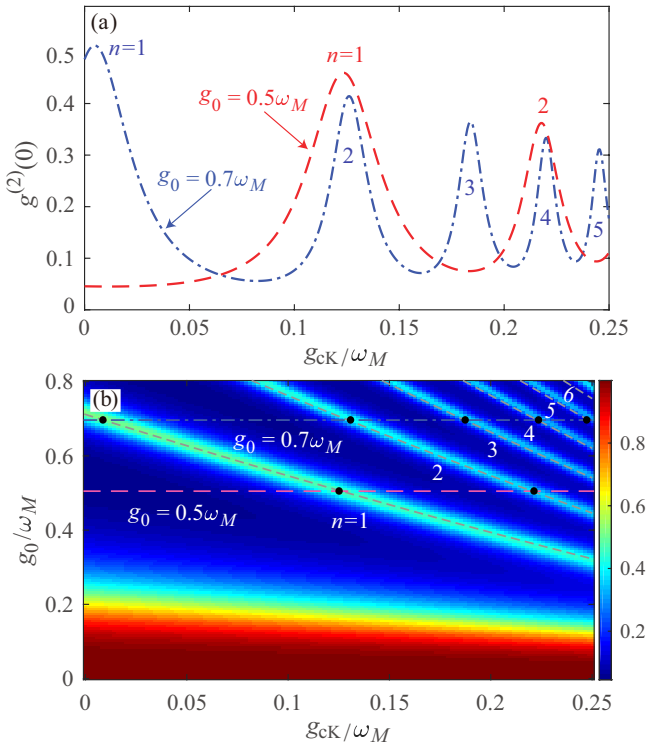


Figure 2: (Color online) (a) Plot of $g^{(2)}(0)$ as a function of $g_{\rm cK}/\omega_M$ under $g_0/\omega_M = 0.5, 0.7$ and the single-photon resonance $\Delta_c = \delta^{[1]}$. (b) Plot of $g^{(2)}(0)$ as a function of $g_{\rm cK}/\omega_M$ and g_0/ω_M at $\Delta_c = \delta^{[1]}$. Other parameters are $\kappa/\omega_M = 0.1$, $\gamma_M/\omega_M = 0.001$, $\Omega/\kappa = 0.01$, and $\bar{n}_M = 0$.

The eigensystem of the Hamiltonian $\hat{H}_{\rm gom}$ can be obtained as

$$\hat{H}_{\rm gom}|m\rangle_a|\tilde{n}(m)\rangle_b = E_{m,n}|m\rangle_a|\tilde{n}(m)\rangle_b, \tag{9}$$

where we introduce the m-photon displaced number states of the mechanical mode as

$$|\tilde{n}(m)\rangle_b \equiv \exp[\xi^{[m]}(\hat{b}^\dagger - \hat{b})]|n\rangle_b. \tag{10}$$

For studying few-photon optomechanical effects, we show the eigenenergy levels of $\hat{H}_{\rm gom}$ in the subspace associated with zero, one, and two photons in Fig. 1(b). Physically, the induced optical nonlinearity depicted by $\delta^{[m]}$ [cf. $\delta^{[1]}$ and $\delta^{[2]}$ in Fig. 1(b)] is the origin of the photon blockade effect in this generalized optomechanical model. In addition, the photon-number-dependent displacement $\xi^{[m]}$ in this model is not a linear function of the photon number m. This nonlinear conditional photon displacement can be used to create quantum superposition states of the mechanical mode.

2 Photon blockade effect

To show the photon blockade effect, we introduce a monochromatic driving field to the cavity. The driving Hamiltonian is given by

$$\hat{H}_d = \Omega(\hat{a}^\dagger e^{i\omega_d t} + \hat{a}e^{-i\omega_d t}), \tag{11}$$

where Ω and ω_d are the driving strength and driving frequency, respectively. For below convenience, we work in a frame rotating at the driving frequency ω_d, then the Hamiltonian of the total system becomes

$$\hat{H}^{(I)}_{\rm sys} = \hat{H}^{(I)}_{\rm gom} + \Omega(\hat{a}^\dagger + \hat{a}), \tag{12}$$

with

$$\hat{H}^{(I)}_{\rm gom} = \Delta_c\hat{a}^\dagger\hat{a} + \omega_M\hat{b}^\dagger\hat{b} - g_0\hat{a}^\dagger\hat{a}(\hat{b}^\dagger + \hat{b}) - g_{\rm cK}\hat{a}^\dagger\hat{a}\hat{b}^\dagger\hat{b}, \tag{13}$$

where $\Delta_c = \omega_c - \omega_d$ is the detuning of the cavity frequency with respect to the driving frequency.

To include the dissipations of the cavity field and the mechanical resonator, we study the photon blockade effect in the open-system case by using the method of quantum master equation. The quantum master equation in the rotating frame is written as

$$\begin{aligned}\frac{d\hat{\rho}(t)}{dt} &= -i[\hat{H}^{(I)}_{\rm sys}, \hat{\rho}(t)] + \kappa\mathcal{D}[\hat{a}]\hat{\rho}(t) + \gamma_M(\bar{n}_M + 1)\mathcal{D}[\hat{b}]\hat{\rho}(t) \\ &\quad + \gamma_M\bar{n}_M\mathcal{D}[\hat{b}^\dagger]\hat{\rho}(t),\end{aligned} \tag{14}$$

where we assume that the cavity field is connected with a vacuum bath, while the mechanical resonator is a heat bath at temperature T. κ and γ_M are, respectively, the decay rates of the cavity field and the mechanical oscillator. The $\bar{n}_M = (e^{\hbar\omega_M/(k_BT)} - 1)^{-1}$ is the average thermal phonon number associated with the mechanical dissipation, with k_B being the Boltzmann constant. The Lindblad superoperators used in Eq. (14) are defined by

$$\mathcal{D}[\hat{o}]\hat{\rho}(t) = \frac{1}{2}[2\hat{o}\hat{\rho}(t)\hat{o}^\dagger - \hat{o}^\dagger\hat{o}\hat{\rho}(t) - \hat{\rho}(t)\hat{o}^\dagger\hat{o}] \tag{15}$$

with $\hat{o} = \hat{a}$, $\hat{b}$, and $\hat{b}^\dagger$.

By numerically solving Eq. (14), we can get the steady-state density operator $\hat{\rho}_{\rm ss}$ of the system, and then the photon-number probabilities $P_{m=0,1,2} = {\rm Tr}[\sum_{n=0}^{\infty}|m\rangle_a|n\rangle_b\ {}_a\langle m|{}_b\langle n|\hat{\rho}_{\rm ss}]$ can be calculated numerically. The second-order correlation function $g^{(2)}(0)$ can also be obtained by $g^{(2)}(0) = {\rm Tr}(\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a}\hat{\rho}_{\rm ss})/[{\rm Tr}(\hat{a}^\dagger\hat{a}\hat{\rho}_{\rm ss})]^2$.

In Fig. 2(a) we plot the correlation function $g^{(2)}(0)$ at the steady state as a function of $g_{\rm cK}/\omega_M$, under given values of g_0/ω_M and $\Delta_c = \delta^{[1]}$. Here we can see that the correlation function exhibits an oscillating pattern with several resonance peaks located at specific values of $g_{\rm cK}/\omega_M$. Moreover, we can see that the value of $g^{(2)}(0)$ of the generalized optomechanical system is greater (less) than those of the typical optomechanicl system when $g_0/\omega_M = 0.5$ (0.7). It indicates that the cross-Kerr interaction could either enhance or suppress the photon blockade effect. A more comprehensive analysis of these phenomena is shown in Fig. 2(b), in which we plot the correlation function as a function of g_0/ω_M and $g_{\rm cK}/\omega_M$ under the single-photon resonant transition $|0\rangle_a|0\rangle_b \to |1\rangle_a|\tilde{0}(1)\rangle_b$. We can see that the value of $g^{(2)}(0)$ is approximately equal to 1 when $g_0/\omega_M < 0.1$, which indicates that the photon blockade effect can not be observed. For a given value of g_0/ω_M, the correlation function $g^{(2)}(0)$ experiences some oscillations with the increasing of the ratio $g_{\rm cK}/\omega_M$.

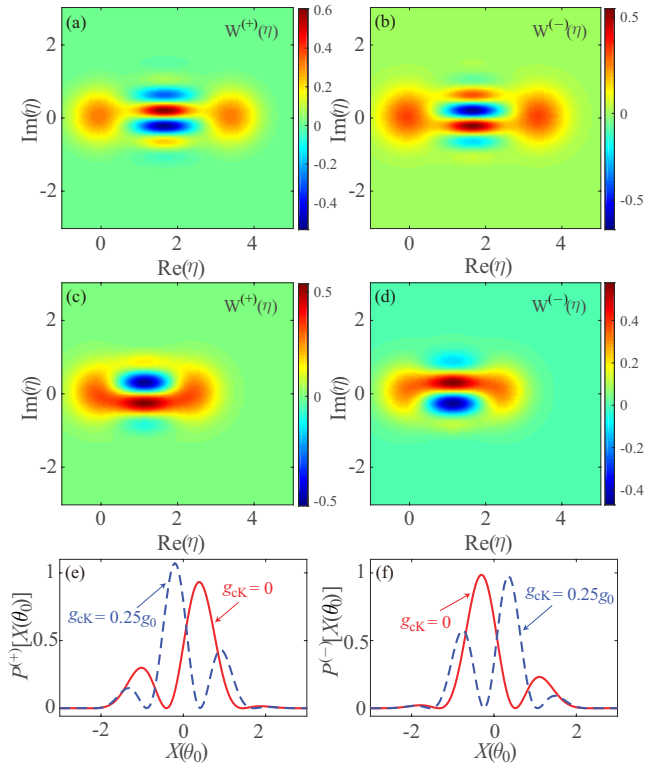


Figure 3: (Color online) The Wigner functions $W^{(\pm)}(\eta)$ for the mechanical oscillator states $|\Phi^{(\pm)}(t_s)\rangle_b$: (a),(b) $g_{\rm cK}/g_0 = 0.25$ and (c),(d) $g_{\rm cK}/g_0 = 0$. (e),(f) The probability distributions $P^{(\pm)}[X(\theta_0)]$ for the states $|\Phi^{(\pm)}(t_s)\rangle_b$ as a function of $X(\theta_0)$ at different value of $g_{\rm cK}/g_0$. Other parameters are $\omega_c/\omega_M = 1000$, and $g_0/\omega_M = 1.2$.

3 Generation of the Schrödinger Cat states

To generate the mechanical cat states, we consider an initial state $|\psi(0)\rangle = (|0\rangle_a + |1\rangle_a)|0\rangle_b/\sqrt{2}$ of the system, where $|m\rangle_a (m = 0, 1)$ denotes the Fock state of the cavity field and $|0\rangle_b$ is the ground state of the mechanical resonator. By utilizing the unitary evolution operator $\hat{U}(t)$, the state of the system at time t can be obtained as

$$\begin{aligned} |\psi(t)\rangle &= \hat{U}(t)|\psi(0)\rangle \\ &= \frac{1}{\sqrt{2}}[|0\rangle_a|0\rangle_b + e^{i\vartheta(t)}|1\rangle_a|\beta(t)\rangle_b], \end{aligned} \quad (16)$$

By expanding the cavity-mode state with basis states $|\pm\rangle_a = (|0\rangle_a \pm |1\rangle_a)/\sqrt{2}$, Eq. (16) becomes

$$|\psi(t)\rangle = \frac{1}{2}\left[\frac{1}{\mathcal{N}_+(t)}|+\rangle_a|\Phi^{(+)}(t)\rangle_b + \frac{1}{\mathcal{N}_-(t)}|-\rangle_a|\Phi^{(-)}(t)\rangle_b\right],$$

where we introduce the mechanical cat states

$$|\Phi^{(\pm)}(t)\rangle_b = \mathcal{N}_\pm(t)[|0\rangle_b \pm e^{i\vartheta(t)}|\beta(t)\rangle_b], \quad (17)$$

which are quantum superposition of the ground state $|0\rangle_b$ and the coherent state $|\beta(t)\rangle_b$. The normalization constants $\mathcal{N}_\pm(t)$ are given by

$$\mathcal{N}_\pm(t) = \left[2\left(1 \pm \cos[\vartheta(t)]e^{-\frac{|\beta(t)|^2}{2}}\right)\right]^{-1/2}. \quad (18)$$

For the mechanical mode in the density matrix $\hat{\rho}_b$, the Wigner function is defined by

$$W(\eta) = \frac{2}{\pi}\mathrm{Tr}[\hat{\rho}_b\hat{D}(\eta)e^{i\pi\hat{b}^\dagger\hat{b}}\hat{D}^\dagger(\eta)], \quad (19)$$

where $\hat{D}(\eta) = \exp(\eta\hat{b}^\dagger - \eta^*\hat{b})$ is a displacement operator.

For the rotated quadrature operator

$$\hat{X}(\theta) = \frac{1}{\sqrt{2}}(\hat{b}e^{-i\theta} + \hat{b}^\dagger e^{i\theta}), \quad (20)$$

its eigenstate is denoted by $|X(\theta)\rangle_b$: $\hat{X}(\theta)|X(\theta)\rangle_b = X(\theta)|X(\theta)\rangle_b$. For the states $|\Phi^{(\pm)}(t)\rangle_b$, we can obtain the probability distributions of the rotated quadrature operator $\hat{X}(\theta)$ as

$$P^{(\pm)}[X(\theta)] = \left|{}_b\langle X(\theta)|\Phi^{(\pm)}(t)\rangle_b\right|^2. \quad (21)$$

In Figs. 3(a) and 3(b), we plot the Wigner functions $W^{(\pm)}(\eta)$ for the mechanical cat states $|\Phi^{(\pm)}(t_s)\rangle_b$ with $t_s = \pi/(\omega_M - g_{\rm cK})$ being the detection time. Here we can see that the positions of the two main peaks in the Wigner functions are located at the origin and the point corresponding to $\beta(t_s)$ in the phase space. Moreover, we see clear interference pattern (in the region between the two peaks) in the Wigner functions. More importantly, the two main peaks in the Wigner functions of the states $|\Phi^{(\pm)}(t_s)\rangle_b$ can be distinguished in the phase space. In addition, in Figs. 3(c) and 3(d) we show the Wigner functions of the two states in the absence of the cross-Kerr interaction. By comparing the Wigner functions in the two cases: $g_{\rm cK}/g_0 = 0.25$ and 0, we can see that the distance between the two peaks is enhanced and that the interference fringes become more clear in the presence of the cross-Kerr interaction. This implies that the cross-Kerr interaction is helpful to the generation of macroscopic mechanical cat state. This enhancement can also be seen from the probability distributions $P^{(\pm)}[X(\theta_0)]$ for the states $|\Phi^{(\pm)}(t_s)\rangle_b$, as shown in Figs. 3(e) and 3(f). Here, the angle of rotation $\theta_0 = \arg[\beta(t_s)] - \pi/2$ is chosen such that the quadrature direction is perpendicular to the link line between the two main peaks. It can be seen that a stronger oscillation exists in the probability distributions corresponding to the generated cat states in the presence of the cross-Kerr interaction.

References

[1] T. T. Heikkilä, F. Massel, J. Tuorila, R. Khan, and M. A. Sillanpää. Enhancing Optomechanical Coupling via the Josephson Effect. Phys. Rev. Lett. **112**, 203603 (2014).

[2] F. Zou, L.-B. Fan, J.-F. Huang, J.-Q. Liao. Enhancement of few-photon optomechanical effects with cross-Kerr nonlinearity. Phys. Rev. A **99**, 043837 (2019).

Quantum random walk on a one-dimensional lattice with two entangled particles

Ibrahim Yahaya Muhammad[+,1], Sikarin Yoo-kong[+,~,2] and Tanapat Deesuwan[+,~,3]

[+]Theoretical and Computational Physics (TCP) Group, Department of Physics, Faculty of Science, King Mongkut's University of Technology Thonburi, 10140, Thailand
[~]Theoretical and Computational Science Center (TaCS), Faculty of Science, King Mongkut's University of Technology Thonburi, 10140, Thailand

Abstract

We study the evolution of a two-particle system on a one-dimensional lattice, subjected to quantum random walk. The quantum random walk of these two particles may contain spatial entanglement, thus offering a resources for quantum information and quantum communication purposes. The degree of spatial entanglement depends on the initial states of both particles and coins. Then we set out to investigate the behavior of the entanglement through the discrete evolution in various scenarios of the initial condition. The result of the study shows that most of the cases the spatial entanglement exhibits damped oscillating behavior throughout the walk causing from the configuration of the particle's state and size of the lattice at n^{th} step. In the asymptotic limit, the degree of the spatial entanglement will approach to a certain value as a result of vanishing battle between loss and gain of the entanglement in the walking process.

Keywords: quantum random walk, spatial entanglement, quantum information and communication

Measurement-device-independent quantification of irreducible entanglement

Yu Guo,[1,2,*] Bai-Chu Yu,[1,2,*] Xiao-Min Hu,[1,2] Bi-Heng Liu,[1,2,†] Yu-Chun Wu,[1,2,‡] Yun-Feng Huang,[1,2] Chuan-Feng Li,[1,2,§] and Guang-Can Guo[1,2]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, People's Republic of China*
[2]*CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

(Dated: July 6, 2019)

One of the core problems of quantum theory lies in the certification and quantification of quantum entanglement, which is the key resource in various quantum information processes. An important physical property in the entanglement certification is the dimension of quantum states, which places an upper bound for the entanglement of a system.

However, studying only on the relation between the dimension of quantum states and the entanglement seems not enough, since the practical application of entanglement is also relevant to the quantum operations that we can perform on these states. If the local quantum operations are limited, we can not make full use of the existing entanglement of the quantum state. Recently it is pointed out in Ref. [1] that a two-ququart maximally entangled state (MES), can actually be written as two two-qubit MES, however, if general joint local operations can not be performed between the two two-qubit states, the entanglement the two-ququart MES can not be thoroughly displayed by these two two-qubit MES. Therefore the authors propose the notion of irreducible dimension. Instead of considering only the dimension of a quantum state, they consider the dimension of a quantum system, which includes two elements, quantum states and a set of quantum operations. A system has reducible dimension if both the quantum states and quantum operations are separable into those of lower-dimensional subsystems, otherwise it has irreducible dimension. We can see that a system with entanglement of irreducible dimension, which we will call irreducible entanglement in short, can make better use of the entanglement than those with reducible one of the same dimension, so it is important to distinguish irreducible entanglement in the certification process.

The most important part of distinguishing irreducible entanglement lies in certifying the irreducibility of the quantum operations, which is directly relevant to the capability of using the existing entanglement. This is not a trivial task in practical entanglement certification scenario, where we usually do not have the information of the systems—we have to treat the measurement apparatus as black boxes, and certify the entanglement only with the measurement statistics it produce. In Ref. [1], the authors show that some device-independent (DI) entanglement witness can not distinguish irreducible entanglement, since it is incapable to detect whether the quantum operations are reducible. A solution for the two-ququart systems is proposed by having additional tests to check the quantum operations, but it is not a general one, and its robustness requires assumptions of constraining the classical communication between the local subsystems and the two distant parties.

In this article we try to give a more general solution to the problem, we show that a recently proposed protocol called quantitative measurement device independent entanglement witness ($\mathcal{Q}$MDIEW) in Ref. [2], developed from measurement device independent (MDI) quantum test and semiquantum scenarios, can naturally distinguish the irreducibility of the quantum operations, thus witnesses irreducible entanglement. We prove that in a $\mathcal{Q}$MDIEW, the quantified entanglement exceeds the upper bound of m-dimensional systems only if the shared system is entangled in irreducible dimension at least $m+1$, and the result is robust against the most general classical communication scheme. We then experimentally demonstrate the protocol on a two-qutrit system and observe a lower bound of its generalized robustness (GR) that exceeds the value of arbitrary 2-dimensional systems.

* These authors contributed equally to this work.
† bhliu@ustc.edu.cn.
‡ wuyuchun@ustc.edu.cn.
§ cfli@ustc.edu.cn.

[1] W. Cong, Y. Cai, J. -D. Bancal, and V. Scarani, Phys. Rev. Lett. **119**, 080401 (2017).
[2] D. Rosset, A. Martin, E. Verbanis, C. C. W. Lim, and R. T. Thew, Phys. Rev. A, **98**, 052332 (2018).

Continuous hidden shift problem on $\mathbb{R}^n$

Eunok Bae[1] * Soojoon Lee[1] †

[1] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 02447, Korea*

Abstract. There have been several research works on the hidden shift problem, quantum algorithms for the problem, and their applications. However, all the results have focused on discrete groups. So, we define a continuous hidden shift problem on $\mathbb{R}^n$ as an extension of the hidden shift problem, and construct a quantum computing algorithm for solving this problem efficiently.

Keywords: quantum algorithm, hidden shift problem, continuous hidden shift problem

1 Introduction

Quantum computers can solve certain problems exponentially faster than classical computers by taking advantage of the quantum mechanical properties such as quantum interference and superposition. Many researchers have been studying algebraic problems which can be solved efficiently on a quantum computer, for instance, hidden subgroup problem [1, 2, 3, 8, 9, 10, 11, 17], hidden shift problem [6, 7, 13, 16], hidden polynomial problem [14, 15, 20], and hidden symmetry subgroup problem [18, 19].

In particular, the hidden shift problem has provided a frame work to solve various problems such as the shift Legendre symbol problem [7], Gauss sum estimation [4], and the stabilizer problem [6]. It has been shown that several interesting and important problems have been related to the hidden shift problem. For example, it was proved that the hidden shift problem for the abelian group $\mathbb{Z}_N$ can be used to solve some lattice problem over $\mathbb{Z}_N$ [3, 5], and it was also discovered that an efficient algorithm of the hidden shift problem for the symmetric group S_n would yield an efficient algorithm for the graph isomorphic problem [14].

The hidden shift problem can be cast in the following terms: Let f_0 and f_1 be two injective functions from a finite group G to a finite set satisfying that there exits an element u in G such that the equality $f_0(x) = f_1(xu)$ holds for all x in G. The task is to find the *hidden shift* u.

Although there is no general algorithm to solve the hidden shift problem even for abelian groups, it has been known that there are efficient algorithms to solve the problem for some groups. Friedl *et. al* [6] found an efficient quantum algorithm for the hidden shift problem over $\mathbb{Z}_p^n$ for any fixed prime number p, and a similar work for the problem over the group $\mathbb{Z}_{p^k}^n$ has been done by Ivanyos [16], where p^k is any fixed prime power. However, when m is not a prime power, the hidden shift problem for the group $\mathbb{Z}_m^n$ still remains unsolved.

All known results on the hidden shift problem have been concerned with only discrete groups. Thus, it is natural to ask whether there exits an efficient quantum algorithm for solving a continuous hidden shift problem, which is the hidden shift problem on a continuous group. Considering a continuous version of a certain problem can be helpful to solve unsolved problems as in the results of Eisenträger *et. al* [21]. They found an efficient quantum algorithm for solving a continuous hidden subgroup problem to compute the unit group of an arbitrary degree number field. It was also shown that the algorithm can pose a threat to certain lattice-based cryptosystems.

In this paper, we consider a hidden shift problem for a continuous group, and answer the question.

2 Hidden shift problem on a continuous group

To deal with the hidden shift problem on a continuous group, we need a suitable definition. The following definition can be considered as a continuous version of the original problem.

Definition 1 (Continuous hidden shift problem) *Let S be the set of unit vectors in some Hilbert space. For two injective functions $f_0, f_1 : \mathbb{R}^n \times \mathbb{Z}_2 \to S$, let $f : \mathbb{R}^n \times \mathbb{Z}_2 \to S$ be defined by $f_a(x) = f(x, a)$, with the following promises:*

1. $f(x, 0) = f(x + u, 1)$
for all $x \in \mathbb{R}^n$ and for some $u \in \mathbb{R}^n$;

2. $\| |f(x, a)\rangle - |f(y, b)\rangle \| \leq \alpha \cdot dist(x - au, y - bu)$
for all $x, y \in \mathbb{R}^n$ and $a, b \in \mathbb{Z}_2$, where $|f(\cdot, \cdot)\rangle$ is a pure state corresponding to $f(\cdot, \cdot)$.

The goal of the problem is to find u, which is called the hidden shift.

Note that the given oracle function f is efficiently computable, and the positive constant α in condition 2 is called a *Lipschitz constant* of the function f.

As in Ref. [20], let us first define a window function $\omega : \mathbb{R} \to \mathbb{C}$ as

$$\omega(x) = \begin{cases} \sqrt{2}\sin(\pi x) & \text{if } x \in [0, 1], \\ 0 & \text{otherwise.} \end{cases}$$

Then ω is a Lipschitz function with unit L^2-norm supported on $[0, 1]$. For a sufficiently large number Δ and a sufficiently small number $\delta = \Delta^{-1}$, let us define

$$w(x_1, \ldots, x_n) = \frac{1}{\Delta^{n/2}} \prod_{j=1}^{n} \omega\left(\frac{x_j}{\Delta}\right)$$

*eobae@khu.ac.kr
†level@khu.ac.kr

for $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. For convenience, we assume that $\Delta = \sqrt{2^q}$ for sufficiently large q with $u_i^2 \leq \Delta$ for all i.

Now, we are ready to construct our algorithm for solving the hidden shift problem with the above materials as follows.

Theorem 2 (Quantum algorithm for solving the hidden shift problem on $\mathbb{R}^n$)
Input: The oracle function $f : \mathbb{R}^n \times \mathbb{Z}_2 \to S$ that hides the shift $u \in \mathbb{R}^n$.

0. If $f(0,0) = f(0,1)$, then output 0.
1. Create the initial state

$$\sqrt{\delta^n/2} \sum_{\tilde{x} \in \mathbb{Z}^n} \sum_{c \in \mathbb{Z}_2} w(x) \left|\tilde{x}\right\rangle \left|c\right\rangle$$

with $x = \delta\tilde{x}$.
2. Apply the oracle function f.
3. Perform the $QFT_{\mathbb{Z}^n \times \mathbb{Z}_2}$, which can be implemented by the phase estimation technique as in Ref. [21], and measure on the first two registers.
4. Consider the samples $(\tilde{y}, 1)$.
5. Use the values of $\tilde{y}$ non-orthogonal to $\tilde{u}$ among the samples $(\tilde{y}, 1)$ to find $\tilde{u}$.
6. Compute $u = \delta\tilde{u}$.

Output: u

Remark 1 *Since it is difficult to compute continuous variables, we need to truncate and discretize the continuous domain $\mathbb{R}^n$ of the oracle functions by using the window function w and the small number δ. As in Ref. [21], we use the following variables in our calculations;*
Real Domain: $x = \delta\tilde{x} \in \delta\mathbb{Z}^n$
Fourier Domain: $y = \delta^{-1}\tilde{y} \in \mathbb{R}^n/\delta^{-1}\mathbb{Z}^n$

- *In Step 2, the state becomes*

$$\left|\psi_\delta\right\rangle = \sqrt{\frac{\delta^n}{2}} \sum_{\tilde{x} \in \mathbb{Z}^n} \sum_{c \in \mathbb{Z}_2} w(x) \left|\tilde{x}\right\rangle \left|c\right\rangle \left|f(x,c)\right\rangle.$$

- *In Step 3, $QFT_{\mathbb{Z}^n \times \mathbb{Z}_2}$ means the quantum Fourier transform performing over the group $\mathbb{Z}^n \times \mathbb{Z}_2$. As in the original hidden shift problem, it is necessary to perform the Fourier transform and measure in the standard basis for the continuous hidden shift problem as well. However, the Fourier transform over any infinite group cannot be implemented by a quantum computer. So, we can perform the approximate quantum Fourier transform on the infinite group by means of a variation of the phase estimation algorithm on the register on the group and ancillary register, which was used in Ref. [21].*

- *In Step 5, we reduce the hidden shift problem to the random-linear-disequations problem to find the hidden shift u as in the method of Ref. [16].*

3 Analysis of our algorithm

In this section, we analyze our quantum algorithm presented in the above section. As in the way of Ref. [21], instead of directly measuring in the Fourier basis of the continuous group directly, we use the phase estimation to approximate the probability distribution $p_\delta(y,1)$ of the variable $\delta^{-1}\tilde{y}$ by the distribution of $p(y,1)$, when δ is close to 0. We can derive these two distributions from the following quantum states:

$$\left|\psi_\delta\right\rangle = \sqrt{\delta^n/2} \sum_{\tilde{x} \in \mathbb{Z}^n} \sum_{c \in \mathbb{Z}_2} \left|\tilde{x}\right\rangle \left|c\right\rangle \left|\psi(x,c)\right\rangle,$$

$$\left|\psi\right\rangle = \frac{1}{\sqrt{2}} \int_{\mathbb{R}^n} \sum_{c \in \mathbb{Z}_2} \left|x\right\rangle \left|c\right\rangle \left|\psi(x,c)\right\rangle dx,$$

where $\left|\psi(x,c)\right\rangle = w(x)\left|f(x,c)\right\rangle$. Precisely, p_δ and p are from the Fourier transform of ψ_δ and ψ, respectively:

$$p_\delta(y,1) = <\hat{\psi}_\delta(y,1)|\hat{\psi}_\delta(y,1)>,$$

$$p(y,1) = <\hat{\psi}(y,1)|\hat{\psi}(y,1)>$$

with $\hat{\psi}_\delta = F_{\delta\mathbb{Z}^n}\psi_\delta$ and $\hat{\psi} = F_{\mathbb{R}^n}\psi$. We can show that p_δ goes to p as δ is close to 0.

So, it is enough to focus on the distribution $p(y,1)$ which can be calculated precisely;

$$p(y,1) = \frac{1}{2} - \frac{1}{2}\cos(2\pi\left\langle u, y\right\rangle) \prod_{i=1}^{n} \cos\left(\frac{\pi u_i}{\Delta}\right).$$

Although the probability that a sample y is orthogonal to u is not zero, which is different from the original hidden shift problem, it can be shown that the probability is (exponentially) small when n is large enough by the following Propositions and Lemma. In other words, the samples $(y,1)$ after the Fourier sampling subroutine are mostly non-orthogonal to u.

In order to show that the probability that a sample y is orthogonal to u is small enough when n is sufficiently large, we consider the case when the number of y satisfying the equation $\langle u, y\rangle = 0$ attains a maximum value. Note that we actually get the samples $\tilde{y}$ instead of y to return $\tilde{u}$ first and recover u from $\tilde{u}$ in the practical implementation of our algorithm.

Lemma 3 *For any $n, k \in \mathbb{N}$, let $q = 4k$, $\Delta = 2^{q/2}$ and $\tilde{u} \in \mathbb{Z}_{2^q}^n$. The number of $\tilde{y} \in \mathbb{Z}_{2^q}^n$ which is orthogonal to $\tilde{u}$ has the maximum value, $2^{k(4n-3)}$, when $\tilde{u} = (\tilde{u}_1, \ldots, \tilde{u}_n) = (\sqrt{\Delta}, \ldots, \sqrt{\Delta})$. Moreover, the probability that $\tilde{y} \in \mathbb{Z}_{2^q}^n$ is orthogonal to $\tilde{u}$ is at most $1/2^{3k}$ in our algorithm.*

Theorem 4 *There is a quantum algorithm for solving the continuous hidden shift problem on $\mathbb{R}^n$ in polynomial time in n.*

4 Discussion

It has been known that the hidden shift problem over discrete groups can affect cryptosystems [23, 24]. In particular, Bonnetain and Naya-Plasencia [24] recently constructed an efficient quantum algorithm to solve the hidden shift problem over the abelian group $\mathbb{Z}_{2^p}^w$, and proved

that the algorithm can be used to establish a quantum attack in a cryptosystem claimed to be secure quantumly.

In this work, we have defined a continuous hidden shift problem over the group $\mathbb{R}^n$, and have shown that a quantum computer can efficiently solve the problem. Thus it is natural to consider whether the continuous version of this problem can also have any crypto-related applications. In fact, a similar consideration has been involved in the previous results. In Refs. [21, 22], it has been shown that a continuous hidden subgroup problem induces a quantum attack on cryptosystems based on the hardness of finding a short generator of a principal ideal, although the discrete hidden subgroup problem cannot break them [10, 12]. Inspired by these results, we expect that our result could have an application related to cryptography.

References

[1] S. Hallgren. On the power of quantum computation. *SIAM J. on Comp.*, 26(5) pages 1474–1483, 1997.

[2] S. Hallgren. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Comp.*, 26(5) pages 1484–1509, 1997.

[3] M. Ettinger and P. Hyer On quantum algorithms for noncommutative hidden subgroups. *Adv. in Appl. Math.*, 25(3) pages 239–251, 2005.

[4] W. van Dam and G. Seroussi. Efficient quantum algorithms for estimating Gauss sums. quant-ph/0207131, 2005.

[5] O. Regev. Quantum computation and lattice problems. *SIAM J. on Comp.*, 33(3) pages 738–760, 2002.

[6] K. Friedl, G. Ivanyos, F. Magniez, M. Santha and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proc. of the 35th ACM STOC*, pages 1–9, 2003.

[7] W. van Dam, S. Hallgren and L. Ip. Quantum algorithms for some hidden shift problems. *SIAM J. on Comp.*, 36(3) pages 763–778, 2006.

[8] M. Ettinger, P. Hyer and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1) pages 43–48, 2004.

[9] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden sub- group problem. *SIAM J. on Comp.*, 35(1) pages 170–188, 2005.

[10] S. Hallgren. Fast quantum algorithm for computing the unit group and class group of a number field. In *Proc. of the 37th ACM STOC*, pages 468–474, 2005.

[11] A. Schmidt and U. Vollmer. Polynomial time quantum algorithm for the computation of the unit group of a number field. In *Proc. of the 37th ACM STOC*, pages 475–480, 2005.

[12] S. Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. In *Proc. of the 37th ACM STOC*, pages 468–474, 2005.

[13] A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. In *Proc. of the 18th SODA*, pages 1225–1232, 2007.

[14] A. M. Childs and P. Wocjan On the quantum hardness of solving isomorphism problems as nonabelian hidden shift problems. *Quantum Information & Computation*, 7(5&6) pages 504–521, 2007.

[15] T.Decker, J. Draisma and P. Wocjan. Efficient quantum algorithm for identifying hidden polynomials. *Quantum Information & Computation*, 9(3) pages 215–230, 2009.

[16] G. Ivanyos. On solving systems of random linear disequations. *Quantum Information & Computation*, 8(6-7):579–594, 2008.

[17] G. Kuperberg. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In *the 8th Conference on the TQC*, 22 pages 20–34, 2013.

[18] S. Hallgren. On the power of quantum computation. In *Proc. of the 37th ACM STOC*, pages 468–474, 2005.

[19] T. Decker, G. Ivanyos, M. Santha and P. Wocjan. Hidden Symmetry Subgroup Problems. *SIAM J. on Comp.*, 42(5) pages 1987–2007, 2013.

[20] T. Decker, P. Hyer, G. Ivanyos and M. Santha. Polynomial time quantum algorithms for certain bivariate hidden polynomial problems. *Quantum Information & Computation*, 14(9&10) pages 790–806, 2014.

[21] K. Eisenträger, S. Hallgrenand, A. Kitaev and F Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Proc. of the 46th ACM STOC*, pages 293–302, 2014.

[22] J. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proc. of the 27th ACM-SIAM SODA*, pages 468–474, 2016.

[23] G. Alagic and A. Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In Advances in Cryptology, EUROCRYPT, pages 65–93, 2017.

[24] X.Bonnetain and M. Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. *Lecture Notes in Computer Science*, 11272 pages 560–592, 2018.

Observation of critical phenomena in parity-time-symmetric quantum dynamics

Lei Xiao[1 2] Kunkun Wang[1 2] Xiang Zhan[1 2] Zhihao Bian[1 2] Kohei Kawabata[3]
Masahito Ueda[3 4] Wei Yi[5 6] Peng Xue[1 2 7 *]

[1] *Beijing Computational Science Research Center, Beijing 100084, China*
[2] *Department of Physics, Southeast University, Nanjing 211189, China*
[3] *Department of Physics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*
[4] *RIKEN Center for Emergent Matter Science (CEMS), Wako, Saitama 351-0198, Japan*
[5] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[6] *CAS Center For Excellence in Quantum Information and Quantum Physics*
[7] *State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, China*

Abstract. We experimentally simulate non-unitary quantum dynamics using a single-photon interferometric network and study the information flow between a parity-time ($\mathcal{PT}$)-symmetric non-Hermitian system and its environment. We observe oscillations of quantum-state distinguishability and complete information retrieval in the $\mathcal{PT}$-symmetry-unbroken regime. We then characterize in detail critical phenomena of the information flow near the exceptional point separating the $\mathcal{PT}$-unbroken and -broken regimes, and demonstrate power-law behavior in key quantities such as the distinguishability and the recurrence time. We also reveal how the critical phenomena are affected by symmetry and initial conditions.

Keywords: critical phenomena, $\mathcal{PT}$-symmetry, non-unitary quantum dynamics

1 Introduction

Parity-time ($\mathcal{PT}$)-symmetric non-Hermitian systems feature unconventional properties in synthetic systems ranging from classical optical systems and microwave cavities to quantum gases and single photons. In these systems, the spectrum is entirely real in the $\mathcal{PT}$-symmetry-unbroken regime, in contrast to the regime with spontaneously broken $\mathcal{PT}$ symmetry. As a result, the dynamics is drastically different in the $\mathcal{PT}$-symmetry-unbroken and -broken regimes, and dynamical criticality occurs at the boundary between the two regimes. In previous experiments, such unconventional dynamical properties as well as signatures of the $\mathcal{PT}$-transition point, or the exceptional point, were observed in classical $\mathcal{PT}$-symmetric systems with balanced gain and loss. Whereas quantum systems with passive $\mathcal{PT}$ symmetry were realized recently, critical phenomena in $\mathcal{PT}$-symmetric quantum dynamics are yet to be experimentally explored. Understanding these critical phenomena in the quantum regime provides an important perspective for the study of open quantum systems and is useful for applications in quantum information.

A paradigmatic example of $\mathcal{PT}$-symmetric non-unitary dynamics in the context of open quantum systems is the reversible-irreversible criticality in the information flow between a system and its environment. Here, information lost to the environment can be fully retrieved when the system is in the $\mathcal{PT}$-symmetry-unbroken regime because of the existence of a finite-dimensional entanglement partner in the environment protected by $\mathcal{PT}$ symmetry. In contrast, the information flow is irreversible when the system spontaneously breaks $\mathcal{PT}$ symmetry. Close to the exceptional point, physical quantities such as distinguishability between time-evolved states and the recurrence time of the distinguishability exhibit power-law behavior.

In this work, we simulate $\mathcal{PT}$-symmetric non-unitary quantum dynamics using a single-photon interferometric network, and experimentally investigate the critical phenomena in the information flow close to the exceptional point. To extract critical phenomena from non-unitary dynamics, a faithful characterization of the long-time dynamics is necessary. This poses a serious experimental challenge, because maintaining and probing coherent dynamics in the long-time regime is difficult. We overcome this difficulty by directly implementing non-unitary time-evolution operators at any given time, and simulate the non-unitary quantum dynamics by performing non-unitary gate operations on the initial state. Since our experimental protocol is general enough to implement a broad class of non-unitary operators, we are able to examine in detail the role of symmetry and initial states on non-unitary quantum dynamics driven by a series of related non-Hermitian Hamiltonians.

2 Experimental setup

To simulate the dynamics of a two-level $\mathcal{PT}$-symmetric system, we encode basis states in the horizontal and vertical polarizations of a single photon, with $|H\rangle = (1,0)^{\mathrm{T}}$ and $|V\rangle = (0,1)^{\mathrm{T}}$. We generate heralded single photons via type-I spontaneous parametric downconversion, with one photon serving as a trigger and the other as a signal photon. The signal photon is then projected into the initial state $|H\rangle$ or $|V\rangle$ with a polarizing beam splitter (PBS) and a half-wave plate (HWP), and is sent to the interferometric network as illustrated in Fig. 1.

Experimentally, instead of implementing a non-

*gnep.eux@gmail.com

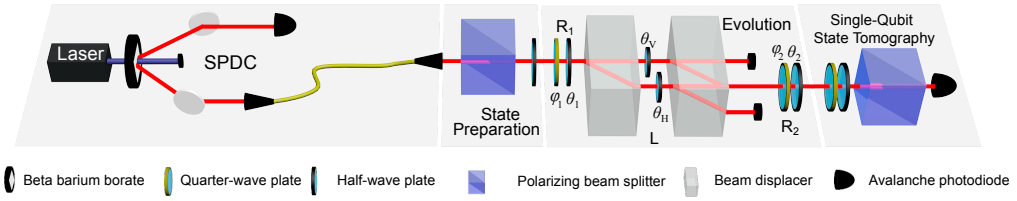


Figure 1: Experimental setup. A photon pair is created via spontaneous parametric downconversion (SPDC). One of the photons serves as a trigger, the other is projected into the polarization state $|H\rangle$ or $|V\rangle$ with a polarizing beam splitter (PBS) and a half-wave plat (HWP), and then goes through various optical elements.

Hermitian Hamiltonian, we directly realize the time-evolution operator U at any given time t and access time-evolved states by enforcing U on the initial state. As illustrated in Fig. 1, this is achieved by decomposing U according to

$$U = R_2(\theta_2, \varphi_2) L(\theta_H, \theta_V) R_1(\theta_1, \varphi_1), \tag{1}$$

where the rotation operator $R_j(\theta_j, \varphi_j)$ $(j = 1, 2)$ is realized using a quarter-wave plate (QWP) at φ_j and a HWP at θ_j, and the polarization-dependent loss operator L is realized by a combination of two beam displacers (BDs) and two HWPs with setting angles θ_H and θ_V.

Here, the setting angles $\{\theta_j, \varphi_j, \theta_H, \theta_V\}$ of wave plates are determined numerically for each given time t, such that $U = e^{-i\hat{H}_{\rm eff}t}$. In our experiment, the effective non-Hermitian Hamiltonian is given by

$$\hat{H}_{\rm eff} = \hat{\sigma}_x + ia(\hat{\sigma}_z - \hat{\mathbb{1}}), \tag{2}$$

where $\hat{\sigma}_{x(z)}$ are the standard Pauli operators, and $\hat{\mathbb{1}}$ is the identity operator. The non-Hermitian Hamiltonian $\hat{H}_{\rm eff}$ possesses passive $\mathcal{PT}$ symmetry, which can be easily mapped to a $\mathcal{PT}$-symmetric Hamiltonian $\hat{H}_{\mathcal{PT}}$ with balanced gain and loss, with $\hat{H}_{\mathcal{PT}} = \hat{H}_{\rm eff} + ia\hat{\mathbb{1}}$. Here, $a > 0$ controls non-Hermiticity, and the Hamiltonian becomes Hermitian for $a = 0$; the system is in the $\mathcal{PT}$-symmetry-unbroken (-broken) regime for $0 < a < 1$ $(a > 1)$, with the exceptional point located at $a = 1$.

The non-unitary dynamics of the system is captured by the time-dependent density matrix

$$\rho_{1,2}(t) = \frac{e^{-i\hat{H}_{\mathcal{PT}}t}\rho_{1,2}(0)e^{i\hat{H}^\dagger_{\mathcal{PT}}t}}{\mathrm{Tr}\left[e^{-i\hat{H}_{\mathcal{PT}}t}\rho_{1,2}(0)e^{i\hat{H}^\dagger_{\mathcal{PT}}t}\right]}, \tag{3}$$

with the initial density matrices $\rho_{1(2)}(0) = |H(V)\rangle\langle H(V)|$. Note that applying $H_{\rm eff}$ or $H_{\mathcal{PT}}$ in Eq. (3) would give the same time-dependent matrices. Experimentally, we construct the density matrix at any given time t via quantum-state tomography after signal photons passed through the interferometric setup. Essentially, we measure the probabilities of photons in the bases $\{|H\rangle, |V\rangle, |P_+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}, |P_-\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}\}$ through a combination of QWP, HWP, and PBS, and then perform a maximum-likelihood estimation of the density matrix. The outputs are recorded in coincidence with trigger photons. Typical measurements yield a maximum of 18,000 photon counts over 3 seconds.

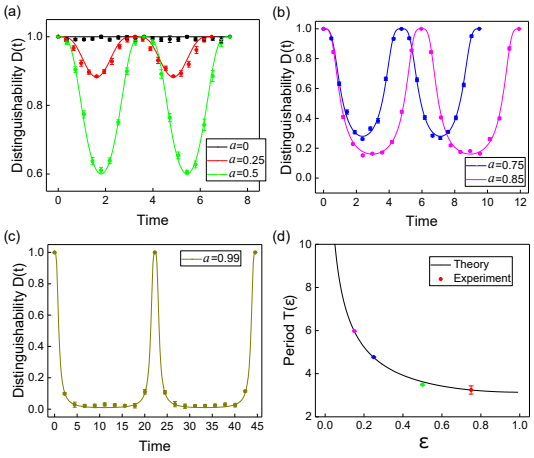


Figure 2: Information retrieval in the $\mathcal{PT}$-symmetry-unbroken regime. (a)-(c) Oscillations of the distinguishability $D(t)$ for $a < 1$, and between the two time-evolved states starting from $|H\rangle$ and $|V\rangle$. Dots with error bars represent the experimental results, while the curves show the theoretical predictions. (d) Recurrence time T of the distinguishability as a function of $\varepsilon = 1 - a$.

3 Measuring distinguishability

We characterize information flowing into and out of the system via the trace distance defined by

$$D\left[\rho_1(t), \rho_2(t)\right] = \frac{1}{2}\mathrm{Tr}\left|\rho_1(t) - \rho_2(t)\right|, \tag{4}$$

with $|A| = \sqrt{A^\dagger A}$. The trace distance D measures the distinguishability of the two quantum states characterized by $\rho_1(t)$ and $\rho_2(t)$. An increase in the distinguishability signifies information backflow from the environment, whereas a monotonic decrease means unidirectional information flow to the environment. In Fig. 2, we show the time evolution of the distinguishability when the system is in the $\mathcal{PT}$-symmetry-unbroken regime with $a < 1$. For comparison, we also show the case of a unitary evolution with $a = 0$. As illustrated in Figs. 2(a-c), $D(t)$ oscillates in time when $a < 1$, suggesting complete information retrieval with the initial trace distance fully restored periodically. The period of the oscillation T, or the recurrence time, increases as the system approaches the exceptional point. We extract the recurrence time by fitting the experimental data with a Fourier series. As shown in Fig. 2(d), the recurrence time agrees well with

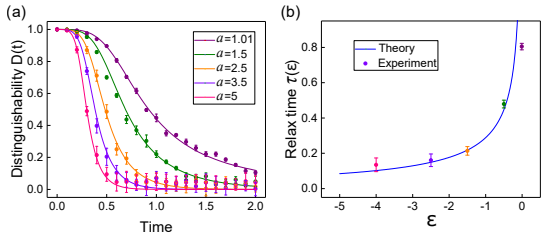


Figure 3: Unidirectional information flow to the environment in the $\mathcal{PT}$-symmetry-broken regime. (a) Decay of the distinguishability in the $\mathcal{PT}$-broken regime with different coefficients $a > 1$. (b) Relaxation time τ of the distinguishability as a function of $\varepsilon = 1 - a$. The blue solid curve shows the theoretical result $\tau = 1/2\sqrt{a^2 - 1}$. We readout the experimental results (dots with error bars) by fitting the experimental data to an exponential function.

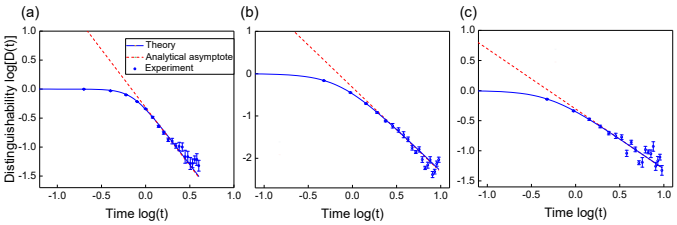


Figure 4: (a) Power-law behavior of the distinguishability $D(t) \sim t^{-2}$ of the $\mathcal{PT}$-symmetric system with initial states $\{|H\rangle, |V\rangle\}$. (b)(c) Power-law behavior of the distinguishability of the time-reversal symmetric system at the exceptional point $a = 1$ with initial states (b) $(|H\rangle \pm |V\rangle)/\sqrt{2}$ or (c) $\{|H\rangle, |V\rangle\}$. The power law behaviors $D(t) \sim t^{-2}$ in (b) and $D(t) \sim t^{-1}$ in (c) demonstrate the dependence of the critical phenomena on the initial state. In the long-time limit, the experimentally measured distinguishability agrees well with theoretical predictions. The blue solid curves show the theoretical prediction, and the red dashed lines indicate their asymptotes.

the analytic expression $T = \pi/\sqrt{1 - a^2}$. In the limit $\epsilon \to 0$ with $\epsilon = 1 - a$, the recurrence time should diverge as $T \sim \epsilon^{-1/2}$.

In Fig. 3(a), we show the time evolution of the distinguishability when the system is in the $\mathcal{PT}$-symmetry-broken regime with $a > 1$. Here, the distinguishability decays exponentially in time. Fitting the experimental data using $D(t) = D(0)e^{-t/\tau}$, where $D(0)$ is a constant and τ is the relaxation time, we find that the relaxation time increases as the system approaches the exceptional point. As shown in Fig. 3(b), the measured τ agrees excellently with the analytical result $\tau = 1/2\sqrt{a^2 - 1}$, which also diverges with a power-law scaling $\tau \sim |\epsilon|^{-1/2}$ as $\epsilon \to 0$.

Finally, at the exceptional point ($a = 1$), the distinguishability exhibits power-law behavior in the long-time limit. As illustrated in Fig. 4(a), the long-time behavior of the distinguishability agrees well with the theoretical prediction $D(t) \sim t^{-2}$. Importantly, the observed critical phenomena do not depend on the details of the system but the order of the exceptional point, which signifies their universality. We note that the measurement suffers from a relatively larger systematic error at long times due to the small $D(t)$.

4 Symmetry and initial states

Since our experimental protocol is quite general and capable of implementing a broad class of non-unitary operators, we are able to investigate the role of symmetry and initial states on the information flow and critical phenomena. In particular, we experimentally simulate non-unitary dynamics governed by i) $\hat{H}_{\mathcal{T}} = \sigma_x + ia\sigma_y$ and ii) $\hat{H} = \sigma_x + (c + ia)\sigma_z$. Whereas $\hat{H}_{\mathcal{T}}$ has time-reversal symmetry $\mathcal{T}\hat{H}_{\mathcal{T}}\mathcal{T}^{-1} = \hat{H}_{\mathcal{T}}$ with complex conjugation $\mathcal{T}$, $\hat{H}$ has no relevant symmetries for $a \neq 0$ and $c \neq 0$.

We first study dynamics under $\hat{H}_{\mathcal{T}}$ with different parameters and initial states $(|H\rangle \pm |V\rangle)/\sqrt{2}$. Since eigenenergies of $\hat{H}_{\mathcal{T}}$ are given as $\pm\sqrt{1 - a^2}$, the exceptional point is located at $a = 1$. As shown in Fig. 4(b), the same critical phenomena emerge under time-reversal symmetry: information is retrieved only in the symmetry-unbroken regime ($0 < a < 1$), and critical scaling is still $D(t) \sim t^{-2}$. However, when we choose the initial states $\{|H\rangle, |V\rangle\}$, the critical scaling at the exceptional point is now $D(t) \sim t^{-1}$, as illustrated in Fig. 4(c). This new universality arises because $|H\rangle$ is one of the eigenstates of $\hat{H}_{\mathcal{T}}$. We note that the same scaling relation can be realized under $\hat{H}_{\mathcal{PT}}$ with the initial states $(|H\rangle \pm i|V\rangle)/\sqrt{2}$ as $(|H\rangle - i|V\rangle)/\sqrt{2}$ is one of the eigenstates of $\hat{H}_{\mathcal{PT}}$. For the dynamics governed by $\hat{H}$, however, the lack of symmetry therein prevents the information retrieval and the distinguishability decays in time just as in the symmetry-broken cases.

5 Conclusion

We have experimentally simulated $\mathcal{PT}$-symmetric quantum dynamics using single-photon interferometric networks. Enforcing non-unitary gate operations on photons and performing quantum-state tomography, we have reconstructed a time-dependent density matrix of the $\mathcal{PT}$ dynamics at arbitrary times.Our work is the first experimental demonstration of critical phenomena in $\mathcal{PT}$-symmetric non-unitary quantum dynamics. We expect that critical phenomena associated with higher-order exceptional points can also be probed using a similar approach.

References

[1] L. Xiao, K. K. Wang, X. Zhan, Z. H. Bian, K. Kawabata, M. Ueda, W. Yi, and P. Xue, Observation of critical phenomena in parity-time-symmetric quantum dynamics. *arXiv:1812.01213v2.*

Higher winding number in a non-unitary photonic quantum walk

Lei Xiao[1] Xingze Qiu[2] Kunkun Wang[1] Zhihao Bian[1] Xiang Zhan[1]
Hideaki Obuse[3] Barry C. Sanders[4] Wei Yi[2] * Peng Xue[1] †

[1] *Beijing Computational Science Research Center, Beijing 100084, China*
[2] *Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*
[3] *Department of Applied Physics, Hokkaido University, Sapporo 060-8628, Japan*
[4] *Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, CAS, Hefei 230026, China*

Abstract. Topological matter exhibits exotic properties yet phases characterized by large topological invariants are difficult to implement, despite rapid experimental progress. A promising route toward higher topological invariants is via engineered Floquet systems, particularly in photonics, where flexible control holds the potential of extending the study of conventional topological matter to novel regimes. Here we implement a one-dimensional photonic quantum walk to explore large winding numbers. By introducing partial measurements and hence loss into the system, we detect winding numbers of three and four in multi-step non-unitary quantum walks, which agree well with theoretical predictions.

Keywords: winding number, quantum walk, partial measurement

1 Introduction

Topological phases are typically characterized by integer-valued topological invariants, associated with the emergence of robust edge states through the so-called bulk-boundary correspondence. Recent experiments reveal and characterize topological edge states and bulk topological invariants in settings ranging from condensed matter to synthetic systems. However, the experimentally detected topological invariants are typically small and limited to two, with the only exception being the recently engineered topological photonic materials in two dimensions, with Chern numbers greater than two having been reported. In one dimension, while topological phases with large winding numbers have been theoretically studied, e.g., in quantum transport or in quantum-walk dynamics, experimental realization is still lacking. Realizing systems with large topological invariants, whether large Chern numbers in two dimensions or large winding numbers in one dimension, is fundamentally important goal for the study of topological matter.

In this work, we report experimental detection of large winding numbers of three and four in photonic non-unitary quantum walks, which are scalable to feature even higher winding numbers. By periodical partial measurements on polarization of the photonic walker, we realize multi-step non-unitary quantum walks in one dimension supporting Floquet topological phases (FTPs). As for two-step non-unitary quantum walks, partial measurement introduces loss to the quantum-walk dynamics and provides a natural detection channel for FTP winding number. Whereas FTPs in two-step non-unitary quantum walks are directly related to those in a lossy Su-Schrieffer-Heeger (SSH) model, the multi-step non-unitary quantum walks here are analogous to adding longer-range hopping terms in the lossy SSH model, which gives rise to higher winding numbers.We detect winding numbers of three and four through average dispacements.

Our experimental detection of large winding numbers in non-unitary FTPs offers the exciting prospect of exploring topological phases characterized by large topological invariants in non-unitary or non-Hermitian settings, which will create further opportunities in engineering unconventional topological phenomena using photonics.

2 Multi-step non-unitary quantum walks

We introduce the photonic setup for multi-step non-unitary quantum walks, where the walker is shifted more than twice at each time step. We focus on three- and four-step non-unitary quantum walk in this work. As illustrated in Fig. 1, the three-step quantum walk is on a one-dimensional lattice L ($L \in \mathbb{Z}$) with periodic boundary condition, and the dynamics is governed by the Floquet operator

$$\widetilde{U}_3' := MU_3' = MR\left(\frac{\theta_1}{2}\right) SR\left(\theta_2\right) SR\left(\theta_2\right) SR\left(\frac{\theta_1}{2}\right). \tag{1}$$

Here, the coin operator $R(\theta)$ rotates single-photon polarization by θ about the y-axis, where coin states are horizontally polarized ($|H\rangle$) and vertically polarized ($|V\rangle$). The polarization-dependent shift operator S moves the walker with coin state $|H\rangle$ ($|V\rangle$) to the left (right) by one lattice site. Non-unitary dynamics is enforced by the loss operator

$$M = \mathbb{1}_{\mathrm{w}} \otimes \left(|+\rangle\langle+| + \sqrt{1-p}\,|-\rangle\langle-|\right), \quad 0 < p \leqslant 1, \tag{2}$$

where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$, and $\mathbb{1}_{\mathrm{w}} = \sum_L |x\rangle\langle x|$ with x denoting the position of the walker. The loss operator is equivalent to performing a partial measurement $M_e = \mathbb{1}_{\mathrm{w}} \otimes \sqrt{p}\,|-\rangle\langle-|$ in the basis $\{|+\rangle, |-\rangle\}$ at each time step, with p the probability of a successful measurement.

*wyiz@ustc.edu.cn
†gnep.eux@gmail.com

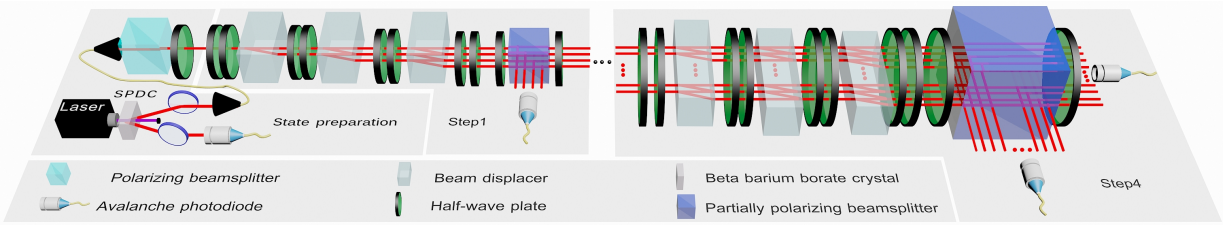


Figure 1: We show a three-step non-unitary quantum walk up to 4 time steps as an example. The photon pair is created via spontaneous parametric downconversion. One photon serves as a trigger. The other photon is projected into the polarization state $|+\rangle$ with a polarizing beamsplitter (PBS) and a half-wave plate (HWP, at 22.5°) and then proceeds through the quantum-walk interferometric network.

Whereas R and S are implemented by using appropriate wave plates and beam displacers (BDs), the partial measurement operator M_e is realized by a sandwich-type setup involving two half-wave plates (HWPs) and a partially polarizing beamsplitter (PPBS). At each measurement step in the quantum-walk dynamics, photons in the state $|-\rangle$ are reflected by the PPBS with probability p. Photons are then detected by single-photon avalanche photodiodes (APDs) and lost from the quantum-walk dynamics.

Topological properties in the experimental three-step non-unitary quantum walk are introduced via the effective non-Hermitian Hamiltonian $H_{\rm eff}^{\prime(3)}$ defined through $\widetilde{U}_3' = \exp\left[-\mathrm{i}H_{\rm eff}^{\prime(3)}\right]$. For the homogeneous single-photon quantum walk considered here, $H_{\rm eff}^{\prime(3)}(k) = E_k \boldsymbol{n}\cdot\boldsymbol{\sigma}$ in momentum k space, with $\boldsymbol{\sigma}$ the Pauli vector, E_k the quasienergy spectrum, and $\boldsymbol{n}$ the direction of the spinor eigen-vector for each momentum $-\pi < k \leq \pi$. Similar to the case of the two-step non-unitary quantum walk, the winding number of the three-step quantum walk, which serves as a topological invariant of the system, is the number of times the real component of $\boldsymbol{n}$ winds around the x-axis as k varies through the first Brillouin zone.

For a given FTP with chiral symmetry, two distinct winding numbers (ν', ν'') exist for Floquet operators fitted in different time frames. Whereas the corresponding winding number for $\widetilde{U}_3'$ is ν', ν'' is similarly defined through the winding of the spinor eigen-vector of the non-Hermitian Hamiltonian $H_{\rm eff}^{\prime\prime(3)}$, where $\widetilde{U}_3'' = \exp\left[-\mathrm{i}H_{\rm eff}^{\prime\prime(3)}\right]$ and

$$\widetilde{U}_3'' := MS_{\rm up}R(\theta_2)SR(\theta_1)SR(\theta_2)S_{\rm down}. \tag{3}$$

Here, $S_{\rm up} = \sum_x \left(|x+1\rangle\langle x|\otimes|V\rangle\langle V| + |x\rangle\langle x|\otimes|H\rangle\langle H|\right)$ and $S_{\rm down} = \sum_x \left(|x\rangle\langle x|\otimes|V\rangle\langle V| + |x-1\rangle\langle x|\otimes|H\rangle\langle H|\right)$. Depending on the coin parameters, the absolute value of the winding numbers can take large integer values up to three, as we show in the phase diagram in Fig. 2(a).

Similar to three-step quantum walks, we define four-step non-unitary quantum walks from constructing the evolution operators

$$\widetilde{U}_4^{\prime(\prime)} := MR\left[\frac{\theta_{1(2)}}{2}\right]SR(0)SR\left[\theta_{2(1)}\right]SR(0)SR\left[\frac{\theta_{1(2)}}{2}\right], \tag{4}$$

By analyzing the effective non-Hermitian Hamiltonians $H_{\rm eff}^{\prime(4)}$ and $H_{\rm eff}^{\prime\prime(4)}$ respectively associated with the Floquet operators $\widetilde{U}_4''$ and $\widetilde{U}_4''$, it is straightforward to demonstrate that FTPs exist for four-step quantum walks, which are characterized by integer-valued winding numbers as large as four. Importantly, both the three- and four-step quantum walks defined in Eqs. (1), (3) and (4) have chiral symmetry in the unitary limit ($p = 0$), with the chiral symmetry operator given by $\Gamma = \sigma_x$ as $\Gamma U \Gamma = U^{-1}$, where U designates the Floquet operator of the corresponding quantum walk. Consistent with previous studies, we find that topological properties of the non-unitary quantum-walk dynamics derive from those in the unitary limit, which are in turn protected by chiral symmetry. Hence, chiral symmetry in the unitary limit is crucial for the perseverance of the FTPs in the non-unitary case ($p > 0$).

3 Detecting topological invariants from losses

In two-step non-unitary quantum walks, topological invariants can be probed by monitoring losses. As we experimentally demonstrate and explain, topological invariants of the multi-step non-unitary quantum walks are determined from losses by measuring average displacement

$$\langle \Delta x\rangle = \sum_x \sum_{t'=1}^{\infty} x P_{\rm th}(x,t'), \tag{5}$$

for the walker-coin system initialized in the state $|\psi_0\rangle = |x=0\rangle\otimes|+\rangle$. Here, the probability of the walker being detected at x during the t-th time step is

$$P_{\rm th}(x,t) = \langle\psi_{t-1}|\, U_3^{\prime\dagger} M_e^{\dagger}\left(|x\rangle\langle x|\otimes \mathbb{1}_{\rm c}\right) M_e U_3' \,|\psi_{t-1}\rangle\,, \tag{6}$$

where $|\psi_t\rangle = (\widetilde{U}_3')^t|\psi_0\rangle$, and $\mathbb{1}_{\rm c}$ is a 2×2 identity operator.

To experimentally probe the average displacement in the non-unitary quantum walk with t steps in total, we perform coincidence measurements on the number of the reflected photons $N_{\rm R}(x,t')$ $(t' = 1, ..., t)$ at each position successively up to t. We then construct the probability

$$P_{\rm exp}(x,t') = \frac{N_{\rm R}(x,t')}{\sum_{x'}\left[\sum_{t''=1}^{t} N_{\rm R}(x',t'') + N_{\rm T}(x',t)\right]}, \tag{7}$$

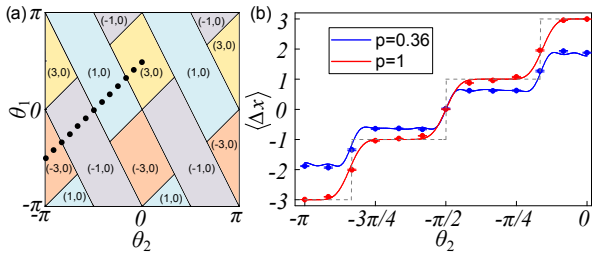


Figure 2: (a) Phase diagram for three-step non-unitary quantum walks characterized by the topological invariants (ν', ν'') as functions of the coin parameters (θ_1, θ_2). (ν', ν'') are calculated from the Floquet operators $\widetilde{U}_3'$ and $\widetilde{U}_3''$, respectively. (b) Measured average displacements of three-step non-unitary quantum walks corresponding to $\widetilde{U}_3'$ with different loss parameters $p = 1, 0.36$. Coin parameters vary along the line $\theta_1 = \theta_2 + \pi/2$, as indicated by dots in Fig. 2(a). The dashed curve indicates expected results of infinite-step quantum walks. The solid curve indicates numerical simulations for quantum walks with 4 time steps and the experimental results are presented by dots. Experimental errors are due to photon-counting statistics.

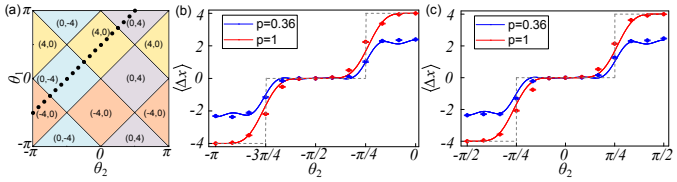


Figure 3: (a) Phase diagram for four-step non-unitary quantum walks in terms of the topological invariants (ν', ν''). (ν', ν'') are calculated from the Floquet operators $\widetilde{U}_4'$ and $\widetilde{U}_4''$ respectively. Measured average displacements of four-step non-unitary quantum walks of $\widetilde{U}_4'$ (b) and $\widetilde{U}_4''$ (c) with different loss parameters $p = 1, 0.36$. Coin parameters vary along the line $\theta_1 = \theta_2 + \pi/2$ as indicated by dots in Fig. 3(a). Experimental errors are due to photon-counting statistics.

where $N_{\mathrm{T}}(x,t)$ is the number of transmitted photons at the last step t. The average displacement is then

$$\langle \Delta x \rangle_{\mathrm{exp}} = \sum_{x} \sum_{t'=1}^{t} x P_{\mathrm{exp}}(x, t'). \tag{8}$$

To detect topological invariants, we realize three-step non-unitary quantum walks with two different loss parameters $p = 1, 0.36$. The corresponding phase diagram is shown in Fig. 2(a), where the topological invariants (ν', ν'') are functions of the coin parameters (θ_1, θ_2). Thirten sets of coin parameters (θ_1, θ_2) are chosen along the line $\theta_1 = \theta_2 + \pi/2$, as indicated in Fig. 2(a). The topological invariant ν' assumes values -3, -1, 1 to 3 along the line, while ν'' is fixed at 0. The walker starts from $x = 0$, and the initial coin state is chosen to be $|+\rangle$.

Measured average displacements are shown in Fig. 2(b) for the Floquet operator $\widetilde{U}_3'$ (as ν'' is always zero, the average displacements for $\widetilde{U}_3''$ are not shown). These results agree well with the numerical simulations of three-step quantum walks up to 4 time steps and demonstrate plateaux close to the quantized values of ν' calculated for quantum walks with infinite time steps. We observe that with increasing loss parameter p, measured average displacements at a given time step converge faster to the quantized values. This result is consistent with the measurement results for two-step non-unitary quantum walks and suggests that the quantum Zeno effect is weak in these systems. Meanwhile, regardless of the loss parameter, it takes much longer for the displacements to converge near topological phase transitions, where the topological invariants undergo abrupt changes.

We then implement four-step non-unitary quantum walks with the loss parameters $p = 1, 0.36$. The corresponding phase diagram is shown in Fig. 3(a). As the coin parameters vary along the dotted line $\theta_1 = \theta_2 + \pi/2$ in the phase diagram, the topological invariants (ν', ν'') change from $(-4, 0)$, $(0, -4)$, $(4, 0)$, to $(0, 4)$. The measured average displacements for the operators $\widetilde{U}_4'$ and $\widetilde{U}_4''$ up to 3 time steps are shown in Figs. 3(b) and 3(c), respectively, which agree well with the corresponding numerical simulations.

4 Discussion

We experimentally realize FTPs with large topological invariants in photonic multi-step non-unitary quantum walks. The topological invariants are detected by monitoring the average displacements of the walker.

Our experimental scheme can be extended to quantum walks with more steps, where FTPs with even higher winding numbers can be prepared and probed. This extension would significantly enrich the experimentally accessible non-unitary FTPs in one dimension, and would stimulate further studies on dynamic properties of non-unitary FTPs.

Another interesting direction would be the exploration of the relation between FTPs in non-unitary quantum-walk dynamics and those in a parity-time-symmetric configuration. This is particularly relevant due to the existence of hidden pseudo-unitarity in our system, which is intimately connected with the reality of the quasienergy spectrum and hence with parity-time symmetry as well. Our experiment, with its excellent extendibility, opens up the avenue toward a hierarchy of FTPs with large winding numbers, and sheds new light on understanding topological phenomena in non-unitary systems.

References

[1] L. Xiao, X. Z. Qiu, K. K. Wang, Z. H. Bian, X. Zhan, H. Obuse, B. C. Sanders, W. Yi, and P. Xue, Higher winding number in a nonunitary photonic quantum walk. *Phys. Rev. A*, 98 063847, 2018.

New proof and Bell-like inequalities of Arrow's impossibility theorem

WoongSeon Yoo[1,2]

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

[2]*Skolkovo Institute of Science and Technology, Russia*

e-mail: *woongseon.yoo@gmail.com*

Information is physical: logical phenomenon correspond to structures of the nature. Landauer principle dictates that it takes at least an unit energy to erase a classical information unit and No-cloning theorem dictates that the quantum information cannot be cloned[1].

Games have information theoretic meanings such as (i) games have physical meanings, (ii) games are governed by dynamics and (iii) games are measures of complexity. Specifically, the voting as a game is a famous concept in Boolean analysis governed by Arrow's impossibility theorem[2,3]: 'dictatorship' is inevitable in the classical voting. It was recently found that its quantum extension does not hold[4].

We propose a new proof of Arrow's impossibility theorem based on the fact that the dictatorship in the voting is equivalent to the cloning operator in the circuit. The equivalence is a meaning of the voting.

We interpret phenomenon in infinite voting with the thermodynamics of the information. It was proven that Arrow's theorem does not hold if either the number of voters or alternatives is infinite. Infinite phenomenon can be explained by thermodynamic limits and Landauer principle.

We suggest Bell-like inequalities of voting where the quantum voting violates. The voting is a well-known communication complexity problem[5]. Bell-violations explain the quantum supremacy of communication complexity problems[6]. Moreover, the thought experiment of voting is presented.

This work is based on the undergraduate thesis of the author whose advisor is Prof.Soo-Jong Rey.

THIS PAPER IS ELIGIBLE FOR BEST STUDENT POSTER AWARD

[1] C.Bennett and R.Landauer, The fundamental physical limits of computation, Scientific American, 253(1):48–57, 1985.

[2] Kenneth J Arrow. Social choice and individual values,1952

[3] Gil Kalai. A fourier-theoretic perspective on the condorcet paradox and arrow's theorem, Advances in Applied Mathematics, 29(3):412 – 426, 2002

[4] N Bao and N. Halpern. Quantum voting and violation of arrow's impossibility theorem, Phys.Rev. A, 95, 062306, Jun 2017

[5] V.Conitzer and T.Sandholm, Communication complexity of common voting rules. In Proceedings of the 6th ACM conference on Electronic commerce, pages 78–87. ACM, 2005

[6] C.Brukner, M.Zukowski, J.Pan, and A.Zeilinger. Bell's inequalities and quantum communication complexity, Phys.Rev.Let92, 127901, Mar 2004.

Quantum tunneling and cat-like steady states in a degenerate parametric oscillator with anharmonic nonlinearity

Feng-Xiao Sun[1 2 3 4] Qiongyi He[1 2 5 *] Qihuang Gong[1 2 5] Run Yan Teh[3]
Margaret D. Reid[3 4] Peter D. Drummond[3 4]

[1] *State Key Laboratory for Mesoscopic Physics and Collaborative Innovation Center of Quantum Matter, School of Physics, Peking University, Beijing 100871, China*
[2] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China*
[3] *Centre for Quantum and Optical Science, Swinburne University of Technology, Melbourne 3122, Australia*
[4] *Institute of Theoretical Atomic, Molecular and Optical Physics (ITAMP), Harvard University, Cambridge, Massachusetts 02138, USA*
[5] *Beijing Academy of Quantum Information Sciences, Haidian District, Beijing 100193, China*

Abstract. Recent experiments in superconducting circuit with Josephson junction nonlinearities give rise to new properties [1]. We obtained exact analytic solutions for the steady-state of this single-mode case of subharmonic generation. In the region of weak nonlinearities, we obtained analytic solutions for the tunneling time over which the time symmetry-breaking is lost [2]. And for strong nonlinearities, we find that a cat-like steady state can be formed, which is a mixed state whose purity will be reduced by the driving. We also show that steady-state pure cats cannot survive with single-photon loss concerned [3].

Keywords: quantum optics, quantum tunneling, Schrödinger cat, DPO, phase space methods.

1 Introduction

Quantum time symmetry breaking is widespread in non-equilibrium quantum optics and superconducting circuits. This is implicit in the use of coherent states, which have a well-defined phase, to describe lasers [4, 5]. *Discrete* time symmetry breaking takes place in intracavity subharmonic generation [6]. For quantum optical systems, an exact solution for the steady-state quantum density matrix [7] is known for special cases. From this, one can calculate quantum tunneling between time phases [8]. Transient Schröinger cats are also possible in this case [9, 10, 11]. Tunneling in these systems demonstrates the existence of long range time order, which has been confirmed in optical experiments [12].

Macroscopic superposition states have been proposed in quantum computation [13], quantum teleportation [14], quantum metrology [15] and quantum key distribution [16]. As well as transient macroscopic superpositions and tunneling, subharmonic generators can generate space-time ordering [17]. These effects are related to time crystals [18], which are recent, similar phenomena. Physically, such devices are quantum squeezed state generators. Below threshold, they are used to reduce quantum noise in gravity-wave detectors [19, 20], while networks of above threshold parametric devices are used for NP-hard optimization [21, 22].

Quantum subharmonic generation with anharmonic nonlinearities has been achieved in superconducting circuits [1]. Relatively large cat states were observed. In our studies [2, 3], we find that the physics of the quantum steady state is different from previous studies, where a complex manifold is introduced. In the region of weak nonlinearities, we obtained analytic solutions for the tunneling time. Our results show that the anharmonicity will enhances quantum tunneling rates, which may have practical applications for escaping a local minimum in quantum neural networks [21, 22]. And in the region of strong nonlinearities, we find that a cat-like steady state can be formed, which is a mixed state whose purity will be reduced by the driving. Since pure cat states are unachievable because of the inevitable single-photon loss, we propose a scheme to form an approximate steady-state cat state in realizable systems.

*qiongyihe@pku.edu.cn

2 Steady state of DOP with anharmonic nonlinearity

We consider a general model for two coupled bosonic modes of an open system. The annihilation and creation operators of the k-th mode are $a_k, a_k^\dagger$ at frequencies ω_k. They have a non-interacting Hamiltonian in the rotating frame of $H_0 = \hbar\sum \Delta_k a_k^\dagger a_k$, where $\Delta_k = \omega_k - k\omega_0 \ll \omega_0$ for a input laser frequency of $2\omega_0$. The interaction Hamiltonian is then given by

$$H_I = \hbar\frac{\chi}{2}a_1^{\dagger 2}a_1^2 + \left(i\hbar\frac{\kappa}{2}a_2 a_1^{\dagger 2} + i\hbar\mathcal{E}_2 a_2^\dagger + h.c.\right). \quad (1)$$

Here $\mathcal{E}_2$ is the envelope amplitude of the driving for the mode a_2, and κ, χ are the parametric and anharmonic nonlinearities [23] respectively. Anharmonic nonlinearities are only included for the mode a_1.

With adiabatic approximation and generalized P-representation [24], we find the steady-state probability distribution $P(\alpha,\alpha^+) = N\exp\left[-\Phi(\alpha,\alpha^+)\right]$, where

$$\Phi\left(\alpha,\alpha^+\right) = -2\alpha^+\alpha - c\ln[\lambda_c - \alpha^2] - c^*\ln[\lambda_c^* - \alpha^{+2}], \quad (2)$$

with dimensionless parameters $c = \gamma/g - 1$ and $\lambda_c = \epsilon/g$, where $\gamma = \gamma_1^{(1)} + i\Delta_1$, $g = \gamma_e^{(2)} + i\chi_e$, $\gamma_e^{(2)} = \gamma_1^{(2)} + \frac{\gamma_2^{(1)}}{2}\left|\frac{\kappa}{\gamma_2^{(1)}+i\Delta_2}\right|^2$, $\chi_e = \chi - \frac{\Delta_2}{2}\left|\frac{\kappa}{\gamma_2^{(1)}+i\Delta_2}\right|^2$ and $\epsilon = \frac{\kappa}{\gamma_2}\mathcal{E}_2$.

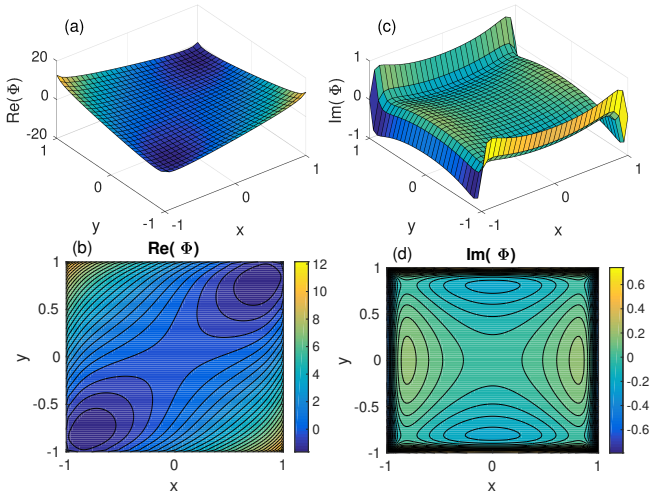


Figure 1: We show the potential $\Phi(\vec{\beta})$ on the manifold. Figure (a) shows the real part of $\Phi(\vec{\beta})$ with the parameterized variables (x, y), and figure (b) shows the related contour figure of $Re[\Phi(\vec{\beta})]$. Figure (c) shows the image part of $\Phi(\vec{\beta})$ with (x, y), and the figure (d) shows the related contour figure of $Im[\Phi(\vec{\beta})]$. In these figures, $c = 1 + 0.5i$ and $\lambda = 3$.

All the parameters here can have complex values, which is necessary when treating the situations in recent quantum circuit experiments [1].

3 Quantum tunneling with weak nonlinearity

Geometrically, we can regard the quantum dynamics as occurring via a distribution function defined on a two-dimensional manifold embedded in a four-dimensional complex space, considering that α and α^+ are two complex independent variables. Then the potential Φ can be expressed as in Fig. 1. We note that there are two local minima and a saddle point in the potential, thus the quantum tunneling will take place.

The analytic solution of the tunneling time is obtained with the potential-barrier approximation. Comparing with the numerical results, they agree with each other in the large tunneling time limit, where the potential-barrier approximation is valid, as shown in Fig. 2.

4 Cat-like steady state with strong nonlinearity

In the region of strong nonlinearities, the probability distribution can be expressed in Fig. 3. In extremely strong nonlinearity limit, $c \to -1$, the distribution approaches the delta-function form, which resembles the Schrödinger cat. And in the large driving limit, $\lambda \to \infty$, the distribution reduce to a classical mixture of coherent states.

Further studies tell us that the delta-form steady-state distribution is a mixed state rather than a pure state, which is only valid in the limit $c \to -1$. We also find that pure steady-state cats are only reachable if there is

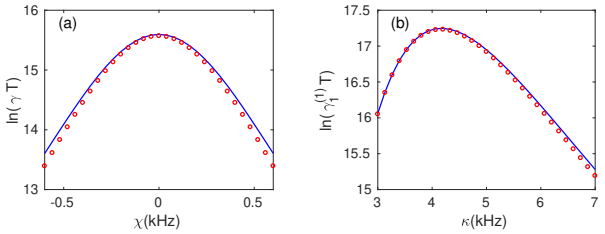


Figure 2: Comparisons of the tunneling times obtained using the P-representation (blue lines) and the number-state expansion (red circles) changing with the anharmonic nonlinearity χ (a) and the parametric nonlinearity κ (b). In figure (a), the other parameters are $\gamma = 1.5$kHz, $\gamma^{(2)} = 0.8$kHz, $\epsilon = 10$kHz. In figure (b), $\gamma = 1.5$kHz, $\gamma_1^{(2)} = 0.1$kHz, $\gamma_2 = 20$kHz, $\chi = 0.1$kHz, $\mathcal{E}_2 = 40$kHz.

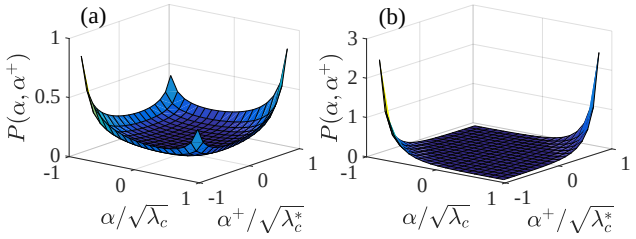


Figure 3: Real parts of steady-state probability distributions for (a) $c = -0.6 - 0.2i$ and $\lambda_c = -0.193 + 0.096i$, and (b) large λ: $c = -0.6 - 0.2i$ and $\lambda_c = -1.93 + 0.96i$.

no single-photon loss, as shown in Fig. 4. This is because the parity symmetry breaks once the single-photon loss is nonzero.

By changing the driving, we show in Fig. 5 that the exact distribution is similar to the mixed delta-form distribution, while the pure cat state is a different distribution which is only vaild if there is no single-photon loss.

5 Summary

We have discussed general properties of quantum tunneling and cat-like steady states in subharmonic generation with anharmonic nonlinearities. In the weak nonlin-

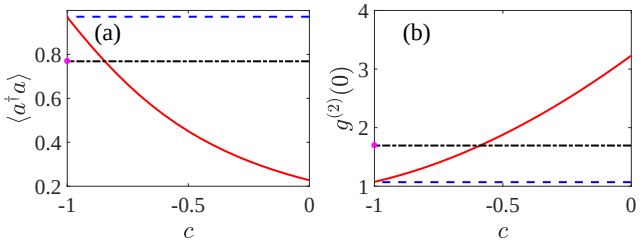


Figure 4: Comparing the average photon numbers (a) and the second order correlation functions (b). The blue dashed line is obtained from the mixed cat distribution, the red solid line from the analytic method, the black dash-dotted line from the pure cat state, and the magenta circles are obtained with $\gamma = 0$ and initial vacuum state.

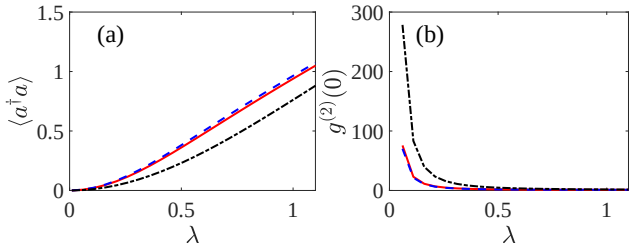


Figure 5: Comparing the average photon number (a) and the second-order correlation function (b) with λ varying. In this case, $c = -0.99 - 0.1i$. The lines have the same meanings as in the Fig. 4.

earity case [2], we obtain analytic solutions for the tunneling time which are confirmed by number state calculations. We find that additional anharmonic terms increase the tunneling rate. This could be useful in quantum neural networks [21, 22] for escaping a local minimum. In the region of strong nonlinearities [3], we get an exact analytic solution for the steady states. We show that in the limit of extremely strong nonlinearities, the steady state will reduce to a cat-like mixed state. We also conclude that true Schrödinger cats cannot survive in the steady state unless there is no single-mode loss.

References

[1] Z. Leghtas, et al. Confining the state of light to a quantum manifold by engineered two-photon loss. *Science*, 347:853-857, 2015.

[2] F.-X. Sun, Q. He, Q. Gong, R. Y. Teh, M. D. Reid, P. D. Drummond. Discrete time symmetry breaking in quantum circuits: exact solutions and tunneling. arXiv:1904.05010, 2019.

[3] F.-X. Sun, Q. He, Q. Gong, R. Y. Teh, M. D. Reid, P. D. Drummond. Can steady-state Schrdinger cats survive in subharmonic generation with anharmonic nonlinearities? arXiv:1905.08010, 2019.

[4] R. J. Glauber. Photon correlations. *Phys. Rev. Lett.* 10:84, 1963.

[5] H. Haken. Cooperative phenomena in systems far from thermal equilibrium and in nonphysical systems. *Rev. Mod. Phys.* 47:67, 1975.

[6] P. Drummond, K. McNeil, D. Walls. Non-equilibrium transitions in sub/second harmonic generation. *Opt. Acta* 27:321-335, 1980.

[7] P. Drummond, K. McNeil, D. Walls. Non-equilibrium transitions in sub/second harmonic generation. *Opt. Acta* 28:211-225, 1981.

[8] P. D. Drummond, P. Kinsler. Quantum tunneling and thermal activation in the parametric oscillator. *Phys. Rev. A* 40:4813, 1989.

[9] M. Reid, B. Yurke. Effect of bistability and superpositions on quantum statistics in degenerate parametric oscillation. *Phys. Rev. A* 46:4131, 1992.

[10] L. Krippner, W. Munro, M. Reid. Transient macroscopic quantum superposition states in degenerate parametric oscillation: Calculations in the large-quantum-noise limit using the positive P representation. *Phys. Rev. A* 50:4330, 1994.

[11] W. Munro, M. Reid. Transient macroscopic quantum superposition states in degenerate parametric oscillation using squeezed reservoir fields. *Phys. Rev. A* 52:2388, 1995.

[12] C. Nabors, S. Yang, T. Day, R. Byer. Coherence properties of a doubly resonant monolithic optical parametric oscillator. *J. Opt. Soc. Am. B* 7:815-820, 1990.

[13] M. Mirrahimi, et al. Dynamically protected cat-qubits: a new paradigm for universal quantum computation. *New J. Phys.* 16:045014, 2014.

[14] S. J. van Enk, O. Hirota. Entangled coherent states: Teleportation and decoherence. *Phys. Rev. A* 64:022313, 2001.

[15] J. Joo, W. J. Munro, T. P. Spiller. Quantum metrology with entangled coherent states. *Phys. Rev. Lett.* 107:083601, 2011.

[16] D. S. Simon, G. Jaeger, A. V. Sergienko. Entangled-coherent-state quantum key distribution with entanglement witnessing. *Phys. Rev. A* 89:012315, 2014.

[17] P. D. Drummond, K. Dechoum. Universality of quantum critical dynamics in a planar optical parametric oscillator. *Phys. Rev. Lett.* 95:083601, 2005.

[18] D. V. Else, B. Bauer, C. Nayak. Floquet time crystals. *Phys. Rev. Lett.* 117:090402, 2016.

[19] C. M. Caves. Quantum-mechanical noise in an interferometer. *Phys. Rev. D* 23:1693, 1981.

[20] A. Pace, M. Collett, D. Walls. Quantum limits in interferometric detection of gravitational radiation. *Phys. Rev. A* 47:3173, 1993.

[21] T. Inagaki, et al. A coherent Ising machine for 2000-node optimization problems. *Science* 354:603-606, 2016.

[22] P. L. McMahon, et al. A fully programmable 100-spin coherent Ising machine with all-to-all connections. *Science* 354:614-617, 2016.

[23] P. Drummond, D. Walls. Quantum theory of optical bistability. I. Nonlinear polarisability model. *J. Phys. A* 13:725, 1980.

[24] P. Drummond, C. Gardiner. Generalised P-representations in quantum optics. *J. Phys. A* 13:2353, 1980.

Skew informations from an operational view via resource theory of asymmetry

Ryuji Takagi[1] *

[1] *Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*

Abstract. The Wigner-Yanase skew information was proposed to quantify the information contained in quantum states with respect to a conserved additive quantity, and it was later generalized to a class called metric-adjusted skew informations. We analyze this general family of the skew informations from an operational point of view by utilizing the fact that they are valid asymmetry resource monotones. We show that such an approach allows for clear physical meanings as well as simple proofs of some of the basic properties of the skew informations. Notably, we constructively prove that any type of skew information cannot be superadditive, where the violation of the superadditivity had been only known for a specific class of skew informations with numerical counterexamples. We further show a weaker version of superadditivity relation applicable to the general class of the skew informations, which proves a conjecture previously proposed for the Wigner-Yanase skew information as a special case. We finally discuss an application of our results for a situation where quantum clocks are distributed to multiple parties.

1 Introduction

Quantifying the information contents is a central theme in information theory, but it becomes subtle when the system has a certain symmetry and possesses a conserved quantity because, in such cases, some observables can be measured more easily than others as observed by Wigner, Araki, and Yanase [2–4]. Motivated by this observation, the Wigner-Yanase skew information was proposed as an information-theoretic quantity that measures the information contents contained in a quantum state with respect to a conserved additive quantity [5]. This is later extended to Wigner-Yanase-Dyson skew informations, and further to the general family of metric-adjusted skew information [6], establishing a connection with with information geometry [7].

The characterization of the skew informations by information geometry then further finds a connection to the measures of asymmetry in the context of resource theories. Resource theories are formal frameworks dealing with quantification and manipulation of intrinsic physical quantities, called resources, associated with given physical settings [8]. In particular, resource theory of asymmetry [9] accounts for the capability of breaking the relevant symmetry possessed by the system. It has been found that not only Wigner-Yanase-Dyson skew informations [10, 11] but the whole family of skew informations [12] serve as valid asymmetry quantifiers, providing another operational aspect to this information-theoretic quantities. It is thus highly desired to unveil the general properties shared by the skew informations in the general family. However, due to the generality of the skew informations as well as restrictions imposed on them, investigating properties of the skew informations usually requires highly involved mathematical techniques [6, 13] that are not physically very intuitive, and it is hoped that the operational view stemming from the resource theory would provide another route that gets around with these difficulties.

Here, we employ an operational approach to analyze the general class of skew informations, extending the argument in Ref. [10] employed for a special class of skew informations. We see that operational views provided by the resource theory allow for richer physical intuitions as well as simpler proofs of some of the important properties. Notably, we constructively show that any skew information cannot be superadditive. The superadditivity of the Wigner-Yanase skew information was listed as a desired property for the skew information to be an information measure, and Wigner and Yanase themselves proved this property for pure bipartite states [5]. It had been widely believed that it would hold in general until counterexamples have been recently found [14–16]. On the other hand, it has been also shown that "classical" states always satisfy the superadditivity [17, 18], so it would be essential to investigate what property of the state contributes to the violation of the superadditivity, since it might be an indicator of some form of "quantumness". However, the previously shown counterexamples are purely numerical examples obtained by exhaustive computational search or semianalytical forms which fail to provide much physical insights. In this work, we find that the violation of the superadditivity is a natural consequence from the resource-theoretic point of view, providing a fully analytical and physically clear proof for the violation of the superadditivity. We also propose and prove a weaker version of superadditivity relation

* rtakagi@mit.edu

that holds for any skew information, which proves the conjecture posed in Ref. [16] as a special case of our results. We finally apply our results to a physical situation where quantum clocks are distributed to multiple parties. The full paper is found in Ref. [1].

2 Preliminaries

We first review the resource theory of asymmetry. The resource theory of asymmetry with group G corresponds to the setting where one has free access to quantum states that are invariant (symmetric) under group action whereas states that can break the group symmetry, asymmetric states, are considered precious, and thus resources. Formally, the state ρ is called a symmetric state if $U_g \rho U_g^\dagger = \rho$, $\forall g \in G$ where U_g is a unitary representation of the group element g. A relevant set of free operations are covariant operations $\mathcal{E}$ satisfying the covariance condition: $\mathcal{E} \circ \mathcal{U}_g^I = \mathcal{U}_g^O \circ \mathcal{E}$ $\forall g \in G$ where $\mathcal{U}_g^X(\cdot)$ refers to the application of unitary representation of g on the system X, and $X = I, O$ correspond to the input system and output system of $\mathcal{E}$. Then, any function R from quantum states to real number satisfying $R(\rho) \geq R(\mathcal{E}(\rho))$, $\forall \rho$ for any covariant operation $\mathcal{E}$ is called asymmetry monotone. Here we only deal with the $U(1)$ group whose unitary representation is labeled by a real number t as $U_X(t) = \exp(iH_X t)$ where H_X is an observable defined on system X.

We next briefly review the skew informations. Suppose the system possesses an additive conserved quantity whose observable is denoted by H. To quantify the information contained by quantum states with respect to the conserved quantity, Wigner and Yanase proposed the Wigner-Yanase skew information $I^{WY}(\rho, H) = -\frac{1}{2}\operatorname{Tr}([\sqrt{\rho}, H]^2)$. Later, a general family of skew informations called metric-adjusted skew informations were introduced

$$I^f(\rho, H) = \frac{f(0)}{2} \operatorname{Tr}\left[(i[H, \rho])\, c_f(L_\rho, R_\rho)\, (i[H, \rho])\right]$$

where $c_f(x, y) := \left[y f(xy^{-1})\right]^{-1}$ is the Morozova-Chentsov function [19], and f is a standard operator monotonic function. Note that the Wigner-Yanase skew information is reconstructed by taking an appropriate form of $c_f(x, y)$. Remarkably, all the skew informations are valid asymmetry monotones [12].

3 Properties of skew informations as asymmetry monotones

In this abstract, we discuss two properties for which resource-theoretic arguments turn out to be useful. An extended list for such properties are found in Ref. [1]

Monotonicity under the partial trace The skew informations of the subsystem are not greater than the skew informations of the total system. $I^f(\rho_{12}, H_{12}) \geq I^f(\rho_1, H_1)$ where $H_{12} = H_1 \otimes \mathbb{I} + \mathbb{I} \otimes H_2$. As asymmetry measures, this relation entails a natural physical meaning; if one throws away a subsystem, the capability of breaking the symmetry (e.g. accuracy of quantum clock) must decrease. From resource-theoretic perspective, this is concisely obtained by that the partial trace is indeed a covariant operation. Also, a related property $I^f(\rho_{12}, H_1 \otimes I) \geq I^f(\rho_1, H_1)$ has been proved in Ref. [13, 20] for Wigner-Yanase-Dyson skew informations by an explicit but involved calculation. By our argument, however, one can immediately prove even more general relation applicable to any skew information as a special case of the monotonicity under partial trace when $H_2 = 0$.

Decrease under measurements not disturbing the conserved quantity In Ref. [21], the dynamics of Wigner-Yanase skew information under the measurement that does not disturb the conserved quantity have been investigated. Specifically, they considered the measurement operation $M(\cdot) = \sum_j E_j \cdot E_j^\dagger$ whose measurement operators commute with the observable corresponding to the conserved quantity; $[E_j, H] = 0$, $\forall j$. This implies $\operatorname{Tr}[M(\rho)H] = \operatorname{Tr}[\rho H]$, so the expectation value of the conserved quantity is not disturbed. For such a measurement, they asked whether the Wigner-Yanase skew information would decrease under deterministic measurement $I^{WY}(M(\rho), H) \leq I^{WY}(\rho, H)$ and under selective measurement $\sum_j p_j I^{WY}(\sigma_j, H) \leq I^{WY}(\rho, H)$ where $p_j = \operatorname{Tr}[E_j \rho E_j^\dagger]$ and $\sigma_j = E_j \rho E_j^\dagger / p_j$. They proved that the former holds in general and proved the latter holds for two-dimensional systems, while they left the higher dimensional cases as a conjecture.

Our resource-theoretic approach immediately proves these relations at the most general level: for general dimensions and for any skew information. To see this, note that the condition $[E_j, H] = 0$, $\forall j$ implies that M is a covariant operation and $E_j \cdot E_j^\dagger$ are covariant completely-positive trace non-increasing maps. Then, these relations follow from the monotonicity and selective monotonicity of the skew informations as asymmetry monotones.

4 Superadditivity

Superadditivity of the skew informations refers to the property that the skew informations for total states are never less than the sum of local skew informations: $I^f(\rho_{1\ldots n}, H_{1\ldots n}) \geq \sum_{k=1}^n I^f(\rho_k, H_k)$ for any $n \in \mathbb{N}$, $\rho_{1\ldots n}$, and $H_{1\ldots n}$ with $H_{1\ldots n} = \sum_{k=1}^n H_k \otimes \mathbb{I}_{\bar{k}}$ where $\rho_k = \operatorname{Tr}_{\bar{k}} \rho_{1\ldots n}$ is the reduced state on the k th subsytem, and $\mathbb{I}_{\bar{k}}$ is the identity operator acting on the subsystems other than k th subsystem.

Here, we employ an operational argument to show the violation of superadditivity relation for any choice of f.

Theorem 1. *Any skew information I^f cannot be superadditive.*

The idea is that one can construct a covariant operation which creates larger sum of the local asymmetry than the global asymmetry. For such a covariant operation, we consider the protocol proposed by Åberg [22], which approximately implements a desired unitary only using covariant operations and a resource state. What is interesting about the protocol is that it is "perfectly repeatable" in the sense that one can reuse the resource state again and again without degrading the quality of the implementation of the unitary. Thus, one can keep applying the approximate unitary that creates local asymmetry forever while the global asymmetry is upper bounded by the asymmetry of the initial resource state because of the covariance of the protocol. This observation naturally leads to the fact that any skew information is prohibited from being superadditive as a valid asymmetry monotone. The detailed proof can be found in Ref. [1].

Weak superadditivity Although the superadditivity does not hold in general, one can still ask whether some weaker version of superadditivity holds. We prove such weak superaditivity relation by an operational approach, proving the conjecture posed in Ref. [16] as a special case.

Theorem 2. *For any $\rho_{1\dots k}$ and $H_{12\dots k} = \sum_j H_j \otimes \mathbb{I}_{\bar{j}}$, $I^f(\rho_{1\dots k}, H_{12\dots k}) \geq \frac{1}{k}\sum_{j=1}^k I^f(\rho_j, H_j)$ holds. Moreover, $\frac{1}{k}$ is the maximum constant for $\beta(k)$ such that $I^f(\rho_{1\dots k}, H_{12\dots k}) \geq \beta(k)\sum_{j=1}^k I^f(\rho_j, H_j)$ holds for any $\rho_{1\dots k}$ and $H_{12\dots k}$.*

The first part can be immediately obtained by using the monotonicity under partial trace. As for the second part, we show that if $\beta(k)$ is larger than $1/k$, the sum of local asymmetry must grow sublinearly with respect to the number of qubits. However, becaue Åberg's protocol is perfectly repeatable, one can construct a state whose local asymmetry grows linearly, which leads to the contradiction. A detailed proof can be found in Ref. [1].

Distributed quantum clocks The above Theorems provide an interesting implication for the situation where quantum clocks are distributed to multiple parties. Suppose that k parties $A_1, A_2, \dots, A_k$ share some number of copies of state $\rho_{1\dots k}$ while each party only has access to their reduced state and does not know the description of the global state $\rho_{1\dots k}$. Assume also that they share a limited amount of entanglement among each other, which only enables them to send a limited number of qubits by quantum teleportation although they can freely make classical communication. This is a situation relevant to the setups such as quantum network and distributed quantum computation [23, 24].

From the perspective that the skew informations are asymmetry monotones, it is natural to see that they serve as quantifiers for how useful they are for metrological tasks [9]. In particular, when the conserved quantity is chosen as the Hamiltonian, the skew informations may be seen as the quality of the state as a quantum clock [25]. Suppose that A_1 desires to possess a quantum clock with high precision that requires the amount of skew information $I^f_{\mathrm{th}} > I^f(\rho_1, H_1)$. In such a situation, A_1 could ask the other parties to send their states via quantum teleportation, but A_1 would like to make sure that it will be indeed possible to achieve the desired level of asymmetry by doing so because otherwise the precious entanglement will be wasted. To this end, suppose A_1 asks the other parties to measure the skew information of their own reduced state (by, for instance, a method provided by Ref. [26]) and report it back by classical communication. A_1 then tries to infer the total skew information she would obtain $I^f(\rho_{1\dots k}, H_{1,\dots,k})$ by reported values $I_f(\rho_j, H_j),\ j = 2, \dots, k$.

Theorem 1 warns A_1 not to make a naive decision in which she asks the other parties to send their states when $\sum_{j=1}^k I^f(\rho_j, H_j) \geq I^f_{\mathrm{th}}$ because it may be the case that $\rho_{1\dots k}$ significantly violates the superadditivity relation such that $I^f(\rho_{1\dots k}, H_{1,\dots,k}) < I^f_{\mathrm{th}}$. On the other hand, Theorem 2 ensures that if A_1 asks the other parties to send their states only when $\frac{1}{k}\sum_{j=1}^k I^f(\rho_j, H_j) \geq I^f_{\mathrm{th}}$, she will certainly obtain the enough amount of asymmetry to implement a quantum clock with the desired accuracy. Moreover, it is the best possible she can do because $1/k$ is the maximum constant to ensure that $I^f(\rho_{1\dots k}, H_{1,\dots,k}) \geq I^f_{\mathrm{th}}$ holds as shown in Theorem 2.

5 Conclusions

We analyzed properties of the general family of skew informations from operational perspectives in the context of resource theory of asymmetry. We showed that such operational approach can give clearer physical meanings as well as simpler proofs of some of the properties of the skew informations. We in particular provided the first full analytical proof for violation of superadditivity property and prove weak superadditivity relations valid for general skew informations. We also discussed an application of our results to a situation where quantum clocks are distributed to multiple parties, providing the optimal strategy for a single party to ensure that the enough amount of asymmetry will be obtained after costly quantum communications.

Our results not only indicate much potential of analyzing information-theoretic quantities from operational perspectives, motivating to extend the analysis to a broader class of the quantities beyond the skew informations, but also shed new light on further applications of resource-theoretic considerations.

References

[1] Ryuji Takagi. Skew informations from an operational view via resource theory of asymmetry. *arXiv preprint arXiv:1812.10453*, 2018.

[2] E.P. Wigner. Die messung quantenmechanischer operatoren. *Z. Physik*, 131:101, 1952.

[3] Huzihiro Araki and Mutsuo M. Yanase. Measurement of quantum mechanical operators. *Phys. Rev.*, 120:622–626, Oct 1960.

[4] Mutsuo M. Yanase. Optimal measuring apparatus. *Phys. Rev.*, 123:666–668, Jul 1961.

[5] E. P. Wigner and M. M. Yanase. Information contents of distribution. *Proceedings of the National Academy of Sciences of the United States of America*, 49:910, June 1963.

[6] Frank Hansen. Metric adjusted skew information. *Proceedings of the National Academy of Sciences*, 105(29):9909–9916, 2008.

[7] Shun-ichi Amari and Hiroshi Nagaoka. *Methods of information geometry*, volume 191. American Mathematical Soc., 2007.

[8] Eric Chitambar and Gilad Gour. Quantum resource theories. *Rev. Mod. Phys.*, 91:025001, Apr 2019.

[9] Gilad Gour and Robert W Spekkens. The resource theory of quantum reference frames: manipulations and monotones. *New J. Phys.*, 10(3):033023, 2008.

[10] Iman Marvian. *Symmetry, asymmetry and quantum information*. PhD thesis, 2012.

[11] Iman Marvian and Robert W Spekkens. Extending noethers theorem by quantifying the asymmetry of quantum states. *Nature communications*, 5:3821, 2014.

[12] Chao Zhang, Benjamin Yadin, Zhi-Bo Hou, Huan Cao, Bi-Heng Liu, Yun-Feng Huang, Reevu Maity, Vlatko Vedral, Chuan-Feng Li, Guang-Can Guo, and Davide Girolami. Detecting metrologically useful asymmetry and entanglement by a few local measurements. *Phys. Rev. A*, 96:042327, Oct 2017.

[13] Elliott H Lieb. Convex trace functions and the wigner-yanase-dyson conjecture. *Advances in Mathematics*, 11(3):267 – 288, 1973.

[14] Frank Hansen. The wigner-yanase entropy is not subadditive. *Journal of Statistical Physics*, 126(3):643–648, Feb 2007.

[15] Robert Seiringer. On the failure of subadditivity of the wigner–yanase entropy. *Letters in Mathematical Physics*, 80(3):285–288, Jun 2007.

[16] Liang Cai, Nan Li, and Shunlong Luo. Weak superadditivity of skew information. *Journal of Physics A: Mathematical and Theoretical*, 41(13):135301, 2008.

[17] Shunlong Luo. Notes on superadditivity of wigner–yanase–dyson information. *Journal of Statistical Physics*, 128(5):1177–1188, Sep 2007.

[18] Shunlong Luo and Qiang Zhang. Superadditivity of wigner-yanase-dyson information revisited. *Journal of Statistical Physics*, 131(6):1169–1177, Jun 2008.

[19] E. A. Morozova and N. N. Chentsov. Markov invariant geometry on manifolds of states. *Journal of Soviet Mathematics*, 56(5):2648–2669, Oct 1991.

[20] X Li, D Li, H Huang, and LC Kwek. Averaged wigner-yanase-dyson information as a quantum uncertainty measure. *Eur. Phys. J. D*, 64(1):147, 2011.

[21] Shunlong Luo and Qiang Zhang. Skew information decreases under quantum measurements. *Theoretical and Mathematical Physics*, 151(1):529–538, Apr 2007.

[22] Johan Åberg. Catalytic coherence. *Phys. Rev. Lett.*, 113:150402, Oct 2014.

[23] L.-M. Duan and C. Monroe. Colloquium: Quantum networks with trapped ions. *Rev. Mod. Phys.*, 82:1209–1224, Apr 2010.

[24] A Pirker, J Wallnfer, and W Dr. Modular architectures for quantum networks. *New Journal of Physics*, 20(5):053054, may 2018.

[25] D. Janzing and T. Beth. Quasi-order of clocks and their synchronism and quantum bounds for copying timing information. *IEEE Transactions on Information Theory*, 49(1):230–240, Jan 2003.

[26] Tomohiro Shitara and Masahito Ueda. Determining the continuous family of quantum fisher information from linear-response theory. *Phys. Rev. A*, 94:062316, Dec 2016.

General resource theories in quantum mechanics and beyond: operational characterization via discrimination tasks

Ryuji Takagi[1] * Bartosz Regula[2] † Kaifeng Bu[3 4] Zi-Wen Liu[5 1] Gerardo Adesso[6]

[1] *Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[2] *School of Physical and Mathematical Sciences, Nanyang Technological University, 637371, Singapore*
[3] *School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, People's Republic of China*
[4] *Department of Physics, Harvard University, Cambridge, MA 02138, USA*
[5] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[6] *School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom*

Abstract. One of the central problems in the study of resource theories is to provide a given resource with an operational meaning, characterizing physical tasks in which the resource can give an explicit advantage over all resourceless objects. We show that this can always be accomplished for all convex resource theories — describing the resource content of not only states, but also measurements and channels — both within quantum mechanics and in general probabilistic theories (GPTs). We in particular find that discrimination tasks provide a unified operational description for quantification and manipulation of resources by showing that the family of robustness resource measures can be understood as the maximum advantage provided by any physical resource in several different discrimination tasks, as well as establishing that such discrimination problems can fully characterize the allowed transformations within the given resource theory. Our results establish a fundamental connection between the operational tasks of discrimination and core concepts of resource theories — the geometric quantification of resources and resource manipulation — valid for all physical theories beyond quantum mechanics with no additional assumptions about the structure of the GPT required.

1 Introduction

A rigorous understanding of quantum resources is one of the ultimate goals in quantum information science. In addition to the apparent theoretical interest, it also has high relevance to burgeoning quantum information technologies such as quantum communication [3, 4], quantum cryptography [5, 6], and quantum computation [7, 8]. Quantum resource theories [9] have recently attracted much attention as powerful tools which offer formal frameworks allowing for the characterization of quantification and manipulation of intrinsic resources associated with quantum systems.

Although applications of the resource-theoretic framework have enhanced systematic studies of many physical settings, these setting-specific resource theories do not tell us much about how to understand the individual properties and results in a unified fashion. One could then wonder whether the generality of the framework allows one to go beyond specific examples and obtain results applicable to a broad class of settings, thus providing a unified picture of resources in general. A complete study of which features are universal among all resources, stemming from only the very foundations of quantum mechanics, therefore remains a major area of investigation, and such a general approach has recently gained much attention [9–18]. In fact, one can pose an even more fundamental question: can common features of resource theories be understood without relying on quantum mechanics at all? This motivates us to extend the framework of resource theories to general probabilistic theories (GPTs) [19–22], a family of physical theories which includes classical and quantum probability theory as special cases, and investigate a unified characterization of general resources in the extensive formalism of GPTs rather than limiting it to quantum mechanics.

In our works [1, 2], we contribute to advancing general resource theories with regard to one of the central questions that can be asked about them: their operational characterization. As the very word "resource" suggests, understanding the operational aspects of resources — how they can be utilized for physical tasks, and what limitations a resource theory places on the conversion of physical resources — has central importance both theoretically and practically. However, it frequently requires resource-specific approaches and does not easily generalize to encompass all physically relevant resource theories, and it is thus highly desired to find a fundamental class of operational tasks that would allow for the understanding of the resourcefulness of a given physical property in general settings. Here, we solve this problem at the most general level — we characterize quantification and manipulation of resources in general convex resource theories defined in any GPT for not only states, but also measurements and channels, in terms of the fundamental tasks of state and channel discrimination. Our results establish tools for the resource quantification and endow fundamental resource measures called *robustness measures* [17, 23–25] with an explicit operational interpretation as the

*rtakagi@mit.edu
†bartosz.regula@gmail.com

advantage that a physical object can provide in various discrimination tasks, and show that such discrimination tasks fully characterize the conversion between states or measurements with free operations of the given resource theory. Our results indicate that many physical quantities, seemingly different and unrelated to each other, can be understood in a unified way and are all encompassed together in the operational perspective of resource theories.

2 Quantification of resources and discrimination tasks

Channel discrimination is one of the most fundamental operational tasks in quantum information theory [26–33] and in GPTs [19, 20, 34–36] where one is to decide which channel was applied to the input state by making a measurement on the output. The average probability of successfully discriminating a channel sampled from the channel ensemble $\{p_i, \Lambda_i\}_i$ with input state ρ and measurement $\{M_i\}_i$ where each M_i is an effect (known as a POVM element in quantum mechanics) is written as $p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \rho) = \sum_i p_i \langle M_i, \Lambda_i(\rho)\rangle$. Note that the canonical bilinear form $\langle E, \omega\rangle$ is understood as the Hilbert-Schmidt inner product $\text{Tr}[E\omega]$ in quantum mechanics. Our first result shows that for any choice of convex and closed set of free states $\mathcal{F}$, any resource state is helpful for some channel discrimination task. This in particular provides clear operational meaning for all the *bound resource states* (e.g. bound entangled [37], magic [38, 39], and genuine non-Gaussian states [40]), whose applicability in physical tasks is often uncertain.

Theorem 1. *Let $\mathcal{F}$ be a convex and closed set of free states. Then, $\rho \notin \mathcal{F}$ if and only if there exist a channel ensemble $\{p_i, \Lambda_i\}$ such that*

$$\frac{\max_{\{M_i\}} p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \rho)}{\max_{\sigma\in\mathcal{F}} \max_{\{M_i\}} p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \sigma)} > 1.$$

The next natural question is about quantification: what is the relation between the resource contents of the given state and the advantage in channel discrimination that it can provide? To this end, we consider the *generalized robustness* resource measure, which can be defined for any convex and closed set of free states $\mathcal{F}$ as $R_{\mathcal{F}}(\rho) = \min\left\{r \,\middle|\, \frac{\rho+r\tau}{1+r} \in \mathcal{F},\ \tau \in D\right\}$ where D refers to the set of all states — that is, $R_{\mathcal{F}}$ corresponds to the least amount of noise (in the form of convex admixtures) that can destroy the resource content of a given state. We will quantify the advantage that a quantum state ρ provides over all free states $\mathcal{F}$ in the discrimination of $\{p_i, \Lambda_i\}_i$ using the measurement strategy $\{M_i\}_i$ as the ratio of $p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \rho)$ to the best success probability when using a free input state, $\max_{\sigma\in\mathcal{F}} p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \sigma)$. The following result shows explicitly that, in any convex resource theory, the maximal such ratio optimized over all choices of channel ensembles and measurement strategies is given precisely by the generalized robustness.

Theorem 2. *Let $\mathcal{F}$ be a convex and closed set of free states. Then, for any state ρ, it holds that*

$$\max_{\substack{\{p_i,\Lambda_i\}\\ \{M_i\}}} \frac{p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \rho)}{\max_{\sigma\in\mathcal{F}} p_{\text{succ}}(\{p_i, \Lambda_i\}, \{M_i\}, \sigma)} = 1 + R_{\mathcal{F}}(\rho).$$

This result ensures that the generalized robustness with respect to any choice of $\mathcal{F}$ admits an operational interpretation: it serves as an exact quantifier for the advantage that a given state enables in a class of channel discrimination problems. In Ref. [1], we also consider relaxing the constraints on measurements under the setting of theory of entanglement, coherence, and magic.

Next, we extend our consideration to measurements. Understanding the discriminative power of restricted sets of measurements is of central importance not only in characterizing the operational consequences precipitated by limitations of physically allowed measurements, but often also in studying the very fundamental structure of the underlying GPT [36, 41, 42]. We will show that a robustness measure associated with the measurement can provide a precise answer to the question. Let $\mathcal{M}_{\mathcal{F}}$ be some convex and closed set of measurements, which we will define as $\mathcal{M}_{\mathcal{F}} := \left\{\{M_i\}_i \in \mathcal{M} \,\middle|\, M_i \in \mathcal{E}_{\mathcal{F}}\ \forall i\right\}$ where $\mathcal{E}_{\mathcal{F}}$ is some chosen convex and closed set of free effects which we are able to access within the constraints of the given resource theory. We define the generalized robustness of measurement with respect to $\mathcal{E}_{\mathcal{F}}$ for a given measurement $\mathbb{M} = \{M_i\}_i$ as $R_{\mathcal{E}_{\mathcal{F}}}(\mathbb{M}) := \min\left\{r \,\middle|\, \frac{M_i+r\,N_i}{1+r} \in \mathcal{E}_{\mathcal{F}}\ \forall i,\ \{N_i\}_i \in \mathcal{M}\right\}$ where $\mathcal{M}$ is the set of all measurements. Consider now the state discrimination task where one is to discriminate states sampled from a state ensemble $\{p_i, \sigma_i\}_i$ by making a measurement $\{M_i\}_i$ with average success probability $p_{\text{succ}}(\{p_i, \sigma_i\}, \mathbb{M}) = \sum_i p_i \langle M_i, \sigma_i\rangle$.

Theorem 3. *Let $\mathcal{M}_{\mathcal{F}}$ be the set of measurements whose effects are elements of $\mathcal{E}_{\mathcal{F}}$. Then,*

$$\max_{\{p_i,\sigma_i\}} \frac{p_{\text{succ}}(\{p_i, \sigma_i\}, \mathbb{M})}{\max_{\mathbb{F}\in\mathcal{M}_F} p_{\text{succ}}(\{p_i, \sigma_i\}, \mathbb{F})} = 1 + R_{\mathcal{E}_{\mathcal{F}}}(\mathbb{M}).$$

The above Theorem establishes an explicit connection between the inherent resourcefulness of a given measurement and the advantage realized in state discrimination tasks with respect to a general set of free measurements, which ensures an operational interpretation to the generalized robustness of measurements in any resource theory corresponding to measurements. We additionally establish a connection between generalized robustness and single-shot information theory in Ref. [2].

However, states and measurements are not the only objects that can be regarded as resourceful — it is often natural to attribute resources to dynamical components of the system, i.e. *channels*,

in many physical situations in information processing. Analogously to the cases of states and measurements, for given convex and closed set of free channels $\mathcal{O}_\mathcal{F}$, we propose the generalized robustness measure for channel Λ with respect to $\mathcal{O}_\mathcal{F}$ as $R_{\mathcal{O}_\mathcal{F}}(\Lambda) \coloneqq \min_\Theta \left\{ r \mid \frac{\Lambda + r\,\Theta}{1+r} \in \mathcal{O}_\mathcal{F},\ \Theta \in \mathcal{T} \right\}$ where $\mathcal{T}$ is the set of all channels. [1] To see the operational meaning of this measure, let us consider the problem of discriminating an ensemble of quantum states by an application of the channel $\mathbb{I} \otimes \Lambda$, with average success probability $p_{\mathrm{succ}}(\{p_j, \sigma_j\}, \{M_j\}, \mathbb{I} \otimes \Lambda) = \sum p_j \operatorname{Tr}\left[\mathbb{I} \otimes \Lambda(\sigma_j) M_j\right]$. We then have the following result, characterizing the robustness measure as the maximum advantage that the given channel provides for such channel-assisted state discrimination tasks.

Theorem 4. *Let $\mathcal{O}_\mathcal{F}$ be a convex and closed set of free channels. Then*

$$\max_{\mathcal{A}, \{M_j\}} \frac{p_{\mathrm{succ}}(\mathcal{A}, \{M_j\}, \mathbb{I} \otimes \Lambda)}{\max_{\Xi \in \mathcal{O}_\mathcal{F}} p_{\mathrm{succ}}(\mathcal{A}, \{M_j\}, \mathbb{I} \otimes \Xi)} = 1 + R_{\mathcal{O}_\mathcal{F}}(\Lambda)$$

where $\mathcal{A}$ refers to a state ensemble. One can take another approach to quantify resourcefulness of channels based on the underlying theory of states. We introduce suitable measures for this approach and provide their operational characterization in Ref. [2].

3 Manipulation of resources and discrimination tasks

Finding the necessary and sufficient conditions for the existence of transformation between a given input object and output object by means of free operations is one of the most important questions to address, as it underlies the operational capabilities of a given resource theory. We call a family of monotones a *complete set of monotones* if it fully characterizes the necessary and sufficient conditions for the existence of a free transformation. Such monotones were found in specific settings [15, 44–53], but no set of general conditions with clear operational meaning was previously known to provide a comprehensive characterization of transformations in general resource theories.

We will now show that performance enhanced by a state or measurement in a class of channel or state discrimination tasks precisely serves as a complete set of monotones for general resource theories defined in any GPT. This, together with the results obtained above, completes a full operational characterization of general resource theories of states and measurements, and strengthens the connection between resource theories and discrimination tasks. In this abstract, we only discuss the state transformation; the argument about measurement transformations goes analogously, and the details can be found in [2].

Let $\mathcal{O}$ be a convex and closed set of free operations. Consider the channel discrimination over all valid choices of channel ensembles, but allow for the application of a single chosen prior transformation from the set $\mathcal{O}$ to the ensemble before applying the channels to be discriminated. The success probability for this task for a choice of channel ensemble $\{p_i, \Lambda_i\}_i$ and measurement $\{M_i\}_i$ is given by $\tilde{p}_{\mathrm{succ}}(\{p_i\}, \{\Lambda_i\}, \{M_i\}, \omega) \coloneqq \max_{\Xi \in \mathcal{O}} \sum_i p_i \left\langle M_i, \Lambda_i \circ \Xi(\omega) \right\rangle$. The following result shows that this success probability serves as a complete set of monotones for state transformations under the free operations $\mathcal{O}$.

Theorem 5. *There exists $\Lambda \in \mathcal{O}$ such that $\omega' = \Lambda(\omega)$ if and only if it holds that $\tilde{p}_{\mathrm{succ}}(\{p_i\}, \{\Lambda_i\}, \{M_i\}, \omega) \geq \tilde{p}_{\mathrm{succ}}(\{p_i\}, \{\Lambda_i\}, \{M_i\}, \omega')$ for all channel ensembles $\{p_i, \Lambda_i\}$ and measurements $\{M_i\}$.*

In fact, we find that the Theorem can be greatly simplified: in particular, it is sufficient to consider only two-outcome measurements to fully describe the transformations allowed within any resource theory, thus providing an accessible method of characterizing resourceful state manipulation. We discuss several other connections between state transformations and discrimination tasks in [2].

4 Concluding remarks

We provided a general operational characterization of quantification and manipulation of resources — two core concepts of resource theories — in terms of state and channel discrimination tasks. The generality of our works is three-fold: our formulations encompass general convex resource theories, are applicable to all types of resource objects (states, measurements, and channels), and major parts of the results are valid in all general probabilistic theories beyond quantum mechanics.

In addition to providing fundamental insights spanning a broad class of physical theories, the results are immediately applicable to a wide range of physical resources in quantum information theory. The resource theories of coherence, (bi- or multipartite) entanglement, magic, athermality, asymmetry, and many others all fit the framework introduced herein and therefore all of our results apply to them immediately. In the case of measurements, many significant insights can be gained from studying classes of measurements such as separable, PPT, incoherent, or Pauli measurements, all of which are again special cases of the resource theories considered in our works. The generality of the results also provides insights into the foundation of quantum mechanics, as our results in particular show an equivalence between the robustness measures (a priori a geometric concept) and the advantage provided in discrimination tasks in any GPT; therefore, one cannot hope to separate a given theory from quantum mechanics by finding a gap between these two quantities. The results also provide an experimentally accessible way of bounding resource measures as well as characterizing resource transformations in any GPT by relating them with discrimination tasks.

[1] For the simplicity of the discussion, here we will limit ourselves to quantum theory although it can be easily generalized to GPTs under suitable assumptions [43].

References

[1] Ryuji Takagi, Bartosz Regula, Kaifeng Bu, Zi-Wen Liu, and Gerardo Adesso. Operational advantage of quantum resources in subchannel discrimination. *Phys. Rev. Lett.*, 122:140402, Apr 2019. published as an Editors' Suggestion.

[2] Ryuji Takagi and Bartosz Regula. General resource theories in quantum mechanics and beyond: operational characterization via discrimination tasks. *arXiv preprint arXiv:1901.08127*, 2019.

[3] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023, 2008.

[4] L.-M. Duan and C. Monroe. Colloquium: Quantum networks with trapped ions. *Rev. Mod. Phys.*, 82:1209–1224, Apr 2010.

[5] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing int. In *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, pages 175–9, 1984.

[6] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[7] Peter W Shor. Fault-tolerant quantum computation. In *Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on*, pages 56–65. IEEE, 1996.

[8] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127–137, Jan 1998.

[9] Eric Chitambar and Gilad Gour. Quantum resource theories. *Rev. Mod. Phys.*, 91:025001, Apr 2019.

[10] Michal Horodecki and Jonathan Oppenheim. (Quantumness in the context of) Resource theories. *Int. J. Mod. Phys. B*, 27:1345019, 2013.

[11] Fernando G. S. L. Brandão and Gilad Gour. Reversible framework for quantum resource theories. *Phys. Rev. Lett.*, 115:070503, 2015.

[12] Lídia Del Rio, Lea Kraemer, and Renato Renner. Resource theories of knowledge. *arXiv preprint arXiv:1511.08818*, 2015.

[13] Bob Coecke, Tobias Fritz, and Robert W. Spekkens. A mathematical theory of resources. *Inf. Comput.*, 250:59–86, 2016.

[14] Zi-Wen Liu, Xueyuan Hu, and Seth Lloyd. Resource destroying maps. *Phys. Rev. Lett.*, 118:060502, Feb 2017.

[15] Gilad Gour. Quantum resource theories in the single-shot regime. *Phys. Rev. A*, 95:062314, Jun 2017.

[16] Anurag Anshu, Min-Hsiu Hsieh, and Rahul Jain. Quantifying resources in general resource theory with catalysts. *Phys. Rev. Lett.*, 121:190504, Nov 2018.

[17] Bartosz Regula. Convex geometry of quantum resource quantification. *J. Phys. A: Math. Theor.*, 51:045303, 2018.

[18] Ludovico Lami, Bartosz Regula, Xin Wang, Rosanna Nichols, Andreas Winter, and Gerardo Adesso. Gaussian quantum resource theories. *Phys. Rev. A*, 98:022335, 2018.

[19] G. Ludwig. *An Axiomatic Basis for Quantum Mechanics: Volume 1 Derivation of Hilbert Space Structure*. Springer-Verlag, Berlin Heidelberg, 1985.

[20] A. Hartkämper and Hans Neumann, editors. *Foundations of Quantum Mechanics and Ordered Linear Spaces*. Springer, 1974.

[21] E. B. Davies and J. T. Lewis. An operational approach to quantum probability. *Commun.Math. Phys.*, 17:239–260, 1970.

[22] Ludovico Lami. *Non-Classical Correlations in Quantum Mechanics and Beyond*. PhD thesis, Universitat Autònoma de Barcelona, 2018.

[23] Guifré Vidal and Rolf Tarrach. Robustness of entanglement. *Phys. Rev. A*, 59:141–155, Jan 1999.

[24] Aram W. Harrow and Michael A. Nielsen. Robustness of quantum gates in the presence of noise. *Phys. Rev. A*, 68:012308, 2003.

[25] Michael Steiner. Generalized robustness of entanglement. *Phys. Rev. A*, 67:054305, May 2003.

[26] A.S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337 – 394, 1973.

[27] C. W. Helstrom. *Quantum detection and estimation theory*. New York: Academic Press, 1976.

[28] A. Y. Kitaev. Quantum computations: Algorithms and error correction. *Russ. Math. Surv.*, 52:1191–1249, 1997.

[29] Anthony Chefles. Quantum state discrimination. *Contemp. Phys.*, 41:401–424, 2000.

[30] Andrew M. Childs, John Preskill, and Joseph Renes. Quantum information and precision measurement. *J. Mod. Opt.*, 47:155–176, 2000.

[31] A. Acìn. Statistical Distinguishability between Unitary Operations. *Phys. Rev. Lett.*, 87:177901, 2001.

[32] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, 2015.

[33] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, Cambridge, 2018.

[34] Gen Kimura, Koji Nuida, and Hideki Imai. Distinguishability measures and entropies for general probabilistic theories. *Reports on Mathematical Physics*, 66:175–206, 2010.

[35] Joonwoo Bae, Dai-Gyoung Kim, and Leong-Chuan Kwek. Structure of Optimal State Discrimination in Generalized Probabilistic Theories. *Entropy*, 18:39, 2016.

[36] Ludovico Lami, Carlos Palazuelos, and Andreas Winter. Ultimate Data Hiding in Quantum Mechanics and Beyond. *Commun. Math. Phys.*, 361:661, 2018.

[37] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80:5239–5242, Jun 1998.

[38] Earl T. Campbell and Dan E. Browne. Bound states for magic state distillation in fault-tolerant quantum computation. *Phys. Rev. Lett.*, 104:030503, Jan 2010.

[39] Victor Veitch, Christopher Ferrie, David Gross, and Joseph Emerson. Negative quasi-probability as a resource for quantum computation. *New J. Phys.*, 14(11):113011, 2012.

[40] Ryuji Takagi and Quntao Zhuang. Convex resource theory of non-gaussianity. *Phys. Rev. A*, 97:062337, Jun 2018.

[41] William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of Quantum States Under Restricted Families of Measurements with an Application to Quantum Data Hiding. *Commun. Math. Phys.*, 291:813–843, 2009.

[42] Guillaume Aubrun, Ludovico Lami, Carlos Palazuelos, Stanisław J Szarek, and Andreas Winter. Universal gaps for xor games from estimates on tensor norm ratios. *arXiv preprint arXiv:1809.10616*, 2018.

[43] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Probabilistic theories with purification. *Phys. Rev. A*, 81:062348, 2010.

[44] M. A. Nielsen. Conditions for a Class of Entanglement Transformations. *Phys. Rev. Lett.*, 83:436–439, 1999.

[45] Francesco Buscemi, Michael Keyl, Giacomo Mauro D'Ariano, Paolo Perinotti, and Reinhard F. Werner. Clean positive operator valued measures. *Journal of Mathematical Physics*, 46(8):082109, 2005.

[46] Francesco Buscemi. All Entangled Quantum States Are Nonlocal. *Phys. Rev. Lett.*, 108:200401, 2012.

[47] Michal Horodecki and Jonathan Oppenheim. Fundamental limitations for quantum and nanoscale thermodynamics. *Nat. Commun.*, 4:2059, 2013.

[48] F. Buscemi. Degradable channels, less noisy channels, and quantum statistical morphisms: An equivalence relation. *Probl Inf Transm*, 52:201–213, 2016.

[49] Francesco Buscemi and Gilad Gour. Quantum relative Lorenz curves. *Phys. Rev. A*, 95:012110, 2017.

[50] F. Buscemi. Comparison of noisy channels and reverse data-processing theorems. In *2017 IEEE Information Theory Workshop (ITW)*, pages 489–493, Nov 2017.

[51] Denis Rosset, Francesco Buscemi, and Yeong-Cherng Liang. Resource Theory of Quantum Memories and Their Faithful Verification with Minimal Assumptions. *Phys. Rev. X*, 8:021033, 2018.

[52] Gilad Gour, David Jennings, Francesco Buscemi, Runyao Duan, and Iman Marvian. Quantum majorization and a complete set of entropic conditions for quantum thermodynamics. *Nat. Commun.*, 9:5352, 2018.

[53] Paul Skrzypczyk and Noah Linden. Robustness of measurement, discrimination games, and accessible information. *Phys. Rev. Lett.*, 122:140403, Apr 2019.

Experimental realization of a quantum autoencoder via a universal two-qubit unitary gate

Chang-Jiang Huang,[1,2] Qi Yin,[1,2] Jun-Feng Tang,[1,2] Daoyi Dong,[3]
Guo-Yong Xiang,[1,2,*] Chuan-Feng Li,[1,2] and Guang-Can Guo[1,2]

[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*
[2]*CAS Center For Excellence in Quantum Information and Quantum Physics*
[3]*School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia*

(Dated: May 22, 2019)

As a ubiquitous aspect of modern information technology, data compression has a wide range of applications. Therefore, quantum autoencoder which can compress quantum information into a reduced space is fundamentally important to achieve atomatical data compression in the field of quantum information. Such a quantum autoencoder can be implemented through training the parameters of a quantum device using machine learning. In this paper, we experimentally realize a universal two-qubit unitary gate and achieve a quantum autoencoder by applying machine learning. Also, this quantum autoencoder can be used to discriminate two groups of nonorthogonal states.

Introduction. A traditional autoencoder can compress classical data into a lower-dimensional space. As shown in Fig.1(a), the input information represnted by yellow dots can be compressed into fewer dots after the encoder ε and a decoder D can reconstruct the input data at the output. For a quantum device to realize an autoencoder, as illustrated in Fig.1(b), a parameterized unitary $U^j(p_1, p_2, \cdots, p_n)$ is trained as a quantum autoencoder where measurement results are considered and an optimization algorithm is employed. Fig.1(b) also indicates the scheme for our experiment: the core issue is to use the same 2-qubit unitary operator U to encode two 2-qubit states $|\varphi_1\rangle, |\varphi_2\rangle$ into two qubit states. In the classical scheme, we use stochastic gradient descent to optimize the parameterized unitary gate.

The setup for a universal two-qubit unitary gate is shown in Fig.1(c). It is well known that any binary quantum alternative of a photon can serve as a qubit. Thus, by choosing polarization and path degrees of freedom as two qubits, we can achieve the 2-qubit universal parameterized unitary gate combining path unitary gate with polarization gate [1].

In this paper, we experimentally realize a universal two-qubit unitary gate and achieve a quantum autoencoder based on the theoretical model in Ref. [2]. Our quantum autoencoder can encode two 2-qubit pure states $|\varphi_1\rangle, |\varphi_2\rangle$ into two qubit states without any other restriction. Besides encoding qubits, our device can also be used to discriminate two groups of nonorthogonal states.

Experiment Setup and Results. In the part of state preparation, since the $Mach-Zehnder$ interferometer in Fig.1(c) is difficult to realize and keep phase stable, we use two phase stable Sagnac interferometers to separately implement state preparation and M–Z interferometer. At the beginning (Fig.2(a)), photon pairs with wave length $\lambda = 808$ nm are created by type-I spontaneous parametric down-conversion (SPDC) in a nonlinear crystal (BBO). One photon is detected by a single-photon counting module (SPCM) as a trigger, another photon is prepared in the state of very pure horizonal polarization noted as $|H\rangle$ through a polarizer beam splitter (PBS). Then a half-wave plate (HWP) along with a PBS can control the path-bit of the photon.

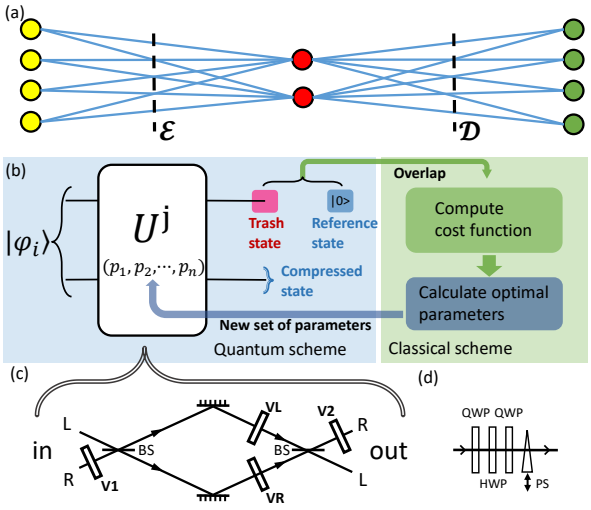


FIG. 1: (a) A graphical representation of encoding and decoding process. The map ε encodes the input data (yellow dots) into a lower-dimensional space (red dots). The decoder D can reconstruct the input data at the output (green dots). (b) The hybrid scheme for training a quantum autoencoder [16]. The input state $|\varphi_i\rangle$ is compressed by parameterized unitary $U^j(p_1, p_2, \cdots, p_n)$. When overlaps between trash state and reference state for all states in the input set are collected, a classical learning algorithm computes and sets a new group of parameters to the unitary $U^{j+1}(p_1, p_2, \cdots, p_n)$. (c) Universal two-qubit unitary gate composed of two beam splitters, two mirrors and four same single-qubit parts (V1,V2,VR,VL). (d) Each single-qubit part is composed of two QWPs, a HWP, and a phase shifter (PS).

In each path, a HWP and a quarter-wave plate (QWP) are used to control the polarization of the photon, as shown in Fig.2(b). Thus, we can produce any expected phase stable two-qubit state thanks to the first Sagnac interferometer.

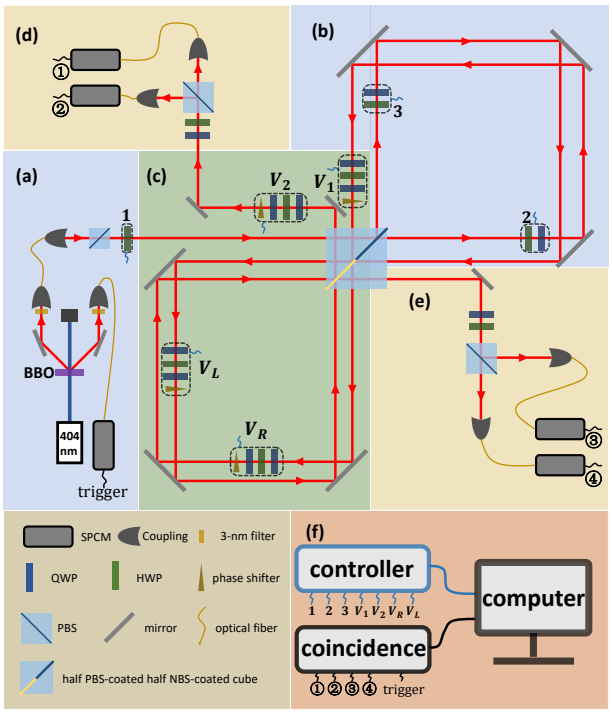


FIG. 2: Experiment setup for realizing a quantum autoencoder. The setup consists of three modules. (a)-(b) state preparation: Photon pairs are created by type-I SPDC through a BBO. One photon is set as a trigger and another photon is prepared in the state $|H\rangle$ through a PBS. Then a HWP along with a PBS can control the path-bit of the photon. In each path, a HWP and a QWP are used to control the polarization of the photon. (c)-(e) parameterized unitary U and measurements: The second Sagnac interferometer contains four unitary polarization operators V_1, V_2, V_R, V_L. Due to the structure of Sagnac interferometer, produced two-qubit states go through the NBS-coated surface twice. Thus, a parameterized universal two-qubit unitary gate is achieved. Then, a QWP, a HWP and a PBS can form any local measurements on polarization. (f) classical optimization algorithm: Our algorithm is mainly carried out by a computer and electronic-controlled devices.

The parameterized unitary U is realized with the help of the second Sagnac interferometer in Fig.2(c). It is worth noting that there is a special beam-splitter cube which is half PBS-coated and half coated by non-polarizer beam splitter (NBS) in the junction of two Sagnac interferometers. The second Sagnac interferometer contains four unitary polarization operators V_1, V_2, V_R, V_L. Each of them is composed of two quarter-wave plates (QWP), a half-wave plate (HWP), and a phase shifter (PS), which are all electronic-controlled. Meanwhile, due to the structure of Sagnac interferometer, produced two-qubit states go through the NBS-coated surface twice. Thus, as illustrated before, we finally achieve the parameterized universal two-qubit unitary gate.

We can construct any local measurements on polarization just by a QWP, a HWP and a PBS in Fig.2(d)-(e). Our classical programme is mainly carried out by a computer and electronic-controlled devices including phase shifter, HWPs and QWPs.

For characterization of our unitary gate, we estimate the process matrix using the maximum-likelihood method [3] for many different but significant gates such as identity gate, controlled-not gate, controlled-Z gate, controlled-Hadamard gate, SWAP gate, $\sqrt{iSWAP}$ gate and so on. Some results of the process tomography are shown in Fig.3. The real elements and the imaginary elements are plotted respectively, with ideal theoretical values overlaid. For clarity, we use red to represent positive and blue to represent negative. Our fidelity is computed by $\mathrm{tr}\sqrt{\sqrt{\chi_{exp}}\chi\sqrt{\chi_{exp}}}$. Here χ_{exp} is the experimental process matrix and χ is the theoretical process matrix. The average fidelity of our gates is 0.953.

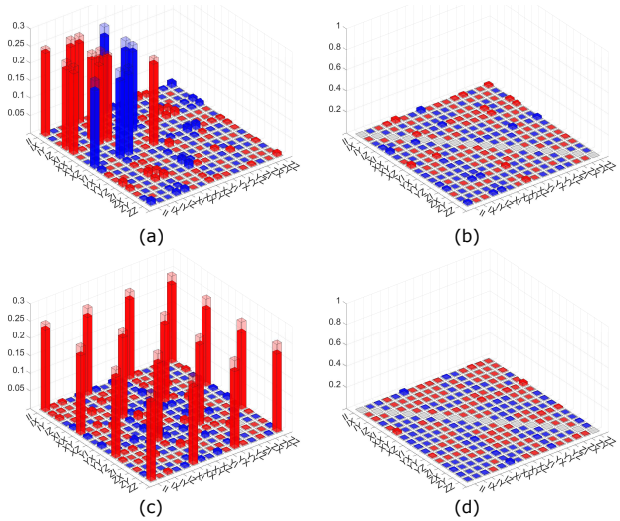


FIG. 3: Characterization of experimentally realized gates. A two-qubit gate can be described by its process matrix $\tilde{\chi}$. Specifically, each input state ρ is mapped to an output $\Sigma_{mn}\tilde{\chi}_{mn}\hat{E}_m\rho\hat{E}_n^\dagger$, where the summation is over all possible two-qubit Pauli operators $\hat{E}_k$. Here we plot the real elements in Fig.3(a) (Fig.3(c)) and the imaginary elements in Fig.3(b) (Fig.3(d)) of CNOT (SWAP), with ideal theoretical values overlaid. For clarity, we use red to represent positive and blue to represent negative. The fidelity of CNOT/SWAP is 0.957/0.948.

Now we turn to the core issue of encoding the quantum information into lower dimension. Our goal is to achieve a 2-qubit unitary operator U which can encode two 2-qubit states $|\varphi_1\rangle, |\varphi_2\rangle$ into two qubit states

$|\varphi_1'\rangle, |\varphi_2'\rangle$. For example, we encode two 2-qubit states $|RH\rangle, |LV\rangle$ into states $|\varphi_1'\rangle|R\rangle, |\varphi_2'\rangle|R\rangle$. Here $|R\rangle/|L\rangle$ stands for path qubit and $|H\rangle/|V\rangle$ stands for polarization qubit. Thus, we can trash the path qubit and obtain the compressed states $|\varphi_1'\rangle, |\varphi_2'\rangle$ which maintain the original quantum information totally in polarization qubit. Similarly, encoding the information into path qubit is also feasible. Fig.4(a) (Fig.4(b)) shows the result of encoding $\{|RH\rangle, |LV\rangle\}$ into path (polarization) qubit. Here infidelity is the cost funtion in our algorithm and iterations indicate the train process. Results of encoding another set of states $\{\frac{1}{2}|RD\rangle + \frac{\sqrt{3}}{2}|LV\rangle, |LV\rangle\}$ into path (polarization) qubit is shown in Fig.4(c) (Fig.4(d)). The performance of our quantum autoencoder is related to the experimental conditions such as imperfect NBS-coated surface, unbalanced coupling efficiency, and uneven wave plates. Though under these imperfect conditions, the cost funtion can still approach 0 after a few iterations.

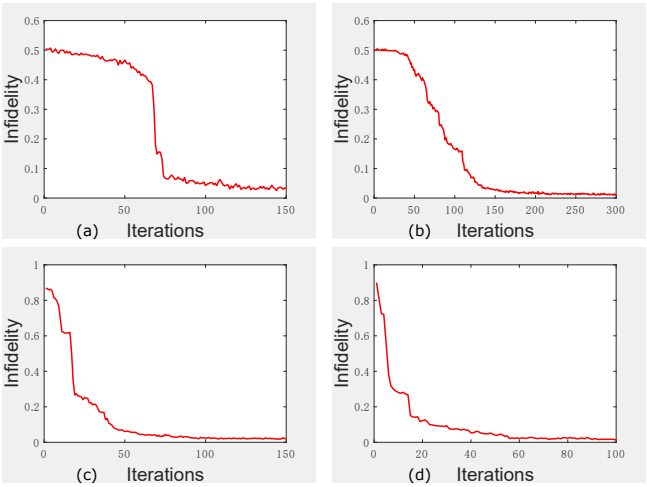


FIG. 4: The results of encoding two 2-qubit states into two qubit states. Here we show the results of encoding different initial states into different qubits (path/polarization). (a) encode $\{|RH\rangle, |LV\rangle\}$ into path qubit. (b) encode $\{|RH\rangle, |LV\rangle\}$ into polarization qubit. (c) encode $\{\frac{1}{2}|RD\rangle + \frac{\sqrt{3}}{2}|LV\rangle, |LV\rangle\}$ into path qubit. (d) encode $\{\frac{1}{2}|RD\rangle + \frac{\sqrt{3}}{2}|LV\rangle, |LV\rangle\}$ into polarization qubit. Here infidelity is the cost funtion in our algorithm and iterations indicate the train process.

Apart from encoding quantum information into lower dimension, we find our quantum autoencoder can also realize the discrimination between two different groups of nonorthogonal states by encoding different groups into orthogonal path/polarization qubits. For example, encode two groups of nonorthogonal states $\{|\phi_i\rangle\}, \{|\varphi_j\rangle\}$ into states $\{|\varphi_i'\rangle|R\rangle\}, \{|\varphi_j'\rangle|L\rangle\}$. Thus we can realize the bound of min-error discrimination between two different groups of nonorthogonal states after some iterations.

We follow the core principle in Ref. [4] to derive

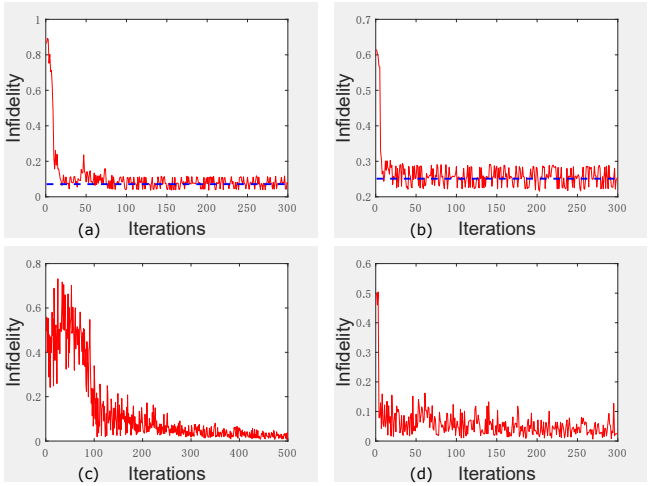


FIG. 5: The results of discriminating two different groups of nonorthogonal states. The bound for (a)-(b) is plotted in blue dashed line. (a) encode $\{\cos\theta_{1/2}|RH\rangle + \sin\theta_{1/2}|RV\rangle,\ \theta_{1/2} = \pm 4^\circ\}$ & $\{\cos\theta_{3/4}|RH\rangle + \sin\theta_{3/4}|RV\rangle,\ \theta_{3/4} = 60^\circ \pm 4^\circ\}$ into different polarization qubits. (b) encode $\{\cos\theta_{1/2}|RH\rangle + \sin\theta_{1/2}|RV\rangle,\ \theta_{1/2} = \pm 2^\circ\}$ & $\{\cos\theta_{3/4}|RH\rangle + \sin\theta_{3/4}|RV\rangle, \theta_{3/4} = 30^\circ \pm 2^\circ\}$ into different polarization qubits. (c) encode $\{\cos\theta_1|RH\rangle + \sin\theta_1|LH\rangle, \theta_1 \in [-50^\circ, 50^\circ]\}$ & $\{\cos\theta_2|RV\rangle + \sin\theta_2|LV\rangle, \theta_2 \in [-50^\circ, 50^\circ]\}$ into different path qubits, (d) encode $\{\cos\theta_1|RH\rangle + \sin\theta_1|RV\rangle, \theta_1 \in [-20^\circ, 20^\circ]\}$ & $\{\cos\theta_2|LH\rangle + \sin\theta_2|LV\rangle, \theta_2 \in [-20^\circ, 20^\circ]\}$ into different polarization qubits. Here infidelity is the cost funtion in our algorithm and iterations indicate the train process.

the error bound and the optimal strategies to realize the min-error discrimination between two groups. Some of the results are shown in Fig.5. The blue dashed line is the bound of min-error discrimination between two different groups of nonorthogonal states. We also show our agent's learning ability by encoding groups of path/polarization orthogonal states into orthogonal polarization/path states in Fig.5(c)-(d).

* Electronic address: gyxiang@ustc.edu.cn

[1] B.-G. Englert, C. Kurtsiefer, H. Weinfurter, Universal unitary gate for single-photon two-qubit states, Physical Review A 63 (3) (2001) 032303.
[2] J. Romero, J. P. Olson, A. Aspuru-Guzik, Quantum autoencoders for efficient compression of quantum data, Quantum Science and Technology 2 (4) (2017) 045001.
[3] M. Ježek, J. Fiurášek, Z. Hradil, Quantum inference of states and processes, Physical Review A 68 (1) (2003) 012305.
[4] C. W. Helstrom, Quantum detection and estimation theory, Journal of Statistical Physics 1 (2) (1969) 231–252.

Experimentally probing quantum communication in a superposition of causal orders

Yu Guo,[1,2] Xiao-Min Hu,[1,2] Zhi-Bo Hou,[1,2] Huan Cao,[1,2] Jin-Ming Cui,[1,2] Bi-Heng Liu,[1,2,*]
Yun-Feng Huang,[1,2] Chuan-Feng Li,[1,2,†] Guang-Can Guo,[1,2] and Giulio Chiribella[3,4,‡]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, People's Republic of China*
[2]*CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, P.R. China*
[3]*Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong, P.R. China*
[4]*Department of Computer Science, University of Oxford, Parks Road, Oxford, UK*

(Dated: July 3, 2019)

Abstract: Communication in a network generally takes place through a sequence of intermediate nodes connected by communication channels. In the standard theory of communication, it is assumed that the communication network is embedded in a classical spacetime, where the relative order of different nodes is well-defined. In principle, a quantum theory of spacetime could allow the order of the intermediate points between sender and receiver to be in a coherent superposition. Here we experimentally realise a table-top simulation of this exotic possibility, by transmitting quantum information through certain entanglement-breaking channels in an optical quantum switch.

Keywords: quantum communication, indefinite causal order, quantum switch

Introduction. The extension of the theory of communication to scenarios where quantum channels act a superposition of orders was recently addressed in a series of works [1–3]. These works demonstrated advantages over the standard communication model where the communication channels are quantum but their order is fixed, as it is normally assumed in the field of quantum Shannon theory [4]. For example, Ref. [1] showed that two completely depolarising channels acting in a superposition of two orders can transmit a non-zero amount of classical information, whereas in the standard model of quantum Shannon theory they would completely block any kind of information. Similar advantages arise in the transmission of quantum information [2], sometimes leading to a complete removal of the noise [3]. The advantages over the standard model of quantum communication suggest that quantum superpositions of spacetimes would have major consequences on quantum communication networks.

Here we experimentally test the consequences of the superposition of causal orders for quantum communication networks, demonstrating the possibility of heralded [2] and deterministic quantum communication [3] through channels that individually have zero quantum capacity. The experimental realisation of communication protocols using quantum channels in a superposition of orders is important not only as a simulation of communication in quantum spacetimes, but also as a step towards a new technology of quantum communication with control over multiple transmission lines.

Communication networks and superposition of orders.— In a network scenario, the communication between the sender and a receiver proceeds through a sequence of intermediate nodes, with the transmission between one node and the next described by a suitable quantum channel. Here we will consider the case of $n = 2$ communication channels, $\mathcal{E}$ and $\mathcal{F}$, the former connecting two intermediate nodes at spacetime points P and P', and the latter connecting two intermediate nodes at spacetime points Q and Q'.

In the standard setting, the causal relations among spacetime points are well-defined, and so is the order of the intermediate nodes between the sender and receiver. For example, one can have the order $P \preceq P' \preceq Q \preceq Q'$, indicating that signals can be transmitted from P to P', and then to Q and to Q'. Assuming for simplicity that no noise takes place in the transmission from P' to Q, this configuration leads to the overall channel $\mathcal{FE}$. In another spacetime configuration, one could have the order $Q \preceq Q' \preceq P \preceq P'$, corresponding to the channel $\mathcal{EF}$ (again, assuming that no noise takes place in the transmission from Q' to P). In either configurations, the sender and receiver are assumed to know the structure of spacetime, and therefore to know whether the overall channel is $\mathcal{EF}$ or $\mathcal{FE}$.

New possibilities arise when the background spacetime is treated quantum mechanically [2]. One can associate the basic configurations $P \preceq P' \preceq Q \preceq Q'$ and $Q \preceq Q' \preceq P \preceq P'$ to two orthogonal states $|0\rangle := |P \preceq P' \preceq Q \preceq Q'\rangle$ and $|1\rangle := |Q \preceq Q' \preceq P \preceq P'\rangle$, forming a basis for an effective two-dimensional quantum system, called the *order qubit*. The order qubit can be interpreted as a coarse-grained description of a quantum spacetime in which the communication network is embedded. Hereafter, the state of the order qubit will be denoted by ω.

The insertion of two quantum channels $\mathcal{E}$ and $\mathcal{F}$ into a quantum spacetime in the state ω can be described by the quantum SWITCH (QS) transformation [5, 6] $\mathcal{S}_\omega : (\mathcal{E}, \mathcal{F}) \mapsto \mathcal{S}_\omega(\mathcal{E}, \mathcal{F})$, defined as

$$\mathcal{S}_\omega(\mathcal{E}, \mathcal{F})(\rho) := \sum_{i,j} W_{ij} (\rho \otimes \omega) W_{ij}^\dagger, \tag{1}$$

with

$$W_{ij} := E_i F_j \otimes |0\rangle\langle 0| + F_j E_i \otimes |1\rangle\langle 1|, \tag{2}$$

where $\{E_i\}$ and $\{F_j\}$ are the Kraus operators of $\mathcal{E}$ and $\mathcal{F}$, respectively. Note that quantum switch is independent of the choice of $\{E_i\}$ and $\{F_j\}$.

We interpret the channel $\mathcal{S}_\omega(\mathcal{E},\mathcal{F})$ as describing the action of the channels $\mathcal{E}$ and $\mathcal{F}$ combined together in a superposition of orders depending on the state of the order qubit ω. In this scenario, it is assumed that the sender cannot encode information in the order qubit, but the receiver can access it and use to enhance the decoding. It is worth stressing that the transformation $\mathcal{S}_\omega : (\mathcal{E},\mathcal{F}) \mapsto \mathcal{S}_\omega(\mathcal{E},\mathcal{F})$ does not provide a way to bypass the channels $\mathcal{E}$ and $\mathcal{F}$, in the sense that there is no way for the sender and the receiver to transmit information independently of the channels $\mathcal{E}$ and $\mathcal{F}$ [2].

The interference between the two alternative orders provides dramatical advantages in both classical and quantum communications over standard quantum Shannon theory, as it was predicted theoretically in a number of examples [1–3]. All these examples involve pairs of Pauli channels, of the form $\mathcal{E}_{\vec{p}} = \sum_{i=0}^{3} p_i \sigma_i \rho \sigma_i$ and $\mathcal{F}_{\vec{q}} = \sum_{i=0}^{3} q_i \sigma_i \rho \sigma_i$, where $(\sigma_0,\sigma_1,\sigma_2,\sigma_3)$ are the Pauli matrices (I,X,Y,Z). Suppose that the two channels $\mathcal{E}_{\vec{p}}$ and $\mathcal{F}_{\vec{q}}$ are combined in a superposition of orders, with the control qubit is in the state $\omega = |+\rangle\langle+|$, corresponding to the uniform superposition $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$. From Equations (1)and (2), the resulting channel $\mathcal{S}_\omega(\mathcal{E}_{\vec{p}},\mathcal{F}_{\vec{q}})$ acts as

$$\mathcal{S}(\mathcal{E}_{\vec{p}},\mathcal{F}_{\vec{q}})(\rho) = r_+ \mathcal{C}_+(\rho) \otimes |+\rangle\langle+| + r_- \mathcal{C}_-(\rho) \otimes |-\rangle\langle-| \,, \tag{3}$$

where r_+ and r_- are the probabilities defined by $r_- := r_{12} + r_{23} + r_{13}$, $r_{ij} := p_i q_j + p_j q_i$, and $r_+ := 1 - r_-$ are probabilities, and $\mathcal{C}_+$ and $\mathcal{C}_-$ are the Pauli channels defined by

$$\mathcal{C}_+ = \frac{(\sum_{i=0}^{3} r_{ii}/2)\rho + \sum_{i=1}^{3} r_{0i}\, \sigma_i \rho \sigma_i}{r_+} \tag{4}$$

and

$$\mathcal{C}_- = \frac{[r_{12}\, \sigma_3 \rho \sigma_3 + r_{23}\, \sigma_1 \rho \sigma_1 + r_{31}\, \sigma_2 \rho \sigma_2]}{r_-} \,. \tag{5}$$

Hence, a receiver who measures the order qubit in the basis $\{|+\rangle,|-\rangle\}$ can separate the two channels $\mathcal{C}_+$ and $\mathcal{C}_-$, and adapt the decoding operations to them.

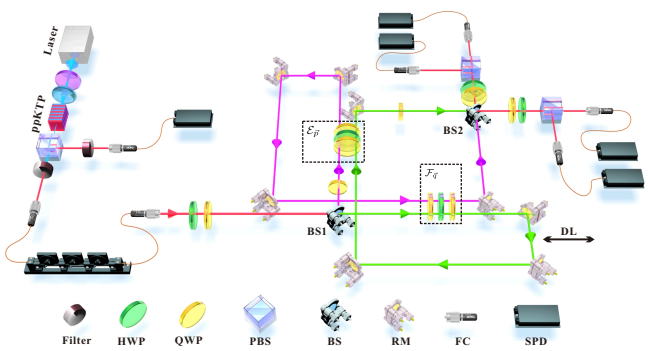


FIG. 1. Experimental setup.

Quantum communication with entanglement-breaking channels.— Consider a bit flip channel $\mathcal{B}_s(\rho) = (1-s)\,\rho + s\,\sigma_1\rho\sigma_1$ and phase flip channel $\mathcal{P}_t(\rho) = (1-t)\,\rho + t\,\sigma_3\rho\sigma_3$, corresponding to Pauli channels $\mathcal{E}_{\vec{p}}$ and $\mathcal{F}_{\vec{q}}$ with $\vec{p} = (1-s,s,0,0)$ and $\vec{q} = (1-t,0,0,t)$, respectively [2]. For $s = t = 1/2$, the two channels are entanglement-breaking, and therefore unable to transmit any quantum information. In contrast, the channel $\mathcal{C}_-$ of Equation (5) is the unitary gate σ_2, and therefore it allows for the noiseless heralded transmission of a qubit, meaning that the receiver can decode the message without any error through the channel $\mathcal{C}_-$.

The possibility of noiseless heralded quantum communication is an important difference between the communication model with independent quantum channels in a superposition of orders and the related communication model with independent quantum channels traversed in a superposition of paths [7–9]. In the second model, noise can be reduced, but never completely removed. While every real experiment involves some level of noise, the in-principle possibility of noiseless communication through superposition of orders implies that the experimental fidelities can be arbitrarily close to 1.

In our experiment, we report an average fidelity of 0.9747 ± 0.0012 with the unitary gate σ_2 predicted by the theory. We reconstructed the channel matrix γ_{ij} from the tomographic data and used it to find the input state that maximises the one-shot coherent information in Eq. (**??**). The optimisation can be reduced to three real parameters (α,θ,ψ) by parameterising the qubit state ρ as $\rho = \alpha_0|\phi\rangle\langle\phi| + (1-\alpha_0)|\phi_\perp\rangle\langle\phi_\perp|$, where $|\phi\rangle = \cos(\theta)|0\rangle + \sin(\theta)e^{i\psi}|1\rangle$ and $|\phi_\perp\rangle = \sin(\theta)|0\rangle - \cos(\theta)e^{i\psi}|1\rangle$ are basis states. Since the entropy exchange is independent of the choice of purification, the parameters (α_0,θ,ψ) completely determine the coherent information. Fig. 2 shows the experimental results for the evaluation of the coherent information $\mathcal{I}_c$ of the channel $\mathcal{C}_-$ and also the whole channel $\mathcal{S}(\mathcal{B}_s,\mathcal{P}_t)$. For channel $\mathcal{C}_-$, the result is a coherent information of about 0.812 ± 0.003, obtained with parameters $\alpha_0 = 0.500$, $\theta = 0.0723\pi$, and $\psi = 0.790\pi$. The deviation of the channel capacities from their theoretical predictions are due to imperfect channel simulations and measurement error. The dependence of the coherent information on α_0 and θ is shown in Fig. 2 (b) for fixed $\psi = 0.790\pi$. More generally, the coherent information Q_1 of the channel $\mathcal{S}(\mathcal{B}_s,\mathcal{P}_t)$ is further show in Fig. 2 (c) as a function of t, with $s = t$. One can find out that, as long as $t > 0.62$, $\mathcal{I}_c$ of $\mathcal{S}(\mathcal{B}_t,\mathcal{P}_t)$ (red line) surpasses the coherent information when the two channels are combined in a fixed order (black line). Our experimental results (cyan rhombuses) verified the existence of the advantage of indefinite causal order and the possibility of heralded, high-fidelity communication.

An even more radical example of quantum communication in a superposition of order corresponds to two entanglement-breaking channels $\mathcal{F}(\rho) = 1/2(\sigma_1\rho\sigma_1 + \sigma_2\rho\sigma_2)$ [3]. In normal conditions, the channel $\mathcal{F}$ cannot transmit any quantum information. Still, when two such channels are inserted in the quantum SWITCH, the channels $\mathcal{C}_+$ and $\mathcal{C}_-$ of Equations

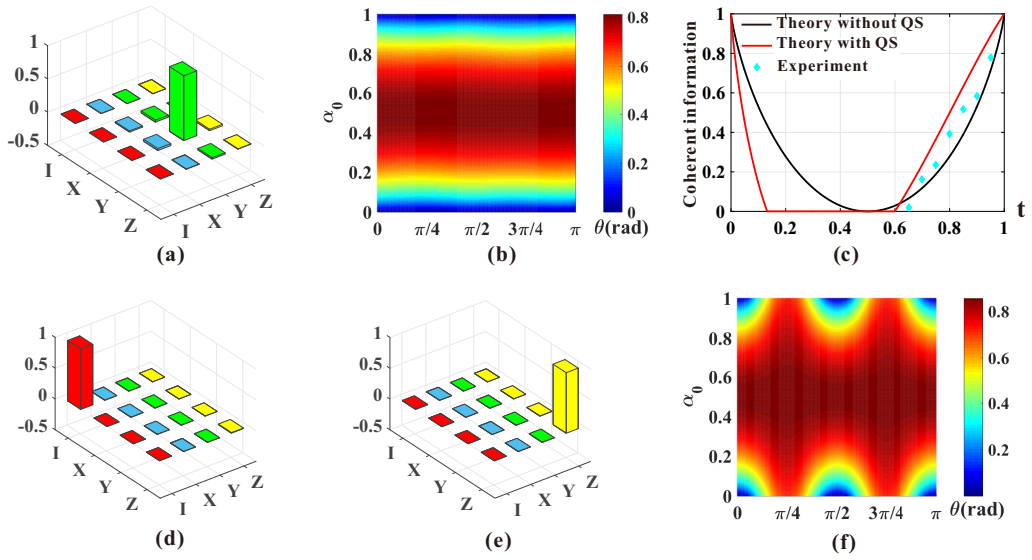


FIG. 2. Quantum communication with entanglement-breaking channels. (a) Real part of the reconstructed matrix of $\mathcal{S}(\mathcal{B}_s, \mathcal{P}_t)$, for $s = t = 1/2$. The fidelity is 0.9747 ± 0.0012. (b) Coherent information $\mathcal{I}_c$ for $\mathcal{S}(\mathcal{B}_s, \mathcal{P}_t)$ with $s = t = \frac{1}{2}$ as a function of θ and α_0, for fixed $\psi = 0.790\pi$. (c) Coherent information Q_1 for the channel $\mathcal{S}(\mathcal{B}_t, \mathcal{P}_t)$ with $t \in [0, 1]$. The experimental results are marked as cyan rhombuses, while the correspond theoretical predictions are plotted in the red line. For comparison, the coherent information of the two dephasing channels combined in a definite order is also shown in the black line. (d-e) Real parts of the reconstructed matrices of $\mathcal{C}_+$ and $\mathcal{C}_-$ of the channel $\mathcal{S}(\mathcal{F}, \mathcal{F})$. (f) Coherent information Q_1 for channel $\mathcal{S}(\mathcal{F}, \mathcal{F})$ as a function of θ and α_0, for fixed $\psi = 0.155\pi$. Error bars are smaller than the marker size.

(4) and (5) are both unitary, enabling the deterministic noiseless transmission of one qubit. This effect it is more dramatic than the heralded noiseless communication discussed in the previous paragraphs. While the heralded noiseless transmission does not guarantee a quantum capacity, the deterministic noiseless transmission of our second example guarantees in principle a maximal capacity.

In our experiment,we find that the conditional channels $\mathcal{C}_+$ and $\mathcal{C}_-$ have fidelities 0.9823 ± 0.0013 and 0.9846 ± 0.0014 with the corresponding unitary gates, respectively. The coherent information is 0.855 ± 0.004 and can be obtained when $\alpha_0 = 0.500$, $\theta = 0.7575\pi$, and $\psi = 0.155\pi$. The corresponding data are presented in Figures 2 (e) and 2 (d). Figure 2 (f) reports the result of coherent information of channel $\mathcal{S}(\mathcal{F}, \mathcal{F})$ varying with the parameters α_0 and θ, while ψ is set to be 0.155π.

* bhliu@ustc.edu.cn

† cfli@ustc.edu.cn

‡ giulio.chiribella@cs.ox.ac.uk

[1] D. Ebler, S. Salek, and G. Chiribella, Physical review letters **120**, 120502 (2018).

[2] S. Salek, D. Ebler, and G. Chiribella, arXiv preprint arXiv:1809.06655 (2018).

[3] G. Chiribella, M. Banik, S. S. Bhattacharya, T. Guha, M. Alimuddin, A. Roy, S. Saha, S. Agrawal, and G. Kar, arXiv preprint arXiv:1810.10457 (2018).

[4] M. M. Wilde, *Quantum information theory* (Cambridge University Press, 2013), ch. 24.7.2.

[5] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Physical Review A **88**, 022318 (2013).

[6] G. Chiribella, Physical Review A **86**, 040301 (2012).

[7] N. Gisin, N. Linden, S. Massar, and S. Popescu, Physical Review A **72**, 012338 (2005).

[8] A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard, arXiv preprint arXiv:1810.09826 (2018).

[9] G. Chiribella and H. Kristjánsson, arXiv preprint arXiv:1812.05292 (2018).

Distribution of high-dimensional orbital angular momentum entanglement at telecom wavelength over 1km vortex fiber

Huan Cao[1,2], She-Cheng Gao[3], Bi-Heng Liu[1,2], Zheng-Wei Zhou[1,2], Jacquiline Romero[5], Zhao-Hui Li[4], Si-Yuan Yu[4], Yun-Feng Huang[1,2],* Chuan-Feng Li[1,2],† and 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, Hefei, 230026, China*
[3]*Department of Electronic Engineering, College of Information Science and Technology, Jinan University, Guangzhou, 510632, China*
[4]*State Key Laboratory of Optoelectronic Materials and Technologies and School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, 510275, China*
[5]*Centre for Engineered Quantum Systems, School of Mathematics and Physics, University of Queensland, Queensland 4072, Australia*

High-dimensional entanglement exhibites massive potential in increasing channel capacity and resistance to noise in quantum information processing. However, its distribution is quite a challenging task. Here we report the first distribution of three-dimensional orbital angular momentum (OAM) entanglement via a 1-km-length vortex fiber. Using an actively-stabilizing phase precompensation technique, we successfully transport one photon of a three-dimensional OAM entangled pair. It still shows a fidelity up to 71% with respect to the three-dimensional maximal-entangled-state (MES). In addition, we certify that the high-dimensional entanglement survives the transportation by generalized Bell inequality, obtaining a violation of ~ 3 standard deviations with $I_3 = 2.12 \pm 0.04$.

Encoding in a multi-dimensional state space is beneficial for increasing channel capacity and improving the tolerance to noise or eavesdropping in secure quantum communications [1–3]. High-dimensional entanglement, exhibits more complex structures of entanglement [4–6], and stronger nonclassical correlation.

OAM allows for encoding large amount of information per photon and its dimension scalability is much more desirable compared to other DOFs. The blossom of OAM manipulating technology in recent years make an essential step toward manipulating quantum system beyond qubit[7–9]. However, undistibuted high-dimensional OAM entanglement becomes a challenging task which will advance the quantum application beyond lab proof-of-principle demonstrations, as is recognized to be a valuable project [10, 11].

There are two method to distribute OAM entanglement. One is free-space propagation, spin-orbit hybrid 2-d entanglement distribution across Vienna has been exploited [12]. However, OAM is highly sensitive to atomospheric turbulence and subject to weather, line-of sight, or time of day. The other potential way is fiber transport. But only two dimensional entanglement can be identified and the transmission distance is just 30 cm in Ref.[13] and 40 cm in Ref.[14].

The main difficulties of sending photonic entanglement through long-distance fiber lie in two aspects: crosstalk and intermodal dispersion. These problem prevent the distribution of entanglement going beyond lab-scale and toward higher-dimension.

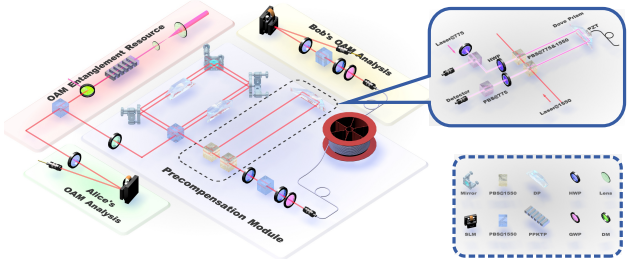


Figure 1. Schematic of the experimental setup. The precompensation module (blue painted area) is used for compensating the intermodal dispersion induced by 1-kilometer-long OAM fiber. SLM: spatial light modulator, DM: dichroic mirrors, DP: dove prism. The phase locking system is detailed in top right inset.

In our experiment, several developments has been made to overcome these problems. The schematic experimental setup is depicted in Fig. 1. First, we develop a high quality three-dimensional OAM entanglement source with a satifying fidelity of 0.888 ± 0.007, considering of the need for balancing the trade-off between high fidelity and narrow bandwidth, which are both important for long-distance distribution. In most cases, the OAM entanglement state is prepared by thin crystal in order to obtain a high-fidelity resource. However, in such cases the bandwidth of the twins photons is too wide for long-distance transmission even though a higher fidelity entanglement is accessible using thin crystal. In the regime of long-distance distribution or quantum memory, a narrow bandwidth is required. We carefully optimize all the optional parameters to make a balance,

* hyf@ustc.edu.cn
† cfli@ustc.edu.cn

finally adjusting properties of entangled source suitable for long-distance distribution. Besides, we experimentally identify the intermodal dispersion simply using coincidence instrument, and we further design an actively-stabilizing precompensation module to eliminate this intermodal dispersion. This module is based on introducing a reverse dispersion to pre-compensate it before entering the 1-km fiber. With these measures we successfully transport one of the three-dimensional OAM entangled twin photon through a 1 km fiber. Owing to the the advantage of vortex fiber, the OAM spiral wavefront could survive the transport hence direct quantum tomography is accessible, quantifying a high surviving fidelity up to 0.71 ± 0.02 with respect to 3*3 maximally entangled state. Furthermore, certification of three-dimension entanglement is approved by testing CGLMP inequality with the violation about 3 standard deviations ($I_3 = 2.12 \pm 0.04$) .

The most tough challenges for distributing high-dimensional OAM entanglement has been settled down, and distributing distance is extended more than three orders over previous work [13, 14], if practical OAM-entanglement-based applications would like to advance beyond laboratory. It is the first time to distribute high-dimensional OAM entanglement and our method is extendable to both higher-dimension and longer-distance in principle. The preserved spiral wavefront make the distributed entangled state capable of further manipulation.We believe that our result will motivate further experimental research into novel protocol of longdistance high-dimensional quantum communications.

[1] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Physical review letters **98**, 060503 (2007).

[2] T. M. Graham, H. J. Bernstein, T.-C. Wei, M. Junge, and P. G. Kwiat, Nature communications **6** (2015).

[3] M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, Physical review letters **90**, 167906 (2003).

[4] J. Romero, D. Giovannini, S. Franke-Arnold, S. Barnett, and M. Padgett, Physical Review A **86**, 012334 (2012).

[5] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, Proceedings of the National Academy of Sciences **111**, 6243 (2014).

[6] M. Malik, M. Erhard, M. Huber, M. Krenn, R. Fickler, and A. Zeilinger, Nature Photonics **10**, 248 (2016).

[7] A. Babazadeh, M. Erhard, F. Wang, M. Malik, R. Nouroozi, M. Krenn, and A. Zeilinger, Physical review letters **119**, 180510 (2017).

[8] M. Erhard, M. Malik, M. Krenn, and A. Zeilinger, arXiv preprint arXiv:1708.03881 (2017).

[9] L.-J. Kong, R. Liu, Z.-X. Wang, Y. Si, W.-R. Qi, S.-Y. Huang, C. Tu, Y. Li, W. Hu, F. Xu, et al., arXiv preprint arXiv:1709.03770 (2017).

[10] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, Light: Science & Applications **7**, 17146 (2018).

[11] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, et al., arXiv preprint arXiv:1803.10138 (2018).

[12] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, Proceedings of the National Academy of Sciences **112**, 14197 (2015).

[13] W. Löffler, T. Euser, E. Eliel, M. Scharrer, P. S. J. Russell, and J. Woerdman, Physical review letters **106**, 240505 (2011).

[14] Y. Kang, J. Ko, S. M. Lee, S.-K. Choi, B. Y. Kim, and H. S. Park, Physical review letters **109**, 020502 (2012).

A Quantum Algorithm for Minimum Steiner Tree Problem

Masayuki Miyamoto *[1] † Masakazu Iwamura[2] ‡ Koichi Kise[2] §

[1] *Department of Communications and Computer Engineering, Graduate School of Informatics, Kyoto University*
[2] *Department of Computer Science and Intelligent Systems, Graduate School of Engineering, Osaka Prefecture University*

Abstract. Minimum Steiner tree problem is a well-known NP-hard problem. For the minimum Steiner tree problem in graphs with n vertices and k terminals, there are many classical algorithms that take exponential time in k. In this paper, to the best of our knowledge, we propose the first quantum algorithm for the minimum Steiner tree problem. The complexity of our algorithm is $\mathcal{O}^*(1.812^k)$. A key to realize the proposed method is how to reduce the computational time of dynamic programming by using a quantum algorithm because existing classical (non-quantum) algorithms in the problem rely on dynamic programming. Fortunately, dynamic programming is realized by a quantum algorithm for the travelling salesman problem, in which Grover's quantum search algorithm is introduced. However, due to difference between their problem and our problem to be solved, recursions are different. Hence, we cannot apply their technique to the minimum Steiner tree problem in that shape. We solve this issue by introducing a decomposition of a graph proposed by Fuchs *et al.*

The full version of this extended abstract is available at `https://arxiv.org/abs/1904.03581`**.**
THIS PAPER IS ELIGIBLE FOR BEST STUDENT POSTER AWARD

Keywords: Minimum Steiner Tree, The Dreyfus-Wagner Algorithm, Dynamic Programming, Grover Search

1 Introduction

Given an undirected graph $G = (V, E)$, a weight $w : E \to \mathbb{R}^+$, and a subset of vertices $K \subseteq V$, usually referred to as terminals, a Steiner tree is a tree that connects all vertices in K. In this paper, let $n = |V|$ be the size of vertices and $k = |K|$ be the size of terminals. A Steiner tree T is the minimum Steiner tree (MST) when the total edge weight $\sum_{e \in E(T)} w(e)$ is the minimum among all Steiner trees of K. Note that all leaves of a Steiner tree T are vertices in K. The task that finds a minimum Steiner tree is called minimum Steiner tree problem, and this problem is known as an NP-hard problem [1]. Note that for fixed k, this problem can be solved in polynomial time, which means that the minimum Steiner problem is *fixed parameter tractable* [2, 3].Although there are difficulties in solving the minimum Steiner tree problem, this problem is applied to solve problems such as power supply network, communication network and facility location problem [4]. Since these practical problems need to be solved, researching the exponential algorithm that has better base is significant.

A naive way to solve the minimum Steiner tree problem is to compute all possible trees. However, the number of all trees in the graph $G = (V, E)$ is $\mathcal{O}(2^{|E|})$ at worst. However, an exhaustive search is not realistic. *The Dreyfus-Wagner algorithm* (the D-W algorithm) is a well-known algorithm based on dynamic programming for solving the Steiner problem in time $\mathcal{O}^*(3^k)$ [5]. The $\mathcal{O}^*$ notation hides a polynomial factor in n and k. This algorithm has been the fastest algorithm for decades. In 2007, Fuchs *et al.* [6] have improved this to $\mathcal{O}^*(2.684^k)$ and Mölle *et al.* [7] to $\mathcal{O}((2+\delta)^k n^{f(\delta^{-1})})$ for any constant $\delta > 0$. For a graph with a restricted weight range, Björklund *et al.* have proposed an $\mathcal{O}^*(2^k)$ algorithm using subset convolution and Möbius inversion [8]. An important thing is that the dynamic programming part of these algorithms [7, 6, 8] use the D-W algorithm.

In order to speed up classical algorithms, use of quantum algorithms is an effective technique. In particular, Grover's quantum search (Grover search) [9] and its generalization, quantum amplitude amplification [10, 11], are widely applicable. Grover search brings quadratic speed up to an unstructured search problem [9, 12]. This is one of the advantages quantum algorithms have over classical algorithms. For NP-hard problems, speeding up using Grover search [9] is a typical method. However, simply applying Grover search to a classical algorithm does not always make faster than the best classical algorithm in many problems. For example, in [13], by using quantum computers, the Travelling Salesman Problem (TSP) for a graph which has n vertices is solved in time $\mathcal{O}^*(\sqrt{n!})$ which is the square root of the classical complexity $\mathcal{O}^*(n!)$ of an exhaustive search. However, the best classical algorithm for TSP takes only $\mathcal{O}^*(2^n)$ [14, 15] which is clearly faster than $\mathcal{O}^*(\sqrt{n!})$.

In order to speed up algorithms for the minimum Steiner tree problem, it is thought that use of Grover search is also an effective technique. Combining classical algorithms with Grover search is one of the ways to make an algorithm faster than the best classical algorithm. For example, Ambainis *et al.* [16] have combined Grover search with algorithms for TSP, Minimum Set Cover Problem and so on that use dynamic programming. A naive way is replacing the dynamic programming part of the algorithm of Ambainis *et al.* by D-W algorithm. However, we cannot use the method of Ambainis *et al.* in the same way because the characteris-

*This research was done when the first author studied in Osaka Prefecture University.

†`miyamoto.masayuki.46s@st.kyoto-u.ac.jp`
‡`masa@cs.osakafu-u.ac.jp`
§`kise@cs.osakafu-u.ac.jp`

Table 1: Comparison of the algorithms.

Algorithm	Complexity	classical or quantum
Dreyfus and Wagner [5]	$\mathcal{O}^*(3^k)$	classical
Fuchs [6]	$\mathcal{O}^*(2.684^k)$	classical
Mölle [7]	$\mathcal{O}((2+\delta)^k n^{f(\delta^{-1})})$	classical
Björklund [8] (best known in the restricted weight case)	$\mathcal{O}^*(2^k)$	classical
This paper	$\mathcal{O}^*(1.812^k)$	quantum

tic of minimum Steiner tree problem differs from that of TSP. Hence, we adapt this method to a method proposed by Fuchs *et al.* [6] for applying Grover search. The decomposition method of Fuchs *et al.* is optimized for a classical computer. We optimize the decomposition for a quantum computer. Our algorithm achieved the complexity $\mathcal{O}^*(1.812^k)$. This improvement of complexity brings more than 10^4 times speed up compared to $\mathcal{O}^*(2^k)$ even in the case of $k = 100$. Table 1 shows the complexity of classical algorithms for minimum Steiner tree problem and our proposed algorithm.

References

[1] Richard M Karp. Reducibility among combinatorial problems. In *Complexity of computer computations*, pages 85–103. Springer, 1972.

[2] Rodney G Downey and Michael Ralph Fellows. *Parameterized complexity*. Springer Science & Business Media, 2012.

[3] Jörg Flum and Martin Grohe. *Parameterized complexity theory*. Springer Science & Business Media, 2006.

[4] Frank K Hwang and Dana S Richards. Steiner tree problems. *Networks*, 22(1):55–89, 1992.

[5] Stuart E Dreyfus and Robert A Wagner. The steiner problem in graphs. *Networks*, 1(3):195–207, 1971.

[6] Bernhard Fuchs, Walter Kern, and Xinhui Wang. Speeding up the Dreyfus–Wagner algorithm for minimum Steiner trees. *Mathematical methods of operations research*, 66(1):117–125, 2007.

[7] Daniel Mölle, Stefan Richter, and Peter Rossmanith. A faster algorithm for the Steiner tree problem. In *Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science*, pages 561–570. Springer, 2006.

[8] Andreas Björklund, Thore Husfeldt, Petteri Kaski, and Mikko Koivisto. Fourier meets Möbius: fast subset convolution. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 67–74, 2007.

[9] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

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

[11] Michele Mosca et al. Quantum searching, counting and amplitude amplification by eigenvector analysis. In *MFCS98 workshop on Randomized Algorithms*, pages 90–100, 1998.

[12] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998.

[13] Karthik Srinivasan, Saipriya Satyajit, Bikash K. Behera, and Prasanta K. Panigrahi. Efficient quantum algorithm for solving travelling salesman problem: An IBM quantum experience, 2018.

[14] Richard Bellman. Dynamic programming treatment of the travelling salesman problem. *J. ACM*, 9(1):61–63, 1962.

[15] Michael Held and Richard M Karp. A dynamic programming approach to sequencing problems. *Journal of the Society for Industrial and Applied Mathematics*, 10(1):196–210, 1962.

[16] Andris Ambainis, Kaspars Balodis, Jānis Iraids, Martins Kokainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs. Quantum speedups for exponential-time dynamic programming algorithms. *arXiv preprint arXiv:1807.05209*, 2018.

Measurement-device-independent verification of channel steering and channel coherence

InU Jeon[1] Hyunseok Jeong[1] *

[1] *Seoul National University Quantum Information Science Group, Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*

Abstract. We propose measurement-device-independent verification protocol of channel coherence and channel steering. We first obtain channel-state duality using any bipartite pure state with full Schmidt-rank, which guarantees that, channel is coherent and steerable if and only if dual state is non-separable and steerable with respect to a bystander. Subsequently, following canonical protocol, we verify the dual state in measurement-device-independent manner, which completes measurement-device-independent verification of channel coherence and channel steering. We further analyze the effect of imperfect preparation of pure states used for obtaining channel-state duality, and found that the lower bound of noise threshold is determined by robustness measures.

Keywords: Channel Steering, Channel Coherence, Measurement-Device-Independent

Extended Abstract

Given a quantum channel from an input to an output system, it is of our interest to check information leakage to a third party, say a bystander. To analyze this, we can come up with a concept of broadcasting channel [1] consisting of one input and two output systems, where one of the outputs is a bystander, by which we can retrieve the original channel by disregarding the bystander's system. If the broadcasting channel can be described by sum of decompositions into subchannel and bystander's local state, we call it an incoherent extension [2]. Intuitively, incoherent extension of the channel implies that the information leakage to the third party is not more than classical randomness. If broadcasting channel is not an incoherent, we call it a coherent extension, which means that the information leakage to the third party is more than classical randomness. We can verify coherence of the extended channel in two different scenarios : whether we trust the bystanders side, or not. If we trust, the verification protocol is device-dependent and we call it as channel coherence, and if we do not trust, the verification protocol is one-sided-device-independent and we call it as channel steering [2].

In this research, we propose the verification protocol of channel coherence and channel steering in measurement-device-independent (MDI) way [3]. To do this, we first obtain the dual state of the given channel using bipartite pure state with full Schmidt-rank, and prove two theorems. 1. The dual state of the extended channel is IO/B entangled, where B is a bystanders system, if and only if the channel extension is coherent. 2. The dual state of the extended channel is steerable by bystanders side if and only if the channel extension is steerable. Consequently, based on two theorems, we convert the given extended channel into tripartite state and verify their entanglement or steerability in the MDI way as suggested in Refs. [4, 5]. This protocol completes the MDI verification of the channel coherence and channel steering. Moreover, we analyze the effect of imperfect preparation of the bipartite pure states with full Schmidt-rank used for obtaining the dual state from the given channel. We found that, for undesired noise which is separable or unsteerable type, the threshold of the noise for successful MDI verification of channel coherence and steering are bounded from below by $R_E/(1+R_E)$ and $R_S/(1+R_S)$, where R_E is the robustness of entanglement [6] and R_S is the robustness of steering [7]. Together with loss-tolerant property of MDI verification protocol [4, 5], this would help us to overcome large amount of noise and uncontrollable affairs in practical situation.

References

[1] J. Yard, P. Hayden and I. Devetak. Quantum Broadcast Channels. *IEEE Trans. Inf. Theory* **57**, 7147-7162, 2011.

[2] M. Piani. Channel Steering. *J. Opt. Soc. Am. B* **32**, A1, 2015.

[3] I.-U Jeon and Hyunseok Jeong. Measurement-device-independent verification of channel steering *arXiv 1905.07840*, 2019.

[4] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin. Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States. *Phys. Rev. Lett* **110**, 060405, 2013.

[5] H.-Y. Ku, S.-L. Chen, H.-B. Chen, F. Nori and Y.-N. Chen. Measurement-device-independent measure of steerability and witnesses for all steerable resources. *arXiv 1807.08901v2*, 2019.

[6] G. Vidal and R. Tarrach. Robustness of entanglement. *Phys. Rev. A* **59**, 141, 1999.

[7] M. Piani and J. Watrous. Necessary and Sufficient Quantum Information Characterization of Einstein-Podolsky-Rosen Steering. *Phys. Rev. Lett.* **114**, 060404, 2015.

*jeongh@snu.ac.kr

Unconditionally secure qubit commitment scheme using quantum maskers

Seok Hyung Lie[1] * Hyukjoon Kwon[2] M.S. Kim[2] Hyunkseok Jeong[1]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea*
[2] *QOLS, Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom*

Abstract. A commitment scheme allows one to commit to hidden information while keeping its value recoverable when needed. Despite considerable efforts, an unconditionally and perfectly secure bit commitment has been proven impossible both classically and quantum-mechanically. The situation is similar when committing to qubits instead of classical bits as implied in the no-masking theorem [K. Modi et al., Phys. Rev. Lett. **120**, 230501 (2018)]. In this work, we find that circumvention of the no-masking theorem is possible with the aid of classical randomness. Based on this, we construct an unconditionally secure quit-commitment scheme that utilises any kind of universal quantum maskers with optimal randomness consumption, which is distributed by a trusted initializer. This shows that randomness, which is normally considered only to obscure the information, can benefit a quantum secure communication scheme. This result can be generalised to an arbitrary dimensional system.

Keywords: AQIS, template

1 Introduction

In a commitment protocol, a sender (say Alice) commits to a secret value in the way that a receiver (Bob) cannot access the value until it is revealed. On the other hand, Bob should be able to reject Alice's cheating of revealing a value different from the originally committed value. A commitment scheme, which has many cryptographical applications[1, 2], is said to be *unconditionally secure* when the scheme does not depend on the computational power of both participants, while it is*perfectly secure* when the scheme works with zero probability of failure. However, an unconditionally and perfectly secure commitment protocol is impossible. If a commitment protocol is unconditionally and perfectly binding, which means that any attempt of Alice to change the already committed secret value can be detected by Bob, then there should be a unique secret value for each commitment provided by Alice to Bob. If so, the protocol, however, cannot be unconditionally and perfectly concealing, i.e., Bob could have some information about the committed value before Alice discloses it, because Bob with unlimited computational power can reveal the secret value by searching through every possible secret values and corresponding commitments.

Quantum bit-commitment is an attempt to circumvent this difficulty by using quantum mechanics [3]. However, it has been proven [4, 5] that an unconditionally secure commitment of a classical value is impossible even with the aid of quantum mechanics. Meanwhile, a fully classical breakthrough was developed by Rivest [6] as introducing a partially credible mediator, "trusted initializer," who is only involved in the beginning (setup) of the protocol and does not receive any information during the remaining protocols. In Ref. [6], it was shown that the trusted initializer enables the construction of unconditionally secure commitment schemes for classical bits.

It transpired that the situation is similar for *qubit commitment*, in which the commited secret value is a qubit. A result recently proven by Modi *et al.* [7] known as *the no-masking theorem* states that it is impossible to encode quantum information in a bipartite pure quantum state so that it is inaccessible to local subsystems. As a corollary, an unconditionally and perfectly secure qubit commitment is also forbidden [7]. It shows that qubit commitment schemes with straightforward protocols are vulnerable to entanglement-based attacks [7].

One might expect that the no-masking theorem can be extended to mixed states similarly as the case of the no-broadcasting theorem [8] extended from the no-cloning theorem [9]. In this work however, we show that this is not the case. We first prove a stronger version of the no-masking theorem by showing that one additionally needs at least $\log_2 d$ bits and $2\log_2 d$ bits of randomness respectively when entanglement is available and when only zero one-way quantum discord is allowed in the masked bipartite quantum state. We then introduce a simple way to circumvent the strengthened no-masking theorem by constructing explicit examples of quantum masker that consumes the minimal amount of randomness.

We further show that the class of universal quantum maskers that consume uniform randomness can be used for unconditionally secure qubit commitment schemes by introducing a trusted initializer, whose role is very similar to that of Rivest's commitment scheme. Our scheme has a security advantage over Rivest's scheme even when applied to the bit commitment as it avoids a certain type of security failure.

References

[1] M. O. Rabon, Technical report TR-81, (1981).

[2] S. Even, O. Goldreich and A. Lempel, *Advances in Cryptography: Proc. Crypto '82*, 205, (1982).

*dielectric@snu.ac.kr

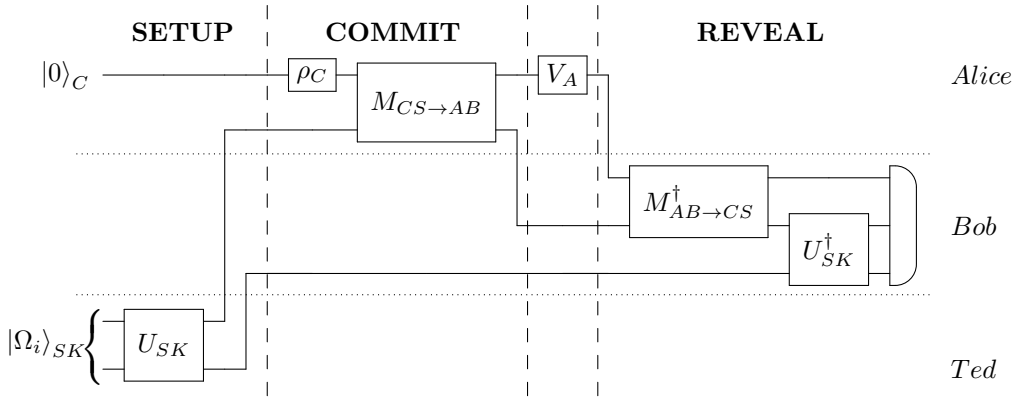


Figure 1: A schematic description of the qubit-commitment protocol proposed in this work. Lane 1-2 belongs to Alice, lane 3-5 to Bob, and lane 6-7 to Ted. ρ_C gate denotes the preparation of the secret state ρ_C to which Alice commits, and V_A denotes the unitary transformation secretly applied on the system A by Alice to cheat Bob. Note that this diagram does not show the classical information flow.

[3] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, 362 (1993).

[4] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[5] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[6] R. Rivest, "Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer", (1999).

[7] K. Modi, A. K. Pati, A. Sen, and U. Sen, Phys. Rev. Lett. **120**, 230501 (2018).

[8] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[9] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

Uncertainty relation for the position of an electron in a uniform magnetic field from quantum estimation theory

Shin Funada[1] * Jun Suzuki[1] †

[1] *Graduate School of Informatics and Engineering, The University of Electro-Communications*
1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan

Abstract. We investigate the uncertainty relation of one electron in a uniform magnetic field by the quantum estimation theory. As the two-parameter unitary models, we use two sets of unitary transformations that make a shift in the position of the electron probability density. The sets of the generators used are the canonical momenta and the mechanical momenta. In both cases, we obtain non-trivial bounds unlike the result of Heisenberg-Robertson uncertainty relation. Although both models make a shift in the position of the position probability density, the uncertainty relation derived from the quantum Cramér-Rao bounds of those two models are different.

Keywords: Uncertainty relation, quantum estimation theory, two-parameter unitary model, quantum Cramér-Rao bound

1 Introduction

The uncertainty relation based on the quantum estimation theory was investigated by many authors [1, 2, 3, 4, 5]. In the present work, we set up a specific physical model, a model of one electron in a uniform magnetic field and investigate the uncertainty relation regarding the position of the electron by the parameter estimation problem of two-parameter unitary model. In this model, the Heisenberg-Robertson uncertainty relation [6, 7] of the position operators of an electron (x, y) only yields to the following trivial inequality. $(\Delta_\rho x)(\Delta_\rho y) \geq |\langle [x, y]\rangle|/2 = 0$, because two position operators x and y commute, i.e., $[x, y] = 0$. In the relation above, Δx denotes the (quantum) standard deviation about x with respect to a state ρ, which is defined by $(\Delta_\rho x)^2 = \mathrm{tr}\,[\rho\,(x - \langle x\rangle)^2] = \langle x^2\rangle_\rho - \langle x\rangle_\rho^2$ with $\langle A\rangle_\rho = \mathrm{tr}\,[\rho\, A]$, the expectation value about an observable A. $\Delta_\rho y$ is defined similarly. Usually, when the uncertainty relation is discussed, the Heisenberg-Robertson uncertainty relation makes sense only for two non-commuting observables, see for example [8, 9, 10]. In contrast, the quantum estimation theoretical formulation of the uncertainly relation is applicable when discussing two-commuting observables as shown in this paper.

In order to derive the uncertainty relation between x and y based on the quantum estimation theory, we need to introduce a parametric model describing the position measurement of the electron. We use the unitary transformation generated by the canonical momenta p_x and p_y with the parameter $\theta = (\theta^1, \theta^2)$. We define the family of states ρ_θ^p generated by this transformation from the reference state ρ_0, which is known:

$$\text{Model 1:}\quad \rho_\theta^p = \mathrm{e}^{-\mathrm{i}\theta^1 p_x}\mathrm{e}^{-\mathrm{i}\theta^2 p_y}\rho_0\mathrm{e}^{\mathrm{i}\theta^2 p_y}\mathrm{e}^{\mathrm{i}\theta^1 p_x}. \tag{1}$$

By estimating the parameter θ^1 (θ^2), we can infer the expectation value of x (y).

Besides this 'natural' unitary transformation, we use an alternative unitary transformation. That is

$$\text{Model 2:}\quad \rho_\theta^\pi = \mathrm{e}^{-\mathrm{i}\theta^1 \pi_x}\mathrm{e}^{-\mathrm{i}\theta^2 \pi_y}\rho_0\mathrm{e}^{\mathrm{i}\theta^2 \pi_y}\mathrm{e}^{\mathrm{i}\theta^1 \pi_x}, \tag{2}$$

where $\vec{\pi} = \vec{p} + e\vec{A}$. The vector potential for the uniform field $\vec{B}$ is denoted by $\vec{A}$. The charge of an electron is $-e$ ($e > 0$). Both Model 1 and Model 2 make a shift in position of the position probability density which is defined by the product of the wave function and its complex conjugate.

As the main contribution, we derive the uncertainty relation by the trade-off relation between the components of mean square error (MSE) matrix by using the quantum Cramér-Rao (C-R) inequality. We compare the results of Model 1 and Model 2. The uncertainty relation from the quantum C-R inequalities of Model 1 and Model 2 are different though both Model 1 and Model 2 make the same shift in the position of the position probability density. In either case of the pure state or the thermal state as the reference state, Model 2 gives more precise measurement for the position of electron.

2 Preliminaries

Hamiltonian With using the two sets of the the creation and annihilation operators, $a, a^\dagger$ and $b, b^\dagger$ such that $[a, a^\dagger] = [b, b^\dagger] = 1$, Hamiltonian H and z component of the angular momentum L are expressed as [11]

$$H = \omega(a^\dagger a + \frac{1}{2}), \tag{3}$$

$$L = xp_y - yp_x = a^\dagger a - b^\dagger b. \tag{4}$$

$\omega = eB/m$ is the cyclotron frequency. We assume the magnetic field $\vec{B}$ is along the z axis i.e., $\vec{B} = (0, 0, B)$. Eqs. (3), (4), and the generators expressed by $a, a^\dagger$ and $b, b^\dagger$ are given in Appendix 5.1.

Reference state Since the energy eigenstate is infinitely degenerated [12], we choose the tensor product of the vacuum states as the reference state ρ_0 which is denoted by

$$\rho_0 = |0\rangle_{a\,a}\langle 0\,| \otimes |0\rangle_{b\,b}\langle 0\,| = |0,\, 0\rangle\,\langle 0,\, 0|\,. \tag{5}$$

The wave function of this state is known as the Lowest Landau Level (LLL), $\psi_{00}(x, y) = \langle x, y\,|\,0, 0\rangle \propto \mathrm{e}^{-\frac{x^2+y^2}{2\lambda^2}}$, where $\lambda^2 = 2(eB)^{-1}$.

* f1941011@edu.cc.uec.ac.jp
† junsuzuki@uec.ac.jp

Unitary transformations We introduce two kinds of unitary transformations, $e^{-i\theta^1 p_x} e^{-i\theta^2 p_y}$ and $e^{-i\theta^1 \pi_x} e^{-i\theta^2 \pi_y}$. We consider that we have them act on the LLL, $\psi_{00}(x, y)$. We can show

$$|e^{-i\theta^1 p_x} e^{-i\theta^2 p_y} \psi_{00}(x, y)|^2 = |\psi_{00}(x - \theta^1, y - \theta^2)|^2,$$
$$|e^{-i\theta^1 \pi_x} e^{-i\theta^2 \pi_y} \psi_{00}(x, y)|^2 = |\psi_{00}(x - \theta^1, y - \theta^2)|^2, \quad (6)$$

where

$$|\psi_{00}(x - \theta^1, y - \theta^2)|^2 \propto e^{-\frac{(x-\theta^1)^2 + (y-\theta^2)^2}{\lambda^2}}. \quad (7)$$

Therefore, both Model 1 and Model 2 make a shift in position of the position density probability.

3 Uncertainty relation for pure state model

It is known that the right logarithmic derivative (RLD) does not exist in general when the reference state is a pure state. Only the symmetric logarithmic derivative (SLD) exists [13]. For the coherent model, the generalized RLD also exists and provides the tight bound [14]. We calculate the SLD and the generalized RLD Fisher information matrices by the method given in [13, 14]. We obtain the uncertainty relation from the quantum C-R inequalities. The inequalities we derived from the the quantum C-R inequality are given in Appendix 5.2. The inverse of the quantum Fisher information matrices are given in Appendix 5.3.

3.1 Model 1: unitary model generated by p_x and p_y

In Model 1, the generators of the unitary transformation p_x and p_y commute. We can show that the SLD's commute on the support of the states and that the SLD C-R bound is achievable [15].

The SLD Fisher information matrix and the MSE matrix are denoted by $G^p_{\rm S}$ and V_θ, respectively. Then, from the SLD C-R inequality $V_\theta \geq (G^p_{\rm S})^{-1}$, we obtain the following inequalities.

$$V_{11} \geq \frac{\lambda^2}{2}, \quad V_{22} \geq \frac{\lambda^2}{2}.$$

where $V_\theta = [V_{ij}]$. The generalized RLD is equal to the SLD.

Figure 1 shows the SLD C-R bound (dotted lines). $\lambda^2/2$ is a half of the square of the spread of the LLL wave function Eq. (7). This result shows that the measurement accuracy is limited by the spread of the probability density of the electron in the LLL, because of the quasi-classical nature of Model 1, i.e., the SLD's commute.

3.2 Model 2: unitary model generated by π_x and π_y

Let $G^\pi_{\rm S}$ denote the SLD Fisher information matrix of Model 2 with respect to the reference state ρ_0 [Eq. (5)]. From $V_\theta \geq (G^\pi_{\rm S})^{-1}$, we obtain the following inequalities.

$$V_{11} \geq \frac{\lambda^2}{4}, \quad V_{22} \geq \frac{\lambda^2}{4}.$$

Notably, the relation $(G^p_{\rm S})^{-1} = 2(G^\pi_{\rm S})^{-1}$ holds.

Let $\tilde{G}^\pi_{\rm R}$ denote the generalized RLD Fisher information. From the generalized RLD C-R inequality $V_\theta \geq (\tilde{G}^\pi_{\rm R})^{-1}$ [14], we obtain the following inequality,

$$(V_{11} - \frac{\lambda^2}{4})(V_{22} - \frac{\lambda^2}{4}) \geq \frac{\lambda^4}{16}. \quad (8)$$

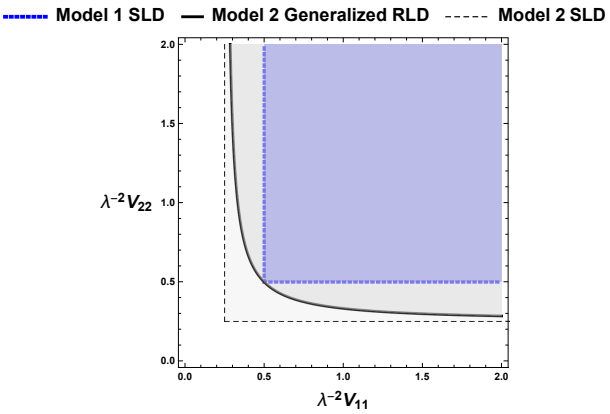


Figure 1: Uncertainty relation of Model 1 and Model 2 given by the quantum C-R inequalities. The SLD C-R bound of Model 1 is the blue dotted lines. The allowed region of Model 1 for the MSE matrix components (V_{11}, V_{22}) given by SLD C-R inequality is the blue region. The allowed region of Model 2 is above the black solid line, the region given by the inequality (8) which is derived from the generalized RLD C-R inequality. The allowed region of Model 2 by the SLD C-R inequality consists of all of the light, dark gray and blue regions .

Figure 1 shows the SLD C-R bound (dashed line) and the generalized RLD C-R bound (solid line) of Model 2 as well. An optimal measurement for Model 1 is to measure x and y, and the SLD C-R bound is achievable. Since Model 2 is a coherent model, the generalized RLD bound is achievable [14]. Unlike the result of Model 1, the bound for Model 2 is not limited by a constant. It is always lower than that for Model 1.

4 Uncertainty relation for mixed state model

Next, we use a mixed state as the reference state to see how the noise affects the measurement accuracy of the electron position. For the purpose, as the mixed state, we choose a thermal state. However, in the current system we are considering, there is no unique thermal state, because the energy eigenstate is (infinitely) degenerated [12]. Then, a thermal state of this system is not uniquely specified by the temperature only. To resolve this degeneracy problem, we impose a condition that the expectation value of the angular momentum $\langle L\rangle_0 = {\rm tr}\,[\rho_0 L]$ is constant. Given an arbitrary value of $\langle L\rangle_0$, the reference state $\rho_{\beta,\mu}$ is denoted by

$$\rho_{\beta,\mu} = Z^{-1}_{\beta,\mu} e^{-\beta H + \mu L}, \quad (9)$$

where $Z_{\beta,\mu} = {\rm tr}\,[e^{-\beta H + \mu L}]$ is the partition function and μ is the chemical potential. By using the coherent states which are defined by

$$a\,|z\rangle_a = z\,|z\rangle_a\,, \quad b\,|z\rangle_b = z\,|z\rangle_b\,. \quad (10)$$

$\rho_{\beta,\mu}$ is expressed as

$$\rho_{\beta,\mu} = \rho_{0,a} \otimes \rho_{0,b}, \quad (11)$$

where

$$\rho_{0,a} = \frac{1}{2\pi\kappa_{\rm a}^2} \int e^{-\frac{|z|^2}{2\kappa_{\rm a}^2}} |z\rangle_{a\,a}\langle z|\, d^2 z, \quad \rho_{0,b} = \frac{1}{2\pi\kappa_{\rm b}^2} \int e^{-\frac{|z|^2}{2\kappa_{\rm b}^2}} |z\rangle_{b\,b}\langle z|\, d^2 z.$$

$2\kappa_{\rm a}^2$ and $2\kappa_{\rm b}^2$ are

$$2\kappa_{\rm a}^2 = (e^{\beta\omega-\mu}-1)^{-1},\ \ 2\kappa_{\rm b}^2 = (e^{\mu}-1)^{-1}. \tag{12}$$

The relation among μ, $\kappa_{\rm a}$, $\kappa_{\rm b}$, and $\langle L\rangle_0$ are given in Appendix 5.4.

The reference state $\rho_{\beta,\mu}$ is expressed as a tensor product of two independent Gaussian states with different temperatures. We obtain the uncertainty relation from the SLD and RLD C-R inequalities [2, 3].

The inverse of the quantum Fisher information matrices calculated from the reference state $\rho_{\beta,\mu}$ are given in Appendix 5.5.

4.1 Model 1: unitary model generated by p_x and p_y

Let $G_{\rm S}^{p\,\rm thermal}$ and $G_{\rm R}^{p\,\rm thermal}$ denote the SLD and RLD Fisher information matrices, respectively. The shape of the uncertainty relation from the quantum C-R bounds changes depending on the value of $|\langle L\rangle_0|$.

Case (i). When $|\langle L\rangle_0| \le 1/2$, the SLD C-R bound defines a tighter lower bound, because the matrix inequality $(G_{\rm S}^{p\,\rm thermal})^{-1} - (G_{\rm R}^{p\,\rm thermal})^{-1} \ge 0$ holds, if and only when $|\langle L\rangle_0| \le 1/2$.

Case (ii). In the other case, $|\langle L\rangle_0| > 1/2$, however, there is no matrix ordering between the RLD and SLD Fisher information matrices. This means that both inequalities contribute to the uncertainty relation. Figure 2 shows an example of the quantum C-R bound given by the current analysis for Case (ii) ($|\langle L\rangle_0| > 1/2$). The allowed region of Model 1 for the MSE matrix components (V_{11}, V_{22}) is the blue region which is defined by two quantum C-R bounds, the SLD and the RLD C-R bounds. The parameters used are $\kappa_{\rm a}^2 = 1$, $\kappa_{\rm b}^2 = 1/2$, $|\langle L\rangle_0| = 1 > 1/2$. The RLD and SLD C-R bounds have two intersection points in this case.

Finally, we briefly discuss achievability of the above uncertainty relation. We can show that Model 1 is not D-invariant. Hence, the RLD C-R bound is not achievable [16]. We can also show that the SLD C-R bound is (asymptotically) achievable if and only if $\langle L\rangle_0 = 0$. In our model, this is equivalent to $\langle L\rangle_0 = 0$. When $\langle L\rangle_0 \neq 0$, neither the RLD C-R bound nor SLD C-R bound is even asymptotically achievable. Therefore, the uncertainty relation is not tight, except for the special choice of the parameter, $\langle L\rangle_0 = 0$.

4.2 Model 2: unitary model generated by π_x and π_y

The SLD and RLD Fisher information matrices of Model 2 are denoted by $G_{\rm S}^{\pi\,\rm thermal}$ and $G_{\rm R}^{\pi\,\rm thermal}$, respectively. Since this model is a Gaussian shift model, the RLD C-R bound is achievable [2, 17].

The RLD C-R inequality gives the following inequalities

$$V_{11} \ge \frac{\lambda^2}{4}(1+4\kappa_{\rm a}^2),\ \ V_{22} \ge \frac{\lambda^2}{4}(1+4\kappa_{\rm a}^2), \tag{13}$$

$$[V_{11} - \frac{\lambda^2}{4}(1+4\kappa_{\rm a}^2)][V_{22} - \frac{\lambda^2}{4}(1+4\kappa_{\rm a}^2)] \ge \frac{\lambda^4}{16}. \tag{14}$$

The SLD C-R inequality gives the following

$$V_{11} \ge \frac{\lambda^2}{4}(1+4\kappa_{\rm a}^2),\ \ V_{22} \ge \frac{\lambda^2}{4}(1+4\kappa_{\rm a}^2).$$

Figure 2 shows the RLD C-R bound (black solid line) and the SLD C-R bound (black dashed lines). We see that the quantum C-R bounds of Model 2 stays lower than those of Model 1.

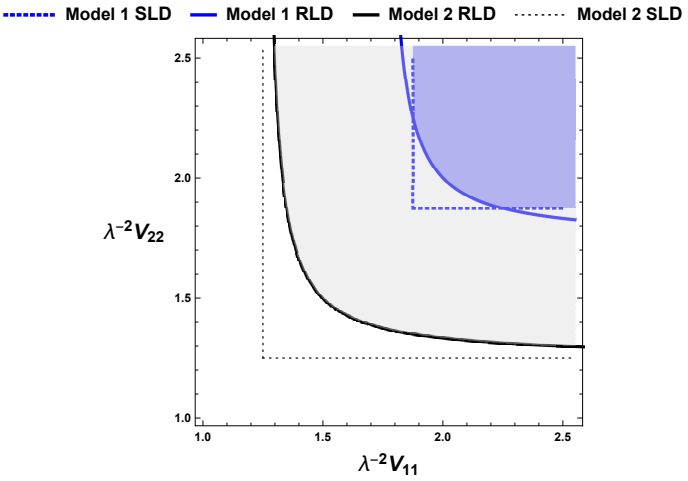


Figure 2: Uncertainty relation of Model 1 and Model 2 given by the quantum C-R inequalites. The temperature parameters used are $\kappa_{\rm a}^2 = 1$, $\kappa_{\rm b}^2 = 1/2$, $\langle L\rangle_0 = 1$, i.e., $\langle L\rangle_0 > 1/2$. The allowed region of Model 1 for the MSE matrix components (V_{11}, V_{22}) is the blue region. The allowed region of Model 1 is given by both the SLD C-R bound (blue dotted lines) and the RLD C-R bound (blue solid line). The allowed region of Model 2 for the MSE matrix components (V_{11}, V_{22}) is the gray region. The RLD C-R bound (black solid line) is achievable.

5 Conclusion

We have investigated the uncertainty relation of one electron in a uniform magnetic field by the parameter estimation of $\theta = (\theta^1, \theta^2)$ in the two-parameter unitary models. Two different sets of generators for the unitary transformation are used. One is a set of canonical momenta, p_x and p_y (Model 1) and the other is a set of mechanical momenta, π_x and π_y (Model 2). In the both cases, we got non-trivial bounds unlike the result of Heisenberg-Robertson uncertainty relation.

Although both models give the same effect to the position probability density defined by the product of the wave function and its complex conjugate, the uncertainty relation from the quantum C-R bounds of both models are different.

With the pure state as the reference state, the C-R bound is quasi-classical for Model 1 and it is quantum mechanical for Model 2. With the thermal state as the reference state, the quantum C-R bound is complicated and its shape changes when the angular momentum $\langle L\rangle_0$ is at 1/2 for Model 1. Model 2 becomes a simple Gaussian shift model. In either case of the pure or thermal state, Model 2 gives more precise measurement.

Acknowledgment

The work is partly supported by JSPS KAKENHI Grant Number JP17K05571. We would like to thank Prof. Hiroshi Nagaoka for the invaluable discussion and suggestion.

References

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

[2] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, Edizioni della Normale, Pisa, 2nd ed (2011).

[3] H. Nagaoka, in *Surikagaku*, no. 508, p. 26–34, Saiense-Sha (2005). (in Japanese)

[4] P. Gibilisco, H. Hiai, and D. Petz, IEEE Trans. Information Theory, Vol. **55**, 439 (2009).

[5] Y. Watanabe, T. Sagawa, and M. Ueda, Phys. Rev. A, Vol. **81**, 042121 (2011).

[6] W. Heisenberg, Zeitschr. Phys. Vol. **43**, 172 (1927).

[7] H. P. Robertson, Phys. Rev. Vol. **34**, 163 (1929).

[8] M. Ozawa, Phys. Lett. A, Vol. **320**, 367 (2004).

[9] P. Busch, T Heinonen, and P. Lahti Rev. Mod. Phys. Rep. Vol. **452**, 155 (2007).

[10] P. Busch, P. Lahti, and R. F. Werner Rev. Mod. Phys. Vol. **86**, 1261 (2014).

[11] I. A. Malkin and V. I. Man'ko, Soviet Physics JETP., Vol. **28**, 527 (1969).

[12] M. Johnson and B. Lippmann, Phys. Rev, Vol. **76**, 828 (1949).

[13] A. Fujiwara, H. Nagaoka Phys. Lett. A, Vol. **201**, 119 (1995).

[14] A. Fujiwara, H. Nagaoka J. Math. Phys., Vol. **40**, 4227 (1999).

[15] K. Matsumoto J. Phys. A, Vol. **35**, 3111 (2002).

[16] J. Suzuki, J. Math. Phys., Vol. **57**, 042201 (2016).

[17] H. Yuen and M. Lax, IEEE Trans. Information Theory, Vol. **IT19**, 740 (1973).

Appendix

5.1 Hamiltonian

Hamiltonian H for an electron motion in a uniform magnetic field in the units, $\hbar = 1$ and $c = 1$ is

$$H = \frac{1}{2m}(\vec{p} + e\vec{A})^2. \tag{15}$$

where $-e$ and m are the charge of an electron, ($e > 0$) and the mass of the electron, respectively. $\vec{A}$ is a vector potential. The canonical observables describing this systems are p_x, x, p_y, and y. We will investigate uncertainty relation of an electron motion in a uniform magnetic field $\vec{B} = (0, 0, B)$, $B > 0$. We use the symmetric gauge. Then, the vector potential is written as $\vec{A} = B(-y/2, x/2, 0)$. We can show that the change in the gauge gives no change in the quantum Fisher information when the magnetic field is uniform.

We will consider the motion in $x - y$ plane only, because z component solution is a plane wave. With a new vector operator, $\vec{\pi} = \vec{p} + e\vec{A}$, our Hamiltonian becomes

$$H = \frac{1}{2m}(\pi_x^2 + \pi_y^2).$$

It is known that the operators π_x, π_y and p_x, p_y are equally described by the two sets of the creation and annihilation operators, $a, a^\dagger$ and $b, b^\dagger$ such that $[a, a^\dagger] = [b, b^\dagger] = 1$ with all other commutation relations vanishing [11].

$$\pi_x = \frac{\mathrm{i}}{\lambda}(a^\dagger - a), \quad \pi_y = \frac{1}{\lambda}(a^\dagger + a),$$
$$p_x = \frac{\mathrm{i}}{2\lambda}[(a^\dagger - a) + (b^\dagger - b)], \quad p_y = \frac{1}{2\lambda}[(a^\dagger + a) - (b^\dagger + b)],$$
$$x = \frac{\lambda}{2}[(a^\dagger + a) + (b^\dagger + b)], \quad y = \frac{\lambda}{2\mathrm{i}}[(a^\dagger - a) - (b^\dagger - b)],$$

where $\lambda = \sqrt{2(eB)^{-1}}$ has the dimension of length. As shown in Eq. (7), λ corresponds to the spread of the probability density of the electron in the LLL.

Hamiltonian H and z component of the angular momentum L are

$$H = \omega(a^\dagger a + \frac{1}{2}),$$
$$L = xp_y - yp_x = a^\dagger a - b^\dagger b.$$

ω is the cyclotron frequency and $\omega = eB/m$.

5.2 Uncertainty relation by quantum Fisher information

The quantum C-R inequality is

$$V_\theta \geq (G_\theta)^{-1}, \tag{16}$$

where G_θ is a quantum Fisher information. Let $(G_\theta)^{-1}$ be

$$(G_\theta)^{-1} = [g_\theta^{ij}], \tag{17}$$

We can show that $g_\theta^{21} = (g_\theta^{12})^*$.

From $G_\theta > 0$, we have g_θ^{11}, $g_\theta^{22} > 0$ and $g_\theta^{11} g_\theta^{22} - |g_\theta^{12}|^2 > 0$. The RLD C-R inequality (16) holds if and only if $\mathrm{tr}\,[V_\theta - (G_\theta)^{-1}] \geq 0$ and $\det[V_\theta - (G_\theta)^{-1}] \geq 0$. Therefore, $V_{11} - g_\theta^{11} \geq 0$, $V_{22} - g_\theta^{22} \geq 0$ and

$$\det\begin{pmatrix} V_{11} - g_\theta^{11} & V_{12} - g_\theta^{12} \\ V_{21} - (g_\theta^{12})^* & V_{22} - g_\theta^{22} \end{pmatrix} \geq 0.$$

The inequality above gives the following inequality.

$$(V_{11} - g_\theta^{11})(V_{22} - g_\theta^{22}) \geq |V_{12} - g_\theta^{12}|^2.$$

The right hand side of the inequality above is written as follows.

$$\begin{aligned} |V_{12} - g_\theta^{12}|^2 &= |V_{12} - \mathrm{Re}\, g_\theta^{12} - \mathrm{i}\,\mathrm{Im}\, g_\theta^{12}|^2 \\ &= |V_{12} - \mathrm{Re}\, g_\theta^{12}|^2 + |\mathrm{Im}\, g_\theta^{12}|^2 \\ &\geq |\mathrm{Im}\, g_\theta^{12}|^2. \end{aligned}$$

Then, we obtain the following inequalities,

$$V_{11} - g_\theta^{11} \geq 0, \quad V_{22} - g_\theta^{22} \geq 0. \tag{18}$$

$$(V_{11} - g_\theta^{11})(V_{22} - g_\theta^{22}) \geq |\mathrm{Im}\, g_\theta^{12}|^2. \tag{19}$$

When $\mathrm{Im}\, g_\theta^{12} = 0$, the uncertainty relation is given by Eq. (18) only.

5.3 Quantum Fisher information matrices: Pure state

5.3.1 Model 1: unitary model generated by p_x and p_y

The SLD Fisher information matrix is calculated by the way given in [13]. The SLD Fisher information matrix is denoted by G_{S}^p. Then, its inverse is

$$(G_{\mathrm{S}}^p)^{-1} = \frac{\lambda^2}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

5.3.2 Model 2: unitary model generated by π_x and π_y

Let G_{S}^π denote the SLD Fisher information matrix of Model 2. Then, the inverse of SLD Fisher information matrix $(G_{\mathrm{S}}^\pi)^{-1}$ is

$$(G_{\mathrm{S}}^\pi)^{-1} = \frac{\lambda^2}{4}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $\tilde{G}_{\mathrm{R}}^\pi$ denote the generalized RLD Fisher information matrix. The inverse of the generalized RLD Fisher information matrix [14] is calculated as

$$(\tilde{G}_{\mathrm{R}}^\pi)^{-1} = \frac{\lambda^2}{4}\begin{pmatrix} 1 & \mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}.$$

5.4 Chemical potential μ, expectation value of angular momentum $\langle L\rangle_0$, and temperature parameters κ_{a} and κ_{b}

From Eqs. (3), (4), and (9),

$$\rho_{\beta,\mu} = Z_{\beta,\mu}^{-1} \mathrm{e}^{-\frac{1}{2}\beta\omega} \mathrm{e}^{-(\beta\omega-\mu)a^\dagger a - \mu b^\dagger b}. \tag{20}$$

$\rho_{\beta,\mu}$ is expressed as

$$\rho_{\beta,\mu} = \rho_{0,a} \otimes \rho_{0,b}, \tag{21}$$

where

$$\rho_{0,a} = \frac{1}{2\pi\kappa_{\mathrm{a}}^2} \int \mathrm{e}^{-\frac{|z|^2}{2\kappa_{\mathrm{a}}^2}} |z\rangle_{a\,a}\langle z|\, d^2z,$$
$$\rho_{0,b} = \frac{1}{2\pi\kappa_{\mathrm{b}}^2} \int \mathrm{e}^{-\frac{|z|^2}{2\kappa_{\mathrm{b}}^2}} |z\rangle_{b\,b}\langle z|\, d^2z.$$

$2\kappa_{\mathrm{a}}^2$ and $2\kappa_{\mathrm{b}}^2$ are

$$2\kappa_{\rm a}^2 = (\mathrm{e}^{\beta\omega-\mu}-1)^{-1},\ \ 2\kappa_{\rm b}^2 = (\mathrm{e}^{\mu}-1)^{-1}. \tag{22}$$

From Eq. (22), we obtain

$$(\mathrm{e}^{\beta\omega}-1)(2\kappa_{\rm a}^2)^2 - [(\mathrm{e}^{\beta\omega}-1)\langle L\rangle_0 + 2]2\kappa_{\rm a}^2 - 1 + \langle L\rangle_0 = 0. \tag{23}$$

$\langle L\rangle_0$ is calculated as

$$\langle L\rangle_0 = \mathrm{tr}\,[L\rho_{\beta,\mu}] = 2\kappa_{\rm a}^2 - 2\kappa_{\rm b}^2. \tag{24}$$

When $\mathrm{e}^{\beta\omega}$ and $\langle L\rangle_0$ are given, $2\kappa_{\rm a}^2$ is the variable of Eq. (23) and Eq. (23) has two solutions for $2\kappa_{\rm a}^2$. However, we can take the larger solution as the solution of Eq. (23), because the smaller one gives the negative $2\kappa_{\rm b}^2$. Then, the relation between μ and $\langle L\rangle_0$ is calculated as

$$\mathrm{e}^{\mu} = \frac{2t}{-t\langle L\rangle_0 + 2 + \sqrt{t^2\langle L\rangle_0^2 + 4t + 4}} + 1, \tag{25}$$

where $t = \mathrm{e}^{\beta\omega} - 1$. At a special case, $\langle L\rangle_0 = 0$, we can see $\mu = \beta\omega/2$ from Eq. (25).

5.5 Quantum Fisher information matrices: Mixed state

5.5.1 Model 1: unitary model generated by p_x and p_y

Let $G_{\rm R}^{p\,\rm thermal}$ and $G_{\rm S}^{p\,\rm thermal}$ be the RLD and the SLD Fisher information matrices, respectively. The inverse of $G_{\rm R}^{p\,\rm thermal}$ is calculated as

$$(G_{\rm R}^{p\,\rm thermal})^{-1} = \frac{\lambda^2}{1+2\kappa_{\rm a}^2+2\kappa_{\rm b}^2} \begin{pmatrix} 2\kappa_{\rm a}^2+2\kappa_{\rm b}^2+8\kappa_{\rm a}^2\kappa_{\rm b}^2 & \mathrm{i}\,(2\kappa_{\rm b}^2-2\kappa_{\rm a}^2) \\ -\mathrm{i}\,(2\kappa_{\rm b}^2-2\kappa_{\rm a}^2) & 2\kappa_{\rm a}^2+2\kappa_{\rm b}^2+8\kappa_{\rm a}^2\kappa_{\rm b}^2 \end{pmatrix}.$$

Next, $(G_{\rm S}^{p\,\rm thermal})^{-1}$ is written as

$$(G_{\rm S}^{p\,\rm thermal})^{-1} = \lambda^2 \frac{\frac{1}{2}+2\kappa_{\rm a}^2+2\kappa_{\rm b}^2+8\kappa_{\rm a}^2\kappa_{\rm b}^2}{1+2\kappa_{\rm a}^2+2\kappa_{\rm b}^2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

5.5.2 Model 2 : unitary model generated by π_x and π_y

The SLD and RLD Fisher information matrices are denoted by $G_{\rm S}^{\pi\,\rm thermal}$ and $G_{\rm R}^{\pi\,\rm thermal}$, respectively. Their inverse matrices are calculated as

$$(G_{\rm S}^{\pi\,\rm thermal})^{-1} = \frac{\lambda^2}{4} \begin{pmatrix} 1+4\kappa_{\rm a}^2 & 0 \\ 0 & 1+4\kappa_{\rm a}^2 \end{pmatrix}, \tag{26}$$

$$(G_{\rm R}^{\pi\,\rm thermal})^{-1} = \frac{\lambda^2}{4} \begin{pmatrix} 1+4\kappa_{\rm a}^2 & \mathrm{i} \\ -\mathrm{i} & 1+4\kappa_{\rm a}^2 \end{pmatrix}. \tag{27}$$

Since this model is a Gaussian shift model [2, 17], the RLD C-R bound is achievable.

Optimal measurements for quantum fidelity between Gaussian states

Changhun Oh[1] Changhyoup Lee[2] Leonardo Banchi[3] Su-Yong Lee[4]
Carsten Rockstuhl[2 5] Hyunseok Jeong[1 *]

[1] *Center for Macroscopic Quantum Control, Department of Physics and Astronomy, Seoul National University, Seoul 08826, Korea*
[2] *Institute of Theoretical Solid State Physics, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany*
[3] *QOLS, Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom*
[4] *School of Computational Sciences, Korea Institute for Advanced Study, Hoegi-ro 85, Dongdaemun-gu, Seoul 02455, Korea*
[5] *Institute of Nanotechnology, Karlsruhe Institute of Technology, 76021 Karlsruhe, Germany*

Abstract. Quantum fidelity is a measure to quantify the closeness between two quantum states. In the present work, we find a closed form of the optimal measurement for quantum fidelity between multi-mode Gaussian states. Based on our general finding, we identify three distinct types of optimal measurements for single-mode Gaussian states: a number detection, projections onto the eigenbasis of operator $\hat{x}\hat{p}+\hat{p}\hat{x}$, and a quadrature variable detection. We also show the equivalence between optimal measurements for quantum fidelity and quantum parameter estimation when two arbitrary states are infinitesimally close. It is applied for simplifying the derivations of quantum Fisher information and the associated optimal measurements, exemplified by displacement, phase, squeezing, and loss parameter estimation using Gaussian states.

Keywords: Quantum Fidelity, Quantum Fisher Information

1 Introduction

Quantum fidelity is a measure of closeness between two quantum states. It has been widely used for assessing quantum information processing protocols such as quantum teleportation, quantum cloning, and quantum error correction. Quantum fidelity is defined as

$$F(\hat{\rho}_0,\hat{\rho}_1)=\min_{\{\hat{E}_x\}}\left(\int\sqrt{p_0(x)p_1(x)}dx\right)^2=\left(\mathrm{Tr}\sqrt{\hat{\rho}_1^{1/2}\hat{\rho}_0\hat{\rho}_1^{1/2}}\right)^2,$$

where $p_j(x)=\mathrm{Tr}[\hat{\rho}_j\hat{E}_x]$ is the probability distribution with POVM $\{\hat{E}_x\}$ for $\hat{\rho}_j(j=0,1)$. It has been found that the optimal measurement for quantum fidelity is given by the projections on the eigenbasis of an operator [1]

$$\hat{M}(\hat{\rho}_0,\hat{\rho}_1)=\hat{\rho}_1^{-1/2}\sqrt{\hat{\rho}_1^{1/2}\hat{\rho}_0\hat{\rho}_1^{1/2}}\hat{\rho}_1^{-1/2}. \quad (1)$$

In the present work, we find the optimal measurement for quantum fidelity between arbitrary Gaussian states.

2 Results

Let us consider two Gaussian states, characterized by the Gibbs matrix G_i and the first moment u_i. The main result is that Eq. (1) can be simplified as [2]

$$\hat{M}\propto\hat{D}(u_1)\exp\left[-\frac{1}{2}\hat{Q}^{\mathrm{T}}G_{\mathrm{M}}\hat{Q}-v_{\mathrm{M}}^{\mathrm{T}}\hat{Q}\right]\hat{D}^{\dagger}(u_1),$$

where G_M satisfies $e^{i\Omega G_{\mathrm{M}}}e^{i\Omega G_1}e^{i\Omega G_{\mathrm{M}}}=e^{i\Omega G_0}$. Here, $\hat{D}(u)=e^{-u^{\mathrm{T}}i\Omega\hat{Q}}$ is the displacement operator. The above expression makes Now, the diagonalization of the operator $\hat{M}$ enables one to find optimal POVMs.

Optimal measurements for quantum fidelity between single-mode Gaussian states can be classified by (Fig. 1)

(i) If the signs of eigenvalues of G_{M} are the same, the eigenbasis of $\hat{M}$ is that of the number operator $\hat{n}=(\hat{x}^2+\hat{p}^2-1)/2$ (up to Gaussian unitary).

(ii) If the signs of eigenvalues are different, the eigenbasis of $\hat{M}$ is that of $\hat{x}\hat{p}+\hat{p}\hat{x}$.

(iii) If only one of the eigenvalues is zero, the eigenbasis of $\hat{M}$ is that of a quadrature operator.

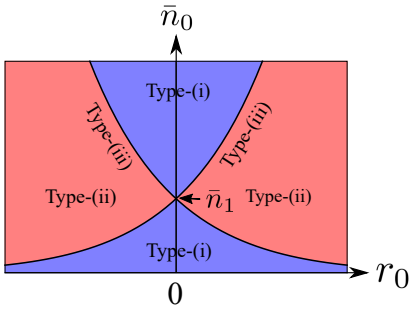


Figure 1: Classification of optimal measurements as a function of r_0 and $\bar{n}_0$ for a given $\bar{n}_1$.

This classification enables one to find optimal setups for given Gaussian states.

We also show the equivalence between optimal measurement for quantum fidelity and that for quantum Fisher information such that the operator $\hat{M}$ is proportional to the symmetric logarithmic derivative (SLD) $\hat{L}_\theta$ which also gives the optimal measurement for quantum parameter estimation of θ. This relation simplifies the derivation of quantum Fisher information and SLD operator, which is exemplified by displacement, phase, squeezing, and loss parameter estimation.

References

[1] C. A. Fuchs and J. V. de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[2] C. Oh, C. Lee, L. Banchi, S.-Y. Lee, C. Rockstuhl, and H. Jeong, arXiv:1901.02994 (2019).

*jeongh@snu.ac.kr

One-shot quantum state exchange

Yonghae Lee[1] * Hayata Yamasaki[2] † Gerardo Adesso[3] ‡ Soojoon Lee[1 3] §

[1] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 02447, Korea*
[2] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*
[3] *School of Mathematical Sciences and Centre for the Mathematics and Theoretical Physics of Quantum Non-Equilibrium Systems, University of Nottingham, University Park, Nottingham NG7 2RD, UK*

Abstract. The quantum state exchange is a quantum communication task in which two users exchange their respective quantum information in the asymptotic setting. In this work, we consider a one-shot version of the quantum state exchange task, in which the users hold a single copy of the initial state, and they exchange their parts of the initial state by means of entanglement-assisted local operations and classical communication. We first derive lower bounds on the least amount of entanglement required for carrying out this task and provide conditions on the initial state with the zero entanglement cost. Based on these results, we figure out two counter-intuitive phenomena in this task, which cannot be explained by the SWAP operation, even though the one-shot quantum state exchange and the SWAP operation operationally provide the same result. One tells how the users deal with their symmetric information to reduce the entanglement cost. The other shows that it is possible for the users to share extra entanglement after this task.

Keywords: quantum communication task, quantum state exchange, optimal entanglement cost

1 One-shot quantum state exchange

The one-shot quantum state exchange is a quantum information task in which two users, Alice and Bob, hold parts A and B of the initial state $|\psi\rangle \equiv |\psi\rangle_{A_1B_1A_2B_2R}$ with systems $A = A_1A_2$ and $B = B_1B_2$, respectively. Their goal is either to exchange their parts A_1 and B_1 or to exchange their whole parts A and B. Specifically, let ψ_{f_1}, and $\psi_{f_{12}}$ be the final states of the the task given by

$$\begin{aligned}\psi_{f_1} &= \left(\mathbb{1}_{A_1\to A_1'} \otimes \mathbb{1}_{B_1\to B_1'} \otimes \mathbb{1}_{A_2B_2R}\right)(\psi),\\ \psi_{f_{12}} &= \left(\mathbb{1}_{A\to A'} \otimes \mathbb{1}_{B\to B'} \otimes \mathbb{1}_{R}\right)(\psi),\end{aligned}$$

where $\psi = |\psi\rangle\langle\psi|$, and the dimension of the system X' is identical to that of the system X. Note that B_1', B' and A_1', A' are Alice's and Bob's systems, respectively.

Definition 1 (One-shot quantum state exchange) *Three joint operations*

$$\begin{aligned}\mathcal{E}^{1}_{\psi,K,L} &: A_1E_{\mathrm{A}}^{\mathrm{in}} \otimes B_1E_{\mathrm{B}}^{\mathrm{in}} \longrightarrow B_1'E_{\mathrm{A}}^{\mathrm{out}} \otimes A_1'E_{\mathrm{B}}^{\mathrm{out}},\\ \mathcal{E}^{1|2}_{\psi,K,L} &: AE_{\mathrm{A}}^{\mathrm{in}} \otimes BE_{\mathrm{B}}^{\mathrm{in}} \longrightarrow B_1'A_2E_{\mathrm{A}}^{\mathrm{out}} \otimes A_1'B_2E_{\mathrm{B}}^{\mathrm{out}},\\ \mathcal{E}^{12}_{\psi,K,L} &: AE_{\mathrm{A}}^{\mathrm{in}} \otimes BE_{\mathrm{B}}^{\mathrm{in}} \longrightarrow B'E_{\mathrm{A}}^{\mathrm{out}} \otimes A'E_{\mathrm{B}}^{\mathrm{out}},\end{aligned}$$

are called the one-shot quantum state exchange *protocols of $|\psi\rangle$, if they are performed by local operations and classical communication between Alice and Bob, and satisfy*

$$\begin{aligned}\psi_{f_1}\otimes\Phi &= \left(\mathcal{E}^{1}_{\psi,K,L}\otimes\mathbb{1}_{A_2B_2R}\right)(\psi\otimes\Psi)\\ &= \left(\mathcal{E}^{1|2}_{\psi,K,L}\otimes\mathbb{1}_{R}\right)(\psi\otimes\Psi),\\ \psi_{f_{12}}\otimes\Phi &= \left(\mathcal{E}^{12}_{\psi,K,L}\otimes\mathbb{1}_{R}\right)(\psi\otimes\Psi),\end{aligned}$$

where Ψ and Φ are pure maximally entangled states with Schmidt rank K and L on systems $E_{\mathrm{A}}^{\mathrm{in}}E_{\mathrm{B}}^{\mathrm{in}}$ and $E_{\mathrm{A}}^{\mathrm{out}}E_{\mathrm{B}}^{\mathrm{out}}$, respectively.

Depending on the types of one-shot quantum state exchange protocols, we define their optimal entanglement costs as follows.

Definition 2 (Optimal entanglement cost) *The following quantities are* optimal entanglement costs *of the one-shot quantum state exchange:*

$$\begin{aligned}\mathbf{e}_{A_1\leftrightarrow B_1}(\psi) &= \inf_{\mathcal{E}^{1}_{\psi,K,L}} \left(\log K - \log L\right),\\ \mathbf{e}^{A_2B_2}_{A_1\leftrightarrow B_1}(\psi) &= \inf_{\mathcal{E}^{1|2}_{\psi,K,L}} \left(\log K - \log L\right),\\ \mathbf{e}_{A\leftrightarrow B}(\psi) &= \inf_{\mathcal{E}^{12}_{\psi,K,L}} \left(\log K - \log L\right),\end{aligned}$$

where the quantity $\log K - \log L$ is called the entanglement cost *of the one-shot quantum state exchange protocol, and the infimums are taken over all joint protocols $\mathcal{E}^{1}_{\psi,K,L}$, $\mathcal{E}^{1|2}_{\psi,K,L}$, and $\mathcal{E}^{12}_{\psi,K,L}$.*

2 Lower and upper bounds

As in the asymptotic quantum state exchange [1, 2], in order to find out a lower bound of the one-shot quantum state exchange of $|\psi\rangle_{A_1B_1A_2B_2R}$, we here imagine that the referee who holds R can assist Alice and Bob to exchange A_1 and B_1.

Theorem 3 *The optimal entanglement cost $\mathbf{e}^{A_2B_2}_{A_1\leftrightarrow B_1}(\psi)$ is lower bounded by*

$$l_{1|2}(\psi) = \sup_{F,\mathcal{N}} \left[F(\mathcal{N}(\psi)_{B_1A_2R_{\mathrm{A}}}) - F(\mathcal{N}(\psi)_{AR_{\mathrm{A}}})\right],$$

where F is an additive and Schur concave function such that $F(\sigma^M) = \log M$ for any M and $\mathcal{N}(\rho)$ is a quantum channel from R to R_{A}.

*yonghaelee@khu.ac.kr
†yamasaki@qi.t.u-tokyo.ac.jp
‡gerardo.adesso@nottingham.ac.uk
§level@khu.ac.kr

From Theorem 3, we obtain the following *computable* lower bound.

Corollary 4

$$\begin{aligned}
\mathbf{e}_{A_1\leftrightarrow B_1}(\psi) &\geq \max_{\alpha\in[0,\infty]} |S_\alpha(\rho_{A_1}) - S_\alpha(\rho_{B_1})|, \\
\mathbf{e}^{A_2B_2}_{A_1\leftrightarrow B_1}(\psi) &\geq l^c_{1|2}(\psi) = \max_{\alpha\in[0,\infty]} f_\psi(\alpha), \\
\mathbf{e}_{A\leftrightarrow B}(\psi) &\geq \max_{\alpha\in[0,\infty]} |S_\alpha(\rho_A) - S_\alpha(\rho_B)|,
\end{aligned}$$

where S_α is the quantum Rényi entropy of order α, and $f_\psi(\alpha)$ is a function of $|\psi\rangle$ and α defined by $f_\psi(\alpha) = \max\{S_\alpha(\rho_{A_1B_2}) - S_\alpha(\rho_B), S_\alpha(\rho_{B_1A_2}) - S_\alpha(\rho_A)\}$.

3 Conditions for the zero entanglement cost

We present conditions on the initial state with the zero entanglement cost.

Let (X, Y) be a pair of two systems, which can be either (A_1, B_1) or (A, B), and consider a spectral decomposition of the reduced state ρ_{XY} for $|\psi\rangle$, $\rho_{XY} = \sum_{i=1}^N \lambda_i |\xi_i\rangle\langle\xi_i|_{XY}$, where $\lambda_i > 0$ with $\sum_{i=1}^N \lambda_i = 1$. For each i, we define the matrix $\Omega^i_{XY}(\psi)$ by

$$\Omega^i_{XY}(\psi) = \sum_{j,k} (\langle j|_X \otimes \langle k|_Y) |\xi_i\rangle_{XY} |j\rangle\langle k|,$$

where $\{|j\rangle\}$ and $\{|k\rangle\}$ indicate the computational bases on Alice's and Bob's systems, respectively. Then we obtain the following sufficient condition.

Theorem 5 *Let (X, Y) be either (A_1, B_1) or (A, B). If there exist isometries U and V such that for each i,*

$$\left(\Omega^i_{XY}(\psi)\right)^t = U\Omega^i_{XY}(\psi)V,$$

then $\mathbf{e}_{X\leftrightarrow Y}(\psi) = 0$, where W^t is the transpose of the matrix W.

From the lower bounds on the optimal entanglement costs $\mathbf{e}_{A_1\leftrightarrow B_1}$ and $\mathbf{e}_{A\leftrightarrow B}$ in Corollary 4, observe that if the spectrum of Alice's state is different from that of Bob's state, then the optimal entanglement cost cannot be zero. Based on this observation, we obtain the following theorem.

Theorem 6 *Let (X, Y) be either (A_1, B_1) or (A, B). If $\mathbf{e}_{X\leftrightarrow Y}(\psi) = 0$, then there exists an isometry $U_{X\to Y}$ such that $\rho_Y = U_{X\to Y}\rho_X(U_{X\to Y})^\dagger$.*

4 Counter-intuitive phenomena

We are now in the position to present two phenomena which show the differences between the one-shot quantum state exchange task and the SWAP operation. We refer the reader to Ref. [4] for more detailed explanations of this section.

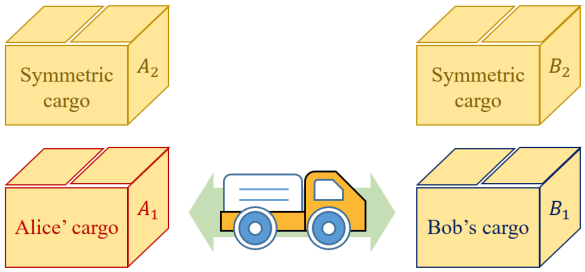


Figure 1: Illustration for the cargo exchange task. The cargoes A_1A_2 and B_1B_2 belong to Alice and Bob, respectively. Assume that the cargoes A_2 and B_2 are symmetric, but A_1 and B_1 are not symmetric. When Alice and Bob exchange their whole cargoes A_1A_2 and B_1B_2, it suffices for them to exchange A_1 and B_1, since A_2 is identical to B_2. In the illustration, the truck indicates the cost needed for exchanging A_1 and B_1.

4.1 Symmetric information

For the initial state $|\psi\rangle$, let us consider a situation that Alice and Bob exchange their whole information A and B. Assume that their parts A_2 and B_2 are symmetric, while the rest parts A_1 and B_1 are not symmetric, i.e., the initial state $|\psi\rangle$ satisfies

$$(\mathrm{SWAP}_{A_1\leftrightarrow B_1})(\psi) \neq \psi \quad \text{and} \quad (\mathrm{SWAP}_{A_2\leftrightarrow B_2})(\psi) = \psi,$$

where $\mathrm{SWAP}_{X\leftrightarrow Y}$ is the operation swapping quantum states in systems X and Y.

From a viewpoint of the SWAP operation, if Alice and Bob want to exchange A and B, then it suffices for them to exchange A_1 and B_1, since A_2 is identical to B_2. This situation can be more easily understood by using a cargo exchange as a metaphor for the SWAP operation as depicted in Fig. 1. In the cargo exchange, assume that Alice and Bob want to exchange their whole cargoes, and some of the cargoes are symmetric. In terms of efficiency, it is reasonable for them to exchange only A_1 and B_1 in order to reduce the cargo exchange cost, because the cargoes A_2 and B_2 are the same.

On the other hand, in the one-shot quantum state exchange, the proper use of the symmetric parts A_2 and B_2 can more efficiently reduce the entanglement cost compared to exchanging only A_1 and B_1 without using A_2 and B_2. To be specific, there exists an initial state $|\psi\rangle$ such that the parts A_2 and B_2 are symmetric and $\mathbf{e}_{A\leftrightarrow B}(\psi) = 0$ while the rest parts A_1 and B_1 are not symmetric. Consider the specific initial state

$$|\phi_1\rangle_{A_1B_1A_2B_2R} = \frac{1}{\sqrt{2}}(|00000\rangle + |01111\rangle),$$

where A_2 and B_2 are symmetric but A_1 and B_1 are not. Since $\Omega^1_{AB}(\phi_1) = |00\rangle\langle 00|$ and $\Omega^2_{AB}(\phi_1) = |01\rangle\langle 11|$, we can show that $\Omega^1_{AB}(\phi_1)$ and $\Omega^2_{AB}(\phi_1)$ satisfy the condition in Theorem 5, by setting

$$U = V = |00\rangle\langle 00| + |01\rangle\langle 11| + |10\rangle\langle 10| + |11\rangle\langle 01|.$$

Thus we obtain that $\mathbf{e}_{A\leftrightarrow B}(\phi_1) = 0$, which means that A and B can be exchanged by means of local operations

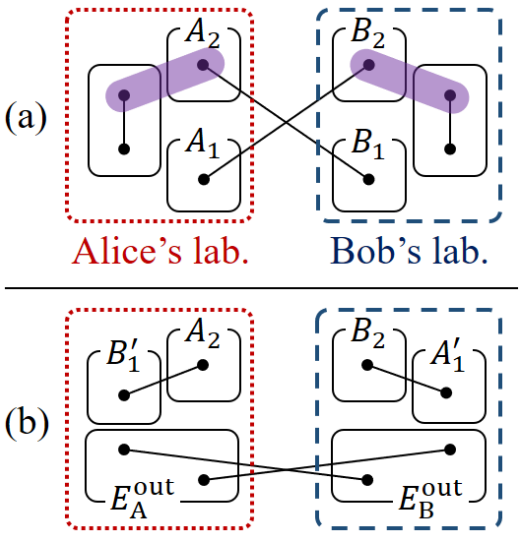


Figure 2: Illustration of a one-shot quantum state exchange protocol of $|\phi_2\rangle$ in Eq. (1). (a) In order to exchange A_1 and B_1, Alice and Bob locally prepare an ebit, respectively, and they apply Bell measurements to the shaded areas. (b) By performing local operations corresponding to the measurement outcomes, the parts A_1 and B_1 can be exchanged. At the same time, Alice and Bob can share two ebits.

and classical communication without consuming any nonlocal resource. As mentioned above, this is somewhat counter-intuitive, since this phenomenon cannot occur when using the SWAP operation.

4.2 Negative entanglement cost

As in the asymptotic quantum state exchange task [1, 2], there exists an initial state to show that the entanglement cost of the one-shot quantum state exchange task can be negative. Assume that Alice and Bob exchange the parts A_1 and B_1 of the initial state

$$|\phi_2\rangle_{A_1B_1A_2B_2} = \frac{1}{2}\sum_{i,j=0}^{1} |i\rangle_{A_1} |j\rangle_{B_1} |j\rangle_{A_2} |i\rangle_{B_2}, \quad (1)$$

where $|\phi_2\rangle$ consists of two ebits $|e\rangle_{A_1B_2}$ and $|e\rangle_{B_1A_2}$. To exchange A_1 and B_1, both Alice and Bob prepare an ebit, respectively, and they locally apply the entanglement swapping [3] by performing two Bell measurements on A_2, B_2, and the parts of the ebits, as described in Fig. 2. Then they can exchange A_1 and B_1, and can share two ebits at the same time. This means that the entanglement cost can be negative. In fact, we have $\mathbf{e}_{A_1\leftrightarrow B_1}^{A_2B_2}(\phi_2) = -2$ from Corollary 4. Compared to the SWAP operation, the negativity of the entanglement cost is quite interesting, since Alice and Bob cannot share entanglement after the SWAP operation.

5 Acknowledgments

We would like to thank Ryuji Takagi and Bartosz Regula for fruitful discussion. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (NRF-2019R1A2C1006337) and the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2018-0-01402) supervised by the IITP (Institute for Information & communications Technology Promotion). H. Y. acknowledges Grant-in-Aid for JSPS Research Fellow, JSPS KAKENHI Grant No. 18J10192, Cross-ministerial Strategic Innovation Promotion Program (SIP) (Council for Science, Technology and Innovation (CSTI)), and CREST (Japan Science and Technology Agency) JPMJCR1671. G. A. acknowledges support from the ERC Starting Grant GQCOP (Grant Agreement No. 637352).

References

[1] J. Oppenheim and A. Winter. Uncommon information (the cost of exchanging a quantum state). quant-ph/0511082, 2008.

[2] Y. Lee, R. Takagi, H. Yamasaki, G. Adesso, and S. Lee. State Exchange with Quantum Side Information. *Phys. Rev. Lett.*, 122(1):010502, 2019.

[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, 1993.

[4] Y. Lee, H. Yamasaki, G. Adesso, and S. Lee. One-shot quantum state exchange. arXiv:1905.12332, 2019.

Reversibility and its Connection to the Quantum Computational Speed-up

Niklas Johansson[1] * Jan-Åke Larsson[1] †

[1] *Institutionen för systemteknik, Linköpings Universitet, 581 83 Linköping, SWEDEN*

Abstract. The speed-up of Quantum Computers is the current drive of an entire scientific field with several large research programs, both in industry and academia world-wide. Many of these programmes are intended to build hardware for quantum computers. A related important goal is to understand the reason for quantum computational speed-up; to understand what resources are provided by the quantum system used in quantum computation. Some candidates for such resources include superposition and interference, entanglement, nonlocality, contextuality, and the continuity of state-space. The standard approach to resource studies is to restrict quantum mechanics and characterize the resources needed to restore the advantage. Our approach instead extend the classical information carriers with an additional degrees-of-freedom, to mirror the quantum information carriers. In this contribution, we will have a look at these additional degrees-of-freedom and how quantum computers make use of them to achieve quantum speedup. We will also discuss whether the additional degrees-of-freedom can be viewed as a "side channel," a term often seen in cryptography, and whether quantum parallelism rather should be viewed as computation performed in this additional degree-of-freedom.

Keywords: Computational Resources, Quantum Algorithms, Conditions for Quantum Computation

For all we know, quantum computers can solve certain problems faster than classical computers. This drives several large research programs in both academia and industry, where one of the important goals is to understand the reason for this speed-up; to understand what resources a quantum system provides that enable the computational advantage. Some candidates for such resources are interference [1], entanglement [7], nonlocality [2], contextuality [3, 8, 5], continuity of the state space [6], and even coherence [9, 10].

Another property that distinguish quantum systems, from those used in classical information processing, is that they have additional degrees-of-freedom. For instance, a qubit can be measured in the computational basis or in the Hadamard basis. These bases are *mutually unbiased*, meaning that a projective measurement along one of the bases gives no information about a projective measurement along the other. And indeed, the observables representing these measurements are orthogonal.

*niklas.johansson@liu.se

†jan-ake.larsson@liu.se

The canonical condition for quantum computation is that the function is computed according to the unitary operator

$$U_f \left|x\right\rangle \left|a\right\rangle = \left|x\right\rangle \left|a \oplus f(x)\right\rangle , \tag{1}$$

or a unitarily equivalent operator. We can make tree important observation from this:

(1) The function is computed reversibly in the computational basis,

(2) any auxiliary systems should be cleared,

(3) while all relative phases $c_{x,y}$ are preserved, that is

$$\begin{aligned} &\sum_{x,y} c_{x,y} \left|x\right\rangle \left|y\right\rangle \\ \mapsto &\sum_{x,y} c_{x,y} \left|x\right\rangle \left|y \oplus f(x)\right\rangle . \end{aligned} \tag{2}$$

For a computation to be reversible it needs to store enough information about its history, so that it can be reversed [11]. Storing this information can lead to an undesirable scaling of

memory usage, but in a special case the input can serve as the history of the computation,

$$(x, 0) \mapsto (x, f(x)). \tag{3}$$

This can always be guaranteed by first computing the function and storing the history, copy out the result of the computation to another register, and then reversing the first computation and thereby also reverse storing the history [12].

$$\begin{aligned} \big(x, 0, 0\big) &\mapsto \big(h, f(x), 0\big) \\ \mapsto \big(h, f(x), f(x)\big) &\mapsto \big(x, 0, f(x)\big) \end{aligned} \tag{4}$$

This is exactly what we see in the computational basis of quantum algorithms, but this is not what happens in the additional degree-of-freedom from which quantum computation gain its advantage. The information processing that takes place in the other degrees-of-freedom is imposed by the condition on the relative phases. By formalizing this explicitly we show how the speed-up emerges from the information carriers having additional degrees-of-freedom together with the requirements of quantum computation.

Our result also has implications to post quantum cryptography. Some cryptographic protocols have been deemed vulnerable to quantum computers, as there are quantum algorithms that can efficiently retrieve their secret [6]. But for some of these protocols [13, 14, 15], employing the attack requires that the secret is built into the quantum circuit. In this case, our result shows that these are so-called side-channel attacks, and should not be deemed vulnerable to quantum computers (since all protocols are vulnerable to side-channel attacks).

References

[1] Richard P. Feynman. "Simulating Physics with Computers". In: *International Journal of Theoretical Physics* 21 (1982), pp. 467–488. DOI: 10.1007/BF02650179.

[2] John S. Bell. "On the Einstein Podolsky Rosen Paradox". In: *Physics (Long Island City, N. Y.)* 1 (1964), pp. 195–200.

[3] Simon Kochen and E. P. Specker. "The Problem of Hidden Variables in Quantum Mechanics". In: *Journal of Mathematics and Mechanics* 17 (1967), pp. 59–87. DOI: 10.2307/24902153.

[4] Jan-Åke Larsson. "A contextual extension of Spekkens' toy model". In: *AIP Conference Proceedings*. Foundations of Probability and Physics - 6. Vol. 1424. AIP Publishing, 2012, pp. 211–220. DOI: 10.1063/1.3688973.

[5] Mark Howard et al. "Contextuality Supplies the 'Magic' for Quantum Computation". In: *Nature* (2014). DOI: 10.1038/nature13460.

[6] P. W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[7] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Physical Review* 47 (1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777.

[8] Matthias Kleinmann et al. "Memory Cost of Quantum Contextuality". In: *New Journal of Physics* 13 (2011), p. 113011. DOI: 10.1088/1367-2630/13/11/113011.

[9] T. Baumgratz, M. Cramer, and M. B. Plenio. "Quantifying Coherence". In: *Physical Review Letters* 113 (2014), p. 140401. DOI: 10.1103/PhysRevLett.113.140401.

[10] Mark Hillery. "Coherence as a Resource in Decision Problems: The Deutsch-Jozsa Algorithm and a Variation". In: *Physical Review A* 93 (2016), p. 012111. DOI: 10.1103/PhysRevA.93.012111.

[11] R. Landauer. "Irreversibility and Heat Generation in the Computing Process". In: *IBM Journal of Research and Development* 5 (1961), pp. 183–191. DOI: 10.1147/rd.53.0183.

[12] C. H. Bennett. “Logical Reversibility of Computation”. In: *Maxwell’s Demon. Entropy, Information, Computing* (1973), pp. 197–204.

[13] H. Kuwakado and M. Morii. “Quantum Distinguisher between the 3-Round Feistel Cipher and the Random Permutation”. In: *2010 IEEE International Symposium on Information Theory*. 2010, pp. 2682–2685. DOI: 10.1109/ISIT.2010.5513654.

[14] H. Kuwakado and M. Morii. “Security on the Quantum-Type Even-Mansour Cipher”. In: *2012 International Symposium on Information Theory and Its Applications*. 2012, pp. 312–316. ISBN: 978-4-88552-267-3.

[15] Marc Kaplan et al. “Breaking Symmetric Cryptosystems Using Quantum Period Finding”. In: *Advances in Cryptology – CRYPTO 2016*. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2016, pp. 207–237. DOI: 10.1007/978-3-662-53008-5_8.

Matrix Product State Based Quantum Classifier

Amandeep Singh Bhatia[12] * Mandeep Kaur Saggi[2] † Ajay Kumar[2] ‡ Sushma Jain[2] §

[1] *Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India*
[2] *Department of Computer Science, Thapar Institute of Engineering & Technology, Punjab, India*

Abstract. In recent years, interest in expressing the success of neural networks to the quantum computing has increased significantly. Tensor network theory has become increasingly popular and widely used to simulate strongly entangled correlated systems. Matrix product state (MPS) is the well-designed class of tensor network states, which plays an important role in processing of quantum information. In this paper, we have shown that matrix product state as one-dimensional array of tensors can be used to classify classical and quantum data. We have performed binary classification of classical machine learning dataset Iris encoded in a quantum state. Further, we have investigated the performance by considering different parameters on the ibmqx4 quantum computer and proved that MPS circuits can be used to attain better accuracy. Further, the learning ability of MPS quantum classifier is tested to classify evapotranspiration (ET_o) for Patiala meteorological station located in Northern Punjab (India), using three years of historical dataset (Agri).

Keywords: Quantum machine learning, classification, tensor network, matrix product state, IBM quantum computer

1 Introduction

In the last decade, the simulation of open and closed quantum systems has got overwhelming response. The study of tensor network theory taking a central role in quantum physics and beyond. It is simply a countable group of tensors associated by contractions. Tensor network states are a new language, based on entanglement, for quantum many-body systems [1]. Tensor network states are classified on the basis of dimensions along which the tensors are traversed. It is widely used to simulate strongly entangled correlated systems and to represent quantum states and circuits [2]. 'Tensor network methods' is the term associated with the tools, which are widely employed in experimental and quantum theoretical applications of machine learning. The matrix product state (MPS) is the most prominent example of tensor network states which is maximally unbalanced.

Matrix product states are compelling for their wide range of practical applications: supervised learning [3], quantum finite state machines [5], unsupervised learning [6], simulating MPS on a quantum computer [7], quantum machine learning MPS [8] and many more. Matrix product states are complete, where low entangled states are represented efficiently, which is not possible with large dimensions tensor network states. Recently, MPS method have been introduced to compress the weights of neural network layers and classify the images.

Huggins et al. [10] proposed tensor network based quantum computing approaches for generative and discriminative tasks. The main purpose is to generate samples from a probability distribution and assign labels to images. The experimentation is executed on quantum hardware using optimization procedure for handwritten classes of images and noise resilience is tested of the training model. Grant et al. [4] introduced the concept of hierarchical quantum classifiers and executed binary classification for classical and quantum data. Two classical machine learning datasets Iris and MNIST are considered and deployed the classifiers on quantum computer. It has shown impressive results and better accuracy by considering different unitary parameters. In this paper, following contributions are claimed: (1) We demonstrate that matrix product state as one-dimensional array of tensors can be used to classify quantum mechanical data in addition to classical dataset. (2) We encode classical dataset (Iris and Agri) into quantum entangled state, which is given as an input to MPS tensor network quantum circuit. (3) Four and six qubit inputs are taken for Iris and Agri dataset and measurement is performed on quantum circuit. (4) To investigate the performance, MPS classifier on real-time quantum device (ibmqx4) is deployed.

2 Matrix product state

Matrix product state concedes the extent of entanglement in bond dimensions. It is a method of tensor network, where the tensors are connected in a one-dimensional geometry. Figure 1 shows the MPS as one-dimensional array of tensors and an instance of finite system of 5 sites. In MPS, a pure quantum state $|\phi\rangle$ is represented as:

$$|\phi\rangle = \sum_{\sigma_1,\sigma_2,...\sigma_L}^{d} Tr[M_1^{\sigma_1} M_2^{\sigma_2} ... M_L^{\sigma_L}] \, |\sigma_1, \sigma_2, ...\sigma_L\rangle \quad (1)$$

where $M_i^{\sigma_i}$ are complex square matrices, d is dimension, σ_i represents the indices i.e. {0, 1} for qubits and $Tr()$ denotes trace of matrices [5].

2.1 Encoding of classical data

In quantum mechanics, the N independent systems can be combine by performing tensor product operation on

*amandeepbhatia.singh@gmail.com
†mandeepsaggi90@gmail.com
‡ajaykumar@gmail.com
§sjain@thapar.edu.in

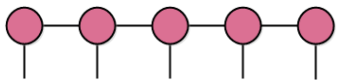


Figure 1: Representation of MPS with 5 sites

their respective state vectors [3, 10]. Consider a feature map

$$\phi^d(x) = \phi^{s_1}(x_1) \otimes \phi^{s_2}(x_2) \otimes ... \otimes \phi^{s_N}(x_N) \qquad (2)$$

where s_j are indices run over the local dimension d such that d=$\{s_1, s_2, ..., s_N\}$. Therefore, each state vector x_j is mapped to full feature map $\phi(x)$ in a d-dimensional space. Fig 2 shows the tensor diagram of full feature map $\phi(x)$.

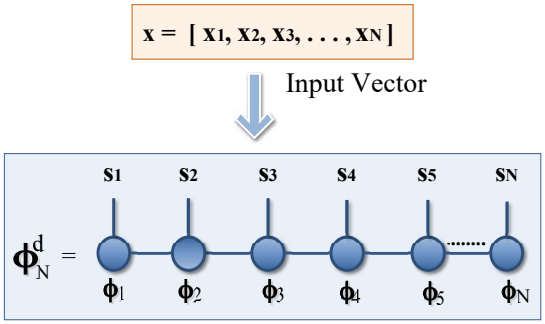


Figure 2: Mapping of input vector to order N tensor

Consider a classical dataset $S = \{(x^d, y^d)\}_{d=1}^D$ for binary classification, where $y^d \in \{0, 1\}$ are class labels for N-dimensional input vectors such that $x^d \in \mathbb{R}^N$. We have normalized the input vectors to lie in $[-\pi, \pi]$. Thus, the qubit ϕ is represented as

$$\phi_n^d = cos(x_n^d)\,|0\rangle + sin(x_n^d)\,|1\rangle \qquad (3)$$

$$\phi_n^d = \begin{bmatrix} cos(x_1^d) \\ sin(x_1^d) \end{bmatrix} \otimes \begin{bmatrix} cos(x_2^d) \\ sin(x_2^d) \end{bmatrix} \otimes ... \otimes \begin{bmatrix} cos(x_N^d) \\ sin(x_N^d) \end{bmatrix} \qquad (4)$$

We map the N-dimensional input vectors $x^d \in \mathbb{R}^N$ to a product state on N qubits by using the feature map Eq. (2). The full quantum data is represented as tensor product $\phi^d = \otimes_{n=1}^N \phi_n^d$ [10, 4]. Thus, the preparation of quantum state is efficient as it only needs single-qubit rotations to encode each segment of classical dataset $n = \{1, 2, ...N\}$ in the amplitude of a qubit. Similar to classical dataset for binary classification, quantum data set for binary classification is denoted as a set $S_q = \{(\phi^d, y^d)\}_{d=1}^D$, where $y^d \in \{0, 1\}$ are class labels for 2^N-dimensional input vectors such that $\phi^d \in \mathbb{C}^{2^N}$. It can be easily checked that quantum data as a output of quantum circuit is in superposition state.

3 Quantum circuit classifier

We now discuss MPS quantum circuit classifier for classification of quantum data, which is made up of unitaries. We followed iterative approach by keeping positive trace values from N-qubit input space to output qubits. We

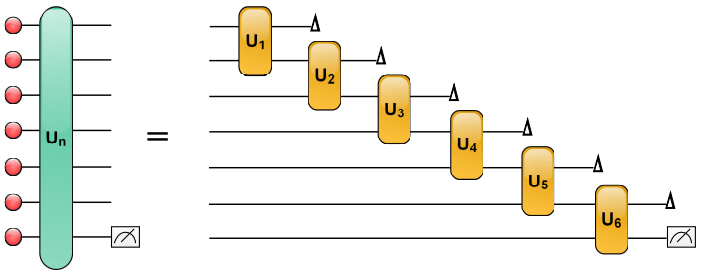


Figure 3: Matrix product state quantum classifier

apply unitaries composed of single qubit rotations around y-axis and CNOT gate to the input set and discard one of the qubits (unobserved) from each unitary. Therefore, we split the qubit into two parts for the next layer of the circuit. This process continues till the last qubit is left to be measured. It can be noted that at each stage of the circuit, we keep one of the qubits resulting from one of the unitary operations of the earlier stage and at last unitary transformation occurs on two qubits from another subpart of the circuit. The unitary blocks in Fig 3 consists of input dataset with ancilla qubit which is initialized to zero. It can be easily traced out. Using ancilla qubit, we can execute large class of non-linear operations. Fig 4 shows the seven stages of our methodology for model development.

In order to assess the quality of actual and predicted values of dataset, we need to calculate the cost function. It measures the difference between actual and predicted values of dataset. It is given as:

$$J_\theta = \frac{1}{D} \sum_{d=1}^{D} (M_\theta(x^d) - y^d)^2 \qquad (5)$$

where x^d and y^d are the input and class labels respectively, M is qubit operator, θ represents the set of parameters to define the unitaries and D is total number of data points. It calculates the average amount that the model's predictions differ from the actual values. The goal is to minimizing the cost function i.e. it must be close to zero.

3.1 Experimental results

Table 1: Performance comparison of MPS for each samples of Iris dataset

Training					
Sample	Cost	ACC	Spec	Sens	Gini
Iris_1	0.11	88.75	0.86	0.90	0.80
Iris_2	0.16	83.75	0.82	0.84	0.80
Iris_3	0.05	95	0.90	1.0	0.92
Testing					
Sample	Cost	ACC	Spec	Sens	Gini
Iris_1	0.15	85	0.85	0.83	0.67
Iris_2	0.2	80	0.71	1.0	0.50
Iris_3	0.1	90	0.84	1.0	0.77

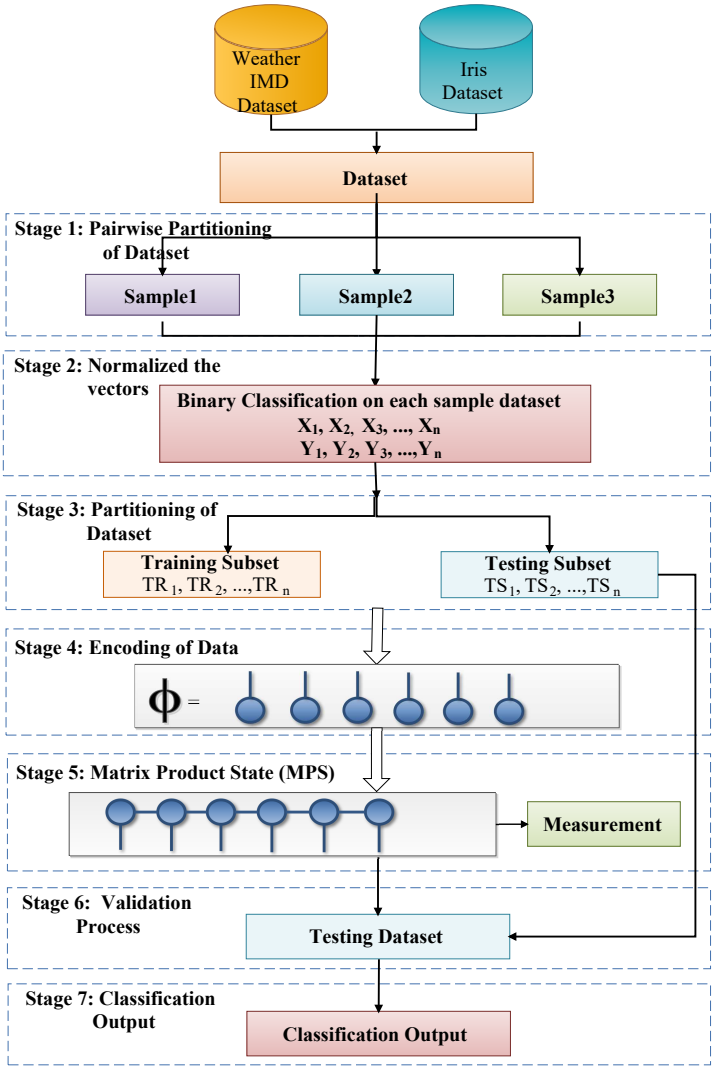


Figure 4: Model development phases for classification

Table 2: Performance comparison of MPS for each samples of Agri dataset

Training					
Sample	Cost	ACC	Spec	Sens	Gini
$Agri_1$	0.20	79.03	0.98	0.72	0.52
$Agri_2$	0.24	75.34	0.68	0.82	0.51
$Agri_3$	0.21	78.73	0.73	0.89	0.61
Testing					
Sample	Cost	ACC	Spec	Sens	Gini
$Agri_1$	0.19	80.65	0.76	0.83	0.53
$Agri_2$	0.26	73.33	0.67	0.79	0.50
$Agri_3$	0.22	77.04	0.77	0.75	0.53

We have tested the ability of MPS quantum classifier to classify Iris dataset and weather Indian Meteorological Department (IMD) dataset. In experimentation, we have given qubit rotations in y-direction to have real values and parameterized the unitaries using ancilla qubit. The performance comparison of MPS for each samples of Iris and Agri datasets is shown in Table 1 and Table 2.

4 Conclusion

In this paper, we have illustrated that matrix product state quantum classifier can be used to classify quantum data efficiently. We have focused on MPS quantum circuit augmented with ancilla qubit that is implemented on quantum computer with restriction on qubit rotations to be real only. The key advantage of executing classification with MPS quantum circuit is that it can be executed efficiently with small number of qubits. The MPS quantum classifier has shown great learning capability for Iris and Agri datasets.

Acknowledgments

Amandeep Singh Bhatia was supported by Maulana Azad National Fellowship (MANF), funded by Ministry of Minority Affairs, Government of India. Mandeep Kaur Saggi was supported by Council of Scientific & Industrial Research (CSIR), funded by R&D organization, India.

References

[1] X. Gao, L.-M. Duan, Efficient representation of quantum many-body states with deep neural networks, Nature communications 8 (1) (2017) 662.

[2] M. Schuld, A. Bocharov, K. Svore, N. Wiebe, Circuit-centric quantum classifiers, arXiv:1804.00633.

[3] E. Miles Stoudenmire, D. J. Schwab, Supervised learning with quantum-inspired tensor networks, arXiv:1605.05775.

[4] E. Grant, M. Benedetti, S. Cao, A. Hallam, J. Lockhart, V. Stojevic, A. G. Green, S. Severini, Hierarchical quantum classifiers, npj Quantum Information 4 (65) (2018).

[5] A. S. Bhatia, A. Kumar, Quantifying matrix product state, Quantum Information Processing 17 (3) (2018) 41.

[6] Z.-Y. Han, J. Wang, H. Fan, L. Wang, P. Zhang, Unsupervised generative modeling using matrix product states, Physical Review X 8 (3) (2018) 031012.

[7] A. S. Bhatia, M. K. Saggi, Implementing entangled states on a quantum computer, arXiv:1811.09833.

[8] J. Biamonte, Quantum machine learning matrix product states, arXiv:1804.02398.

[9] B. Gardas, M. M. Rams, J. Dziarmaga, Quantum neural networks to simulate many-body quantum systems, Physical Review B 98 (18) (2018) 184304.

[10] W. Huggins, P. Patel, K. B. Whaley, E. M. Stoudenmire, Towards quantum machine learning with tensor networks, arXiv:1803.11537.

Quantum State Smoothing for Linear Gaussian Systems

Kiarn T. Laverick[1] * Areeya Chantasri[1] † Howard M. Wiseman[1] ‡

[1] *Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, Nathan, Queensland 4111, Australia*

Abstract. Quantum state smoothing is a technique for assigning a valid quantum state to a partially observed dynamical system, using measurement records both prior and posterior to an estimation time. We show that the technique is greatly simplified for Linear Gaussian quantum systems, with wide physical applicability. We derive a closed-form solution for the quantum smoothed state, which is more pure than the standard filtered state, whilst still being described by a physical quantum state. We apply the theory to an on-threshold optical parametric oscillator, exploring optimal conditions for purity recorvery. This work has recently been published in *Physical Review Letters*, see Ref. [1].

Keywords: Quantum State Estimation, Smoothing, Linear Gaussian Systems

Smoothing and filtering are techniques in classical estimation of dynamical systems to calculate probability density functions (PDFs) of quantities of interest at some time t, based on available data from noisy observation of such quantities in time. In filtering, the observed data up to time t is used in the calculation. In smoothing, the observed data both before (past) and after (future) t can be used. For dynamical systems where real-time estimation of the unknown parameters is not required, smoothing almost always gives more accurate estimates than filtering. In the quantum realm, numerous formalisms have been introduced which use past and future information [2–8]. Many of these ideas have been applied, theoretically and experimentally, to the estimation of unknown classical parameters affecting quantum systems [9–15], or of hidden results of quantum measurements [16–21]. The optimal improvement obtained by using future information in these applications comes from using classical Bayesian smoothing to obtain the PDF of the variables of interest.

Despite such applications of smoothing to quantum parameter estimation, a quantum analogue for the classical smoothed state (i.e. the PDF) was still missing. As quantum operators for a system at time t do not commute with operators representing the results of later measurements on that system [22], a naïve generalisation of the classical smoothing technique would not result in a proper quantum state [5, 6, 8]. As elucidated by Tsang [5], such a procedure would result in a "state" that gives the (typically anomalous) weak-value [3] as its expectation value for any observable. Thus, we refer to this type of smoothed "state" for a quantum system as the Smoothed Weak-Value (SWV) state. In contrast to this, Guevara and Wiseman [23] recently proposed a theory of quantum state smoothing which also generalises classical smoothing but which gives a proper smoothed quantum state, i.e., both Hermitian and positive semi-definite.

The quantum state smoothing theory of Ref. [23] considers an open quantum system coupled to two baths. An observer, Alice, monitors one bath and thereby obtains an "observed" measurement record $\mathbf{O}$. Another observer, Bob (who is hidden from Alice), monitors the remaining bath, unobserved by Alice, and thereby obtains an "unobserved" record $\mathbf{U}$. If Alice knew $\overleftarrow{\mathbf{U}}$ as well as $\overleftarrow{\mathbf{O}}$ (the back-arrows indicating records in the past), she would have maximum knowledge of the quantum system, i.e., the "true" state $\rho_{\overleftarrow{\mathbf{O}},\overleftarrow{\mathbf{U}}}$ at that time. Alice's smoothed state is then defined as

$$\rho_{\mathrm{S}} = \sum_{\overleftarrow{\mathbf{U}}} \wp_{\mathrm{S}}(\overleftarrow{\mathbf{U}}) \rho_{\overleftarrow{\mathbf{O}},\overleftarrow{\mathbf{U}}}\,, \tag{1}$$

where the summation is over all possible records unobserved by Alice and $\wp_{\mathrm{S}}(\overleftarrow{\mathbf{U}}) = \wp(\overleftarrow{\mathbf{U}}|\overleftrightarrow{\mathbf{O}})$ conditioned on Alice's *past-future record* $\overleftrightarrow{\mathbf{O}}$. By construction, Eq. (1) guarantees the positivity of the smoothed quantum state.

Here we present the theory of quantum state smoothing for Linear Gaussian Quantum (LGQ) systems. This can be applied to a large number of physical systems, e.g., multimodal light fields [24, 25], optical and optomechanical systems [14, 21, 22, 26–36], cold atomic ensembles [37, 38], and Bose-Einstein condensates [39]. Due to the nice properties of LGQ systems, we are able to obtain closed-form solutions for the smoothed LGQ state. This makes them much easier to study even than the two-level system originally considered in [23], as there is no need to generate numerically the numerous unobserved records appearing in the summation of Eq. (1). The simplicity of our theory will enable easy application to numerous physical systems, and also allows analytical treatment of various measurement efficiency regimes.

Classical LG smoothing.— We will briefly review classical LG state estimation before moving on to the quantum case. Consider a classical dynamical system described by a vector of M parameters $\mathbf{x} = \{x_1, x_2, ..., x_M\}^\top$. Here $\top$ denotes transpose. This system is regarded as an LG system if and only if it satisfies three conditions [22, 40–45]. First, its evolution can be described by a linear Langevin equation

$$\mathrm{d}\mathbf{x} = A\mathbf{x}\mathrm{d}t + E\mathrm{d}\mathbf{v}_{\mathrm{p}}\,. \tag{2}$$

Here A (the drift matrix) and E are constant matrices and $\mathrm{d}\mathbf{v}_{\mathrm{p}}$ is the process noise, i.e., a vector of independent Wiener increments satisfying

$$\mathrm{E}[\mathrm{d}\mathbf{v}_{\mathrm{p}}] = \mathbf{0}\,, \qquad \mathrm{d}\mathbf{v}_{\mathrm{p}}(\mathrm{d}\mathbf{v}_{\mathrm{p}})^\top = I\mathrm{d}t\,. \tag{3}$$

*kiarn.laverick@griffithuni.edu.au
†ar.chantasri@gmail.com
‡prof.h.wiseman@gmail.com

Here E[...] represents an ensemble average, and I is the $M \times M$ identity matrix. Second, knowledge about the system is conditioned on a measurement record $\mathbf{y}$ that is linear in $\mathbf{x}$, $\mathbf{y}\mathrm{d}t = C\mathbf{x}\mathrm{d}t + \mathrm{d}\mathbf{v}_\mathrm{m}$, where C is a constant matrix and the measurement noise $\mathrm{d}\mathbf{v}_\mathrm{m}$ is a vector of independent Wiener increments satisfying similar conditions to Eq. (3). It is possible for the process noise and the measurement noise to be correlated, e.g., from measurement back-action, which is described by the cross-correlation matrix $\Gamma^\top \mathrm{d}t = E\mathrm{d}\mathbf{v}_\mathrm{p}(\mathrm{d}\mathbf{v}_\mathrm{m})^\top$. The third condition is that the initial state of the system (i.e., the initial PDF of $\mathbf{x}$, denoted as $\wp(\mathbf{x})|_{t=0}$) is Gaussian; then the linearity conditions (first and second) guarantee the conditioned state will remain Gaussian: $\wp_\mathrm{C}(\mathbf{x}) = g(\mathbf{x}; \langle\mathbf{x}\rangle_\mathrm{C}, V_\mathrm{C})$, which is fully described by its mean $\langle\mathbf{x}\rangle_\mathrm{C}$ and variance (strictly, covariance matrix) $V_\mathrm{C} \equiv \langle\mathbf{x}\mathbf{x}^\top\rangle_\mathrm{C} - \langle\mathbf{x}\rangle_\mathrm{C}\langle\mathbf{x}\rangle_\mathrm{C}^\top$, throughout the entire evolution.

If the above criteria are met, one can compute a filtered LG state conditioned only on the past record. The filtered mean and variance are given by,

$$\mathrm{d}\langle\mathbf{x}\rangle_\mathrm{F} = A\langle\mathbf{x}\rangle_\mathrm{F}\mathrm{d}t + \mathcal{K}^+[V_\mathrm{F}]\mathrm{d}\mathbf{w}_\mathrm{F}\,, \tag{4}$$

$$\frac{\mathrm{d}V_\mathrm{F}}{\mathrm{d}t} = AV_\mathrm{F} + V_\mathrm{F}A^\top + D - \mathcal{K}^+[V_\mathrm{F}]\mathcal{K}^+[V_\mathrm{F}]^\top\,, \tag{5}$$

where $\mathrm{d}\mathbf{w}_\mathrm{F} \equiv \mathbf{y}\mathrm{d}t - C\langle\mathbf{x}\rangle_\mathrm{F}\mathrm{d}t$ is a vector of innovations, $D = EE^\top$ is the diffusion matrix, and we have defined a "kick" matrix, a function of V, via $\mathcal{K}^\pm[V] \equiv VC^\top \pm \Gamma^\top$.

To solve for a smoothed LG state, one needs to include conditioning on the future record, which can be obtained from the backwards-evolving retrofiltering equations

$$-\mathrm{d}\langle\mathbf{x}\rangle_\mathrm{R} = -A\langle\mathbf{x}\rangle_\mathrm{R}\mathrm{d}t + \mathcal{K}^-[V_\mathrm{R}]\mathrm{d}\mathbf{w}_\mathrm{R}, \tag{6}$$

$$-\frac{\mathrm{d}V_\mathrm{R}}{\mathrm{d}t} = -AV_\mathrm{R} - V_\mathrm{R}A^\top + D - \mathcal{K}^-[V_\mathrm{R}]\mathcal{K}^-[V_\mathrm{R}]^\top\,, \tag{7}$$

where $\mathrm{d}\mathbf{w}_\mathrm{R} \equiv \mathbf{y}\mathrm{d}t - C\langle\mathbf{x}\rangle_\mathrm{R}\mathrm{d}t$. Combining the filtered and retrofiltered solutions Eqs. (4)–(7), one obtains a smoothed LG state conditioned on the entire measurement record,

$$\langle\mathbf{x}\rangle_\mathrm{S} = V_\mathrm{S}(V_\mathrm{F}^{-1}\langle\mathbf{x}\rangle_\mathrm{F} + V_\mathrm{R}^{-1}\langle\mathbf{x}\rangle_\mathrm{R})\,, \tag{8}$$

$$V_\mathrm{S} = (V_\mathrm{F}^{-1} + V_\mathrm{R}^{-1})^{-1}\,. \tag{9}$$

LGQ systems.— For a quantum system analogous to the classical LG one, the system's observables require unbounded spectrums, represented by N bosonic modes. We denote such a system by a vector of $M = 2N$ observable operators $\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, ..., \hat{q}_N, \hat{p}_N)^\top$, where $\hat{q}_k$ and $\hat{p}_k$ are canonically conjugate position and momentum operators for the kth mode, obeying the commutation relation $[\hat{q}_k, \hat{p}_l] = i\hbar\delta_{kl}$. The system is called an LGQ system if its dynamical and measurement equations are isomorphic to those of a classical LG system [22, 26, 46–49]. For quantum systems there are additional constraints on the system's dynamics [22], such as the initial state must satisfy the uncertainty relation, $V + i\hbar\Sigma/2 \geq 0$. Here $\Sigma_{kl} = -i[\hat{x}_k, \hat{x}_l]$ and V is the covariance matrix $V_{kl} = \langle\hat{x}_k\hat{x}_l + \hat{x}_l\hat{x}_k\rangle/2 - \langle\hat{x}_k\rangle\langle\hat{x}_l\rangle$, for $\hat{x}_k$ being an element of $\hat{\mathbf{x}}$ and $\langle\cdot\rangle$ being the usual quantum expectation value. These let us represent the quantum state of an LGQ system by its Gaussian Wigner function [22] defined as $W(\check{\mathbf{x}}) = g(\check{\mathbf{x}}; \langle\hat{\mathbf{x}}\rangle, V)$, using dummy variable $\check{\mathbf{x}}$.

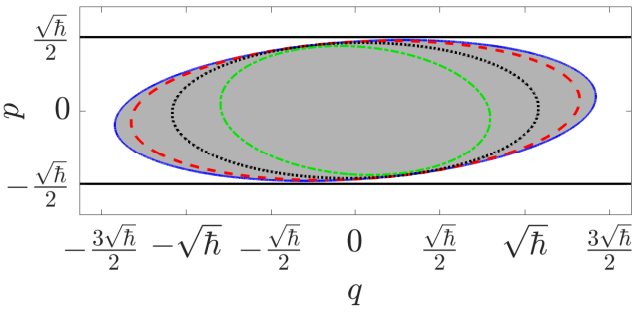


Figure 1: Various long-time states of the on-threshold OPO system in Eq. (15), represented by their 1-SD Wigner function contours in phase space, centred at the origin. The homodyne angles used by Alice and Bob (θ_o, θ_u) are at the black dot in Fig. 3. The unconditional state (solid black) shows infinite and finite variances in q and p, respectively, as a result of the damping and squeezing. Alice's filtered and smoothed states, are blue (filled grey) and dashed-red ellipses, respectively. The dotted-black and the dot-dashed green ellipse shows the (pure) true state and the SWV "state", respectively.

LGQ State Smoothing.— We now apply the quantum state smoothing technique [23] to LGQ systems. Following the Alice-Bob protocol introduced in Eq. (1), a true state of the LGQ system, denoted by the mean $\langle\hat{\mathbf{x}}\rangle_\mathrm{T}$ and a variance V_T, is obtained given both $\overleftarrow{\mathbf{O}}$ and $\overleftarrow{\mathbf{U}}$ records. That is, the filtering equations (4)-(5) apply, but conditioned both on Alice's observed record $\mathbf{y}_\mathrm{o}\mathrm{d}t = C_\mathrm{o}\langle\hat{\mathbf{x}}\rangle_\mathrm{T}\mathrm{d}t + \mathrm{d}\mathbf{w}_\mathrm{o}$, and on Bob's record, unobserved by Alice, $\mathbf{y}_\mathrm{u}\mathrm{d}t = C_\mathrm{u}\langle\hat{\mathbf{x}}\rangle_\mathrm{T}\mathrm{d}t + \mathrm{d}\mathbf{w}_\mathrm{u}$, with independent Wiener noises. The equations for the true state are

$$\mathrm{d}\langle\hat{\mathbf{x}}\rangle_\mathrm{T} = A\langle\hat{\mathbf{x}}\rangle_\mathrm{T}\mathrm{d}t + \mathcal{K}_\mathrm{o}^+[V_\mathrm{T}]\mathrm{d}\mathbf{w}_\mathrm{o} + \mathcal{K}_\mathrm{u}^+[V_\mathrm{T}]\mathrm{d}\mathbf{w}_\mathrm{u}\,, \tag{10}$$

$$\frac{\mathrm{d}V_\mathrm{T}}{\mathrm{d}t} = AV_\mathrm{T} + V_\mathrm{T}A^\top + D - \mathcal{K}_\mathrm{o}^+[V_\mathrm{T}]\mathcal{K}_\mathrm{o}^+[V_\mathrm{T}]^\top - \mathcal{K}_\mathrm{u}^+[V_\mathrm{T}]\mathcal{K}_\mathrm{u}^+[V_\mathrm{T}]^\top\,, \tag{11}$$

where $\mathcal{K}_\mathrm{r}^\pm[V] = VC_\mathrm{r}^\top + \Gamma_\mathrm{r}^\top$, for $\mathrm{r} \in \{\mathrm{o},\mathrm{u}\}$.

Since Alice has no access to Bob's record, her smoothed state is obtained by summing over all possible true states of the system, with probability weights conditional on Alice's observed record $\overleftrightarrow{\mathbf{O}}$, as in Eq. (1). For LGQ systems, the state depends on $\overleftarrow{\mathbf{U}}$ only via the mean, Eq. (10). Therefore, we can replace the (symbolic) sum in Eq. (1) by an integral: $\rho_\mathrm{S} = \int \wp_\mathrm{S}(\langle\hat{\mathbf{x}}\rangle_\mathrm{T})\rho_\mathrm{T}(\langle\hat{\mathbf{x}}\rangle_\mathrm{T})\mathrm{d}\langle\hat{\mathbf{x}}\rangle_\mathrm{T}$. By applying the classical notion of smoothing to the PDF $\wp_\mathrm{C}(\langle\hat{\mathbf{x}}\rangle_\mathrm{T})$, we are able to derive [1] the LGQ state smoothing equations

$$\langle\hat{\mathbf{x}}\rangle_\mathrm{S} = (V_\mathrm{S} - V_\mathrm{T})[(V_\mathrm{F} - V_\mathrm{T})^{-1}\langle\hat{\mathbf{x}}\rangle_\mathrm{F} + (V_\mathrm{R} + V_\mathrm{T})^{-1}\langle\hat{\mathbf{x}}\rangle_\mathrm{R}]\,, \tag{12}$$

$$V_\mathrm{S} = \left[(V_\mathrm{F} - V_\mathrm{T})^{-1} + (V_\mathrm{R} + V_\mathrm{T})^{-1}\right]^{-1} + V_\mathrm{T}\,, \tag{13}$$

as the main result of this research.

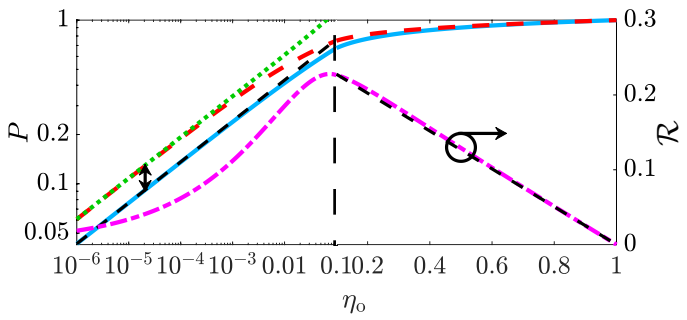


Figure 2: Purities, and the RPR, Eq. (14), at the starred point in Fig. 3, for the full range of Alice's measurement efficiency η_o, with the lower efficiencies plotted on a log scale and the higher efficiencies on a linear scale, where the dashed vertical line at $\eta_o = 0.1$ indicates the split. On both sides, we plot: purities of the filtered (solid blue), smoothed (dashed red) and the SWV (dotted green) states, all on a log scale (left-hand-side axis); and the RPR ($\mathcal{R}$) (dot-dashed magenta), on a linear scale (the right-hand-side axis). For $\eta_o \to 0$, P_F matches the simple analytic expression [1] $\sqrt{2|\cos\theta_o|}\eta_o^{1/4}$ (dashed black on left), and smoothing gives a factor of $\sqrt{2}$ improvement [1], as shown by the small $\updownarrow$ symbol. For $\eta_o \to 1$, the RPR is $\propto (1-\eta_o)$ (dashed black on right).

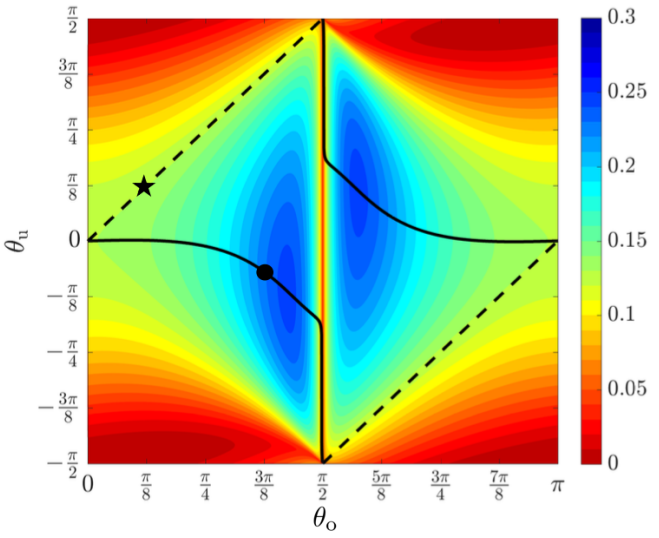


Figure 3: (Top) Contour plots of the RPR, Eq. (14), for the OPO system for different values of observed and unobserved homodyne phases using $\eta_o = 0.5$. The dashed line represents $\theta_o = \theta_u$ and the solid line is the maximum RPR. The circle and the star relate to Figs. 1 and 2, respectively.

The advantages LGQ state smoothing offers over filtering are readily seen in Fig. 1, where we note that the purity for a Gaussian state is defined as $P = (\hbar/2)\sqrt{|V|^{-1}}$ [22] for a variance V. The smoothed state has a smaller variance (higher purity) than the filtered state, but has a larger variance than a pure state (purity less than unity). In contrast, the SWV state for the same system (i.e., using Eqs. (8)–(9)) is unphysical (its ellipse is smaller than that of a pure state).

We now investigate some interesting limits in Alice's measurement efficiency η_o, the fraction of the system output which is observed by Alice. If, as in the OPO system we will define later, the unconditioned ($\eta_o = 0$) variance diverges, then Alice's conditioned (filtered and retrofiltered) variances, if finite, must grow as $\eta_o \to 0$. From Eqs. (12)–(13), when V_F and V_R are large, compared to V_T, the smoothed LGQ state reduces to the SWV state Eqs. (8)–(9). The SWV state has the same form as classical smoothed states, which often have the same scaling as filtered states, but with a multiplicative constant improvement [9, 15, 50]. Consequently, in the limit $\eta_o \to 0$, we expect $P_{SWV} = P_S \propto P_F$ as functions of η_o. This is confirmed in Fig. 2 when considering the OPO system.

In the opposite limit, $\eta_o \to 1$, we analytically show [1] that the relative purity recovery (RPR),

$$\mathcal{R} = \frac{P_S - P_F}{1 - P_F}\,, \tag{14}$$

a measure of how much the purity is recovered from smoothing over filtering relative to the maximum recovery possible, usually scales with the unobserved efficiency. That is, $\mathcal{R} \propto \eta_u \equiv 1 - \eta_o$. As seen in Fig. 2, this linear decay in the RPR holds surprisingly well, for the OPO system, even outside the high efficiency regime.

Example.— We now apply quantum state smoothing to the on-threshold OPO [22, 26], an LGQ system with $N = 1$ described by the master equation

$$\hbar\dot{\rho} = -i[(\hat{q}\hat{p} + \hat{p}\hat{q})/2, \rho] + \mathcal{D}[\hat{q} + i\hat{p}]\rho\,. \tag{15}$$

The first term defines a Hamiltonian giving squeezing along the p-quadrature, while the second term describes the oscillator damping. Here, we have $A = \mathrm{diag}(0, -2)$ and $D = \hbar I$. Let us assume that Alice observes the damping channel via homodyne detection. Therefore, $C_o = 2\sqrt{\eta_o/\hbar}\,(\cos\theta_o, \sin\theta_o)$, where θ_o is the homodyne phase [22, 26]. For simplicity, we assume Bob also performs a homodyne measurement, with a different phase θ_u, so that $C_u = 2\sqrt{\eta_u/\hbar}\,(\cos\theta_u, \sin\theta_u)$ and $\Gamma_r = -\hbar C_r/2$, for r $\in$ {o,u}.

We now solve for filtered and smoothed states for the OPO in steady state. We are particularly interested in the RPR of smoothing over filtering, and in the combinations of homodyne phases that result in the largest RPR. The RPR is always positive (see Fig. 3), meaning that the smoothed quantum state always has higher purity than the corresponding filtered one. If Alice's phase θ_o is fixed, one might guess that Bob's phase giving the best purity improvement should be the same, $\theta_u = \theta_o$. However, that is not at all true (see Fig. 3). The optimal θ_u^{opt} is not a trivial function of θ_o. Rather, $\theta_u^{opt} \approx 0$, i.e., Bob should measure the q-quadrature, which is presumably related to the fact that, without measurement in, the variance in q diverges.

References

[1] K. T. Laverick, Areeya Chantasri, and H. M. Wiseman. Quantum state smoothing for linear gaussian systems. *Phys. Rev. Lett.*, 122:190402, 2019.

[2] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz. Time symmetry in the quantum process of measurement. *Phys. Rev.*, 134:B1410–B1416, 1964.

[3] Y. Aharonov, D. Z. Albert, and L. Vaidman. How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100. *Phys. Rev. Lett.*, 60:1351–1354, 1988.

[4] M. Tsang. Time-symmetric quantum theory of smoothing. *Phys. Rev. Lett.*, 102(25):250403, 2009.

[5] M. Tsang. Optimal waveform estimation for classical and quantum systems via time-symmetric smoothing. *Phys. Rev. A*, 80(3):033840, 2009.

[6] S. Gammelmark, B. Julsgaard, and K. Mølmer. *Past Quantum States of a Monitored System. Phys. Rev. Lett.*, 111:160401, 2013.

[7] A. Chantasri, J. Dressel, and A. N. Jordan. Action principle for continuous quantum measurement. *Phys. Rev. A*, 88:042110, 2013.

[8] K. Ohki. A smoothing theory for open quantum systems: The least mean square approach. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 4350–4355, 2015.

[9] T. A. Wheatley, D. W. Berry, H. Yonezawa, D. Nakane, H. Arao, D. T. Pope, T. C. Ralph, H. M. Wiseman, A. Furusawa, and E. H. Huntington. Adaptive optical phase estimation using time-symmetric quantum smoothing. *Phys. Rev. Lett.*, 104:093601, 2010.

[10] M. Tsang, H. M. Wiseman, and C. M. Caves. Fundamental quantum limit to waveform estimation. *Phys. Rev. Lett.*, 106:090401, 2011.

[11] H. Yonezawa, D. Nakane, T. A. Wheatley, K. Iwasawa, S. Takeda, H. Arao, K. Ohki, K. Tsumura, D. W. Berry, T. C. Ralph, H. M. Wiseman, E. H. Huntington, and A. Furusawa. Quantum-enhanced optical-phase tracking. *Science*, 337(6101):1514–1517, 2012.

[12] K. Iwasawa, K. Makino, H. Yonezawa, M. Tsang, A. Davidovic, E. Huntington, and A. Furusawa. Quantum-limited mirror-motion estimation. *Phys. Rev. Lett.*, 111:163602, 2013.

[13] A. A. Budini. Smoothed quantum-classical states in time-irreversible hybrid dynamics. *Phys. Rev. A*, 96:032118, 2017.

[14] Z. Huang and M. Sarovar. Smoothing of gaussian quantum dynamics for force detection. *Phys. Rev. A*, 97:042106, 2018.

[15] K. T. Laverick, H. M. Wiseman, H. T. Dinani, and D. W. Berry. Adaptive estimation of a time-varying phase with coherent states: Smoothing can give an unbounded improvement over filtering. *Phys. Rev. A*, 97:042334, 2018.

[16] N. W. M. Ritchie, J. G. Story, and R. G. Hulet. Realization of a measurement of a "weak value". *Phys. Rev. Lett.*, 66:1107–1110, 1991.

[17] P. Campagne-Ibarcq, L. Bretheau, E. Flurin, A. Auffèves, F. Mallet, and B. Huard. Observing interferences between past and future quantum states in resonance fluorescence. *Phys. Rev. Lett.*, 112:180402, 2014.

[18] D. Tan, S. J. Weber, I. Siddiqi, K. Mølmer, and K. W. Murch. Prediction and retrodiction for a continuously monitored superconducting qubit. *Phys. Rev. Lett.*, 114:090403, 2015.

[19] T. Rybarczyk, B. Peaudecerf, M. Penasa, S. Gerlich, B. Julsgaard, K. Mølmer, S. Gleyzes, M. Brune, J. M. Raimond, S. Haroche, and I. Dotsenko. Forward-backward analysis of the photon-number evolution in a cavity. *Phys. Rev. A*, 91:062116, 2015.

[20] D. Tan, M. Naghiloo, K. Mølmer, and K. W. Murch. Quantum smoothing for classical mixtures. *Phys. Rev. A*, 94:050102(R), 2016.

[21] J. Zhang and K. Mølmer. Prediction and retrodiction with continuously monitored gaussian states. *Phys. Rev. A*, 96:062131, 2017.

[22] H. M. Wiseman and G. J. Milburn. *Quantum Measurement and Control*. Cambridge University Press, Cambridge, England, 2010.

[23] I. Guevara and H. Wiseman. Quantum state smoothing. *Phys. Rev. Lett.*, 115:180407, 2015.

[24] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, 2005.

[25] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, 2012.

[26] H. M. Wiseman and A. C. Doherty. Optimal unravellings for feedback control in linear quantum systems. *Phys. Rev. Lett.*, 94(7):070405, 2005.

[27] M. Zhang, G. S. Wiederhecker, S. Manipatruni, A. Barnard, P. McEuen, and M. Lipson. Synchronization of micromechanical oscillators using light. *Phys. Rev. Lett.*, 109(23):233906, 2012.

[28] M. Tsang and R. Nair. Fundamental quantum limits to waveform detection. *Phys. Rev. A*, 86:042115, 2012.

[29] S. Z. Ang, G. I. Harris, W. P. Bowen, and M. Tsang. Optomechanical parameter estimation. *New J. Phys.*, 15(10):103028, 2013.

[30] W. P. Bowen and G. J. Milburn. *Quantum Optomechanics*. CRC Press, 2015.

[31] M. G. Genoni, J. Zhang, J. Millen, P. F. Barker, and A. Serafini. Quantum cooling and squeezing of a levitating nanosphere via time-continuous measurements. *New J. Phys.*, 17(7):073019, 2015.

[32] W. Wieczorek, S. G. Hofer, J. Hoelscher-Obermaier, R. Riedinger, K. Hammerer, and M. Aspelmeyer. Optimal state estimation for cavity optomechanical systems. *Phys. Rev. Lett.*, 114:223601, 2015.

[33] J. Vovrosh, M. Rashid, D. Hempston, J. Bateman, M. Paternostro, and H. Ulbricht. Parametric feedback cooling of levitated optomechanics in a parabolic mirror trap. *JOSA B*, 34(7):1421–1428, 2017.

[34] J. Liao, M. Jost, M. Schaffner, M. Magno, M. Korb, L. Benini, F. Tebbenjohanns, R. Reimann, V. Jain, M. Gross, A. Militaru, M. Frimmer, and L. Novotny. Fpga implementation of a kalman-based motion estimator for levitated nanoparticles. *IEEE Trans. Instrum. Meas.*, pages 1–13, 2018.

[35] C. F. Ockeloen-Korppi, E. Damskägg, J. M. Pirkkalainen, M. Asjad, A. A. Clerk, F. Massel, M. J. Woolley, and M. A. Sillanpää. Stabilized entanglement of massive mechanical oscillators. *Nature*, 556(7702):478, 2018.

[36] A. Setter, M. Toroš, J. F. Ralph, and H. Ulbricht. Real-time kalman filter: Cooling of an optically levitated nanoparticle. *Phys. Rev. A*, 97:033822, 2018.

[37] L. B. Madsen and K. Mølmer. Spin squeezing and precision probing with light and samples of atoms in the gaussian description. *Phys. Rev. A*, 70:052324, 2004.

[38] J. Kohler, J. A. Gerber, E. Dowd, and D. M. Stamper-Kurn. Negative-mass instability of the spin and motion of an atomic gas driven by optical cavity backaction. *Phys. Rev. Lett.*, 120:013601, 2018.

[39] A. C. J. Wade, J. F. Sherson, and K. Mølmer. Squeezing and entanglement of density oscillations in a bose-einstein condensate. *Phys. Rev. Lett.*, 115:060401, 2015.

[40] S. Haykin. *Kalman Filtering and Neural Networks*. Wiley, New York, 2001.

[41] H. L. Weinert. *Fixed Interval Smoothing for State Space Models*. Kluwer Academic, New York, 2001.

[42] H. L. Van Trees and K. L. Bell. *Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory*. John Wiley and Sons, New York, 2 edition, 2013.

[43] R. G. Brown and P. Y. C. Hwang. *Introduction to Random Signals and Applied Kalman Filtering*. Wiley, New York, 4 edition, 2012.

[44] G. A. Einicke. *Smoothing, filtering and prediction: Estimating the past, present and future*. InTech Rijeka, 2012.

[45] B. Friedland. *Control system design: an introduction to state-space methods*. Courier Corporation, 2012.

[46] V. P. Belavkin. *Information, complexity and control in quantum physics*. Springer, New York, 1987.

[47] V. P. Belavkin. Quantum continual measurements and a posteriori collapse on ccr. *Commun. Math. Phys.*, 146(3):611–635, 1992.

[48] A. C. Doherty and K. Jacobs. Feedback control of quantum systems using continuous state estimation. *Phys. Rev. A*, 60(4):2700, 1999.

[49] A. C. Doherty, S. Habib, K. Jacobs, H. Mabuchi, and S. M. Tan. Quantum feedback control and classical control theory. *Phys. Rev. A*, 62(1):012105, 2000.

[50] M. Tsang, J. H. Shapiro, and S. Lloyd. Quantum theory of optical temporal phase and instantaneous frequency. ii. continuous-time limit and state-variable approach to phase-locked loop design. *Phys. Rev. A*, 79:053843, 2009.

Bell type measurements in the 1D infinite spin-1 chain

Dongkeun Lee[1 2] Wonmin Son[1 *]

[1] *Department of Physics, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul 04107, Republic of Korea*
[2] *Research Institute for Basic Science, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul 04107, Republic of Korea*

Abstract. The quantities such as the entanglement entropy, the fidelity, and the mutual information are recently exploited to detect the quantum phase transitions and analyze other various properties of many-body physics. The Bell correlations has been also studied in one-dimensional(1D) spin-1/2 chain. Here, we analyze the 1D infinite spin-1 XXZ chain with the on-site anisotropy as applying the Bell correlation function of CGLMP type for the many-body ground state. Since the ground state of the 1D infinite spin-1 chain cannot be calculated analytically, we utilized numerical approaches, infinite Matrix Product States(iMPS) representation and infinite density matrix renormalization group(iDMRG) method.

Keywords: CGLMP, Bell correlation, spin-1 chain, iMPS, iDMRG

1 Introduction

The concepts and theories in Quantum Information has been recently studied in many-body systems that have been originally described by the statistical physics and the condensed matter theory. The quantum phase transitions in many-body systems are generally modeled by the (spontaneous) symmetry breaking, the spin-spin correlation function, and the nonanalyticity of the derivative of the ground energy. It is quite recent that the quantum entanglement is exploited to detect the quantum phase transitions[1, 2] and analyze other various properties of many-body system[3]. Not only the quantum entanglement but also any other concepts such as the fidelity, the mutual information, and the quantum coherence is utilized to study the correlations in many-body systems[4]. The correlation of Bell operators has been also studied in many-body system, especially one-dimensional(1D) spin-1/2 chain such as [5, 6, 7]. In this poster, we are going to study the Bell measurement of CGLMP type in the 1D spin-1 chain with the on-site anisotropy It is renowned that the 1D spin-1 chain demonstrates completely different physics from 1D spin-1/2 chains(e.g., Haldane phase). Since it is restrictive to find the exact ground state in 1D spin-1 XXZ chain, we are using various numerical approaches like the MPS representation and iDMRG method.

2 The CGLMP-type Bell correlation

Bell inequality examines the correlation between two parties who have each side of the quantum state and determines which quantum states is nonlocal throughout the violation of its classical bounds. Especially, it is CGLMP inequality that each of two parties performs the two kinds measurements with d possible outcomes. In order to describe the CGLMP correlation not as the form of probability but in terms of the operators, we use the notations from SLK paper [14]. The CGLMP correlation is the expectation value of the Bell operator $\hat{\mathcal{B}}_{cglmp}$ for any quantum state, where

$$\hat{\mathcal{B}}_{cglmp} = \frac{1}{4}\sum_{n=1}^{d-1} f_c \left(\hat{A}_1^n + \omega^{n/2}\hat{B}_1^n\right) \otimes \left(\hat{A}_2^n + \omega^{n/2}\hat{B}_2^n\right)^\dagger + h.c., \tag{1}$$

where $f_c \equiv \frac{2}{(d-1)}\omega^{\frac{n}{4}} \sec\left[\frac{n\pi}{2d}\right]$ and d is the dimension of the basis for each party. The measurement operators $\hat{A}_j$ and $\hat{B}_j$ represent two kinds of measurements for jth party(i.e., $V_j \in \{A_j, B_j\}$) and $j \in \{1, 2\}$ can be either the first or the second party. The definition of the measurement operator $\hat{V}$ in Eq.(1) is given by

$$\hat{V} \equiv \sum_{\alpha=0}^{d-1} \omega^\alpha |\alpha\rangle_V \langle\alpha|, \tag{2}$$

where $\omega \equiv e^{\frac{2\pi i}{d}}$ and the basis $|\alpha\rangle$ comes from the maximally entangled state $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{\alpha=0}^{d-1}|\alpha,\alpha\rangle$. As CGLMP did in their paper[15], Alice chooses the Fourier transform basis and Bob does the inverse Fourier basis such that

$$|\alpha\rangle_{V_j} = \frac{1}{\sqrt{d}}\sum_{\beta=0}^{d-1} \omega^{-(\alpha+\phi_{V_j})\beta}|\beta\rangle, \tag{3}$$

where the phase shifts become $\phi_{A_1} = 0$, $\phi_{B_1} = 1/2$, $\phi_{A_2} = -1/4$, and $\phi_{B_2} = 1/4$ in Fig. 1 and $|\beta\rangle$ is the spin-z basis. Thereby it is possible to construct the measurement operators for $\hat{A}_1$, $\hat{A}_2$, $\hat{B}_1$, and $\hat{B}_2$. From Eq.(3), one can derive the identity such that

$$\frac{1}{2}(\hat{A}_1^n + \omega^{n/2}\hat{B}_1^n) = \hat{J}^n \tag{4}$$

$$\frac{1}{2}(\hat{A}_2^n + \omega^{n/2}\hat{B}_2^n) = \omega^{n/4}\hat{J}^n \tag{5}$$

where $\hat{J}^n \equiv \sum_{\beta=n}^{d-1}|\beta\rangle\langle\beta-n|$ is the n-level lowering operator. It is remarkable that the operator $\hat{J}$ is the same as the spin lowering operator $\hat{S}^-$. Consequently, the CGLMP operator $\hat{\mathcal{B}}_{cglmp}$ can be simplified as

$$\hat{\mathcal{B}}_{cglmp} = \sum_{n=1}^{d-1} \sec\left[\frac{n\pi}{6}\right]\left(\hat{J}^n \otimes (\hat{J}^n)^\dagger + (\hat{J}^n)^\dagger \otimes \hat{J}^n\right), \tag{6}$$

*sonwm71@gmailcom

We will use the operator as an entanglement witness of a d-dimensional many-body system and phase quantification.

3 The 1D Spin-1 Antiferromagnetic Chain

The Hamiltonian of the one-dimensional(1D) spin-1 XXZ chain with on-site anisotropy is described as

$$\hat{H} = \sum_{i=1}^{N-1} \hat{S}_i^x \hat{S}_{i+1}^x + \hat{S}_i^y \hat{S}_{i+1}^y + J_z \hat{S}_i^z \hat{S}_{i+1}^z + D \sum_{i=1}^{N} (\hat{S}_i^z)^2, \quad (7)$$

where $\hat{S}_i^a$ denotes the spin-1 operators for $a = x, y, z$ at site i, J_z is the anisotropy of spin-exchange interaction along z direction, and D characterizes the on-site anisotropy. The role of the last term is to manifest phase transition between the topologically trivial phase(Large-D phase) and the topologically nontrivial phase(Haldane phase). The physical properties for each phase and phase transition will be discussed in Sec.5

4 The iMPS representation

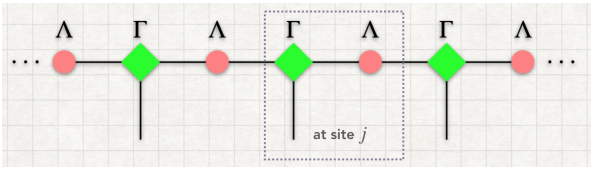


Figure 1: The graphical notation of iMPS in the canonical form. Due to the translational symmetry, the rank-3 tensors Γ and the matrices Λ are the same for all sites.

We introduce the infinite matrix product state(iMPS) representation to describe the ground-energy state in the thermodynamic limit and use the infinite density-matrix renormalization group(iDMRG) method to obtain the ground state as a iMPS form. Translational invariance plays a pivotal role to represent the infinite 1D systems. The ground state $|\psi\rangle$ in the canonical form of iMPS is given by

$$|\psi\rangle = \sum_{s_1,\cdots,s_N} \mathrm{Tr}\left[\Gamma^{s_1}\Lambda\Gamma^{s_2}\Lambda\cdots\Gamma^{s_N}\Lambda\right]|s_1\cdots s_N\rangle, \ N\to\infty \quad (8)$$

where Γ^{s_j} is the $\chi\times\chi$ matrices for $s_j \in \{1, 2, \cdots, d\}$ and Λ is a real, diagonal, and nonnegative matrix of dimension $\chi \times \chi$. As the bond dimension χ goes to infinity, Eq.(8) gets close to the exact one.

5 Results & Discussion

By using the iDMRG algorithm [16, 17], we are going to simulate the Hamiltonian Eq.(7) in the thermodynamic limit to ignore the boundary conditions and the finite size effect. Here, CGLMP measurement is defined

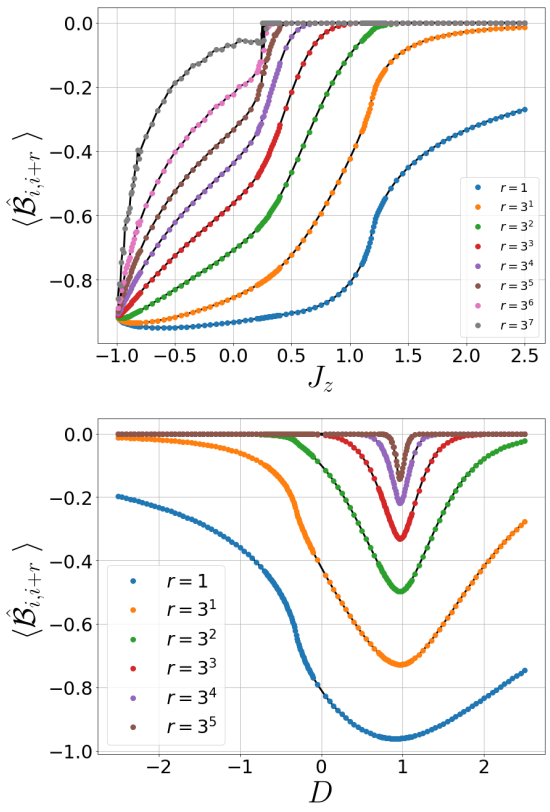


Figure 2: The CGLMP measurement (a) at $D = 0$ and (b) at $J_z = 0$.

as $\langle \hat{\mathcal{B}}_{cglmp}^{i,i+r} \rangle$ for the ground states. For $d = 3$, $\hat{\mathcal{B}}_{cglmp}^{i,i+r}$ of Eq.(6) can be expressed in terms of the spin-1 operator

$$\hat{\mathcal{B}}_{cglmp}^{i,i+r} = \frac{2}{\sqrt{3}}\left[\hat{S}_i^+ \otimes \hat{S}_{i+r}^- + \hat{S}_i^- \otimes \hat{S}_{i+r}^+\right] + 2\left[(\hat{S}_i^+)^2 \otimes (\hat{S}_{i+r}^-)^2 + (\hat{S}_i^-)^2 \otimes (\hat{S}_{i+r}^+)^2\right].$$

Thus, $\langle \hat{\mathcal{B}}_{cglmp}^{i,i+r} \rangle$ is the linear combination of transverse spin-spin correlation like $\langle \hat{S}_i^+ \hat{S}_j^- \rangle$ and $\langle (\hat{S}_i^+)^2 (\hat{S}_{i+r}^-)^2 \rangle$.

In Fig.2(a), the discontinuity occurs at $J_z = -1$ and there is an inflection point at around $J_z \approx 1.2$. Fig.2(b) shows the one inflection point between the AFM phase and the Haldane phase and a minimum point at the Gaussian phase transition(or the Haldane-Large D phase transition). The transverse spin-spin correlation decays algebraically(i.e., $\langle \hat{S}_i^+ \hat{S}_{i+r}^- \rangle \sim r^{-\eta_{+-}}$) in the gapless XY phase, whereas the other phases like the Haldane phase decay exponentially with respect to the distance between two parties. It is remarkable that near the Haldane phase-Large D phase transition the spin correlation function decays like the one in the gapless phase.

References

[1] A. Osterloh et al., Nature **416**, 608 (2002)

[2] T. J. Osborne and M. A. Nielsen, Phys. Rev. A, **66**, 032110 (2002)

[3] Luigi Amico et al., Rev. Mod. Phys. **80**, 517 (2008)

[4] A. L. Malvezzi et al., Phys.Rev. B **93**, 184428 (2016)

[5] J.Batle and M. Casas, Phys. Rev. A **82**, 062101 (2010)

[6] L. Justino and Thiago R. Oliveira, Phys. Rev. A **85**, 052128 (2012)

[7] Zhao-Yu Shu et al., Phys. Rev A **89**, 022101 (2014); Phys. Rev A **90**, 062129 (2014); Phys. Rev A **92**, 022120 (2015)

[8] Frank Pollmann et al., Phys. Rev. B 81, 064439 (2010)

[9] Xie Chen, Zheng-Cheng Gu, and Xiao-Gang Wen, Phys. Rev. B **84**, 235128 (2011)

[10] Wei Chen, Kazuo Hida, and B. C. Sanctuary, Phys. Rev. B **67**, 104401 (2003)

[11] Guifré Vidal, Phys. Rev. Lett. **91**, 147902 (2003)

[12] Ulrich. Schollwöck, Ann. Phys. **326** 96 (2011)

[13] Steven R. White, Phys. Rev. Lett. **69**, 2863 (1992);

[14] W. Son, Jinhyoung Lee, and M. S. Kim, Phys. Rev. Lett. **96**, 060406 (2006)

[15] Daniel Collins et al., Phys. Rev. Lett. **88**, 040404 (2002) Phys. Rev. B **48**, 10345 (1993)

[16] Jonas A. Kjäll et al., Phys. Rev. B **87**, 235106 (2013)

[17] I. P. McCulloch, arXiv:0804.2509.

Measurement-device-independent quantum secret sharing using high-dimensional quantum states

Yonggi Jo[1 2] Wonmin Son[1 *]

[1] *Department of Physics, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul 04107, Republic of Korea*
[2] *Research Institute for Basic Science, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul 04107, Republic of Korea*

Abstract. A quantum secret sharing (QSS) protocol which has an improved secret key rate by exploiting d-dimensional quantum states is presented. The scheme is performed among d authorized parties without generation of an entangled state. The scheme provides the measurement-device-independent security against a potential eavesdropper since a result of the measurement only reveals a correlation among d-dimensional quantum states sent from the d parties, not the exact quantum states. We show that our protocol can be implemented with current state-of-the-art technologies, and it can be more practical and efficient than an entanglement-based QSS protocol using d-dimensional quantum states. The security of the proposed protocol is analysed for the cases, when all players are trusted and there is a malicious player, as well.

Keywords: Quantum cryptography, Quantum secret sharing, High-dimensional quantum system, Measurement-device-independent security

1 Introduction

Secret sharing is a scheme proposed for distributing a secret among participants [1, 2]. In the scheme, one party, called a dealer, gives a part of the secret to participants, called players. Each player cannot access full information on the secret since a player has only a share of the secret. The secret can be reconstructed only when the sufficient number of players cooperates by combining their shares. Quantum secret sharing (QSS) was proposed as a quantum counterpart of classical secret sharing [3, 4]. In QSS, Greenberger-Horne-Zeilinger (GHZ) state [5] is exploited to share a secret, and it was proven that QSS provides information-theoretic security based on the principles of quantum mechanics [6–8].

To improve a key rate of QSS, a high-dimensional quantum system can be applied [9], since a high-dimensional quantum state can carry more information per single photon and has enhanced security against eavesdropping [10, 11]. However, generation of a high-dimensional GHZ state needs demanding technologies as it was reported in the recent paper [12]. Here, we propose a feasible QSS protocol using d-dimensional quantum states among d parties without generation of an entangled state. In this protocol, measurement-device-independent (MDI) security is guaranteed since measurement devices are separated from all the authorized parties [13, 14].

2 Result and Discussion

As an example, a schematic diagram of MDIQSS using 3-dimensional quantum states (3d-MDIQSS), is shown in Figure 1. Three authorized parties and one untrusted party participate in this protocol. One authorized party, called Alice, is the dealer, and the other two authorized parties, called Bob_1 and Bob_2, are the players. The authorized parties generate a 3-dimensional number and encode it into an orbital angular momentum (OAM) value of a single photon, respectively. Subsequently, they send their photons to an untrusted party, Charlie. Charlie performs the measurement onto the incoming photons of which result is a correlation among the OAM value of the three photons. Subsequently, Charlie announces the result, and then Alice distributes the encrypted classical secret by using her encoded number and the measurement result. In this protocol, both Bob_1's and Bob_2's encoded numbers are necessary to decrypt the secret. We show the protocol can be extended to d-party MDIQSS using d-dimensional quantum states (d-MDIQSS) in the presentation.

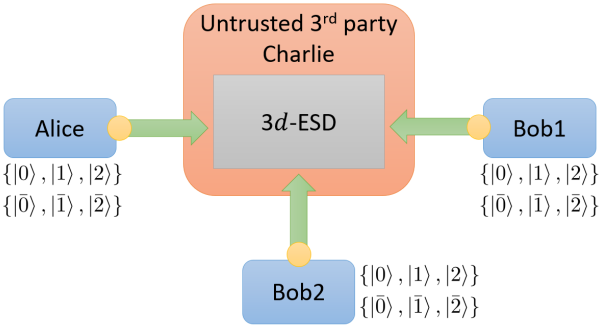


Figure 1: A schematic diagram of 3d-MDIQSS. There are three authorized parties, Alice, Bob_1, and Bob_2, and one untrusted party, Charlie. Each of the authorized parties generates a single photon state according to their choice of an encoding basis and 3-dimensional information, $\{0, 1, 2\}$. They send the quantum states to Charlie who measures a correlation among the OAM mode of the three photons by means of tripartite 3-dimensional entangled state discrimination measurement (3d-ESD). The three authorized parties can share a secret by using their encoded information and the result of the 3d-ESD.

This protocol is more feasible compared with the existing QSS protocol using d-partite d-dimensional GHZ

*sonwm71@sogang.ac.kr

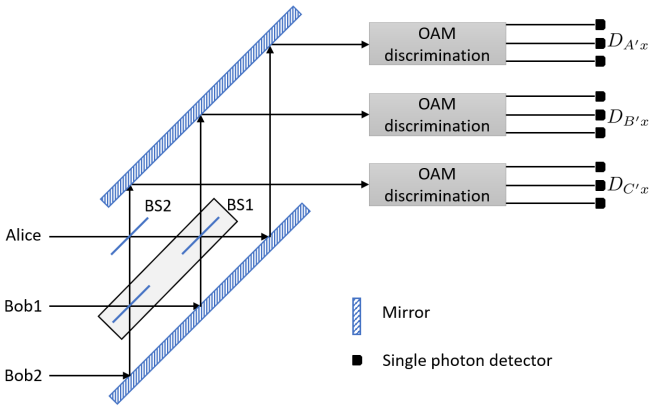


Figure 2: A schematic diagram of the 3d-ESD. Three photons sent from the authorized parties enter into a 3-port interferometer, called a tritter. After interference in the tritter, an OAM value and a label of existing outport of the photons are measured by means of OAM discrimination elements and single photon detectors. Charlie can discriminate a part of tripartite 3-dimensional entangled states from a combination of clicked detectors. D_{Xy} : a detector corresponding the OAM state $|y\rangle$ on the path X; BS1 : 50:50 beam splitter; BS2 : beam splitter of which transmissivity is 2/3.

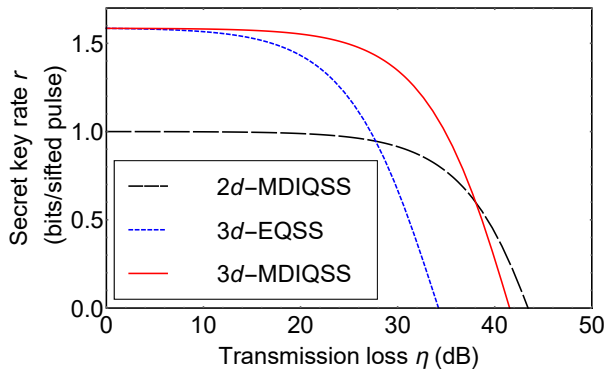


Figure 3: The secret key rates per sifted pulse with experimental factors. The secret key rates of the 2d-MDIQSS protocol (black dashed line), an entanglement-based 3d-QSS protocol (blue dotted line), and the 3d-MDIQSS protocol (red solid line) are plotted. Experimental factors, transmission loss η and a dark count rate of a single photon detector, are considered in the plots. The dark count rate is assumed as 10^{-5} per pulse.

states [9] since generation of an entangled state is not necessary. We show that the measurement setup, called an entangled state discrimination (ESD) setup, can be implemented with linear optical elements and OAM discrimination setups. An example of the setup is shown in Figure 2 for the 3-dimensional case.

The security of the d-MDIQSS is analyzed as well. One of the analyses, secret key rates per sifted pulse against experimental factors is drawn in Figure 3. In the plot, transmission loss of a photon and a dark count of a single photon detector are considered as error factors. As shown in the plot, 3d-MDIQSS has advantage over a secret key rate against the experimental factors compared with the conventional QSS protocol and an entanglement-based 3-dimensional QSS protocol.

Acknowledgment

This research was supported by the R&D Convergence Program through the National Research Council of Science and Technology (NST) of the Republic of Korea (Grant No. CAP-15-08-KRISS). Y. Jo thanks to the Agency for Defense Development (ADD) of the Republic of Korea for the graduate student scholarship program. W. Son acknowledges the University of Oxford and the Korea Institute for Advanced Study (KIAS) for their visitorship program.

References

[1] A. Shamir, Commun. ACM **22**, 612 (1979).

[2] G. R. Blakley, in *Managing Requirements Knowledge, International Workshop on(AFIPS)* (1899) p. 313.

[3] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[4] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[5] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[6] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[7] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001).

[8] M. Choi, Y. Lee, and S. Lee, Quantum Inf. Process. **17**, 258 (2018).

[9] W.-J. Kim, S.-H. Cha, S.-W. Lee, and J. Lee, J. Korean Phys. Soc. **48**, 1218 (2006).

[10] D. Bruß and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).

[11] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, Sci. Adv. **3** (2017).

[12] M. Erhard, M. Malik, M. Krenn, and A. Zeilinger, Nat. Photon. **12**, 759 (2018).

[13] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[14] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).

Perfect Discrimination of Non-Orthogonal Separable Pure States on Bipartite System in General Probabilistic Theory

Hayato Arai[1] * Yuuya Yoshida[1] † Masahito Hayashi[1 2 3] ‡

[1]*Graduate School of Mathematics, Nagoya University, Nagoya, Japan*
[2]*Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Nanshan District, Shenzhen 518055, People's Republic of China*
[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542, Singapore*

Abstract. We address perfect discrimination of two separable states. When available states are restricted to separable states, we can theoretically consider a larger class of measurements than the class of measurements allowed in quantum theory. The framework composed of the class of separable states and the above extended class of measurements is a typical example of general probabilistic theories. In this framework, we give a necessary and sufficient condition to discriminate two separable pure states perfectly. In particular, we derive measurements explicitly to discriminate two separable pure states perfectly, and find that some non-orthogonal states are perfectly distinguishable. However, the above framework does not improve the *capacity*, namely, the maximum number of states that are simultaneously and perfectly distinguishable.

Keywords: perfect discrimination, separable states, general probabilistic theories

1 Introduction

Entanglement is a resource for miracle performance of quantum information processing [1, 2]. Even when a quantum state has no entanglement, entanglement in a measuring process brings us performance that measuring processes without quantum correlation cannot realize. In fact, when we discriminate the n-fold tensor products of two quantum states, the performance of measurements with quantum correlation is beyond that of any measurement without quantum correlation, e.g., local operation and classical communication (LOCC) and separable measurement [3–7]. The difference between the first and second performance can be derived from the following two classes of measurements. One is the class of measurements allowed in quantum theory and the other is the class of measurements with only separable form. The first class achieves strictly better performance than the second class in the above discrimination.

All the above studies of state discrimination considered classes of measurements allowed in quantum theory, but there is a theoretical possibility that a larger class of measurements brings us more miracle performance of state discrimination than that of quantum theory. In order to consider a larger class of measurements, we need to restrict available states. Such a framework is discussed in general probabilistic theories (GPTs) [8–23], which are a generalization of quantum theory and classical probability theory. GPTs are the most general framework to characterize states, measurements, and time evolution. Although some preceding studies compared GPTs with quantum theory [11, 13, 15–18], few studies clarified the difference between quantum theory and other GPTs in the viewpoint of state discrimination. Hence, to clarify the difference, we focus on the following typical GPT on a bipartite system: we restrict available states to separable states on the composite system and this restriction allows us to consider theoretically measurements that are not allowed in quantum theory. The framework composed of the class of separable states and the class of such measurements is a typical example of GPTs and is denoted by SEP.

The difference between quantum theory and SEP can be characterized by the relation between the *positive and dual cones* appeared in quantum theory and SEP. A *positive cone* defines the set of all states in a GPT so that a state is given as an element of a positive cone whose trace is one. For example, the positive cone of quantum theory is the set of all positive semi-definite matrices and the positive cone of SEP is the set of all matrices with separable form. Thus, states in SEP are restricted to separable states, and the positive cone of SEP is smaller than that of quantum theory. This restriction makes bit commitment possible under SEP [14]. Furthermore, the *dual cone* of a positive cone defines measurements of a GPT so that a measurement is given as a decomposition $\{M_i\}_i$ of the identity matrix I. More precisely, all elements M_i lie in the dual cone and satisfy $\sum_i M_i = I$. For example, the dual cone of quantum theory is also the set of all positive semi-definite matrices and the dual cone of SEP is the set of all matrices Y that satisfy $\mathrm{Tr}\, XY \geq 0$ for all matrices X with separable form. Thus, the dual cone of SEP is larger than that of quantum theory. Therefore, measurements of SEP contain not only those of quantum theory but also those that quantum theory cannot realize.

In this paper, we address perfect discrimination of two pure states in SEP. A main goal of this paper is to reveal how much better the performance of perfect discrimination in SEP is than that in quantum theory. In quantum theory, it is well-known that orthogonality of two states is necessity and sufficiency to discriminate two states perfectly [24]. This fact is not changed even if we restrict the

*m18003b@math.nagoya-u.ac.jp
†m17043e@math.nagoya-u.ac.jp
‡masahito@math.nagoya-u.ac.jp

class of measurements to LOCC [25]. However, as shown in this paper, there exists a non-orthogonal pair of two separable pure states that can be discriminated in SEP. Moreover, we derive a necessary and sufficient condition for state discrimination in SEP. The necessary and sufficient condition implies that $2n$-copies $\rho_1^{\otimes 2n}$ and $\rho_2^{\otimes 2n}$ of pure states are perfectly distinguishable for a sufficiently large n if $\rho_1 \neq \rho_2$. In this sense, SEP is completely different from quantum theory.

Since our necessary and sufficient condition reveals that some non-orthogonal states in SEP can be discriminated perfectly, one might think that the *capacity* in SEP is improved in comparison with the capacity in quantum theory. Here the capacity in a GPT is the maximum number of states that are simultaneously and perfectly distinguishable in the GPT, and expresses the limit of communication quantity per single use of quantum communication. The capacity in quantum theory is equal to the dimension of a quantum system, and an interesting relation for the capacities in GPTs has been derived [10]. Using the relation [10, lemma 24], we find that the capacity in SEP is equal to that in quantum theory.

2 Perfectly distinguishable pairs of two pure states in SEP

First, let us describe our framework SEP and notational conventions. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two finite-dimensional complex Hilbert spaces. We denote by $\mathcal{T}(AB)$ and $\mathcal{T}_+(AB)$ the set of all Hermitian matrices on $\mathcal{H}_A \otimes \mathcal{H}_B$ and the set of all positive semi-definite matrices on $\mathcal{H}_A \otimes \mathcal{H}_B$, respectively. The sets $\mathcal{T}(A)$, $\mathcal{T}(B)$, $\mathcal{T}_+(A)$, and $\mathcal{T}_+(B)$ are defined similarly. In quantum theory, available states are elements of $\mathcal{T}_+(AB)$ with trace one. However, in this paper we look at the scenario where the only available states are separable states. We restrict available states to separable states, i.e., elements of

$$\mathrm{SEP}(A;B) := \left\{ \sum_i X_i^A \otimes X_i^B \;\middle|\; X_i^A \in \mathcal{T}_+(A),\ X_i^B \in \mathcal{T}_+(B)\ (\forall i) \right\}$$

with trace one. In order to address state discrimination, we must also define measurements of SEP. In quantum theory, measurements are given as positive-operator valued measures (POVMs). That is, a measurement $\{M_i\}_i$ satisfies $M_i \in \mathcal{T}_+(AB)$ and $\sum_i M_i = I$ for any outcome i. However, since we restrict available states to separable states, measurements of SEP form a larger class than those of quantum theory. A measurement $\{M_i\}_i$ of SEP is defined by the conditions

$$M_i \in \mathrm{SEP}^*(A;B)\ (\forall i), \quad \sum_i M_i = I,$$

where $\mathrm{SEP}^*(A;B)$ denotes the dual cone of $\mathrm{SEP}(A;B)$ and is defined as

$$\mathrm{SEP}^*(A;B) = \{\, Y \in \mathcal{T}(AB) \mid \mathrm{Tr}\, XY \geq 0\ (\forall X \in \mathrm{SEP}(A;B)) \,\}.$$

Since the inclusion relation $\mathrm{SEP}^*(A;B) \supset \mathcal{T}_+(AB)$ holds, measurements of SEP form a larger class than those of quantum theory.

Now, let us consider state discrimination in SEP. Let $\{\rho_i\}_{i=1}^n$ be a family of n states. Then we say that $\{\rho_i\}_{i=1}^n$ is *perfectly distinguishable* in SEP (resp. quantum theory) if there exists a measurement $\{M_j\}_{j=1}^n$ of SEP (resp. quantum theory) such that $\mathrm{Tr}\, M_j\rho_i = \delta_{ij}$, where δ_{ij} denotes the Kronecker delta. It is well-known that $\{\rho_i\}_{i=1}^n$ is perfectly distinguishable in quantum theory if and only if any two distinct states of $\{\rho_i\}_{i=1}^n$ are orthogonal, i.e., $\mathrm{Tr}\,\rho_i\rho_j = \delta_{ij}$ for all $i \neq j$. In this paper, we address the case $n = 2$ mainly.

We give an example that two states are perfectly distinguishable and not orthogonal. For this purpose, we consider the case where $\mathcal{H}_A$ and $\mathcal{H}_B$ are two-dimensional (hereinafter, it is called the $(2,2)$-dimensional case). In this case, the dual cone $\mathrm{SEP}^*(A;B)$ can be expressed explicitly by using the partial transpose operation Γ, which throughout the paper we assume to be on subsystem B. Since for 2×2 matrices $C = (c_{ij})_{i,j}$ and $D = (d_{ij})_{i,j}$ the tensor product matrix $C \otimes D$ is expressed as

$$C \otimes D = \left[\begin{array}{cc:cc} c_{11}d_{11} & c_{11}d_{12} & c_{12}d_{11} & c_{12}d_{12} \\ c_{11}d_{21} & c_{11}d_{22} & c_{12}d_{21} & c_{12}d_{22} \\ \hdashline c_{21}d_{11} & c_{21}d_{12} & c_{22}d_{11} & c_{22}d_{12} \\ c_{21}d_{11} & c_{21}d_{12} & c_{22}d_{11} & c_{22}d_{12} \end{array}\right],$$

the partial transpose $\Gamma(X)$ of a matrix $X = (x_{ij})_{i,j}$ is

$$\Gamma(X) = \left[\begin{array}{cc:cc} x_{11} & x_{21} & x_{13} & x_{23} \\ x_{12} & x_{22} & x_{14} & x_{24} \\ \hdashline x_{31} & x_{41} & x_{33} & x_{43} \\ x_{32} & x_{42} & x_{34} & x_{44} \end{array}\right].$$

As stated above, we can express the dual cone $\mathrm{SEP}^*(A;B)$ explicitly. Indeed, the combination of [26] and [27] implies the following proposition.

Proposition 1. *If* $(\dim \mathcal{H}_A, \dim \mathcal{H}_B) = (2,2)$*, then*

$$\mathrm{SEP}^*(A;B) = \{\, T + \Gamma(T') \mid T, T' \in \mathcal{T}_+(AB) \,\}.$$

Next, we give an example of two pure states that are perfectly distinguishable in SEP despite being non-orthogonal. What follows is also a special case of our main result.

Example 1 (Perfect discrimination of non-orthogonal pure states in SEP)**.** Suppose that two pure states $\rho_1, \rho_2 \in \mathrm{SEP}(A;B)$ are given as

$$\begin{aligned} \rho_1 &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \\ \rho_2 &= \begin{bmatrix} 1-\alpha_1 & \beta_1 \\ \beta_1 & \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} 1-\alpha_2 & \beta_2 \\ \beta_2 & \alpha_2 \end{bmatrix}, \end{aligned} \tag{1}$$

where $\alpha_i \in [0,1]$, $\beta_i \geq 0$, and $\beta_i^2 = \alpha_i(1-\alpha_i)$ for all $i = 1,2$. Assume $\alpha_1 + \alpha_2 = 1$ here. Then we show that ρ_1 and ρ_2 are perfectly distinguishable in SEP. Let us give a measurement $\{T_1 + \Gamma(T_1), T_2 + \Gamma(T_2)\}$ with positive semi-definite matrices T_1 and T_2. Since T_1 and

Table 1: Necessary and sufficient (NS) conditions of perfect discrimination of two pure states, and capacities.

GPTs	SEP	Quantum theory
NS condition	$\mathrm{Tr}\,\rho_1^A\rho_2^A + \mathrm{Tr}\,\rho_1^B\rho_2^B \leq 1$	$(\mathrm{Tr}\,\rho_1^A\rho_2^A)(\mathrm{Tr}\,\rho_1^B\rho_2^B) = 0$
Capacity	$\dim(\mathcal{H}_A \otimes \mathcal{H}_B)$	$\dim(\mathcal{H}_A \otimes \mathcal{H}_B)$

T_2 are positive semi-definite, proposition 1 implies that $T_i + \Gamma(T_i) \in \mathrm{SEP}^*(A;B)$ for all $i = 1, 2$. Now, we set the positive semi-definite matrices T_1 and T_2 as

$$T_1 = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}, \quad T_2 = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Then $\{T_1 + \Gamma(T_1), T_2 + \Gamma(T_2)\}$ is a measurement of SEP because $(T_1 + \Gamma(T_1)) + (T_2 + \Gamma(T_2)) = I$. The measurement $\{T_1 + \Gamma(T_1), T_2 + \Gamma(T_2)\}$ discriminates ρ_1 and ρ_2 perfectly. Let us verify it. First, the equation $\mathrm{Tr}\,\rho_1(T_2 + \Gamma(T_2)) = 0$ follows from the definitions. Next, note that the assumption $\alpha_1 + \alpha_2 = 1$ implies $\beta_1 = \beta_2 = \sqrt{\alpha_1\alpha_2}$. Since (i) $\Gamma(\rho_2) = \rho_2$ and (ii) $\alpha_1 + \alpha_2 = 1$ ($\beta_1 = \beta_2 = \sqrt{\alpha_1\alpha_2}$), we have

$$\begin{aligned} \mathrm{Tr}\,\rho_2(T_1 + \Gamma(T_1)) &\overset{\text{(i)}}{=} 2\,\mathrm{Tr}\,\rho_2 T_1 \\ &= (1-\alpha_1)(1-\alpha_2) + \alpha_1\alpha_2 - 2\beta_1\beta_2 \overset{\text{(ii)}}{=} 0. \end{aligned}$$

Thus the equation $\mathrm{Tr}\,\rho_2(T_1 + \Gamma(T_1)) = 0$ also follows. Finally, the equation $\mathrm{Tr}\,\rho_i(T_i + \Gamma(T_i)) = 1$ follows from $(T_1 + \Gamma(T_1)) + (T_2 + \Gamma(T_2)) = I$ and $\mathrm{Tr}\,\rho_i(T_j + \Gamma(T_j)) = 0$ for all $i \neq j$. Therefore, the measurement $\{T_1 + \Gamma(T_1), T_2 + \Gamma(T_2)\}$ discriminates ρ_1 and ρ_2 perfectly. Here, note that ρ_1 and ρ_2 are not orthogonal if $\alpha_1, \alpha_2 \neq 1$. Thus perfect discrimination of two pure states in SEP is possible even when the two states are not orthogonal.

Example 1 gives a sufficient condition of perfect discrimination, but it does not give a necessary condition. Thus we give the following theorem as a necessary and sufficient condition for two pure states to be discriminated perfectly.

Theorem 2. *Two pure states $\rho_1 = \rho_1^A \otimes \rho_1^B$ and $\rho_2 = \rho_2^A \otimes \rho_2^B$ are perfectly distinguishable in SEP if and only if*

$$\mathrm{Tr}\,\rho_1^A\rho_2^A + \mathrm{Tr}\,\rho_1^B\rho_2^B \leq 1.$$

Here, let us compare the necessary and sufficient condition in SEP with that in quantum theory. In quantum theory, the condition $(\mathrm{Tr}\,\rho_1^A\rho_2^A)(\mathrm{Tr}\,\rho_1^B\rho_2^B) = 0$ is necessary and sufficient to discriminate the two state in theorem 2 perfectly. Thus we can find that measurements of SEP improve the performance of state discrimination.

Measurements of SEP improve the performance of multiple-copy state discrimination more dramatically. To see this fact, let us consider perfect discrimination of $2n$-copies $\rho_1^{\otimes 2n}$ and $\rho_2^{\otimes 2n}$ of pure states. Then $\rho_i^{\otimes 2n} = \rho_i^{\otimes n} \otimes \rho_i^{\otimes n}$ is a separable pure state on a bipartite system for $i = 1, 2$. Thus $\rho_1^{\otimes 2n}$ and $\rho_2^{\otimes 2n}$ are perfectly distinguishable in SEP if

$$2(\mathrm{Tr}\,\rho_1\rho_2)^n = \mathrm{Tr}\,\rho_1^{\otimes n}\rho_2^{\otimes n} + \mathrm{Tr}\,\rho_1^{\otimes n}\rho_2^{\otimes n} \leq 1.$$

This inequality always holds for a sufficiently large n if $\rho_1 \neq \rho_2$. Therefore, $\rho_1^{\otimes 2n}$ and $\rho_2^{\otimes 2n}$ are perfectly distinguishable in SEP. Of course, such a measurement to realize the above perfect discrimination is impossible in quantum theory.

Next, we discuss how many states are simultaneously and perfectly distinguishable in SEP. That is, our interest is the *capacity* N_{SEP} defined as the maximum number of simultaneously and perfectly distinguishable states in SEP:

$$\begin{aligned} &N_{\mathrm{SEP}} := \\ &\max\{\, n \in \mathbb{N} \mid \exists\{\rho_i\}_{i=1}^n,\ \exists\{M_j\}_{j=1}^n \text{ s.t. } \mathrm{Tr}\,\rho_i M_j = \delta_{ij} \,\}, \end{aligned}$$

where $\{\rho_i\}_{i=1}^n$ and $\{M_j\}_{j=1}^n$ are a family of states in SEP and a measurement of SEP, respectively. As stated in the previous paragraph, the performance of state discrimination in SEP is higher than that in quantum theory. Hence one might guess that the capacity in SEP is greater than that in quantum theory. However, the following proposition shows that this is not the case.

Proposition 3. *The capacity N_{SEP} is $\dim(\mathcal{H}_A \otimes \mathcal{H}_B)$.*

Since the capacity in quantum theory is equal to the dimension of a quantum system, Proposition 3 means that SEP has the same capacity as quantum theory. Actually, Proposition 3 follows from [10, Lemma 24 (iii)] which is a more general statement on capacities. However, using [10, Lemma 24 (iii)] needs to be careful. For details, see the full version [28].

Table 1 summarizes the necessary and sufficient conditions of perfect discrimination and the capacities in quantum theory and SEP. The performance of perfect discrimination in SEP is better than that in quantum theory but the capacity in SEP is equal to that in quantum theory.

Acknowledgments

MH is grateful to Prof. Giulio Chiribella, Prof. Oscar Dahlsten, and Dr. Daniel Ebler for helpful discussions. He is also thankful to Mr. Kun Wang for his comments. The authors are grateful to Mr. Seunghoan Song for providing many helpful comments for this paper. MH was supported in part by Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (A) No. 17H01280, (B) No. 16KT0017, and Kayamori Foundation of Informational Science Advancement. YY was supported by JSPS Grant-in-Aid for JSPS Fellows No. 19J20161.

References

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels". *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[2] C. H. Bennett and S. J. Wiesner. "Communication via one- and two-particle operators on einstein-podolsky-rosen states". *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[3] F. Hiai and D. Petz. "The proper formula for relative entropy and its asymptotics inquantum probability". *Comm. Math. Phys.*, 143:99–114, 1991.

[4] H. Nagaoka and T. Ogawa. "Strong converse and stein's lemma in quantum hypothesis testing". *IEEE Trans. Inf. Theory*, 46:2428–2433, 2000.

[5] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz Tapia, E. Bagan, Ll. Masanes, A. Acin, and F. Verstraete. *Phys. Rev. Lett.*, 98:160501, 2007.

[6] M. Nussbaum and A. Szkola. *Ann. Stat.*, pages 1040–1057, 2009.

[7] M. Hayashi. *Quantum Information Theory Mathematical Foundation*. Springer, Verlag Berlin Heidelberg, 2 edition, 2017.

[8] G. Kimura, K. Nuida, and H. Imai. "Physical equivalence of pure states and derivation of qubit in general probabilistic theories". arXiv:1012.5361, 2010.

[9] G. Kimura, J. Ishiguro, and M. Fukui. "Entropies in general probabilistic theories and its application to holevo bound". *Phys. Rev. A*, 94(042113), 2016.

[10] M. P. Müller, O. C. O. Dahlsten, and V. Vedral. "Unifying typical entanglement and coin tossing: on randomization in probabilistic theories". *Comm. Math. Phys.*, 316:441–487, 2012.

[11] P. Janotta and R. Lal. "Generalized probabilistic theories without the no-restriction hypothesis". *Phys. Rev. A*, 87:052131, May 2013.

[12] P. Janotta and H. Hinrichsen. "Generalized probability theories: what determines the structure of quantum theory?". *J. Phys. A*, 47(32):323001, 2014.

[13] H. Barnum, J. Barrett, M. Leifer, and A. Wilce. "Cloning and broadcasting in generic probabilistic theories". arXiv:quant-ph/0611295, 2006.

[14] H. Barnum, O. C.O. Dahlsten, M. Leifer, and B. Toner. "Nonclassicality without entanglement enables bit commitment". In *Proceedings of IEEE Information Theory Workshop*, pages 386–390, 2008.

[15] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, and S. Wehner. "Local quantum measurement and no-signaling imply quantum correlations". *Phys. Rev. Lett.*, 104 14:140401, 2010.

[16] O. C. O. Dahlsten, D. Lercher, and R. Renner. "Tsirelson's bound from a generalised data processing inequality". *New J. Phys.*, 14:063024, 2012.

[17] L. Lami, C. Palazuelos, and A. Winter. "Ultimate data hiding in quantum mechanics and beyond". arXiv:1703.03392, 2017.

[18] I. Hamamura. "Separability criterion for quantum effects". *Phys. Lett. A*, 382:2573–2577, 2018.

[19] Y. Yoshida and M. Hayashi. "Mixing and asymptotically decoupling properties in general probabilistic theory". arXiv:1801.03988, 2018.

[20] G. Aubrun, L. Lami, C. Palazuelos, S. J. Szarek, and A. Winter. "Universal gaps for xor games from estimates on tensor norm ratios". arXiv:1809.10616, 2018.

[21] K. Matsumoto and G. Kimura. "Information storing yields a point-asymmetry of state space in general probabilistic theories". arXiv:1802.01162, 2018.

[22] A. J. Short and S. Wehner. "Entropy in general physical theories". *New J. Phys.*, 12(3):033023, 2010.

[23] Joonwoo Bae, Dai-Gyoung Kim, and Leong Kwek. Structure of optimal state discrimination in generalized probabilistic theories. *Entropy*, 18:39, 01 2016.

[24] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2000.

[25] Jonathan Walgate, Anthony J. Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.*, 85:4972–4975, Dec 2000.

[26] M. Horodecki, P. Horodecki, and R. Horodecki. "Separability of mixed states: necessary and sufficient conditions". *Phys. Lett. A*, 223:1–8, 1996.

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

[28] H. Arai, Y. Yoshida, and M. Hayashi. "Perfect discrimination of non-orthogonal separable pure states on bipartite system in general probabilistic theory". arXiv:1903.01658, 2019.

Graph States as a Resource for Quantum Metrology

Nathan Shettell[1] * Damian Markham[1] †

[1] *Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, 4 place Jussieu, 75005 Paris, France*

Abstract. The GHZ state is an ideal resource state for quantum metrology as it can achieve the Heisenberg limit. However, upon the loss of a single qubit the GHZ state becomes useless for quantum metrology. We provide a method to construct graph states which attains a quantum Fisher information of at least $n^{2-\log_n k}$, we call these states bundled graph states. We demonstrate that bundled graph states yield a quantum advantage after being subjected to dephasing or a small number of erasures, making them more robust than the GHZ state.

Keywords: Metrology, Graph States, Stabilizer States, Quantum Fisher Information, Robustness

1 Introduction

Quantum metrology describes the framework for estimation strategies which surpass the precision limit of classical strategies [1, 2]. Classically, a system with n probes used to estimate an unknown parameter θ, can achieve a precision where the variance scales inversely to the number of probes: $\Delta\theta^2 = 1/n$. In a quantum system, where the probes can be entangled, the highest achievable precision scales quadratically to the number of qubits: $\Delta\theta^2 = 1/n^2$, otherwise known as the Heisenberg limit (HL).

Entanglement is a requirement to yield a quantum advantage, however it is not sufficient [3]. Oszmaniec et al. showed that most quantum states are not useful for metrology, despite having a large amount of entanglement. Given a quantum resource, ρ, the highest achievable precision attainable is bounded by $\mathcal{Q}(\rho)$, the quantum Fisher information (QFI): $\Delta\theta^2 \geq 1/\mathcal{Q}(\rho)$.

We investigate the usefulness of graph states for quantum metrology and construct a family of graph states which achieve a QFI of at least $\mathcal{Q} \geq n^{2-\log_n k}\ \forall k \geq 2$; we call these states bundled graph states. Additionally, we show that bundled graph states retain a quantum advantage when subjected to independent and identically distributed (iid) dephasing and a small number of erasures.

2 Stabilizer States

Definition 1 *An n-qubit stabilizer state is the simultaneous $+1$-eigenstate of n independent operators in the Pauli-n group: $g_1, \ldots, g_n$ [8]. The corresponding stabilizer group $\mathcal{S}$ is generated from these operators and the stabilizer state, ρ, can be expressed as a sum of all operators in the stabilizer group:*

$$\mathcal{S} = \langle g_1, \ldots, g_n \rangle \tag{1}$$

$$\rho = \frac{1}{2^n}\prod_{i=1}^{n}(\mathbb{I} + g_i) = \frac{1}{2^n}\sum_{S\in\mathcal{S}} S \tag{2}$$

We begin by computing $N_{n,\epsilon}$: the number of stabilizer states which have a QFI of at least $\mathcal{Q} \geq n^{2-\epsilon}$. In this study we only consider the canonical case of phase estimation:

$$\rho \to \rho_\theta = e^{-i\theta H}\rho e^{i\theta H} \tag{3}$$

$$H = \frac{1}{2}\sum_{j=1}^{n} X_j \tag{4}$$

Fact 1 *The QFI of a pure state $|\psi\rangle$ which the encoding is described by equation 3 can be computed via: [1]:*

$$\mathcal{Q}(|\psi\rangle) = 4\Delta H^2 = 4\langle\psi|H^2|\psi\rangle - 4\langle\psi|H|\psi\rangle^2 \tag{5}$$

Fact 2 *By choosing generators which maximize equation 5 we show that:*

$$\tilde{N}_{n,\epsilon} \geq \sum_{j=k-1}^{n-1} 2^{j+1}\binom{n-1}{j} N_{n-j+1} \geq 2^n \tag{6}$$

Where $k = n^{1-\epsilon/2}$ and N_m is the the number of m qubit stabilizer states defined in [7].

3 Graph States

In this section we quantify the usefulness of graph states (a subclass of stabilizer states) for quantum metrology based off of the corresponding simple graph.

Definition 2 *An n qubit graph state $G = (V, E)$ is defined in one to one correspondence with a simple graph with $|V| = n$ vertices and edges E. The corresponding generators are:*

$$g_i = X_i \bigotimes_{j\in N(i)} Z_j \tag{7}$$

Where $N(i)$ is the neighbourhood of the ith vertex.

Fact 3 *The QFI of a graph G with no isolated vertices ($|N(i)| \geq 1\ \forall i$) is equal to the number of pairs of vertices (i, j) with $N(i) = N(j)$.*

Proof. For any stabilizer state ρ and pauli P:

$$\mathrm{Tr}(\rho P) = \begin{cases} \pm 1 & \text{if } \pm P \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

*nathan.shettell@lip6.fr

†damian.markham@lip6.fr

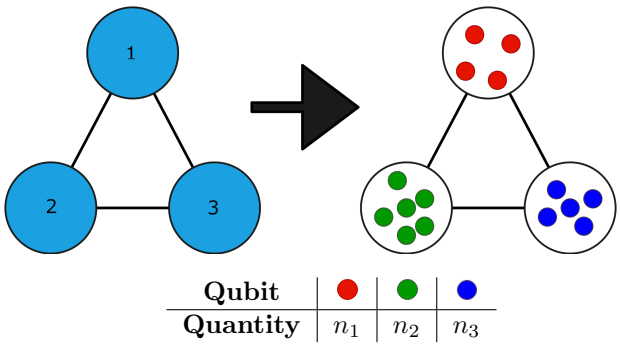


Figure 1: Bundle graph state constructed from a 3-qubit cyclic graph, $\mathcal{Q}(G_{\text{bundle}}) = n_1^2 + n_2^2 + n_3^2 \geq n^{2-log_n 3}$.

Combining the above with equation 5. The only non-vanishing terms are of the form $\text{Tr}(GX_iX_j)$ such that $N(i) = N(j)$. Thus, the QFI of a graph state is equal to the number of pairs (i, j) such that $N(i) = N(j)$:

$$\mathcal{Q}(G) = \sum_{i,j=1}^{n} \delta_{N(i),N(j)} \tag{9}$$

□

4 Bundled Graph States

In this section we provide a method to construct graph states with a QFI of at least $n^{2-\log_n k}$ $\forall k \geq 2$. We call these states bundled graph states. We also explore how robust these states are against iid dephasing and a small number of erasures.

4.1 Construction

To construct a bundle graph $G_{\text{bundle}} = (V', E')$:

1. Begin with any connected graph $G = (V, E)$ with $|V| = k < n$.
2. The jth vertex, v_j, is replaced with n_j qubits, labelled $v_j^1, \ldots, v_j^{n_j}$, such that $\sum_{j=1}^{k} n_j = n$.
3. If $(v_i, v_j) \in E$ then $(v_i^x, v_j^y) \in E'$ $\forall x, y$.

$$V' = \{v_1^1, \ldots, v_1^{n_1}, \ldots, v_k^1, \ldots v_k^{n_k}\} \tag{10}$$
$$E' = \{(v_i^x, v_j^y)\ \forall x, y \mid (v_i, v_j) \in E\} \tag{11}$$

We say vertices $v_j^1, \ldots, v_j^{n_j}$ are bundled together since they all share the same neighbourhood; the necessary condition to attain a high QFI. Using equation 9:

$$\mathcal{Q}(G_{\text{bundle}}) \geq \sum_{j=1}^{k} n_j^2 \geq \frac{n^2}{k} = n^{2-\log_n k} \tag{12}$$

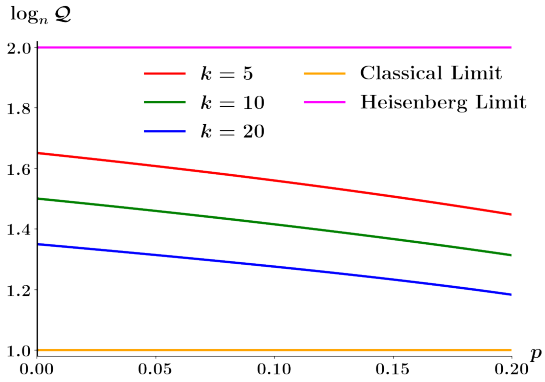


Figure 2: Robustness of $n = 100$ qubit bundled cyclic graphs subjected to iid dephasing with dephasing probability p. The graphs are divided into k bundles of $j = n/k$ qubits. For small p we observe that $\log_n \mathcal{Q}$ decreases linearly, which is expected from equation 13.

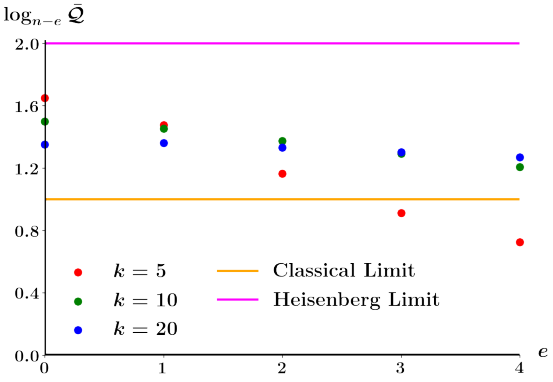


Figure 3: Robustness of $n = 100$ qubit bundled cyclic graphs subjected e erasures. The graphs are divided into k bundles of $j = n/k$ qubits. As k increases, the more erasures a bundled cyclic graph can withstand whilst keeping a quantum advantage (on average); which is expected from equation 14.

4.2 Robustness Against Dephasing

We first investigate if bundled graph states are robust against iid dephasing. A closed form expression for a general graph subjected to iid dephasing is computed in the main study. Assuming that the dephasing probability p is small and the size of all neighbourhoods are large, we make the following approximation:

$$\begin{aligned}\mathcal{Q}(G_{\text{bundle}}^{\text{dephasing}}) &\approx (1-2p)^2 \mathcal{Q}(G_{\text{bundle}}) + 4np(1-p) \\ &\geq (1-2p)^2 \frac{n^2}{k} \\ &= n^{2-\log_n k - \frac{4}{\ln n}p + \mathcal{O}(p^2)}\end{aligned} \tag{13}$$

4.3 Robustness Against Erasures

Next we explore if bundled graph states yield a quantum advantage after a small number of erasures e. For comparision, the GHZ state becomes useless for quantum

metrology after losing a single qubit [1]. The general expression for the QFI of a graph state after e erasures is dependent on the shape of the graph and which qubits are lost. To quantify the robustness of a graph state after experiencing e erasures, we compute $\bar{\mathcal{Q}}$; the average QFI of the system over all $\binom{n}{e}$ permutations of losing e qubits.

We compute the closed form expression of $\bar{\mathcal{Q}}$ for a bundled cyclic graph divided into k nodes of $j = n/k$. The equation holds for $1 \leq e < 2j$:

$$\bar{\mathcal{Q}}_{\text{cycle}} = \frac{2\binom{n-4j}{e} - \binom{n-5j}{e}}{\binom{n}{e}} \frac{n^2}{k} + \frac{2\binom{n-2j}{e} - \binom{n-3j}{e}}{\binom{n}{e}} n \quad (14)$$

5 Single Qubit Measurements

In practise, achieving a precision of $\Delta\theta^2 = 1/\mathcal{Q}$ can only be achieved by measuring in the basis of the symmetric logarithmic derivative [1, 10]. This measurement may not be realistic.

Fact 4 *If the following two conditions are satisfied, we can achieve a precision of $\Delta\theta^2 = 1/\mathcal{Q}$ using graph states:*

1. *The phase we are trying to estimate is small.*
2. *There exists a stabilizer, S_M, for the graph which consists entirely of Y and Z operators.*

The desired precision can be attained by measuring in the S_M basis.
Proof.

$$\begin{aligned}
\langle S_M \rangle &= \langle G | e^{i\frac{\theta}{2}\sum_{i=0}^{n} X_i} S_M e^{-i\frac{\theta}{2}\sum_{i=0}^{n} X_i} | G \rangle \\
&= \langle G | e^{i\theta\sum_{i=0}^{n} X_i} | G \rangle \\
&= \sum_{m=0}^{\infty} \frac{(i\theta)^m}{m!} \langle G | \big(\sum_{i=0}^{n} X_i\big)^m | G \rangle \\
&= 1 - \frac{\theta^2}{2}\mathcal{Q} + \mathcal{O}(\theta^3)
\end{aligned} \quad (15)$$

Using the error propagation formula:

$$\begin{aligned}
\Delta\theta^2 &= \frac{\Delta S_M^2}{|\partial_\theta \langle S_M \rangle|^2} \\
&= \frac{\theta^2\mathcal{Q} + \mathcal{O}(\theta^3)}{\theta^2\mathcal{Q}^2 + \mathcal{O}(\theta^3)} \\
&\approx \frac{\theta^2\mathcal{Q}}{\theta^2\mathcal{Q}^2} \\
&= \frac{1}{\mathcal{Q}}
\end{aligned} \quad (16)$$

□

For a bundled cyclic graph the above conditions can only be satisfied if the number of bundles is a multiple of 4. There are many other graph states where the second condition cannot be satisfied. We show that by using a graph state with one additional qubit we can still achieve a precision of $\Delta\theta^2 = 1/\mathcal{Q}$.

6 Conclusion and Remarks

In this study we have quantified which graph states can achieve a high QFI based off of their topology. We provide a simple construction method to create graph states with a QFI of at least $\mathcal{Q} \geq n^{2-\log_n k}$. We call these states bundled graph states, as they have a large number of qubits with identical neighborhoods; the required property for a graph state to have a high QFI. We also show that bundled cyclic graphs retain a quantum advantage after being subjected to iid dephasing or a small number of erasures. Lastly, we devise a measurement startegy for graph states to achieve a precision of $\Delta\theta = 1/\mathcal{Q}$. All of the aforementioned properties in combination with the fact that graph states can be efficiently generated [6] make them an ideal candidate for quantum metrology.

References

[1] G. Tóth and I. Apellaniz. Quantum metrology from a quantum information science perspective. *J. Phys. A: Math. Theor.*, 47-424006 (2014).

[2] V. Giovannetti, S. Lloyd and L. Maccone. Advances in Quantum Metrology. *Nat. Photonics*, 5 222-229 (2011).

[3] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín and M. Lewenstein. Random Bosonic States for Robust Quantum Metrology. *Phys. Rev. X*, 6-041044 (2016).

[4] R. Demkowicz-Dobrzański, J. Kołodyński and M. Guţă. The Elusive Heisenberg Limit in Quantum-Enhanced Metrology. *Nat, Commun.*, 3-1063 (2012).

[5] S. Zhou, M. Zhang, J. Preskill and L. Jiang. Achieving the Heisenberg limit in quantum metrology using quantum error correction. *Nat. Commun.*, 9-78 (2018).

[6] D. Gottesman. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. *Quantum Information Science and Its Contributions to Mathematics, Proceedings of Symposia in Applied Mathematics*, Amer. Math. Soc., Providence, Rhode Island, 13-58 (2010).

[7] S. Aaronson and D. Gottesman. Improved Simulation of Stabilizer Circuits. *Phys. Rev. A*, 70-052328 (2004).

[8] K. Fujii. Stabilizer Formalism and Its Applications. *Quantum Computation with Topological Codes: From Qubit to Topological Fault-Tolerance*, SpringerBriefs in Mathematical Physics, Singapore, 24-55 (2015).

[9] H. L. van Trees. Detection, Estimation, and Modulation Theory, Part I. *Wiley*, New York (1968).

[10] D. Petz and C. Ghinea. Introduction to quantum Fisher information. arXiv:1008.2417 (2010).

Network Integration of Quantum Dot Device and Entanglement in Cambridge Fiber Network

Z-H. Xiang[1,2], J. Huwer[1], R. M. Stevenson[1], J. Skiba Szymanska[1], M. B. Ward[1], I. Farrer[2,†], D. A. Ritchie[2], and A. J. Shields[1]

1 Toshiba Research Europe Limited, Cambridge Research Laboratory, 208 Science Park, Milton Road, Cambridge, CB4 0GZ, UK.
2 Cavendish Laboratory, JJ Thomson Ave, Cambridge, CB3 0HD, UK.
† Present Address: Department of Electronic & Electrical Engineering, University of Sheffield, Sheffield S1 3JD, UK.
Author e-mail address: zx238@cam.ac.uk

Abstract: Quantum dots are considered to be one of the most important quantum emitters due to their ability of emitting entangled single photons, which have not yet been practically used for large-scale quantum communication. In this work, we integrated a semiconductor quantum dot (QD) device in the Cambridge Fiber Network and realized the transmission of emitted polarization-encoded entangled single photons at the telecommunication O-band. A polarization maintaining system is in operation to compensate for changes in birefringence naturally occurring in installed fiber networks. Stable transmission of high-fidelity (91.3%) entanglement has been maintained over one week, which is a significant step toward the real-life application of quantum dots.

Key Words: Entanglement, Quantum Dot, Field Trial.

1.1. Introduction

Entanglement provides means to transfer quantum information between distant nodes of a network and serves as the key resource for scalable quantum networks. Its practical use requires the integration of robust entangled photon sources, making the semiconductor-based QD light sources a promising candidate system. In this work [1], we have integrated an entangled QD device with the Cambridge Fiber Network. Such installed fiber typically suffers the variation of fiber birefringence over time, putting a negative impact on the transmission of entanglement. To compensate for these drifts, we have introduced a polarization maintaining sub-system, enabling stable long-term transmission of entangled photon pairs over 18km of installed fiber from a sub-Poissonian entangled photon pair source

1.2. Entangled photon generation and polarization stabilization system

To enable high-fidelity entanglement transmission over an urban fiber network, we have built a transmission system consisting of a photon emission and detection sub-system and a polarization maintenance sub-system, as is shown in Figure 1. The quantum dot photon source is located in a cryostat and optically excited with a laser at 1064nm. It emits entangled photons at telecom O-band via the so-called biexciton (XX) – exciton (X) cascade. XX and X photons are separated using a spectral filter. One of the entangled photons is detected directly in the lab, whereas the partner photon is sent over an installed loop-back fiber before being measured.

We have implemented a polarization stabilization scheme using a polarization reference feedback system. Reference light generated from a laser at the same wavelength (1320nm) as the transmitted photons is split into two modes and the outputs of both arms are aligned to have orthogonal directions on Poincaré sphere before being sent over the same fiber. The polarization state after the transmission is detected using two power meters after a polarizing beam splitter and a polarization controller. By stabilizing both references using an electronic polarization controller (EPC 5) and a fiber wave plate (FWP), we effectively lock arbitrary polarization rotation to a minimum on Poincaré sphere. The classical references are time-multiplexed with the quantum channel, controlled by optical switches (OSW 1 and 2).

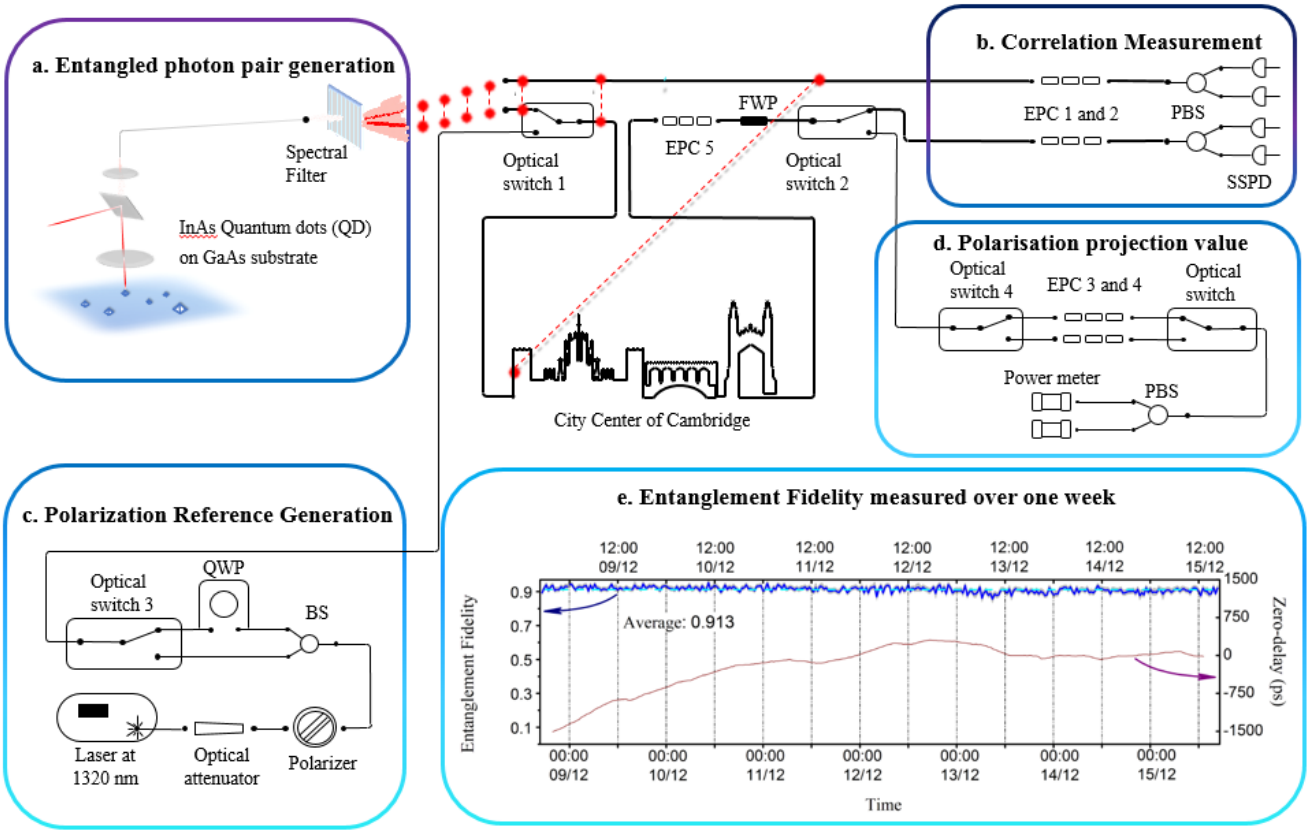


Figure 1 Experimental setup for entangled photon transmission over installed fiber: The whole setup consists of 4 parts, entangled photon generation, correlation measurement, classical polarization reference generation and polarization reference measurement. The entangled photons are generated from an optically excited quantum dot in (a), whose entanglement fidelity is evaluated by correlation measurements in (b). Two classical polarization references are created using a 1320nm laser in (c), whose polarization state is detected in (d). Optical switches 1 and 2 are used for time-multiplexing the quantum and reference signal. EPC 5 and FWP are used for compensating the polarization drift of the field fiber that is installed across the Cambridge city center. The result of the entanglement measurement over one-week time as well as the drift of the time-of-flight of the photons over the field fiber are shown in (e).

1.3. Measurement of Entanglement

The entanglement is evaluated by measuring correlations c_{PQ} between X and XX photons for co- and cross-polarized states P and Q in three detection bases HV, DA and RL and by using the following equation [2]:

$$F = (1 + C_{HV} + C_{DA} - C_{RL})/4$$

In which C_{MN} denotes the correlation contrast. The detection bases are switched every 10 minutes. We apply a post selection scheme with a 48ps window around the zero-delay of the arriving photons to extract the entanglement data.

1.4. Conclusion

We have recorded correlation data for 7 days and observe a stable transmission of entanglement with a high fidelity of 91.3%. This corresponds to a drop by 3.4% compared to the measurements taken without photon transmission over the field fiber. The main factor contributing to the drop is the high 11.70dB loss of the 18km loop-back fiber at 1320nm, which reduces the signal-to-noise ratio by 27 times. The polarisation maintenance system has a low loss of 3.49dB and operates with a high duty cycle of 98%, enabling a high transmission efficiency of the photons. These results indicate a great potential for the practical use of QD entangled photon pair sources over existing telecommunication networks.

[1] Xiang, Zi-Heng, et al. "Long-term transmission of entangled photons from a single quantum dot over deployed fiber." Scientific reports 9.1 (2019): 4111.
[2] Ward, M. B., et al. "Coherent dynamics of a telecom-wavelength entangled photon source." Nature communications 5 (2014): 3316.

Necessary and Sufficient Condition of Asymptotic Decoupling for Markovian Quantum Dynamics

Yuuya Yoshida[1] * Masahito Hayashi[1 2 3] †

[1] *Graduate School of Mathematics, Nagoya University*
[2] *Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology*
[3] *Centre for Quantum Technologies, National University of Singapore*

Abstract. We address *asymptotic decoupling* in the context of Markovian quantum dynamics. Asymptotic decoupling is an asymptotic property on a bipartite quantum system, and asserts that the correlation between two quantum systems is broken after a sufficiently long time passes. In this paper, we show that asymptotic decoupling is equivalent to *local mixing* which asserts the convergence to a unique stationary state on at least one quantum system. In our previous study [18th AQIS, 8–12 September 2018, Nagoya], we defined and discussed asymptotic decoupling, but considered it only for special Markovian quantum dynamics with discrete-time. To compensate for this weak point, we address general Markovian quantum dynamics with discrete/continuous-time. The full version of this paper is available at arXiv:1801.03988

Keywords: Markovian quantum dynamics, asymptotic decoupling, mixing, C_0 semigroup

1 Introduction

Decoupling asserts that a quantum channel breaks the correlation between two quantum systems, and attracts attention in open quantum systems [1] and quantum information [2–4]. For example, Dupuis et al. [3] proved a decoupling theorem and clarified a relation between the accuracy of decoupling and conditional entropies. Since the correlation between two quantum systems should be small for instance in evaluating information leakage [5,6], it is an interesting topic to investigate decoupling in the context of quantum dynamics. In this paper, we introduce *asymptotic decoupling* in the context of Markovian quantum dynamics, and clarify a necessary and sufficient condition of asymptotic decoupling. By our necessary and sufficient condition, asymptotic decoupling is closely related to another fundamental property in the study of Markovian dynamics.

Markovian dynamics has been often discussed in the context of statistical mechanics [7–9]. In such studies, it is important how an initial state changes after a sufficiently long time passes. In particular, the convergence (called *mixing*) and the convergence of the long-time average (called *ergodicity*) interest many researchers [10, 11]. Hence mixing has been discussed in the context of relaxation to thermal equilibrium [7–9]. However, beyond the study of relaxation processes, these properties have found important applications in several fields of quantum information theory. In particular, in quantum control [12], quantum estimation [13], quantum communication [14], and the study of efficient tensorial representations of critical many-body quantum systems [15]. Actually, mixing is closely related to asymptotic decoupling, and we show that asymptotic decoupling is equivalent to *local mixing* which asserts the convergence to a unique stationary state on at least one quantum system. As far as we know, preceding studies except for our previous study [16] have not associated decoupling with mixing.

*m17043e@math.nagoya-u.ac.jp
†masahito@math.nagoya-u.ac.jp

$$\rho \xrightarrow{\Gamma} \Gamma(\rho) \xrightarrow{\Gamma} \Gamma^2(\rho) \xrightarrow{\Gamma} \cdots \xrightarrow{\Gamma} \Gamma^n(\rho) \xrightarrow{\Gamma} \cdots$$

Figure 1: Markovian quantum dynamics with discrete-time.

Therefore, a contribution of this paper is to associate decoupling with mixing closely. Moreover, addressing the discrete and continuous cases is a feature of this paper.

The remaining of this paper is organized as follows. Section 2 gives our main result, i.e., a necessary and sufficient condition of asymptotic decoupling. Section 3 addresses continuous-time evolution.

2 Main result

As Figure 1, consider dynamics given by n applications of a quantum channel Γ to an initial quantum state ρ. Then we are interested in the asymptotic behavior of the n-th state $\Gamma^n(\rho)$ as $n \to \infty$. In particular, when Γ (resp. ρ) is a bipartite quantum channel (resp. state), we are interested in vanishing the correlation between two quantum systems asymptotically. If the correlation vanishes asymptotically, we say that Γ is asymptotically decoupling.

In order to define asymptotic decoupling mathematically, let us introduce some notations. Consider two finite-dimensional quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$ of our interest. For a number $i \in \{1, 2\}$ and a quantum state $\tilde{\rho}$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, the reduced state on $\mathcal{H}_i$ of $\tilde{\rho}$ is denoted by $\pi_i(\tilde{\rho})$ to emphasize a remaining system instead of a deleted system. That is, by using the partial traces Tr_1 and Tr_2, we have $\pi_1(\tilde{\rho}) = \mathrm{Tr}_2\, \tilde{\rho}$ and $\pi_2(\tilde{\rho}) = \mathrm{Tr}_1\, \tilde{\rho}$. From now on, we use *tilde* to express to be bipartite. For instance, a bipartite quantum state is denoted by $\tilde{\rho}$, and a bipartite quantum channel is denoted by $\tilde{\Gamma}$.

Now, the mathematical definition of asymptotic decoupling is below:

Definition 1 (Asymptotic decoupling [16])**.** *A quantum*

channel $\tilde{\Gamma}$ is asymptotically decoupling if any state $\tilde{\rho}$ satisfies

$$\tilde{\Gamma}^n(\tilde{\rho}) = \pi_1(\tilde{\Gamma}^n(\tilde{\rho})) \otimes \pi_2(\tilde{\Gamma}^n(\tilde{\rho})) + o(1) \quad (n \to \infty).$$

Since the above right-hand side is a product state, it means to be no correlation. Next, to clarify a necessary and sufficient condition of asymptotic decoupling, we introduce another asymptotic property, namely, mixing:

Definition 2 (Mixing [10, 11, 16])**.** *A quantum channel Γ is mixing if there exists a state ρ_0 such that any state ρ satisfies*

$$\lim_{n\to\infty} \Gamma^n(\rho) = \rho_0.$$

The state ρ_0 is called the stationary state.

Note that a quantum channel is given as a trace-preserving and completely positive linear map (TP-CP map). Thus asymptotic decoupling and mixing are asymptotic properties for TP-CP maps. Now, we give a necessary and sufficient condition of asymptotic decoupling. For simplicity, first, we give it for a tensor product quantum channel $\Gamma_1 \otimes \Gamma_2$:

Theorem 3. *For any two quantum channels Γ_1 and Γ_2, the following conditions are equivalent.*

1. *$\Gamma_1 \otimes \Gamma_2$ is asymptotically decoupling.*
2. *Γ_1 or Γ_2 at least one is mixing.*

Condition 2 can be represented as a simple phrase *local mixing*. Hence, simply speaking, asymptotic decoupling is equivalent to local mixing. Since spectral criterion [10, Theorem 7] and another criterion [16, Theorem 1] are known as criteria of mixing, these criteria determine whether a tensor product quantum channel is asymptotically decoupling or not. These are why Theorem 3 is simple and meaningful. Moreover, the above equivalence also holds for a general quantum channel:

Theorem 4. *For any quantum channel $\tilde{\Gamma}$, the following conditions are equivalent.*

1. *$\tilde{\Gamma}$ is asymptotically decoupling.*
2. *There exist a number $i_1 \in \{1, 2\}$ and a state ρ_{0,i_1} on $\mathcal{H}_{i_1}$ such that any state $\tilde{\rho}$ satisfies*

   $$\tilde{\Gamma}^n(\tilde{\rho}) = \rho_{0,i_1} \otimes \pi_{i_2}(\tilde{\Gamma}^n(\tilde{\rho})) + o(1) \quad (n \to \infty),$$

   where i_2 is an element of $\{1, 2\}$ except for i_1.

Condition (2) can be explicitly written as

Case $(i_1, i_2) = (1, 2)$ $\quad \tilde{\Gamma}^n(\tilde{\rho}) = \rho_{0,1} \otimes \pi_2(\tilde{\Gamma}^n(\tilde{\rho})) + o(1),$

Case $(i_1, i_2) = (2, 1)$ $\quad \tilde{\Gamma}^n(\tilde{\rho}) = \pi_1(\tilde{\Gamma}^n(\tilde{\rho})) \otimes \rho_{0,2} + o(1).$

Since the state $\rho_{0,1}$ or $\rho_{0,2}$ is something like a stationary state, condition (2) can also be regarded as local mixing. Hence, for a general quantum channel, the same simple equivalence also holds: asymptotic decoupling is equivalent to local mixing.

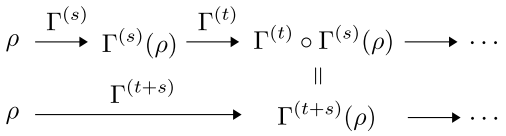


Figure 2: Markovian quantum dynamics with continuous-time.

3 Continuous-time evolution

Next, we address continuous-time evolution. In the discrete case, $\Gamma^n(\rho)$ has denoted the state at time $n \in \mathbb{N}$. Since we address continuous-time evolution in this section, we denote by $\Gamma^{(t)}(\rho)$ the state at time $t > 0$. Moreover, it is natural that the family $\{\Gamma^{(t)}\}_{t>0}$ of quantum channels should satisfy

- $\Gamma^{(t)} \circ \Gamma^{(s)} = \Gamma^{(t+s)}$ for all $t, s > 0$,
- $\Gamma^{(t)} \to \mathrm{id}_{\mathcal{T}(\mathcal{H})}$ as $t \downarrow 0$.

where $\mathrm{id}_{\mathcal{T}(\mathcal{H})}$ denotes the identity map on the set $\mathcal{T}(\mathcal{H})$ of all Hermitian matrices on $\mathcal{H}$. The above first condition is illustrated by Figure 2. It asserts that the state at time $t + s$ equals the state after a time s passes from the state at time t. A family $\{\Gamma^{(t)}\}_{t>0}$ satisfying the above two conditions is called a C_0 *semigroup*. It can be easily checked that any C_0 semigroup $\{\Gamma^{(t)}\}_{t>0}$ is right-continuous everywhere. The definition of a C_0 semigroup is simple and intuitive in the finite-dimensional case, but the infinite-dimensional case needs a few technical conditions. Although there are many studies on C_0 semigroups of finite/infinite-dimensions, we use no existing results on C_0 semigroups and only use the above two conditions. In the context of Markovian quantum dynamics, C_0 semigroups are also called *quantum dynamical semigroups* [17].

In order to state our results in the continuous case, we need to define the continuous versions of asymptotic decoupling and mixing. Fortunately, once replacing Γ^n and $n \to \infty$ with $\Gamma^{(t)}$ and $t \to \infty$ respectively, the continuous versions of asymptotic decoupling and mixing are defined. In this setting, the continuous versions of Theorems 3 and 4 are below:

Theorem 5. *For any two C_0 semigroups $\{\Gamma_1^{(t)}\}_{t>0}$ and $\{\Gamma_2^{(t)}\}_{t>0}$, the following conditions are equivalent.*

1. *$\{\Gamma_1^{(t)} \otimes \Gamma_2^{(t)}\}_{t>0}$ is asymptotically decoupling.*
2. *$\{\Gamma_1^{(t)}\}_{t>0}$ or $\{\Gamma_2^{(t)}\}_{t>0}$ at least one is mixing.*

Theorem 6. *For any C_0 semigroup $\{\tilde{\Gamma}^{(t)}\}_{t>0}$, the following conditions are equivalent.*

1. *$\{\tilde{\Gamma}^{(t)}\}_{t>0}$ is asymptotically decoupling.*
2. *There exist a number $i_1 \in \{1, 2\}$ and a state ρ_{0,i_1} on $\mathcal{H}_{i_1}$ such that any state $\tilde{\rho}$ satisfies*

   $$\tilde{\Gamma}^{(t)}(\tilde{\rho}) = \rho_{0,i_1} \otimes \pi_{i_2}(\tilde{\Gamma}^{(t)}(\tilde{\rho})) + o(1) \quad (t \to \infty),$$

   where i_2 is an element of $\{1, 2\}$ except for i_1.

Table 1: Difference from our previous result.

	Dynamical map	Time evolution
Previous result [16]	$\Gamma^{\otimes 2}$ $\Gamma \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H})}$	Discrete
This paper	$\Gamma_1 \otimes \Gamma_2$ General $\tilde{\Gamma}$	Discrete Continuous

Similarly to the discrete case, asymptotic decoupling is equivalent to local mixing. Theorem 6 is derived from Theorem 4 at the end of this section. Table 1 summarizes the difference between this paper and our previous result [16, Theorem 1], with respect to asymptotic decoupling.

Some readers might consider that Theorems 5 and 6 are more general than Theorems 3 and 4. However, it is not true due to the following reason. Any C_0 semigroup $\{\Gamma^{(t)}\}_{t>0}$ can be represented as an exponential function [18, Theorem I.3.7]: there exists a linear map $\mathcal{L}$ such that $\Gamma^{(t)} = e^{t\mathcal{L}}$ for all $t > 0$. Thus $\Gamma^{(t)}$ does not have the eigenvalue zero. However, the discrete case allows that Γ has the eigenvalue zero. Moreover, $\{\Gamma^{(t)}\}_{t>0}$ is a C_0 semigroup of CP maps if and only if $\{(\Gamma^{(t)})^{\otimes 2}\}_{t>0}$ is a C_0 semigroup of positive maps [19, Theorem 1]. This fact is completely different from the case with CP maps: positivity for $\Gamma^{\otimes 2}$ does not imply complete positivity for Γ. These are why the continuous case is somewhat restricted. The above generator $\mathcal{L}$ is called a *Lindbladian* and was characterized by Lindblad [17].

Proof of Theorem 6 *assuming Theorem* 4. 2⇒1. This implication follows from the definition.

1⇒2. Assume condition 1. Since $(\tilde{\Gamma}^{(1)})^n = \tilde{\Gamma}^{(n)}$ for all $n \in \mathbb{N}$, the quantum channel $\tilde{\Gamma}^{(1)}$ is asymptotically decoupling. Thus Theorem 4 implies that $\tilde{\Gamma}^{(1)}$ satisfies condition 2 in Theorem 4. Without loss of generality, we may assume $(i_1, i_2) = (1, 2)$. Thus any state $\tilde{\rho}$ satisfies

$$\begin{aligned} \tilde{\Gamma}^{(n)}(\tilde{\rho}) &= \rho_{0,1} \otimes \pi_2(\tilde{\Gamma}^{(n)}(\tilde{\rho})) + o(1), \\ \pi_1(\tilde{\Gamma}^{(n)}(\tilde{\rho})) &= \rho_{0,1} + o(1). \end{aligned} \tag{1}$$

Now, let $\Gamma_{0,1}$ be the quantum channel defined as $\Gamma_{0,1}(\rho) = \rho_{0,1}$ for any state ρ on $\mathcal{H}_1$. Also, let $n = n(t) := \lfloor t \rfloor$ and $\delta = \delta(t) := t - n(t)$ for all $t > 0$. Then any state $\tilde{\rho}$ satisfies

$$\begin{aligned} \pi_1(\tilde{\Gamma}^{(t)}(\tilde{\rho})) &= \pi_1 \circ \tilde{\Gamma}^{(n)}(\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho}) + \pi_1 \circ \tilde{\Gamma}^{(n)}(\tilde{\rho}) \\ &= \pi_1 \circ \tilde{\Gamma}^{(n)}(\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho}) + \rho_{0,1} + o(1), \end{aligned} \tag{2}$$

where the last equality follows from (1). Moreover, since (1) implies that $\pi_1 \circ \tilde{\Gamma}^{(n)}$ converges to $\Gamma_{0,1}$ as $n \to \infty$, we obtain

$$\begin{aligned} &\|\pi_1 \circ \tilde{\Gamma}^{(n)}(\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho})\|_1 \\ &= \|\pi_1 \circ \tilde{\Gamma}^{(n)}(\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho}) - \Gamma_{0,1}(\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho})\|_1 \\ &= \|(\pi_1 \circ \tilde{\Gamma}^{(n)} - \Gamma_{0,1})(\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho})\|_1 \\ &\le \|\pi_1 \circ \tilde{\Gamma}^{(n)} - \Gamma_{0,1}\|_{1,1} \cdot \|\tilde{\Gamma}^{(\delta)}(\tilde{\rho}) - \tilde{\rho}\|_1 \\ &\le 2\,\|\pi_1 \circ \tilde{\Gamma}^{(n)} - \Gamma_{0,1}\|_{1,1} \xrightarrow{t\to\infty} 0, \end{aligned} \tag{3}$$

where $\|\cdot\|_1$ denotes the trace norm, and $\|\cdot\|_{1,1}$ denotes the operator norm based on the trace norm: $\|\Theta\|_{1,1} = \sup_{\|X\|_1 \le 1} \|\Theta(X)\|_1$ for a linear map Θ on $\mathcal{T}(\mathcal{H})$. Therefore, (2) and (3) yield $\pi_1(\tilde{\Gamma}^{(t)}(\tilde{\rho})) = \rho_{0,1} + o(1)$. This equation and condition 1 imply condition 2. □

Acknowledgments

The authors are grateful to Ziyu Liu for discussing the continuous case together. YY was supported by Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for JSPS Fellows No. 19J20161. MH was supported in part by a JSPS Grant-in-Aids for Scientific Research (A) No. 17H01280 and for Scientific Research (B) No. 16KT0017, and Kayamori Foundation of Information Science Advancement.

References

[1] L. Viola, E. Knill, and S. Lloyd, "Dynamical decoupling of open quantum systems," *Phys. Rev. Lett.* **82** 2417 (1999).

[2] F. Dupuis, "The decoupling approach to quantum information theory," PhD Thesis, Université de Montréal, defended December 2009; arXiv:1004.1641.

[3] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, "One-shot decoupling," *Commun. Math. Phys.* **328** 251–284 (2014).

[4] C. Majenz, M. Berta, F. Dupuis, R. Renner, and M. Christandl, "Catalytic decoupling of quantum information," *Phys. Rev. Lett.* **118** 080503 (2017).

[5] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, 10th Anniversary Edition, Cambridge University Press, Cambridge, (2010).

[6] M. Hayashi, *Quantum Information Theory Mathematical Foundation*, Second Edition, Springer, Berlin, (2017).

[7] R. F. Streater, *Statistical Dynamics: A Stochastic Approach to Nonequilibrium Thermodynamics*, Second Edition, Imperial College Press, London (2009).

[8] H. P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems*, Oxford University Press, New York (2002).

[9] F. Benatti and R. Floreanini (Eds.), *Irreversible Quantum Dynamics*, Lecture Notes in Physics vol. 622, Springer, Berlin (2003).

[10] D. Burgarth and V. Giovannetti, "The generalized Lyapunov theorem and its application to quantum channels," *New J. Phys.* **9** 150 (2007).

[11] D. Burgarth, G. Chiribella, V. Giovannetti, P. Perinotti, and K. Yuasa, "Ergodic and mixing quantum channels in finite dimensions," *New J. Phys.* **15** 073045 (2013).

[12] T. Wellens, A. Buchleitner, B. Kümmerer, and H. Maassen, "Quantum state preparation via asymptotic completeness," *Phys. Rev. Lett.* **85** 3361 (2000).

[13] M. Guţă, "Fisher information and asymptotic normality in system identification for quantum Markov chains," *Phys. Rev. A* **83** 062324 (2011).

[14] V. Giovannetti and D. Burgarth, "Improved transfer of quantum information using a local memory," *Phys. Rev. Lett.* **96** 030501 (2006).

[15] M. Fannes, B. Nachtergaele, and R. Werner, "Finitely correlated states on quantum spin chains," *Commun. Math. Phys.* **144** 443–490 (1992).

[16] Y. Yoshida and M. Hayashi, "Asymptotically decoupling and mixing properties in quantum system," 18th Asian Quantum Information Science Conference (AQIS), 8–12 September 2018, Nagoya, Japan.

[17] G. Lindblad, "On the generators of quantum dynamical semigroups," *Commun. Math. Phys.* **48**, 119–130 (1976).

[18] K.-J. Engel and R. Nagel, *One-Parameter Semigroups for Linear Evolution Equations*, Graduate Texts in Mathematics **194**, Springer, New York (2000).

[19] F. Benatti, D. Chruściński, and S. Filippov, "Tensor power of dynamical maps and positive versus completely positive divisibility," *Phys. Rev. A* **95** 012112 (2017).

Incompatibility robustness of quantum measurements: a unified framework

Sébastien Designolle[1] * Máté Farkas[2] † Jędrzej Kaniewski[3] ‡

[1] *Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*
[2] *Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdansk, 80-952 Gdansk, Poland*
[3] *Center for Theoretical Physics, Polish Academy of Sciences, Al. Lotników 32/46, 02-668 Warsaw, Poland*

Abstract. Several measures have been proposed to quantify the incompatibility of quantum measurements, however their properties are not well-understood. We develop a general framework that encompasses all robustness-based measures of incompatibility. We study five commonly used measures and find that some of them do not fulfil some basic requirements, and that what constitutes the most incompatible measurement pair depends on the specific measure. We prove that for one of the measures, measurements corresponding to mutually unbiased bases are among the most incompatible pairs in every dimension, but also that this is not the case for some of the remaining measures.

Keywords: joint measurability, incompatibility robustness, mutually unbiased bases

1 Introduction

In quantum theory, measurements possess certain counter-intuitive features. In classical theories they merely amount to reading out pre-existing properties of the physical system. Quantum measurements, however, disturb the system and their outcomes are fundamentally impossible to predict with certainty. This gives rise to a plethora of non-classical phenomena, one of which is known as *incompatibility* of measurements, manifested for example in the inability to simultaneously measure the position and momentum of a quantum mechanical particle.

Conversely, we say that two measurements are *compatible*, or *jointly measurable*, if they can be simultaneously measured by performing a so-called *parent* measurement [1]. Compatible measurements do not provide any quantum advantage in nonlocality and steering [2, 3, 4], and therefore characterising incompatible measurements is a fundamentally important task.

One such characterisation method is to quantify to *what extent* a pair of measurements is incompatible. A natural way is to introduce *robustness-based* measures of incompatibility, which quantify how much noise the measurements can tolerate before becoming compatible. Several measures of this type have already been proposed [1], but their properties and the relations between them are not well-understood.

In particular, it is not understood whether some of these measures satisfy certain natural monotonicity properties motivated by resource theories [5, 6]. Such measures are meaningful quantifiers of incompatibility, and therefore the question "what are the most incompatible measurement pairs?" is justified with respect to them.

In this work, we take the following steps towards filling the gap in the general understanding of robustness-based measures of incompatibility:

- We introduce a unified framework for analysing robustness-based measures with respect to an arbitrary noise model. We provide explicit connections between the desired properties of the measures and certain properties of the noise models.
- We analyse five measures widely used in the literature and show that some of them do not satisfy certain natural properties.
- We show that what constitutes the most incompatible measurement pair in general depends on the specific measure. For one measure we show that mutually unbiased bases (MUBs) are among the most incompatible measurement pairs in every dimension. However, we also show that this is not the case for some other measures by providing explicit measurements that are more incompatible than MUBs.

2 Concepts and tools

We utilise the positive operator-valued measure (POVM) model for finite d dimensional measurements. Given a pair of POVMs $\{A_a\}_{a=1}^{n_A}$ and $\{B_b\}_{b=1}^{n_B}$, we say that they are compatible (or jointly measurable), $(A,B) \in \mathbf{JM}_d^{n_A,n_B}$, if there exists a parent POVM $\{G_{ab}\}_{a=1,b=1}^{n_A,n_B}$ such that $\sum_b G_{ab} = A_a$ for all a and $\sum_a G_{ab} = B_b$ for all b. Such a parent POVM provides an operational way of simultaneously measuring A and B, while if a parent POVM does not exist, we say that A and B are incompatible (not jointly measurable). Note that the set of jointly measurable pairs $\mathbf{JM}_d^{n_A,n_B}$ is a convex subset of all POVM pairs $\mathbf{POVM}_d^{n_A,n_B}$.

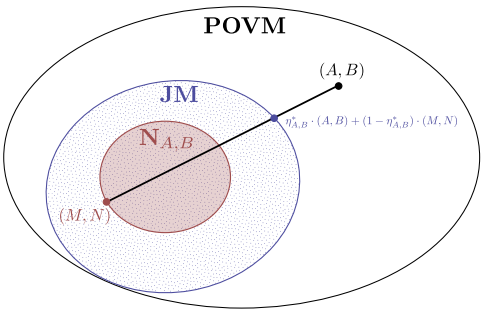
Given a POVM pair (A,B), we define a noisy version of it by the pair $\eta\cdot(A,B)+(1-\eta)\cdot(M,N)$, where $\eta \in [0,1]$ is the *visibility* and $(M,N) \in \mathbf{N}_{A,B} \subseteq \mathbf{POVM}_d^{n_A,n_B}$ is a POVM pair from the *noise set* $\mathbf{N}_{A,B}$. For any noise model defined by $\mathbf{N}_{A,B}$ that is closed and contains at least one jointly measurable pair, we can define a corre-

*sebastien.designolle@unige.ch
†mate.farkas@phdstud.ug.edu.pl
‡jkaniewski@cft.edu.pl

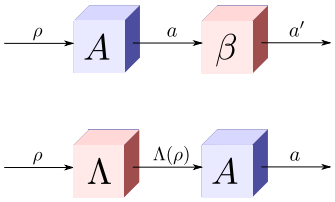
sponding *incompatibility robustness* measure

$$\eta^*_{A,B} = \max_{\substack{\eta\in[0,1]\\(M,N)\in\mathbf{N}_{A,B}}} \Big\{\eta \,\Big|\, \eta\cdot(A,B)+(1-\eta)\cdot(M,N)\in\mathbf{JM}\Big\},$$

which is the highest visibility allowed within this noise model such that the noisy version of (A,B) is still compatible. For any noise model, $\eta^*_{A,B}=1$ if and only if $(A,B)\in\mathbf{JM}$, and the more incompatible the measurements are, the lower $\eta^*_{A,B}$ is. These measures can be visualised using the sets $\mathbf{JM}$ and $\mathbf{N}_{A,B}$:



To obtain unitarily invariant measures, it is sufficient that the corresponding noise set is covariant with respect to unitaries. Motivated by resource theories, measurements should not become more incompatible under operations Φ that preserve joint measurability. We are then looking for noise models that give rise to measures that do not decrease under some natural operations. We consider two joint measurability-preserving operations acting on the outputs and the inputs of the measurements, respectively. *Post-processings* apply a response function to the measurement outcomes, while *pre-processings* apply a quantum channel to the input state, see the figures below.



We show that whenever the image of the noise set under such an operation is contained in the noise set of the image, that is, $\Phi(\mathbf{N}_{A,B})\subseteq\mathbf{N}_{\Phi(A,B)}$ for all (A,B), the corresponding measure is non-decreasing under the operation, $\eta^*_{\Phi(A,B)}\geq\eta^*_{A,B}$ for all (A,B). Taking convex combinations also preserves joint measurability, and we identify a simple constraint on the noise set which together with its convexity implies that the corresponding measure is non-decreasing under convex combinations. However, we show using explicit counterexamples that none of the measures that we study are concave.

Identifying operations under which a measure is non-decreasing is crucial for finding the most incompatible pairs with respect to this measure. As an example, if we want to find the most incompatible pairs for a fixed dimension, and the measure is non-decreasing under post-processings, it is enough to look at pairs from which any other pair can be obtained via post-processing, that is, pairs of rank-one POVMs. We use this technique to find the most incompatible pairs under some measures.

For finding the most incompatible measurement pairs under a measure, it is also important to derive bounds on its value. We make use of the semidefinite programming (SDP) formulation of incompatibility robustness measures. From the primal and dual SDPs, we obtain lower and upper bounds, respectively, on the measures by finding feasible points using ansatz solutions.

3 Results

3.1 Five relevant measures

In our work we analyse five widely used measures by applying our unified framework.

Incompatibility depolarising robustness – η^{d}
The noise set is

$$\mathbf{N}^{\mathrm{d}}_{A,B}=\left\{\left(\left\{\mathrm{tr}(A_a)\frac{\mathbb{I}_d}{d}\right\}_{a=1}^{n_A},\left\{\mathrm{tr}(B_b)\frac{\mathbb{I}_d}{d}\right\}_{b=1}^{n_B}\right)\right\},$$

the one-element set containing the trivial measurements weighted with the traces. We show that this measure is not non-decreasing under pre-processings, and it is not concave, contrary to what is stated in Refs. [7] and [8], respectively. Using its SDP formulation, we derive the tightest lower bound on η^{d} known so far.

Incompatibility random robustness – η^{r}
The noise set is

$$\mathbf{N}^{\mathrm{r}}_{A,B}=\left\{\left(\left\{\frac{\mathbb{I}_d}{n_A}\right\}_{a=1}^{n_A},\left\{\frac{\mathbb{I}_d}{n_B}\right\}_{b=1}^{n_B}\right)\right\},$$

the one-element set containing the trivial measurements. We show that this measure is not non-decreasing under post-processings, which makes it difficult to derive good universal bounds on it.

The following three measures satisfy all the natural properties that we discuss, and using their SDP formulation, we derive new bounds on them.

Incompatibility probabilistic robustness – η^{p}
The noise set is

$$\mathbf{N}^{\mathrm{p}}_{A,B}=\left\{\left(\{p_a\,\mathbb{I}_d\}_{a=1}^{n_A},\{q_b\,\mathbb{I}_d\}_{b=1}^{n_B}\right)\right\},$$

the trivial measurements weighted with probabilities p and q.

Incompatibility jointly measurable rob. – η^{jm}
The noise set is

$$\mathbf{N}^{\mathrm{jm}}_{A,B}=\mathbf{JM}_d^{n_A,n_B},$$

the set of all jointly measurable pairs.

Incompatibility generalised robustness – η^{g}
The noise set is

$$\mathbf{N}^{\mathrm{g}}_{A,B}=\mathbf{POVM}_d^{n_A,n_B},$$

the set of all POVMs. In this case, we derive a universal lower bound on η^{g} and show that measurements corresponding to a pair of MUBs saturate this bound, and therefore they are among the most incompatible pairs in any dimension with respect to this measure.

3.2 Relations between the measures, example

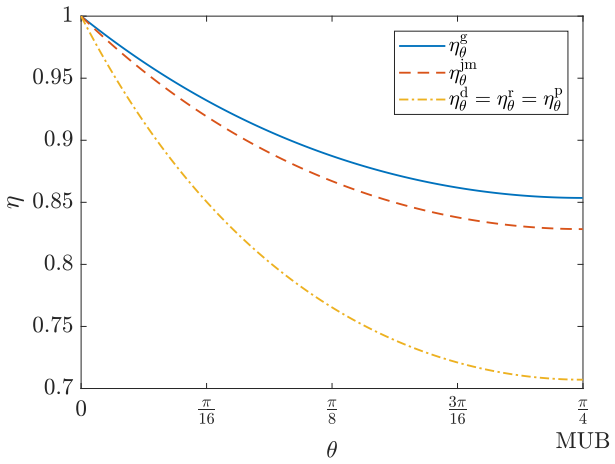
The inclusions between the noise sets

$$(\mathbf{N}^{\mathrm{d}}_{A,B} \cup \mathbf{N}^{\mathrm{r}}_{A,B}) \subseteq \mathbf{N}^{\mathrm{p}}_{A,B} \subseteq \mathbf{N}^{\mathrm{jm}}_{A,B} \subseteq \mathbf{N}^{\mathrm{g}}_{A,B}$$

imply the ordering of the corresponding measures

$$\max\{\eta^{\mathrm{d}}_{A,B}, \eta^{\mathrm{r}}_{A,B}\} \leq \eta^{\mathrm{p}}_{A,B} \leq \eta^{\mathrm{jm}}_{A,B} \leq \eta^{\mathrm{g}}_{A,B}.$$

We demonstrate this order, and the applicability of our techniques by plotting the exact value of all the measures for a pair of rank-one projective qubit measurements with angle 2θ between their Bloch vectors on the figure below.



3.3 Mutually unbiased bases

We are also able to calculate the exact value of the measures $\eta^{*}_{\mathrm{MUB}}(d)$ for a pair of MUBs in any dimension d. In dimension 2, we obtain

$$\eta^{\mathrm{d}}_{\mathrm{MUB}}(2) = \eta^{\mathrm{r}}_{\mathrm{MUB}}(2) = \eta^{\mathrm{p}}_{\mathrm{MUB}}(2) = \frac{1}{\sqrt{2}},$$

$$\eta^{\mathrm{jm}}_{\mathrm{MUB}}(2) = 2(\sqrt{2}-1), \quad \eta^{\mathrm{g}}_{\mathrm{MUB}}(2) = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right),$$

whereas in higher dimensions we get

$$\eta^{\mathrm{d}}_{\mathrm{MUB}}(d) = \eta^{\mathrm{r}}_{\mathrm{MUB}}(d) = \eta^{\mathrm{p}}_{\mathrm{MUB}}(d) = \frac{1}{2}\left(1+\frac{1}{\sqrt{d}+1}\right),$$

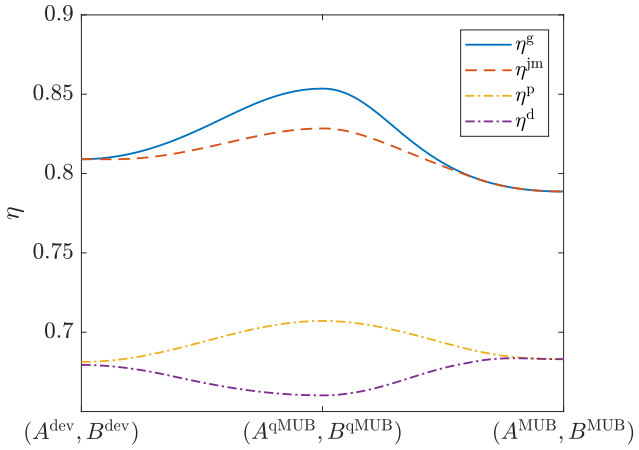
$$\eta^{\mathrm{jm}}_{\mathrm{MUB}}(d) = \eta^{\mathrm{g}}_{\mathrm{MUB}}(d) = \frac{1}{2}\left(1+\frac{1}{\sqrt{d}}\right).$$

While it is not obvious that in higher dimensions these values do not depend on the specific choice of MUB pair, it turns out to be the case for these measures.

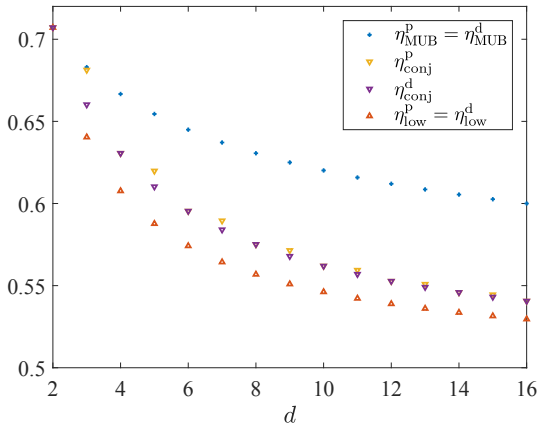
3.4 The most incompatible measurements

In dimension 2, pairs of MUBs turn out to saturate the universal bounds that we derive for η^{d}, η^{p}, η^{jm} and η^{g}, and therefore they are among the most incompatible pairs with respect to these measures.

In dimension 3, the picture changes dramatically, and for some measures we find explicit rank-one projective measurements that are more incompatible than MUBs. To demonstrate this, we plot the value of four measures on a particular path of rank-one projective measurements. For η^{d}, a pair of MUBs on a two dimensional subspace $(A^{\mathrm{qMUB}}, B^{\mathrm{qMUB}})$ outperforms qutrit MUBs and is our candidate for the most incompatible pair. For η^{p}, we find another rank-one projective pair $(A^{\mathrm{dev}}, B^{\mathrm{dev}})$ that outperforms both qutrit and qubit MUBs. This shows that the most incompatible measurement pair in general depends on the specific measure of incompatibility.



In dimensions higher than 3, our conjectures for the most incompatible pairs for η^{d} and η^{p} are direct sums of the optimal pairs in dimensions 2 and 3. Below we plot the value of the measures η^{d} and η^{p} in dimensions 2 to 16 for a pair of MUBs (blue circles), for our conjectured optimal pairs (purple and yellow downward pointing triangles), and our analytical lower bounds (orange upward pointing triangles). Note that our new constructions are the currently known most incompatible pairs under these measures. Regarding the other measures, we show that $\eta^{\mathrm{r}} = 1/2$ can be achieved in any dimension by adding zero outcomes to the measurements. Therefore, the question of the most incompatible pairs for fixed dimension is trivial for this measure. For η^{jm} our numerical search did not lead to any improvement on the MUB value, and for η^{g} we have analytically proven that MUBs are among the most incompatible pairs in every dimension.



References

[1] T. Heinosaari, T. Miyadera, and M. Ziman, "An invitation to quantum incompatibility," *Journal of Physics A: Mathematical and Theoretical*, vol. 49, no. 12, p. 123001, 2016.

[2] M. M. Wolf, D. Perez-Garcia, and C. Fernandez, "Measurements incompatible in quantum theory cannot be measured jointly in any other no-signaling theory," *Phys. Rev. Lett.*, vol. 103, p. 230402, 2009.

[3] M. T. Quintino, T. Vértesi, and N. Brunner, "Joint measurability, Einstein–Podolsky–Rosen steering, and Bell nonlocality," *Phys. Rev. Lett.*, vol. 113, p. 160402, 2014.

[4] R. Uola, C. Budroni, O. Gühne, and J.-P. Pellonpää, "One-to-one mapping between steering and joint measurability problems," *Phys. Rev. Lett.*, vol. 115, p. 230402, 2015.

[5] B. Coecke, T. Fritz, and R. W. Spekkens, "A mathematical theory of resources," *Information and Computation*, vol. 250, pp. 59–86, 2016.

[6] T. Fritz, "Resource convertibility and ordered commutative monoids," *Mathematical Structures in Computer Science*, vol. 27, no. 6, pp. 850–938, 2017.

[7] T. Heinosaari, J. Kiukas, and D. Reitzner, "Noise robustness of the incompatibility of quantum measurements," *Phys. Rev. A*, vol. 92, p. 022115, 2015.

[8] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, "Simulating positive-operator-valued measures with projective measurements," *Phys. Rev. Lett.*, vol. 119, p. 190501, 2017.

Coherence distribution and depletion in training quantum classifier

Min Namkung[1] * Younghun Kwon[1] †

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

Abstract. What is a quantum resource in quantum machine learning? This question is not clearly understood yet. In this study, we attack the question. For the purpose of the study, we consider a quantum classifier as a tool of quantum machine learning. First of all, we show that in training quantum classifier the coherence plays a major role in training quantum classifier. We display that parametric quantum circuit of trained quantum classifier increases coherence of index register state but decreases accessible coherence of index register. Further, we show that Grover algorithm of trained quantum classifier diminishes coherence of index register state and the success probability of quantum classifier is related with the depletion of coherence of index register state. Therefore, they imply that coherence distribution and depletion are the important quantum resources in training quantum classifier. Because quantum classifier can be exploited to solve supervised learning, coherence can be considered ultimately as a quantum resource in supervised learning.

Keywords: quantum supremacy, coherence, accessible coherence, coherence distribution, coherence depletion, quantum machine learning, quantum perceptron

Introduction

It is well known that quantum computers can solve certain problems more efficient than classical counterparts[1, 2]. This phenomena are so called quantum supremacy[3]. Many researchers have investigated quantum resources that contributes to supremacy. Entanglement was considered as one of the quantum resource[4, 5]. However, it was shown that every quantum algorithm does not uses entanglement. Deterministic quantum computation with one-qubit(DQC1)[6] is the well-known example that has quantum speed-up without entanglement. A. Datta *et al.*[7] proposed that non-zero quantum discord[8] can be related with speed-up of DQC1. Because entanglement is affected by quantum discord[9, 10], discord was considered as a valuable resource rather than entanglement. However, quantum discord does contributes to speed-up for every quantum algorithms, involving Grover algorithm[11].

Recently, *quantum coherence* has been widely focused by researchers as a unified quantum resource[13, 14]. Coherence was firstly proposed by T. Baumgratz *et al.*[12] to define superposition[15] in a strict manner. They proposed mathematical conditions that coherence measures should obey. They also showed that l_1-norm coherence and relative entropy of coherence can satisfy these conditions. Until now, many researchers have proposed various coherence measures[16, 17, 18, 19, 20, 21] considering conditions from Ref.[12]. Coherence can be defined in multipartite systems as well as single systems[22]. Especially, bipartite coherence can unify entanglement, quantum discord and nonlocality[23, 24, 25, 26, 27, 28]. Further, coherence can contribute to speed-up in DQC1,[29], Deutsch-Josza algorithm[30], Grover algorithm and Shor algorithm[31].

Among quantum algorithms, Grover algorithm can be applied to construct various quantum machine learning tasks[32]. And Coherence have potential to be related with supremacy for quantum AI. In this study, we propose that coherence is an important quantum resource for quantum machine learning. We use quantum classifier proposed by Y. Du *et al.*[33] as a tool of quantum machine learning. We note that the quantum classifier includes Grover algorithm in order to perform perceptron[34]. In the view of *coherence distribution*[35] and *coherence depletion*[11], we argue that coherence can contribute to training quantum classifier(see Fig.1). In the view of coherence distribution, we display that parametric quantum circuit of trained quantum classifier increases coherence of index register states but decreases accessible co-

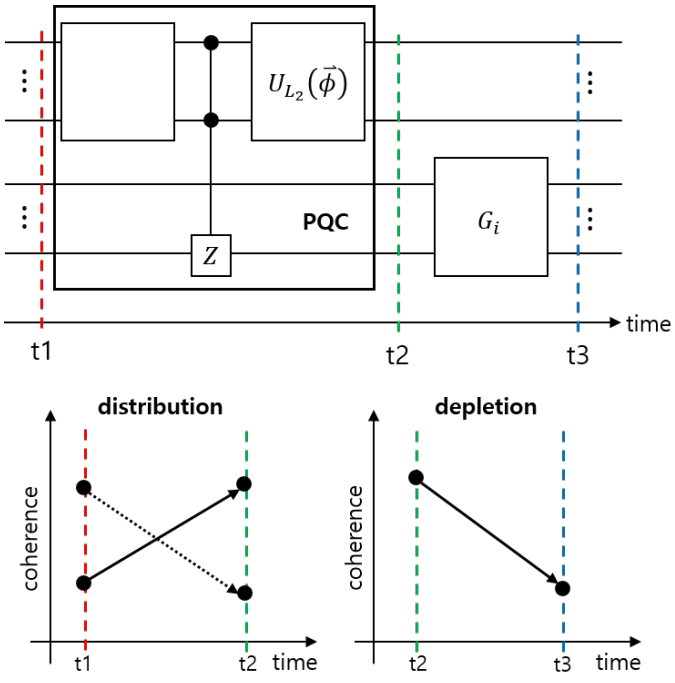


Figure 1: Coherence distribution and depletion in quantum classifier. Here, PQC is parametric quantum circuit and G_i is Grover algorithm.

*mslab.nk@gmail.com
†yyhkwon@hanyang.ac.kr

herence of index register. In the view of coherence depletion, we show that Grover algorithm of quantum classifier diminishes coherence of index register state. It implies that coherence distribution and depletion are the important quantum resources in training quantum classifier. Because quantum classifier can be exploited to solve supervised learning, this result tells ultimately that coherence can contribute to constructing quantum computers solving supervised learning.

Coherence distribution in bipartite system

The total coherence $C(\rho_{AB})$ of bipartite system AB is expressed as[35].

$$C(\rho_{AB}) = C(\rho_A) + C_A^{acc} + C(\rho_B) + C_B^{acc} + C_{AB}^{rem} \quad (1)$$

Here, $C(\rho_X)$ is a coherence of system $X \in \{A, B\}$ state. and C_X^{acc} is accessible coherence of system X. The local coherence of system X is expressed as $C(\rho_X) + C_X^{acc}$ and C_{AB}^{rem} is not localized coherence which is called a remaining coherence. If coherence measure $C(\cdot)$ is l_1-norm coherence or relative entropy of coherence, C_{AB}^{rem} is nonnegative[35]. Therefore,when l_1-norm coherence or relative entropy of coherence is used as coherence measure, we can use the structure of Eq.(1).

Structure of quantum classifier

In this work, we study the quantum resouce for quantum machine learning. Because there are many methods for quantum machine learning, we use quantum classifier, which is discussed in the work of Y. Du *et al.*[33], as a tool of quantum machine learning. And we show that coherence is used for training quantum classifier. The quantum classifier of Ref.[33] consists of feature register(F) and index register(I). The purpose of quantum classifier is to find a data vector $\vec{x}_i$ which is mislabeled in dataset $\{\vec{x}_i, y_i\}_{i=1}^N (\vec{x}_i \in \mathbb{R}^M,\ y_i \in \{-1, +1\})$, with a maximum probability.

Coherence in quantum classifier

In this study, we show that coherence provides a major role in training quantum classifier. Specially, the role of coherence in quantum classifier is investigated in terms of coherence distribution and coherence depletion.

Coherence depletion: According to previous work by H.-L. Shi *et al.*[11], coherence depletion can contribute to speed-up in Grover algorithm. Therefore, we show that coherence depletion contributes to training quantum classifier. In order to show this, we compare success probability with coherence depletion in index register state. Here, we use l_1-norm coherence[12] as a coherence measure. Coherence depletion can be related with success probability of quantum classifier. It implies that coherence depletion is a quantum resource of speed-up in quantum classifier.

Coherence distribution: As we argued before, Grover algorithm of trained quantum classifier diminishes coherence of index register state. Therefore, parametric quantum circuit of quantum classifier increase coherence of index register state. Exploiting the structure of Eq.(1), we obtain the following results related with coherence distribution.

- parametric quantum circuit in trained quantum classifier increases coherence of index register state.
- parametric quantum circuit in trained quantum classifier decreases accessible coherence of index register.

Conclusion

We show that coherence is an important resource for training quantum classifier. We investigate this argument in the view of coherence distribution and coherence depletion. In the view of coherence distribution, parametric quantum circult of trained quantum classifier increases coherence of index register state but decreases accessible coherence of index register. In the view of coherence depletion, Grover algorithm of trained quantum classifier diminishes coherence of index register. These facts imply that coherence distribution and depletion are resources for quantum classifier. Therefore, we can see that quantum classifier can be exploited to solve supervised learning and coherence has a potential to be a quantum resource to attack supervised learning.

Acknowledgement

We thank Hyunseong Jang for his insightful discussion and Yuxuan Du for checking our simulation. This work is supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (NRF2015R1D1A1A01060795 & NRF2018R1D1A1B07049420).

References

[1] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Comp.*, **26**, 1484, 1997.

[2] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th ACM STOC*, pages 212–219, 1996.

[3] A. W. Harrow and A. Montanaro. Quantum computational supremacy. Nature **549**, 203, 2017.

[4] C. H. Bennett and S. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. **69**, 2881, 1992.

[5] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature **302**, 390, 1999.

[6] E. Knill and R. Laflamme. On the Power of One Bit of Quantum Information. Phys. Rev. Lett. **81**, 5672, 1998.

[7] A. Datta, A. Shaji, and C. M. Cave. Quantum discord and the power of one qubit. Phys. Rev. A **100**, 050502, 2008.

[8] H. Ollivier and W. H. Zurek. Quantum Discord: A Measure of the Quantumness of Correlations. Phys. Rev. Lett. **88**, 017901, 2001.

[9] M. Koashi and A. Winter. Monogamy of quantum entanglement and other correlations. Phys. Rev. A **69**, 022309, 2004.

[10] A. Streltsov. Quantum Correlations Beyond Entanglement and Their Role in Quantum Information Theory. Springer, 2015.

[11] H.-L. Shi. Coherence depletion in the Grover quantum search algorithm. Phys. Rev. A **95**, 032307, 2017.

[12] T. Baumgratz, M. Cramer, and M. B. Plenio. Quantifying Coherence. Phys. Rev. Lett. **113**, 140401, 2014.

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

[14] H. Zhou, X. Yuan, and X. Ma. Unification of quantum resources in distributed scenarios. Phys. Rev. A **99**, 022326, 2019.

[15] V. Scarani. *Quantum Physics - A First Encounter: Interference, Entanglement, and Reality.* Oxford University Press, 2006.

[16] D. Girolami. Observable Measure of Quantum Coherence in Finite Dimensional Systems. Phys. Rev. Lett. **113**, 17040, 2014.

[17] M. Piani, M. Cianciaruso, T. R. Bromley, C. Napoli, N. Johnston, and G. Adesso. Robustness of asymmetry and coherence of quantum states. Phys. Rev. A **93**, 042107, 2016.

[18] S. Luo and Y. sun. Partial coherence with application to the monotonicity problem of coherence involving skew information. Phys. Rev. A **96**, 022136, 2017.

[19] C.-L. Liu, D.-J. Zhang, X.-D. Yu, Q.-M. Ding, and L. Liu. A new coherence measure based on fidelity. Quant. Inf. Process. **16**, 198, 2017.

[20] A. Streltsov, G. Adesso, and M. B. Plenio. Colloquium: Quantum coherence as a resource. Rev. Mod. Phys. **89**, 041003, 2017.

[21] C. Xiong, A. Kumar, M. Huang, S. Das, U. Sen, and J. Wu. Partial coherence and quantum correlation with fidelity and affinity distances. Phys. Rev. A **99**, 032305, 2019.

[22] Z. Xi. Coherence distribution in multipartite systems. J. Phys. A: Math. Theor. **51**, 414016, 2018.

[23] C.-S. Yu and H.-S. Song. Bipartite concurrence and localized coherence. Phys. Rev. A **80**, 022324, 2009.

[24] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso. Measuring Quantum Coherence with Entanglement. Phys. Rev. Lett. **115**, 020403, 2015.

[25] E. Chitamber and M.-H. Hsieh. Relating the Resource Theories of Entanglement and Quantum Coherence. Phys. Rev. Lett. **117**, 020402, 2016.

[26] Y. Sun, Y. Mao, and S. Luo. From quantum coherence to quantum correlations. EPL **118**, 60007, 2017.

[27] M.-L. Hu and H. Fan. Relative quantum coherence, incompatibility, and quantum correlations of states. Phys. Rev. A **95**, 052106, 2017.

[28] M.-L. Hu, X. Hu, J. Wang, Y. Peng, and H. Fan. Quantum coherence and geometric quantum discord. Phys. Rep. **762**, 1, 2018.

[29] J. Ma, B. Yadin, D. Girolami, V. Vedral, and M. Gu. Converting Coherence to Quantum Correlations. Phys. Rev. Lett. **116**, 160407, 2016.

[30] M. Hillery. Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation. Phys. Rev. A **93**, 012111, 2016.

[31] Y.-C. Liu, J. Shang, and X. Zhang. Coherence Depletion in Quantum Algorithms. Entropy **21**, 260, 2019.

[32] P. Wittek. *Quantum Machine Learning: What Quantum Computing Means to Data Mining.* Elsevier, 2016.

[33] Y. Du, M.-H. Hsieh, T. Liu, and D. Tao. Implementable Quantum Classifier for Nonlinear Data. arXiv:1809.06056.

[34] P. Rosenblatt. The perceptron: A probabilistic model for information storage and organization in the brain. Psychological Review **65**, 386, 1958.

[35] T. Ma, M.-J. Zhao, H.-J. Zhang, S.-M. Fei, and G.-L. Long. Accessible Coherence and Coherence Distribution. Phys. Rev. A **95**, 042328, 2017.

[36] A. Berlinet and C. Thomas-Agnan. *Reproducing kerner Hilbert spaces in probability and statistics.* Springer Science & Business Media, 2011.

[37] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii. Quantum Circuit Learning. Phys. Rev. A **98**, 032309, 2018.

Optimal Discrimination of Four Qubit States when Postmeasurement information on subsystem is available

Jaehee Shin[1] * Donghoon Ha[1] † Younghun Kwon[1] ‡

[1] *Department of Applied Physics, Hanyang University (ERICA), Ansan, Republic of Korea*

Abstract. In quantum state discrimination of some cases, postmeasurement information may lead a perfect discrimination of nonorthogonal quantum states. However, in general case of nonorthogonal qubit states, even with the help of postmeasurement information, perfect discrimination is impossible. Therefore, it is interesting to investigate the structure for discrimination of nonorthogonal qubit states when postmeasurement information exists. Along the line, we consider an optimal discrimination of qubit state ensemble with the help of postmeasurement information, in which the ensemble consists of two subensembles containing two qubit states. We show thar the problem of optimal discrimination with postmeasurement information can be understood as that of a minimum error discrimination to provide the geometric optimality conditions. In addition, using our appoach we provide the way to find optimal measurement of the problem.

Keywords: postmeasurement information, subensemble, minimum error discrimination, qubit states

In quantum physics, nonorthogonal quantum states cannot be discriminated perfectly. The indistinguishability is directly related to the security of quantum key distribution protocols [1]. In the optimal eavesdropping strategy, quantum state discrimination [2–4] is a significant task, which has various strategies including minimum-error discrimination(ME) [5–11], unambiguous discrimination(UD) [12–16], maximum-confidence discrimination(MC) [17].

ME is a discrimination scheme to minimize errors on average, where measurements provide only conclusive results. UD and MC are strategies that allow inconclusive results. In UD, measurements discriminate states without any error. And, in MC, measurements provide conclusive results with maximum confidence. UD requires linear independence of quantum states, but MC does not. MC is equal to UD when the confidences of conclusive results are equal to unity. In addition to ME, there is a discrimination scheme(FRIR) to minimizes the average error probability, in which case the rate of inconclusive results is fixed [18–25]. FRIR corresponds to ME when the fixed rate of inconclusive results is zero.

When quantum state ensemble consists of subensembles, one may discriminate nonorthogonal states perfectly with the help of postmeasurement information [26]. To be precisely, nonorthogonal quantum states may be perfectly discriminated by postprocessing measurement results and postmeasurement information about the prepared subensemble. This perfect discrimination scheme cannot be applied to every ensemble having nonorthogonal quantum states as UD. Specifically, nonorthogonal qubit states cannot be perfectly discriminated even with postmeasurement information [26]. Therefore, to minimize the average error probability with the help of postmeasurement information (MEPI) is as important as ME. Note that, as FRIR has a modified FRIR problem with ME, MEPI also has a modified problem [27].

*mslab.shin@gmail.com
†mslab.h@gmail.com
‡yyhkwon@hanyang.ac.kr

In this paper, we consider MEPI of ensemble composed of four qubit states. The ensemble consists of two subensembles containing two quantum states. We consider a modified problem of MEPI to employ the geometric approach developed in [8–11] and provide geometric optimality conditions.

Theorem 1 shows a concrete relation between the maximum success probability $P_{\text{succ}}^{\max}$ and optimal measurements $\{M_{ab}\}_{ab}$ for MEPI.

Theorem 1 *Suppose $\mathcal{E}$ is a qubit state ensemble,*

$$\mathcal{E} = \{q_x, \mathcal{E}_x\}_{x\in\{0,1\}} = \{q_{xa}, \rho_{xa}\}_{x,a\in\{0,1\}}. \qquad (1)$$

$\mathcal{E}$ means that subensemble $\mathcal{E}_x$ is prepared with probability q_x. There exists $\mathcal{I} \subseteq \mathcal{A} = \{00, 01, 10, 11\}$ satisfying

1. *$\{q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b}\}_{ab\in\mathcal{I}}$ forms a $(|\mathcal{I}|-1)$-simplex,*
2. *$H_{\mathcal{I}}^{\triangle}$ is a set with exactly one element $\boldsymbol{k}$,*
3. *$P_{\text{succ}}^{\max} = q_{0a} + q_{1b} + \|\boldsymbol{k} - q_{0a}\boldsymbol{v}_{0a} - q_{1b}\boldsymbol{v}_{1b}\|_2 \ \forall ab \in \mathcal{I}$,*

where $\boldsymbol{v}_{xa}$ is the Bloch vector of ρ_{xa},

$$H_{\mathcal{I}}^{\triangle} = \{\boldsymbol{t} \in \triangle_{\mathcal{I}} \mid \text{for all } ab, a'b' \in \mathcal{I} \text{ with } ab \neq a'b',$$

$$\|q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b} - \boldsymbol{t}\|_2 - \|q_{0a'}\boldsymbol{v}_{0a'} + q_{1b'}\boldsymbol{v}_{1b'} - \boldsymbol{t}\|_2$$

$$= q_{0a'} + q_{1b'} - q_{0a} - q_{1b} \ \} \quad \text{for} \quad \mathcal{I} \subseteq \mathcal{A},$$

and

$$\triangle_{\mathcal{I}} = \{ \textstyle\sum_{ab\in\mathcal{I}} \theta_{ab}(q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{0b}) \mid$$

$$\theta_{ab} > 0 \ \forall ab \in \mathcal{I} \ \text{ and } \ \textstyle\sum_{ab\in\mathcal{I}} \theta_{ab} = 1 \ \}.$$

Then, every POVM $\{M_{ab}\}_{ab}$ satisfying the following constraints is a MEPI measurement for $\mathcal{E}$.

$$M_{ab} \ \propto \ I + \left(\tfrac{q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b} - \boldsymbol{k}}{\|q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b} - \boldsymbol{k}\|_2}\right) \cdot \boldsymbol{\lambda} \quad \forall ab \in \mathcal{I},$$

$$M_{ab} \ = \ 0 \qquad\qquad\qquad\qquad \forall ab \notin \mathcal{I}.$$

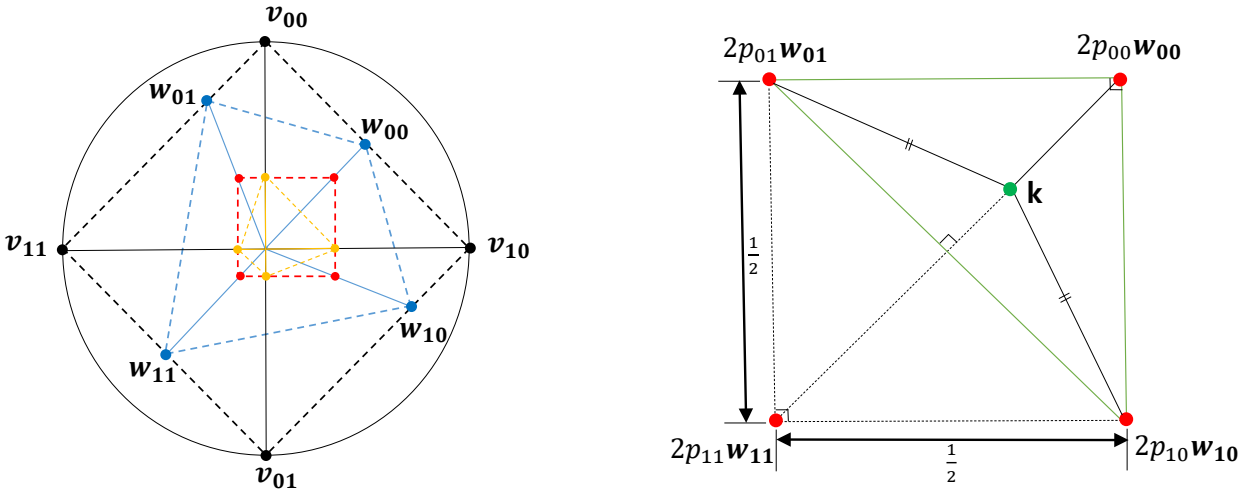


Figure 1: Overview of example with $q_0 = q_1$, $q_{0|x} \neq q_{1|x} (x = 0, 1)$. (Left) $\{\boldsymbol{v}_{xa}\}_{x,a}$(black points) forms a square and $\{q_{xa}\boldsymbol{v}_{xa}\}_{x,a}$(yellow points) a parallelogram. Meanwhile, $\{2p_{ab}\boldsymbol{w}_{ab}\}_{ab}$(red points) forms a square again contrary to the poor symmetry of $\{\boldsymbol{w}_{ab}\}_{ab}$(blue points). (Right) $\boldsymbol{k}$(grean point), determining an optimal measurement for MEPI, is situated in a relative interior of right-triangle $\{2p_{ab}\boldsymbol{w}_{ab}\}_{ab\in\mathcal{I}} (\mathcal{I} = \{00, 01, 10\})$.

Theorem 2 shows necessary and sufficient condition for the existence of MEPI measurement with zero operators.

Theorem 2 *When $\boldsymbol{k}$ is included in $H_{\mathcal{A}}^{\triangle}$, we have*

$$P_{\text{succ}}^{\max} = q_{0a} + q_{1b} + \|\boldsymbol{k} - q_{0a}\boldsymbol{v}_{0a} - q_{1b}\boldsymbol{v}_{1b}\|_2 \ \forall ab \in \mathcal{A}.$$

Then, every POVM $\{M_{ab}\}_{ab\in\mathcal{A}}$ satisfying the following constraints is a MEPI measurement for $\mathcal{E}$.

$$M_{ab} \propto I + \left(\frac{q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b} - \boldsymbol{k}}{\|q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b} - \boldsymbol{k}\|_2}\right) \cdot \boldsymbol{\lambda} \quad \forall ab \in \mathcal{A}. \quad (2)$$

If $\{q_{0a}\boldsymbol{v}_{0a} + q_{1b}\boldsymbol{v}_{1b}\}_{ab\in\mathcal{A}}$ forms a tetrahedron(3-simplex), $\boldsymbol{k}$ is the only element in $H_{\mathcal{A}}^{\triangle}$ and MEPI measurement consists of four nonzero operators satisfying (2). That is, there is no MEPI measurement with zero operators. However, if $H_{\mathcal{A}}^{\triangle}$ is empty or $\{q_{0a}\boldsymbol{v}_{0a}+q_{1b}\boldsymbol{v}_{1b}\}_{ab\in\mathcal{A}}$ fails to form a 3-simplex, there exists MEPI measurement containing zero operators.

Theorem 3 shows necessary and sufficient condition for ensemble $\mathcal{E}$ to yield MEPI measurement containing four nonzero elements.

Theorem 3 *When $P_{\text{succ}}^{\max}$ is larger than $\max_{ab\in\mathcal{A}}(q_{0a} + q_{1b})$, there exists a MEPI measurement with four nonzero operators if and only if $H_{\mathcal{A}}^{\triangle}$ is nonempty.*

$P_{\text{succ}}^{\max} = q_{0a}+q_{1b}$ means that a MEPI is to guess the given state is ρ_{0a} or ρ_{0b} according to the subensemble $\mathcal{E}_0$ or $\mathcal{E}_1$.

We consider an example satisfying $q_0 = q_1$ and $q_{0|x} \neq q_{1|x} (x = 0, 1)$

$$q_{00} = \tfrac{1}{4}(1+p), \quad \rho_{00} = |0\rangle\langle 0| \quad = \tfrac{1}{2}(I + \hat{\boldsymbol{z}} \cdot \boldsymbol{\lambda}),$$

$$q_{01} = \tfrac{1}{4}(1-p), \quad \rho_{01} = |1\rangle\langle 1| \quad = \tfrac{1}{2}(I - \hat{\boldsymbol{z}} \cdot \boldsymbol{\lambda}),$$

$$q_{10} = \tfrac{1}{4}(1+p), \quad \rho_{10} = |+\rangle\langle +| \quad = \tfrac{1}{2}(I + \hat{\boldsymbol{x}} \cdot \boldsymbol{\lambda}),$$

$$q_{11} = \tfrac{1}{4}(1-p), \quad \rho_{11} = |-\rangle\langle -| \quad = \tfrac{1}{2}(I - \hat{\boldsymbol{x}} \cdot \boldsymbol{\lambda}).$$

The maximal success probability $P_{\text{succ}}^{\max}$ is as follows.

$$P_{\text{succ}}^{\max} = \frac{1+p}{2} + \frac{1-p^2}{2\sqrt{2}+4p}. \quad (3)$$

Next, we consider another example satisfying $q_0 \neq q_1$ and $q_{0|x} = q_{1|x} (x = 0, 1)$

$$q_{00} = \tfrac{1+p}{4}, \quad \rho_{00} = |0\rangle\langle 0| \quad = \tfrac{1}{2}(I + \hat{\boldsymbol{z}} \cdot \boldsymbol{\lambda}),$$

$$q_{01} = \tfrac{1+p}{4}, \quad \rho_{01} = |1\rangle\langle 1| \quad = \tfrac{1}{2}(I - \hat{\boldsymbol{z}} \cdot \boldsymbol{\lambda}),$$

$$q_{10} = \tfrac{1-p}{4}, \quad \rho_{10} = |+\rangle\langle +| \quad = \tfrac{1}{2}(I + \hat{\boldsymbol{x}} \cdot \boldsymbol{\lambda}),$$

$$q_{11} = \tfrac{1-p}{4}, \quad \rho_{11} = |-\rangle\langle -| \quad = \tfrac{1}{2}(I - \hat{\boldsymbol{x}} \cdot \boldsymbol{\lambda}).$$

The maximal success probability $P_{\text{succ}}^{\max}$ is as follows.

$$P_{\text{succ}}^{\max} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+p^2}{2}}. \quad (4)$$

References

[1] J. Bae and L.-C. Kwek, J. Phys. A: Math. Theor. **48** 083001 (2015).

[2] A. Chefles, Contemp. Phys. **41** 401 (2000).

[3] S. M. Barnett and S. Croke, Adv. Opt. Photon. **1** 238 (2009).

[4] J. A. Bergou, J. Mod. Opt. **57** 160 (2010).

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

[6] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Thoery* (North-Holland, 1979).

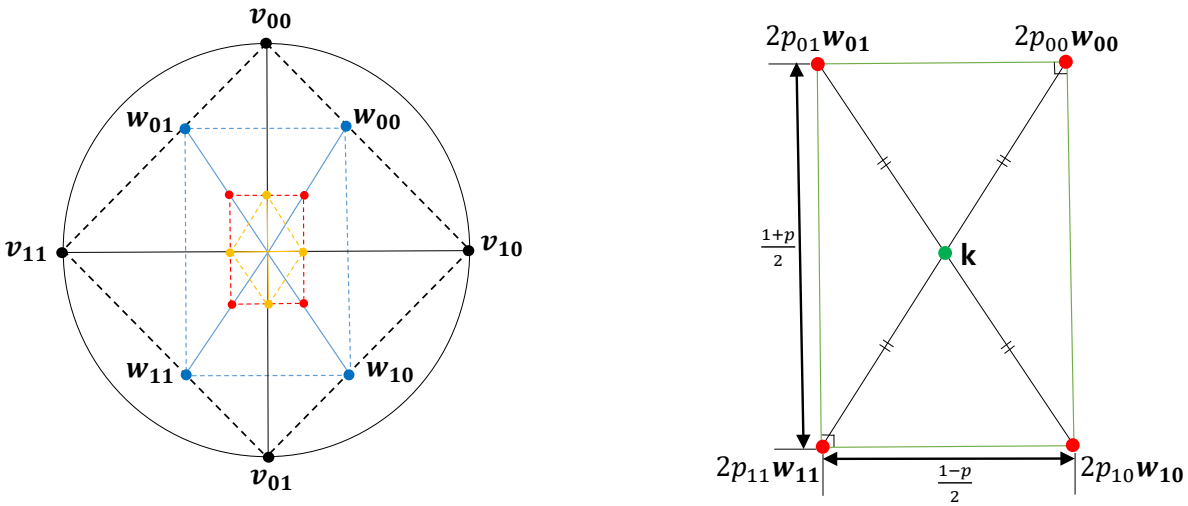


Figure 2: Overview of example with $q_0 \neq q_1$, $q_{0|x} = q_{1|x} (x = 0, 1)$. (Left) $\{\boldsymbol{v}_{xa}\}_{x,a}$(black points) forms a square and $\{q_{xa}\boldsymbol{v}_{xa}\}_{x,a}$(yellow points) forms a rhombus. However, $\{\boldsymbol{w}_{ab}\}_{ab}$(blue points) and $\{p_{ab}\boldsymbol{w}_{ab}\}_{ab}$(red points) both form a similar rectangle. (Right) $\boldsymbol{k}$(grean point), determining an optimal measurement for MEPI, is situated in a relative interior $\triangle_{\mathcal{A}}$ of rectangle $\{2p_{ab}\boldsymbol{w}_{ab}\}_{ab}$.

[7] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **21** 125 (1975).

[8] J. Bae and W.-Y. Hwang, Phys. Rev. A **87**, 012334 (2013).

[9] J. Bae, New J. Phys. **15**, 073037 (2013).

[10] D. Ha and Y. Kwon, Phys. Rev. A **87**, 062302 (2013).

[11] D. Ha and Y. Kwon, Phys. Rev. A **90**, 022330 (2014).

[12] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[13] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[14] A. Peres, Phys. Lett. A **128**, 19 (1988).

[15] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).

[16] D. Ha and Y. Kwon, Phys. Rev. A **91**, 062312 (2015).

[17] S. Croke, E. Andersson, S.M. Barnett, C. R. Gilson, J. Jeffers, Phys. Rev. Lett. **96**, 070401 (2006).

[18] C. W. Zhang, C. F. Li, and G. C. Guo, Phys. Lett. A **261**, 25 (1999).

[19] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).

[20] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).

[21] U. Herzog, Phys. Rev. A **86**, 032314 (2012).

[22] E. Bagan, R. Muñoz-Tapia, G. A. Olivares-Rentería, and J. A. Bergou, Phys. Rev. A **86**, 040303(R) (2012).

[23] K. Nakahira, T. S. Usuda, and K. Kato, Phys. Rev. A **91**, 022331 (2015).

[24] U. Herzog, Phys. Rev. A **91**, 042338 (2015).

[25] D. Ha and Y. Kwon, Quantum Inf. Process. **16**, 273 (2017).

[26] S. Akibue, G. Kato, and N. Marumo, Phys. Rev. A **99**, 020102(R) (2019).

[27] D. Gopal and S. Wehner, Phys. Rev. A **82**, 022326 (2010).

Quantum information transmission of a multiphoton qubit using optical hybrid entanglement

Seongjeon Choi[1] Seokhyung Lee[1] Hyunseok Jeong[1] *

[1] *Department of Physics and Astronomy, Seoul National University, Seoul 151-742, Korea*

Abstract. Multiphoton qubit is a promising optical qubit in linear optics, which has a nearly deterministic scheme for the Bell-state measurement. However, the multiphoton qubit is fragile under a lossy environment. In this research, we propose a scheme for quantum information transmission via quantum teleportation using the hybrid entanglement with loss-resilient qubits. We mainly consider a single-photon polarization qubit and a coherent-state qubit with a few photons as the loss-resilient qubits. We show our scheme improves the transmission in terms of quantum fidelity and success probability of Bell-state measurement. Also, we propose practically possible schemes to generate the required hybrid entangled states.

Keywords: quantum communication, hybrid entanglement, quantum teleportation

1 Introduction

Recently, a multi-photon polarization qubit(MPQ),

$$|\psi_{\rm m}\rangle = a\,|H\rangle^{\otimes N} + b\,|V\rangle^{\otimes N}$$

, encoded in N-photon optical polarization state is proposed by Lee, Park, Ralph, and Jeong[4] to overcome the limitation of Bell-state measurement in linear optics. In linear optics, the success probability of Bell measurement is usually limited by 1/2. Notably, MPQ encoding achieves an average success probability $1-2^{-N}$ for Bell measurement.

MPQ is generally in the form of the Greenberger-Horne-Zeilinger(GHZ)-type state, $a\,|H\rangle^{\otimes N} + b\,|V\rangle^{\otimes N}$. Unfortunately, it is well known that GHZ-type state is fragile under a lossy environment. To overcome the weakness, we examine teleportation for long-distance transmission and exploit hybrid entanglement between MPQ and other qubit encodings which serve as loss-resilient information carrier under the lossy environment. In this research, we utilize a coherent-state qubit(CSQ), $|\psi_{\rm c}\rangle$, and single-photon polarization qubit(SPQ), $|\psi_{\rm p}\rangle$, as the information carriers:

$$|\psi_{\rm c}\rangle = \mathcal{N}(|\alpha\rangle + |-\alpha\rangle)$$
$$|\psi_{\rm p}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

Our strategy is basically to send a loss-resilient qubit to the environment while reducing loss effect on a MPQ. We show that such hybrid approach shows higher fidelity and success probability.

While the hybrid approaches have many merits in quantum information processing [6, 1, 3], generating the hybrid entanglement is generally not trivial. Though, we also suggest a generation scheme for the hybrid entanglement between MPQ and CSQ and between MPQ and SPQ.

*jeongh@snu.ac.kr

2 Time-evolution under a lossy environment

We describe the lossy environment with the photon-loss model by the master equation under the Born-Markov approximation with a zero-temperature:

$$\frac{\partial\rho}{\partial\tau} = \sum_{i=1}^{N}\gamma_i\left(a_i\rho a_i^\dagger - \frac{1}{2}a_i^\dagger a_i\rho - \frac{1}{2}\rho a_i^\dagger a_i\right) \qquad (1)$$

where a_i(or, $a_i^\dagger$) represents the annihilation(or, creation) operator of mode i and γ_i is the decay constant of i mode. The evolution of a density operator is equivalently described by a beam-splitter model with setting the transmittance $t_i = e^{-\gamma_i\tau/2}$ and the reflectance $r_i = \sqrt{1-t_i^2}$ [5].

Suppose we directly transmit the information of an unknown qubit $|\psi_{\rm in}\rangle = a\left|H^N\right\rangle + b\left|V^N\right\rangle$ over lossy environment. Assuming that all transmissivities are equal to t, the evolution in the direct transmission is described by solving Eq.[1] with an initial condition $\rho(0) = |\psi_{\rm in}\rangle\langle\psi_{\rm in}|$:

$$\rho(t) = t^{2N}\,|\psi\rangle\langle\psi| + (1-t^{2N})\rho_{loss} \qquad (2)$$

where ρ_{loss} represent a event when more than one photon is lost. ρ_{loss} is orthogonal to $|\psi\rangle$ and has no off-diagonal element. In this case, we obtain quantum fidelity $F(t) = \langle\psi|\rho(t)|\psi\rangle = t^{2N}$. This means the decoherence of MPQ is exponentially increasing with N. Therefore, although the failure probability of Bell-measurement in MPQ exponentially decreases with the photon number of one qubit, the decoherence effect for given t also increases expoentially.

Now, we investigate the time evolution of hybrid entangled states between MPQ and CSQ and between MPQ and SPQ under photon-loss environment. We denote m, c, and p for MPQ, CSQ, and SPQ. We use the following entangled states:

$$|\psi_{\rm mc}\rangle = \frac{1}{\sqrt{2}}\left(\left|H^N\right\rangle|\alpha\rangle + \left|V^N\right\rangle|-\alpha\rangle\right)$$
$$|\psi_{\rm mp}\rangle = \frac{1}{\sqrt{2}}\left(\left|H^N\right\rangle|H\rangle + \left|V^N\right\rangle|V\rangle\right). \qquad (3)$$

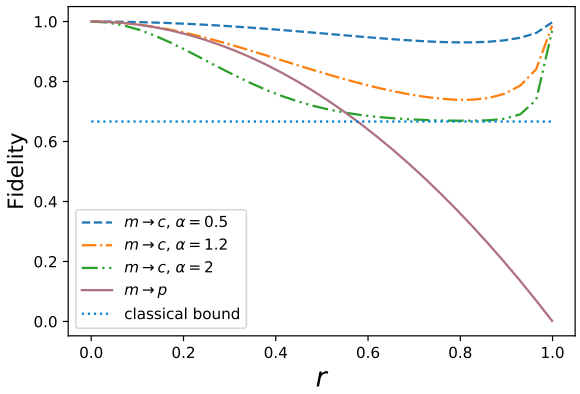


Figure 1: Averaged quantum fidelity between the output states and the corresponding target states against the reflectance $r = r_2$. CSQ is chosen with $\alpha = 0.5, 1.2$ and 2. We average the fidelity over all possible input states. The classical bound 2/3 for SPQ is obtained by teleportation without entanglement.

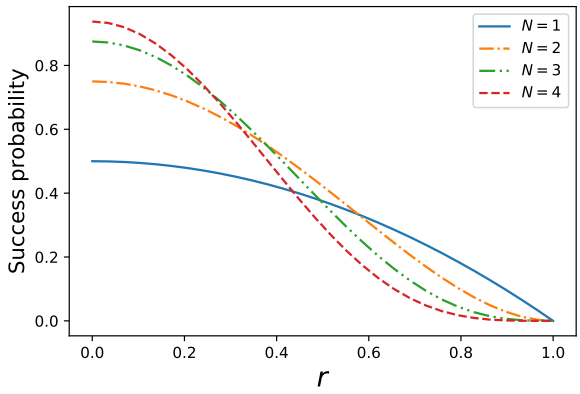


Figure 2: Success probabilities of teleportation against the reflectance $r = r_1$ with different photon number N =1, 2, 3, and 4

Without loss of generality, we assume $\alpha > 0$.

Loss occurs when we distribute the entangled states. Since we want to preserve the MPQ as intact as we can, we assume an asymmetric environment that the transmittance of each mode of MPQ part is t_1 and that of CSQ or SPQ part is t_2. By solving Eq.(1) with the initial state $|\psi_{\rm mc}\rangle$ and $|\psi_{\rm mp}\rangle$, we get entangled states $\rho_{\rm mc}(t_1, t_2)$ and $\rho_{\rm mp}(t_1, t_2)$ as following:

$$\begin{aligned}&\rho_{\rm mc}(t_1,t_2)\\&= \frac{t_1^{2N}}{2}\Big[\big|H^N, t_2\alpha\big\rangle\big\langle H^N, t_2\alpha\big| + \big|V^N, -t_2\alpha\big\rangle\big\langle V^N, -t_2\alpha\big|\\&+ e^{-2|\alpha|^2(1-t_2^2)}\big(\big|H^N, t_2\alpha\big\rangle\big\langle V^N, -t_2\alpha\big| + \text{H.c}\big)\Big] + \rho_{\rm loss}^{\rm mc}\end{aligned} \tag{4}$$

$$\begin{aligned}&\rho_{\rm mp}(t_1,t_2)\\&= t_1^{2N}\left[t_2^2\,|\psi_{\rm mp}\rangle\langle\psi_{\rm mp}| + r_2^2\left(\big|H^N\big\rangle\big\langle H^N\big| + \big|V^N\big\rangle\big\langle V^N\big|\right)\right.\\&\left.\otimes\,|0\rangle\langle 0| + \rho_{\rm loss}^{\rm mp}\right.\end{aligned} \tag{5}$$

where $r_i = \sqrt{1-t_i^2}$ is reflectance for $i = 1, 2$. $\rho_{\rm loss}^{\rm mc,mp}$ terms are orthogonal to the Bell states in MPQ basis with N photons and have nothing to do with the results of the teleportation.

3 Transmission via quantum teleportation

Now, we explore quantum teleportation using the hybrid entangled states. We employ the multi-photon Bell-state measurement scheme proposed by S.-W. Lee, *et al.*[4]. Assuming that $\big|B_1^N\big\rangle \propto \big|H^N H^N\big\rangle + \big|V^N V^N\big\rangle$ is detected, we express the output qubit by

$$\rho_{\rm out} = \frac{\big\langle B_1^N\big|\left(|\psi_{in}\rangle\langle\psi_{in}|\otimes\rho_{\rm hybrid}\right)\big|B_1^N\big\rangle}{\mathrm{tr}\left[\big|B_1^N\big\rangle\big\langle B_1^N\big|\left(|\psi_{in}\rangle\langle\psi_{in}|\otimes\rho_{\rm mc}\right)\right]}$$

where $\rho_{\rm hybrid} = \rho_{\rm mc}$ or $\rho_{\rm mp}$. When the other Bell states are detected, we do proper unitary operations on the output qubit.

The failure occurs when (i) the photons in MPQ are lost so the MPQ part of the entangled state is orthogonal to the Bell states, or (ii) the multi-photon Bell-state measurement scheme fails with probability $1/2^N$. Therefore, the success probability of the Bell-state measurement depends on t_1 and N. If the Bell-state measurement is succeeded, the effect of loss on the MPQ side is filtered so that the output qubits only depend on t_2. After obtaining the output qubits, we can calculate quantum fidelity between the output qubit $\rho_{\rm out}$ and the target state $|\psi_{\rm c}\rangle$ or $|\psi_{\rm p}\rangle$ where, in the case of CSQ, we use a qubit basis $\{|\pm t\alpha\rangle\}$ in order to reflect decrease of the amplitude. To summarize the results, we draw a plot demonstrating the performance of our schemes (Fig. 1 and 2).

4 Schemes for the generation of the hybrid entangled states

We discuss schemes for the generation of the hybrid entangled states $|\psi_{\rm mc}\rangle$ and $|\psi_{\rm mp}\rangle$ in Eq. (3). First, we consider $|\psi_{\rm mc}\rangle$. Note that $|\psi_{\rm mp}\rangle = \frac{1}{\sqrt{2}}\big(\big|H^N\big\rangle|H\rangle + \big|V^N\big\rangle|V\rangle\big)$ is GHZ state of SPQ with $N+1$ photons. Therefore, it is enough to generate GHZ state in which we can at least access one single photon among $N+1$ photons to utilize for SPQ. Note that four-photon GHZ state with a high fidelity of 98% is reported[8].

To generate $|\psi_{\rm mc}\rangle = \frac{1}{\sqrt{2}}\big(\big|H^N\big\rangle|\alpha\rangle + \big|V^N\big\rangle|-\alpha\rangle\big)$, we can utilize a theoretical scheme for generating a hybrid entangled state between SPQ and CSQ, proposed by H. Kwon and H. Jeong [2]. In their scheme, they use linear optics, photo-detector, and a ancillary resource state $|\mathrm{SCS}_\phi(\alpha)\rangle = A_\phi\big(|\alpha\rangle + e^{i\phi}|-\alpha\rangle\big)$ to essentially devise a operation $\hat{O}(\phi) = |t\alpha\rangle\langle V| + e^{i\phi}|-t\alpha\rangle\langle H|$ with a success probability $P(t,\alpha) = A_\phi^2(1-t^2)\alpha^2 e^{-2(1-t^2)\alpha^2}$ where $0 \le t \le 1$ is transmittance. If we perform $\hat{O}(0)$ on GHZ state with $N+1$ photons and phase-gate: $|\pm\alpha\rangle \to |\mp\alpha\rangle$,

then we can obtain the desired hybrid entangled state $|\psi_{\rm mc}\rangle$ where the number of photon of MSQ is N. Within our knowledge, the recent record of amplitude of SCS is $\alpha = 1.6$ [7]. Therefore, we, in principle, can obtain a hybrid entangled state between MPQ with 3 photons and CSQ with $\alpha < 1.6$ from 4 photon GHZ state

5 Conclusion

Our schemes suggest to utilize quantum teleportation using hybrid entangled states in order to get higher quantum fidelity and success probability.

From Fig. 1, Eq. 4, and 5, the dependence of the fidelity on $t_1 = \sqrt{1-r_1^2}$ is $O(t_1^2)$, which is considerably improved compared to $O(t^{2N})$ of the direct transmission. Moreover, since there is no dependence on the photon number N, we confirm that N can be chosen only by maximizing the Bell-state measurement. Also, CSQ shows higher fidelity than SPQ if α is small enough.

In Fig. 2, we note that the larger number of photons N in MPQ actually make the success probability worse. Hence, to choose N properly is important to do maximize the Bell-state measurement. Again, N and t_1 does not affect the fidity of the output states.

We suggest the schemes for the generation of hybrid entangled states, and our schemes require GHZ-state with $N+1$ photons to transmit quantum information of $N-photon$ MPQ. The state of the art technology shows such entanglement with 3-photon MPQ is possible. Therefore, our schemes show the usefulness of hybrid entangled state in a realistic situation.

References

[1] H. Kwon and H. Jeong. Violation of the bell–clauser-horne-shimony-holt inequality using imperfect photodetectors with optical hybrid states. *Phys. Rev. A*, 88:052127, Nov 2013.

[2] H. Kwon and H. Jeong. Generation of hybrid entanglement between a single-photon polarization qubit and a coherent state. *Phys. Rev. A*, 91:012340, Jan 2015.

[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, Feb 2013.

[4] S.-W. Lee, K. Park, T. C. Ralph, and H. Jeong. Nearly deterministic bell measurement for multiphoton qubits and its application to quantum information processing. *Phys. Rev. Lett.*, 114:113603, Mar 2015.

[5] U. Leonhardt. Quantum statistics of a lossless beam splitter: Su(2) symmetry in phase space. *Phys. Rev. A*, 48:3265–3277, Oct 1993.

[6] Y. Lim, J. Joo, T. P. Spiller, and H. Jeong. Loss-resilient photonic entanglement swapping using optical hybrid states. *Phys. Rev. A*, 94:062337, Dec 2016.

[7] A. Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier. Generation of optical 'schrödinger cats' from photon number states. *Nature*, 448:784 EP –, Aug 2007.

[8] C. Zhang, Y.-F. Huang, C.-J. Zhang, J. Wang, B.-H. Liu, C.-F. Li, and G.-C. Guo. Generation and applications of an ultrahigh-fidelity four-photon greenberger-horne-zeilinger state. *Opt. Express*, 24(24):27059–27069, Nov 2016.

A classical-quantum hybrid oracle architecture for an oracle identification problem in the NISQ era

Wooyeong Song[1] Marcin Wieśniak[2,3] Nana Liu[4] Marcin Pawłowski[3]
Jinhyoung Lee[1] * Jaewan Kim[5] † Jeongho Bang[5] ‡

[1] *Department of Physics, Hanyang University, Seoul 04763, Korea*
[2] *Insitute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-308 Gdańsk, Poland*
[3] *International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-308 Gdańsk, Poland*
[4] *John Hopcroft Center for Computer Science, Shanghai Jiao Tong University, Shanghai 200240, China*
[5] *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea*

Abstract. Quantum algorithms usually runs and are enabled with embedding large classical information into quantum states engaging the quantum parallelism. To circumvent this requirement, we propose a new classical-quantum hybrid architecture where the classical input data are unchanged but relatively small (single-qubit only, in our case) quantum system is employed for speed-ups. This idea is applied to a Boolean oracle identification problem, that is to identify an unknown black-box operation, i.e., oracle, by minimizing the queries. We show that in our scheme the success rates of the query can be improved and it leads to reduction of the sample complexity in machine learning. The proposed architecture is, indeed, realizable with the noisy intermediate-scale quantum (NISQ) devices.

Keywords: Quantum computing, Quantum machine learning, Oracle identification

1 Introduction

Quantum computation would promise the computational speed-ups. However, such speed-ups appear difficult to achieve with the NISQ machine, which runs on only a few hundred noisy qubits [1]. One of the main reasons is that many useful algorithms demand very high costs in embedding 'big' classical data into quantum states, e.g., by implementing so-called quantum random-access memory (QRAM). Thus, here we touch on this issue by considering the following question: Is it possible to achieve a quantum computational advantage, avoiding the aforementioned QRAM costs?

One approach is to cast a classical-quantum hybrid strategy. Recently, studies exploring the useful interplay between "classical" and "quantum" have received increasing attention. Consistent with this trend, we also consider a classical-quantum hybrid architecture, in which (*i*) the large input data remains classical and (*ii*) achieving the quantum advantage is enabled by small-scale quantum system.

We apply our idea to a "Boolean oracle identification" problem, which aims to identify the correct oracle amongst a list of candidates. To solve this problem, we employ a classical-quantum hybrid oracle, designed based on (*i*) and (*ii*). Here, we assume that this hybrid oracle can also generate incorrect outputs with errors arising from noisy (internal) quantum devices. This is often casted in realistic models, referred to as noisy query model [2]. In this setting, we demonstrate, both analytically and numerically, that our hybrid oracle can exhibit higher success rates of query if the amount and variance in the errors are not at some gross level. It thus enhances our ability to explore a much larger candidate-solution space and enables us to deal with larger problems. The quantum advantage in Boolean oracle identification leads to a reduction in the sample complexity bound in the "probably-approximately-correct (PAC)" learning model [3].

*hyoung@hanyang.ac.kr
†jaewan@kias.re.kr
‡jbang@kias.re.kr

2 Problem and our approach

Boolean oracle identification is a fundamental computational problem and is defined as follows: Given a Boolean oracle $h^\star$ which maps an n-bit binary string $\mathbf{x} = x_1 x_2 \dots x_n$ ($x_j \in \{0,1\}\ \forall j = 1,\dots,n$) to a binary value $h^\star(\mathbf{x}) \in \{0,1\}$, the task is to identify $h^\star$, while minimizing the number of queries to the oracle.

In our classical-quantum hybrid scheme, we consider an oracle $O_{\mathbf{x}}$ that consists of n-bit classical "input/output (I/O)" channels and single-qubit system for process [See Fig. 1(a)]. Then, our oracle $O_{\mathbf{x}}$ implements the operation, such that $(\mathbf{x}, |\alpha\rangle) \xrightarrow{O_{\mathbf{x}}} (\mathbf{x}, |\psi_{\text{out}}(\mathbf{x})\rangle)$. Here, the query-output state $|\psi_{\text{out}}(\mathbf{x})\rangle$ is defined, without loss of generality, as

$$|\psi_{\text{out}}(\mathbf{x})\rangle = \sqrt{P(\mathbf{x})}\,|h^\star(\mathbf{x})\rangle + \sqrt{1-P(\mathbf{x})}\,|h^\star(\mathbf{x})\oplus 1\rangle \quad (1)$$

where $P(\mathbf{x})$ is the probability of getting the correct query output [2]. After the process of $O_{\mathbf{x}}$, a measurement is performed on $|\psi_{\text{out}}(\mathbf{x})\rangle$ to identify the oracle's answer.

This oracle is assumed to be realized by a circuit illustrated in Fig. 1(b). The circuit contains 2^n gates acting on the ancilla qubit: the single-qubit gate $\hat{a}_0$ and 2^n-1 of gates $\hat{a}_k$ ($k = 1,2,\dots,2^n-1$) conditioned on the classical bit values $x_1, x_2, \dots, x_n$ in $\mathbf{x}$. Here the gates $\hat{a}_k$ are

$$\hat{a}_k \in \{\hat{\sigma}_z, i\hat{\sigma}_y\}\,, \text{ for all } k = 0,1,\dots,2^n-1, \quad (2)$$

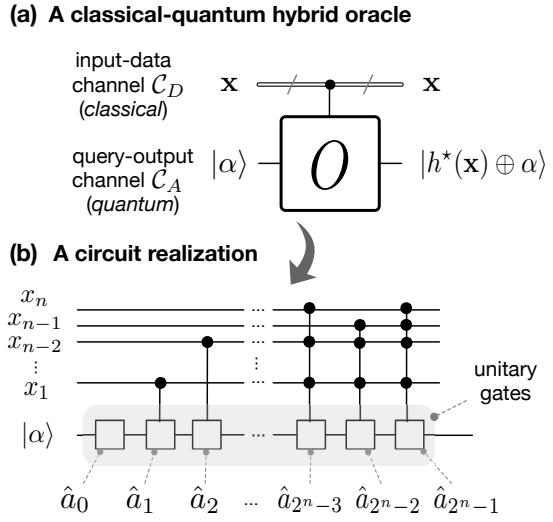


Figure 1: (a) A schematic picture of our hybrid oracle and (b) of the realization of our hybrid oracle (see the main text or Ref. [4]).

where $\hat{\sigma}_x$, $\hat{\sigma}_y$, and $\hat{\sigma}_z$ are the Pauli operators. This circuit realization of the oracle is inspired by the binary-classification formula

$$\begin{aligned} h^\star(\mathbf{x}) \quad &= \quad a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_1 x_2 \\ &\quad \oplus \cdots \oplus a_{2^n-1} x_1 x_2 \ldots x_n, \end{aligned} \tag{3}$$

where $a_k \in \{0, 1\}$ $(k = 0, 1, \ldots, 2^n - 1)$ are known as the Reed-Muller coefficients. Each a_k has a corresponding gate operation $\hat{a}_k$, where $a_k = 0$ means that $\hat{a}_k$ leaves the bit-signal unchanged (identity) and $a_k = 1$ means that $\hat{a}_k$ flips the bit-signal (logical-not). Thus, the oracle is characterized by a fixed set of $\hat{a}_k$ operators for a given $h^\star$. Note that since the oracle is treated as a *black-box*, the gates $\hat{a}_k$ are predetermined.

We then consider systematic error that can occur in the circuit, which arises from errors in the $\hat{a}_k$ gates and no errors are presented for the classical signal $\mathbf{x}$. In a fully-classical model, these errors are usually modeled in the following way: the bit-signal is flipped (i.e., $0 \rightleftharpoons 1$) with a certain probability $\eta_k \geq \frac{1}{2}$ before or after applying k-th gate $\hat{a}_k$. Then the corresponding quantum error can be described by $|\psi_k(\mathbf{x})\rangle \to |\psi'_k(\mathbf{x})\rangle = \hat{\epsilon}_k |\psi_k(\mathbf{x})\rangle$, where $|\psi_k(\mathbf{x})\rangle$ is the state passing through the gate $\hat{a}_k$. Here $\hat{\epsilon}_k$ is a bit-flip operation defined by $\hat{\epsilon}_k = \sqrt{1-\eta_k}\hat{\mathbf{1}} \pm i\sqrt{\eta_k}\hat{\sigma}_x$.

3 Analysis and results

We now analyze the query-success probability $P_{C,Q}$, defined in Eq. (1). Here, the subscripts "Q" and "C" refer to when the ancilla state in our oracle is respectively quantum or classical. First, let us define a set $\Omega_{\mathbf{x}} = \{0, l_1, l_2, \ldots, l_{\kappa-1}\}$ whose elements are taken to be the indices of the gates $\hat{a}_k$ which are 'activated' (i.e., when the corresponding classical control bit $x_k = 1$). The number of these activating gates is given by $\kappa = 2^{\omega(\mathbf{x})}$, where the factor $\omega(\mathbf{x})$ denotes the Hamming-weight of $\mathbf{x}$. Then, $P_{C,Q}$ can be written in terms of ω. When the ancilla state is classical, $P_C(\omega)$ can be estimated as

$$P_C(\omega) \simeq \sum_j^{\kappa/2} \binom{\kappa}{2j} (1-\overline{\eta})^{2j}\, \overline{\eta}^{\kappa-2j} \simeq \frac{1}{2}\left(1 + e^{-\frac{2\omega}{c}}\right), \tag{4}$$

where $\overline{\eta}$ is defined as the average error probability. The factor c—named "characteristic constant"—is given as

$$c = -\frac{1}{\ln(1-2\overline{\eta})} \simeq (2\overline{\eta})^{-1} \quad \left(\text{for } O(\overline{\eta}^2) \to 0\right). \tag{5}$$

However, when the ancilla state is quantum, the corresponding success probability $P_Q(\omega)$ is given by

$$P_Q(\omega) = \left|\langle h^\star(\mathbf{x})|\, \hat{\epsilon}_{l_{\kappa-1}} \hat{a}_{l_{\kappa-1}} \cdots \hat{\epsilon}_{l_1} \hat{a}_{l_1} \hat{\epsilon}_0 \hat{a}_0\, |\alpha\rangle\right|^2. \tag{6}$$

Then, by using the following condition

$$\{\hat{\sigma}_x, \hat{a}_k\}_+ = \hat{\sigma}_x \hat{a}_k + \hat{a}_k \hat{\sigma}_x = 0, \tag{7}$$

we can show that $P_Q(\omega)$ becomes unity in the limit of $\Delta_\eta \to 0$. Thus, so long as the gate errors are regular $\eta_k = \overline{\eta}$ $(\forall k \in \Omega_{\mathbf{x}})$ [2], we can always have $P_Q(\omega) = 1$. We can see that our gates $\hat{a}_k$ in Eq. (2) clearly satisfies the anti-commutation relation in Eq. (7). This anti-commutation relation enables the amplitudes associated with the errors to be 'canceled out' by destructive interference.

However, it is impractical to achieve such a perfect errorlessness, since in a realistic situation we will have $\Delta_\eta > 0$. Then, $P_Q(\omega)$ has a form analogous to that in Eq. (4). Here the characteristic constant c is replaced with an 'effective' characteristic constant $c_{\text{eff}} \simeq (2\overline{\eta}_{\text{eff}})^{-1}$ where again $O(\overline{\eta}^2) \to 0$. Here $\overline{\eta}_{\text{eff}}$ is defined in terms of an effective average error that $\hat{a}_k$'s experience. $\overline{\eta}_{\text{eff}}$ is much smaller than $\overline{\eta}$, because $\overline{\eta}_{\text{eff}}$ comes from remaining errors only after destructive interference. Interestingly, this feature does not depends on $\overline{\eta}$, but rather on the variance Δ_η. From this feature, i.e., $\overline{\eta}_{\text{eff}} \leq \overline{\eta}$ or equivalently $c_{\text{eff}} \geq c$, we can show a quantum advantage with our scheme. In particular, it is shown that, on average, our hybrid oracle is useful up to the length $n = 2\log_2 c_{\text{eff}}$ of input-bit strings, whereas $n = 2\log_2 c$ is the upper limit in the purely classical case. So if $c_{\text{eff}} \geq c$, our hybrid oracle can be useful for larger bit-string inputs. It also implies expansion of the search space which can be explored by the given noisy oracle, approximately from $O(e^{(2\overline{\eta})^{-2}\ln 2})$ to $O(e^{\gamma^2(2\overline{\eta})^{-2}\ln 2})$, where the factor $\gamma = \frac{c_{\text{eff}}}{c} \geq 1$ (for details, see our ArXiv paper [4]).

The quantum advantage described above can also be applied to quantum machine learning. It leads to a reduction of the sample complexity bound in the context of the computational learning theory [3]. To see this, consider a learning algorithm with access to our hybrid oracle. Then, we can find the bound of the learning sample complexity; namely, if the learning is completed with the samples satisfying

$$M \geq 2A_Q \ln\left(\frac{2\,|\mathfrak{H}|}{\delta}\right)^{\frac{1}{\epsilon^2}}, \tag{8}$$

we can define a legitimate learner—a so-called $(\epsilon,\ \delta)$ probably-approximately-correct (PAC) learner—which

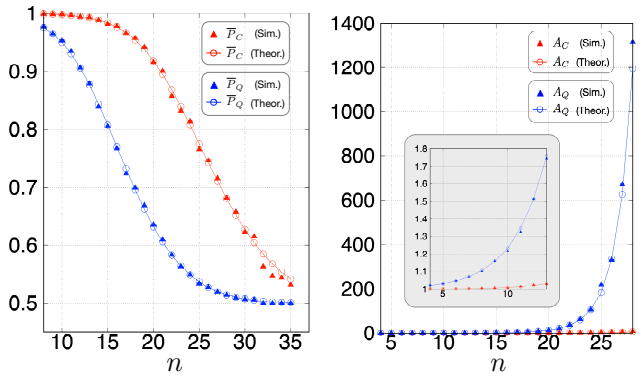


Figure 2: **Numerical plot of $\bar{P}_{C,Q}$ (left) and $A_{C,Q}$ (right) against n.** Here we use $\overline{\eta} = 10^{-3}$ with $\Delta_\eta = 0.05\overline{\eta}$. The theoretical values are also presented for comparison.

identifys $h^\star$ in the hypothesis space $\mathfrak{H}$. Here, ϵ and δ are defined as the inaccuracy and learning-failure probability, respectively. However, it is nontrivial to evaluate A_Q, particularly when the oracle is erroneous [5]. In our study, A_Q can be found as

$$A_Q = \left(2\overline{P}_Q(n) - 1\right)^{-2}, \tag{9}$$

where $\overline{P}_Q(n)$ is the average query-success probability, given by $\overline{P}_Q(n) = \frac{1}{2^n}\sum_{\omega=0}^{n}\binom{n}{\omega}P_Q(\omega)$. Noting that the classical counterpart to A_Q, say A_C, is characterized by c instead of c_{eff}, the reduction of the sample complexity, i.e., $A_Q \leq A_C$, is achieved. Here, what is remarkable is that the quantum learning advantage is achieved with classical input data directly without need of embedding the classical data into quantum states at all.

In addition to our theoretical analysis, we include accompanying numerical simulations, in which $P_{C,Q}(\omega)$ are evaluated by counting a large number ($\simeq 10^5$) of queries for each given number of $\omega(\mathbf{x})$ and they are averaged over the trials ($\simeq 10^3$). The results are given in Fig. 2. Indeed, the obtained simulation results confirm our theoretical analysis, allowing us to identify c_{eff} and γ for a given noise level; when $\overline{\eta} = 10^{-3}$ with $\Delta_\eta = 5\%$ of $\overline{\eta}$, our hybrid oracle would be applicable up to $n \simeq 27.23$ even in the presence of $\overline{\chi} = 10^{-2}$ of phase-flip, whereas $n \simeq 17.93$ would be the limit of the purely classical case. Equivalently, the hybrid oracle can cover up to size $\simeq e^{1.09\times10^8}$ of the candidate space, which is much larger than $\simeq e^{1.73\times10^5}$ allowed in the classical case (for detailed method and analysis, see our ArXiv paper [4]).

4 Summary

We have studied how a quantum advantage would be achieved by the NISQ devices. Our basic idea was to consider a classical-quantum hybrid scheme of computation. The key feature of our proposal was to remain the ('big') input data classical so that we do not need to use ('big') quantum data constructed, e.g., by the QRAM. Instead, we tried to achieve the quantum advantage by employing a relatively small (a single qubit, in our case) quantum system. We applied the presented idea to a Boolean oracle identification problem. On the basis of the theoretical and numerical analysis, it was shown that not only can this new hybrid framework reduce the query complexity of the problem, exploring much larger search space, but it is also effective in the presence of realistic noise. Furthermore, we can establish a link to the speed-up of the quantum machine learning.

References

[1] J. Preskill, Quantum **2**, 79 (2018).

[2] A. W. Cross, G. Smith, and J. A. Smolin, Phys. Rev. A **92**, 012327 (2015).

[3] L. G. Valiant, Communications of the ACM **27**, 1134 (1984).

[4] W. Song, M. Wiesniak, N. Liu, M. Pawlowski, J. Lee, J. Kim, and J. Bang, arXiv preprint arXiv:1905.05751v1 (2019).

[5] D. Angluin, and D. K. Slonim, Machine Learning **14**, 7 (1994).

Detection of multipartite Einstein-Podolsky-Rosen steering in Greenberger-Horne-Zeilinger-like states

Do Kien Tri[1 2 *] Yu Xiang[1 3 4 †] Qiongyi He[1 3 4]

[1] *State Key Laboratory for Mesoscopic Physics and Collaborative Innovation Center of Quantum Matter, School of Physics, Peking University, Beijing 100871, China*

[2] *Humboldt-Universität zu Berlin, Institut für Physik, Germany*

[3] *Beijing Academy of Quantum Information Sciences, Haidian District, Beijing 100193, China*

[4] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China*

Abstract. Einstein-Podolsky-Rosen (EPR) steering can be realized as a multiparty EPR paradox, and is an intermediate type of quantum correlation between entanglement and Bell nonlocality. A linear optical network built up from several off-line squeezed states and beamsplitters is a common platform to generate multipartite steerable states. Here, we propose criteria to detect the $N-$partite EPR steering for two typical structures of linear optical networks to prepare continuous-variable Greenberger-Horne-Zeilinger-like states. We examine the influence of inefficiency during the modes transmissions, and the robustness against thermal noise on the input states. We find that the properties of multipartite steering are independent on the structure of optical network as long as their inferred variances are optimized. The present multipartite steering correlation may have potential applications in certain quantum information tasks where the issue of trust is important, such as one-sided device-independent quantum secret sharing.

Keywords: multipartite EPR steering, CV GHZ-like state, linear optical network

Introduction- Einstein-Podolsky-Rosen (EPR) paradox [1] established a link between entanglement and nonlocality in quantum mechanics, by showing that there are correlated quantum states which demonstrate an inconsistency between the completeness of quantum mechanics and the concept of local realism. In the same year, Schrödinger introduced the term steering [2] to describe this apparent correlation where measurements made by one observer at a location A can immediately "steer" the state of another observer, at location B. Until 2007, works of Wiseman [3, 4] formalized the meaning of steering in terms of violations of local hidden state models, and revealed that EPR steering is a realization of EPR paradox, which can be viewed as a strong form of entanglement.

Despite that, EPR steering has a special usefulness to quantum information tasks, such as one-sided device independent cryptography [5, 6, 7, 8] and secure teleportation [9, 10, 11]. For these reasons, there has been an escalation in the amount of both theoretical and experimental interests.

Here, we investigate properties of multipartite steering in continuous-variable (CV) Greenberger-Horne-Zeilinger (GHZ)like states, which can be prepared by two typical structures of linear optical network, one is a structure where all squeezed states are arranged on one arm [12], and the other one is a structure where all squeezed modes are half-to-half distributed in two arms [13] (see Fig. 2). By introducing the amplitude $\hat{x}$ and phase $\hat{p}$ quadrature of the output modes, we measure their inferred variance of EPR steering [14], where one given mode can be steered by the remaining $N-1$ parties. We further show the robustness against imperfect transmission as well as thermal noise involved in the input states. We find that the properties of multipartite steering are independent on the structure of optical networks as long as their inferred variances are optimized.

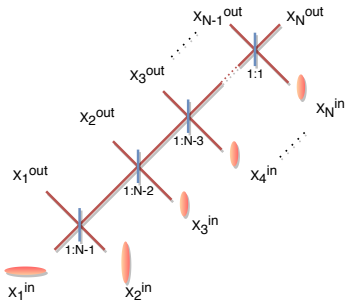


Figure 1: Experimental set up for the linear optical networks with one arm.

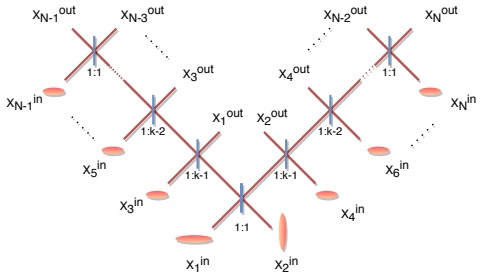


Figure 2: Experimental set up for the linear optical networks with two arms. Note that for the two arms case, when N is odd, replace the bottom beamsplitter with $N-1:N+1$ and the left arm starts with $1:k-2$ instead of $1:(k-1)$, where $k=(N+1)/2$.

Preliminary- The CV GHZ-like state of the optical field is prepared by coupling one phase-squeezed and one amplitude-squeezed states of light on an optical beamsplitter network, which consists of $N-1$ optical beam-

*dokien@hu-berlin.de

†xiangy.phy@pku.edu.cn

splitters. As shown in Fig. 2, the output states of two different structures are fully symmetric by adjusting the transmittance of beamsplitters, respectively. To characterize the output states, the amplitude and phase quadratures of each mode are defined as $\hat{x} = \hat{a} + \hat{a}^\dagger$ and $\hat{p} = (\hat{a} - \hat{a}^\dagger)/i$, where $\hat{a}$ and $\hat{a}^\dagger$ are bosonic annihilation and creation operators of a quantized optical field, respectively. (In the following we will drop the hat notation.) To introduce the imperfect transmission, we distribute every output mode in a lossy channel. The output mode at i is given by

$$a_{i,\eta} = \sqrt{\eta_i} a_i + \sqrt{1-\eta_i} a_i^{\rm vac}, \tag{1}$$

where η_i and $a_i^{\rm vac}$ represent the transmission efficiency of the quantum channel and the vacuum mode induced by loss into the quantum channel, respectively. Besides that, extra thermal noises barrier are considered, which acts on each input mode. The influence of thermal noises can be read as

$$\Delta^2 x_{i,n} = (2n+1)\Delta^2 x_i, \tag{2}$$

where n represent the initial thermal photon number of the noises barrier.

Method- The criterion for multipartite steering is based on an accuracy of the inferred variances of a linear combination of the quadrature components measured locally on each party. To verify whether one given mode can be steered by the remaining $N-1$ parties or not, we assume that only the subsystem being steered is constrained to be a quantum state, i.e., whose x_1 and p_1 satisfy the Heisenberg uncertainty relation, while all the remaining $N-1$ subsystems are not assumed to arise from a local quantum state so that there is no constraint for the variances of their local states [15]. By collaborating all outputs from their local measurements, the remaining $N-1$ parties try to infer the values of the steered mode's quadratures, which can be written as a linear combination of their measurement outcomes $\sum_{j=1}^{N-1} g_j x_j$ and $\sum_{j=1}^{N-1} h_j p_j$. The inferred variance of the steered mode are given by

$$\Delta^2_{\rm inf} x_{1|N-1} = \Delta^2 \left(x_1 - \sum_{j=1}^{N-1} g_j x_j \right),$$
$$\Delta^2_{\rm inf} p_{1|N-1} = \Delta^2 \left(p_1 - \sum_{j=1}^{N-1} h_j p_j \right). \tag{3}$$

Here, the subscript $N-1$ means the total number of steering modes. Then we can conclude that the first mode can be steered by the group of $N-1$ modes, if

$$EPR_{1|N-1} = \Delta^2_{\rm inf} x_{1|N-1} \Delta^2_{\rm inf} p_{1|N-1} \geq 1 \tag{4}$$

can be violated. The inferred variance can be optimized by the gain factors g_j and h_j.

Results- First, we give the general expression of the inferred variance $\Delta^2_{\rm inf} x_{1|N-1}$ for the one arm structure. Here we set the variances of the input states from the third to last equal with the second mode, and the transmission efficiency of the first output state is η_1, while other modes are η_2.

$$\begin{aligned}\Delta^2_{\rm inf} x^{\rm one}_{1|N-1} &= \frac{1}{N}\left(\sqrt{\eta_1} - \sqrt{\eta_2} g N + \sqrt{\eta_2} g\right)^2 (2n+1) {\rm e}^{2\,r_1} \\ &+ \frac{N-1}{N}\left(\sqrt{\eta_1} + g\sqrt{\eta_2}\right)^2 (2n+1) {\rm e}^{-2\,r_1} \\ &- \eta_1 + g^2 (N-1)(1-\eta_2) + 1,\end{aligned}$$

when setting the squeezing level of all input states equal. We were able to use the same gain factors for each steering mode, as all the output modes are equivalent. The inferred error can then be optimized by

$$g = -\frac{4\sqrt{\eta_1\eta_2}\sinh(2\,r)\,(2\,n+1)\,(N-1)}{N\left[2\,(N-1)\,(\eta_2-1) - \frac{2\,\eta_2\,{\rm e}^{-2\,r}\,(2\,n+1)\,(N-1)\,(N\,{\rm e}^{4\,r} - {\rm e}^{4\,r}+1)}{N}\right]}.$$

Similarly, we can get the expression of $\Delta^2_{\rm inf} p^{\rm one}_{1|N-1}$. For the two arm structure, the expressions of inferred variance have two cases, which depend on the total number of modes is even or odd. When the total number of modes N is even, we have

$$\begin{aligned}\Delta^2_{\rm inf} x^{\rm two,even}_{1|N-1} = (2\,n+1)/N &\left\{ {\rm e}^{2\,r_1}\left[\sqrt{\eta_2}\,g_1\,\left(\frac{N}{2}-1\right) - \sqrt{\eta_1} + \frac{N\sqrt{\eta_2}\,g_2}{2}\right]^2 + {\rm e}^{2\,r_2}\,(N-2)\,\left(\sqrt{\eta_2}\,g_1 + \sqrt{\eta_1}\right)^2\right] \\ &+ {\rm e}^{-2\,r_1}\left[\sqrt{\eta_1} - \frac{\sqrt{\eta_2}\,g_1\,(N-2)}{2} + \frac{N\sqrt{\eta_2}\,g_2}{2}\right]^2\Bigg\} - \left(\frac{N\,{g_1}^2}{2} + \left(\frac{N}{2}-1\right){g_2}^2\right)(\eta_2-1) - \eta_1 + 1\end{aligned} \tag{5}$$

and for the odd case, we have

$$\begin{aligned}\Delta^2_{\rm inf} x^{\rm two,odd}_{1|N-1} = (2\,n+1)\,(N+1)^{-1} &\Big\{ {\rm e}^{2\,r_2}\,(N-1)\,\left(\sqrt{\eta_2}\,g_1 + \sqrt{\eta_1}\right)^2 \\ &+ {\rm e}^{2\,r_1}\,N^{-1}(N-1)^{-1}\Big[\sqrt{\eta_2}\,g_1\,(N-1)^2/2 - \sqrt{\eta_1}\,(N-1) + \sqrt{\eta_2}\,g_2\,(N-1)\,(N+1)/2\Big]^2\Big\} \\ &+ (2\,n+1)\,{\rm e}^{-2\,r_1}(2\,N)^{-1}\left[2\sqrt{\eta_1} - \sqrt{\eta_2}\,g_1\,(N-1) + \sqrt{\eta_2}\,g_2\,(N-1)\right]^2 \\ &- \eta_1 - \frac{(N-1)\,(\eta_2-1)\,\left({g_1}^2 + {g_2}^2\right)}{2} + 1.\end{aligned} \tag{6}$$

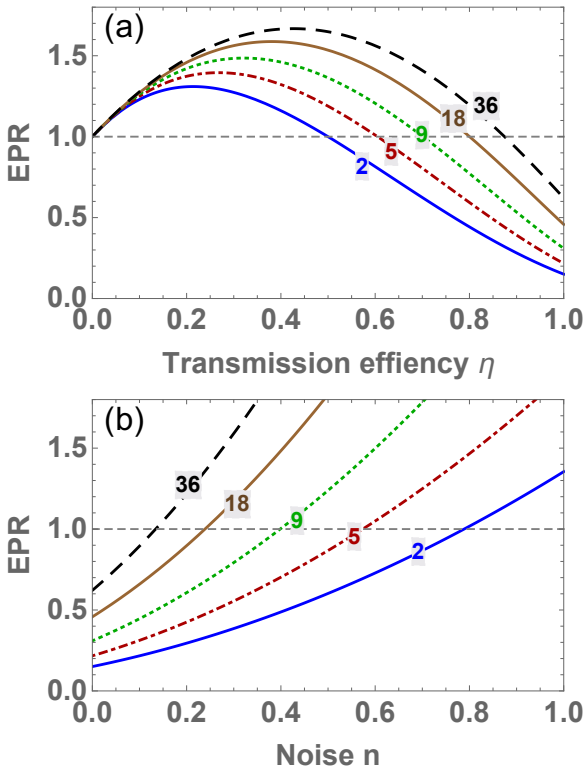


Figure 3: (a)EPR steering parameter versus the transmission efficiency. In this case, the squeezing level is set to $r = 0.8$ and no thermal noise. (b) EPR steering parameter versus the thermal noise. Now the transmission efficiency is assumed to be ideal.

Similarly, we can get the expression of $\Delta^2_{\inf} p^{\text{two}}_{1|N-1}$. The expressions for g_1 and g_2 are too long and are therefore not being displayed here. For simplification it is further assumed that $\eta_1 = \eta_2 = \eta$ and $r_1 = r_2 = r$. We find that the properties of multipartite steering are independent on the structure of optical networks as long as their inferred variances are optimized (also independent from wether N is even or odd), which means $EPR^{\text{one}}_{1|N-1} = EPR^{\text{two}}_{1|N-1}$. We further show the robustness against imperfect transmission as well as thermal noise involved in the input states, as shown in Fig. 3. Given perfect efficiency, we find the thresholds of thermal noise to lose EPR steering to be:

$$n_{tr} = \frac{\mathrm{e}^{-2r}\left[\sqrt{(N\,\mathrm{e}^{4r} - \mathrm{e}^{4r} + 1)\,(N + \mathrm{e}^{4r} - 1)} - N\,\mathrm{e}^{2r}\right]}{2N}. \tag{7}$$

Analytical solutions for thresholds of efficiencies can also be obtained. The expressions for both systems are the same. However, the terms are too long to show simply. *QSS application-* A (l, m) quantum secret sharing (QSS) scheme enables a dealer to split a secret into m secrets, distributing it to m players. Then at least $l < m$ players are required to cooperate together to recover the secret of the dealer. The monogamy of EPR steering [16] states that if a party A can steer party B, then no other distinctive party C can steer B. This is a nice framework for Secret Sharing. A secured keyrate for such a scheme can be calculated by the Devetak-Winter-formula. In [17, 18], the authors showed that a secured keyrate is related to collective steerability of the system. We are currently investigating up to which number of participants collective steering is possible based on the above linear optical network.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777–780 (1935).

[2] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555–563 (1935).

[3] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[4] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).

[5] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[6] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).

[7] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).

[8] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janoušek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Optica **3**, 634–642 (2016).

[9] M. D. Reid. Phys. Rev. A, **88**, 062338 (2013).

[10] Q. He, L. Rosales-Zárate, G. Adesso, and M. D. Reid, Phys. Rev. Lett. **115**, 180502 (2015).

[11] C.-Y. Chiu, N. Lambert, Teh-Lu Liao, F. Nori, and C.-M. Li, NPJ Quantum Information **2**, 16020 (2016).

[12] M. Wang, Y. Xiang, Q. Y. He, and Q. H. Gong, Phys. Rev. A **91**, 012112 (2015).

[13] S. Armstrong, M.Wang, R. Y. Teh, Q. H. Gong, Q. Y. He, J. Janousek, H. A. Bachor, M. D. Reid, and P. K. Lam, Nat. Phys. **11**, 167–172 (2015).

[14] M. D. Reid, Phys. Rev. A **40**, 913–923 (1989).

[15] Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).

[16] M. D. Reid, Phys. Rev. A **88**, 062108 (2013).

[17] Y. Xiang, I. Kogias, G. Adesso, and Q. Y. He, Phys. Rev. A **95**, 010101(R) (2017).

[18] I. Kogias, Y. Xiang, Q. Y. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).

Robustness and inference of structural complexity of quantum models of stochastic processes

Matthew Ho[1 2 *] Mile Gu[1 2 3 †] Thomas J. Elliott[2 1 ‡]

[1] *School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Singapore.*

[2] *Complexity Institute, Nanyang Technological University, Singapore 637335, Singapore*

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

Abstract. Modelling stochastic processes is a crucial element in the study and understanding of the quantitative sciences. Quantum models have shown to compress the amount of information contained in these processes beyond classical limits. They are constructed based on prior knowledge of their optimal classical counterparts. We introduce an inference protocol that bypasses the requirement of knowing the optimal classical models to estimate the memory required for modelling of stochastic processes. Structural complexity is discontinuous with statistical fluctuations. Unlike optimal classical models, the inference protocol is robust to these statistical fluctuations.

Keywords: Quantum modelling, stochastic processes, model inference, quantum advantage, structural complexity, quantum information, quantum memory.

Complex, stochastic processes underpin quantitative science. It is therefore of paramount importance to study and understand the behaviour of such processes for the crucial twin purposes of modelling and prediction. These tasks are typically resource-intensive, motivating the need for methods that ameliorate these requirements. A promising recent development to this end [1–3, 7–12] , using a cross-disciplinary blend of tools from quantum and complexity science, has highlighted that quantum simulators can operate with much smaller memories than the minimal possible classical models [13–15] , while providing equally accurate predictions.

This information compression bears both fundamental and applied consequences. On the applied side the benefits are immediately apparent – we can use quantum technologies to construct simulators of complex stochastic processes that function with (in some cases drastically [2, 4, 7, 8, 10, 11]) reduced memory requirements relative to optimal classical counterparts. Within complexity science, the minimal amount of information that must be stored about the past of a process to replicate its future is considered to be a measure of structure in the process, called the *statistical complexity* [13–15] . When one considers this minimisation to also encompass quantum models the reduction has a profound effect on our perception of structure, fundamentally altering whether or not a process should be considered complex [5, 6].

In this work [16], we show that the quantum analogue of statistical complexity is robust to perturbations to the process, and is hence a more stable measure of structure than the classical measure, which can change discontinuously under infinitesimal variations to a process' underlying probability distribution. This allows us to introduce a protocol for estimating the quantum measure of structure in a stochastic process directly from a time-series formed from observations of the process. Previously, this same task was performed by first inferring the minimal classical model and then quantising, thus inheriting errors introduced by certain measures needed to mitigate the issues associated with a non-smoothly-varying classical statistical complexity – our protocol avoids the need to suffer such drawbacks. This forms a key step in the application of these quantum-enhanced models to understand complex stochastic processes, and further, is a crucial first step towards inferring such models from raw data.

*hosh0021@e.ntu.edu.sg

†mgu@quantumcomplexity.org

‡physics@tjelliott.net

References

[1] M. Gu, K. Wiesner, E. Rieper, and V. Vedral. *Nat. Commun.* **3**, 762 (2012).

[2] J. R. Mahoney, C. Aghamohammadi, and J. P. Crutchfield. *Sci. Rep.* **6**, 20495 (2016).

[3] M. S. Palsson, M. Gu, J. Ho, H. M. Wiseman, and G. J. Pryde. *Sci. Adv.* **3**, e1601302 (2017).

[4] A. J. P. Garner, Q. Liu, J. Thompson, and J. P. Crutchfield. *New Journal of Physics* **19**, 103009 (2017).

[5] C.A Aghamohammadi, J. R. Mahoney, and J. P. Crutchfield, *Phys. Lett. A* **381**, 1223 (2017).

[6] W. Y. Suen, J. Thompson, A. J. P . Garner, V. Vedral, and M. Gu *Quantum* **1**, 25 (2017)

[7] C. Aghamohammadi, S. P. Loomis, J. R. Mahoney, and J. P. Crutchfield. *Phys. Rev. X* **8**, 11025 (2018).

[8] T. J. Elliott and M. Gu. *npj Quantum Information* **4**, 18 (2018).

[9] F. C. Binder, J. Thompson, and M. Gu. *Phys. Rev. Lett.* **120**, 240502 (2018).

[10] J. Thompson, A. J. P. Garner, J. R. Mahoney, J. P. Crutchfield, V. Vedral, and M. Gu. *Phys. Rev. X* **8**, 031013 (2018).

[11] T. J. Elliott, A. J. P. Garner, and M. Gu. *New Journal of Physics* **21**, 013021 (2018).

[12] Q. Liu, T. J. Elliott, F. C. Binder, C. D. Franco, and M. Gu. arXiv:1810.09668v1 (2018).

[13] J. P. Crutchfield and K. Young. *Phys. Rev. Lett.* **63**, 105 (1989).

[14] C. R. Shalizi and J. P. Crutchfield. *J. Stat. Phys* **104**, 817 (2001).

[15] J. P. Crutchfield. *Nat. Phys.* **9**, 382 (2013).

[16] M. Ho, M. Gu, and T. J. Elliott. *In preparation.*

Quantum ensembles which is error tolerant in prior probability when minimum error discrimination is performed on two quantum states

Jihwan Kim[1] * Donghoon Ha[1] † Younghun Kwon[1] ‡

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

Abstract. In this paper, we consider the minimum error discrimination of two quantum states, where the optimal strategy is tolerant to errors in the prior probability. In general, optimal measurements and guessing probability in minimum error discrimination depend on prior probabilities and different prior probabilities for the quantum states may require the change of optimal measurement. However, an ensemble composed of certain quantum states preserves optimal measurement even if minor errors occur in the prior probability. In this work, we study the conditions that the prior probability error tolerant ensembles satisfy. In addition, we investigate which kind of quantum state satisfy the condition.

Keywords: prior probability, error tolerant, minimum error discrimination

1 Introduction

Quantum state discrimination is an essential process in quantum information processing and quantum computation. It is a process, where by measurement one decodes classical information encoded in quantum states[1–5]. In quantum theory, perfect distinguishability of states depends on orthogonality between quantum states and the information encoded in non-orthogonal quantum states can not always be perfectly decoded. Therefore, various strategies are used[2–5], depending on whether inconclusive results are allowed or not. Minimum error discrimination[1] is a strategy which can not gurantee the correctness of the measurement results, but maximizes the probability of satisfying the correctness on average. This strategy does not allow inconclusive results. Unambiguous discrimination[6–10], on the other hand, has a result that can gurantee correctness, and its optimal strategy is maximizing the probability of results that can ensure correctness. This strategy allows inconclusive results, in order to produce results that gurantee correctness. As another strategy, there are various strategies such as maximum confidence[11] or discrimination with fixed rate of inconclusive results[12–15].

Quantum state discrimination[1–5] is described as follows. The quantum state in which a sender called Alice encodes the classical information $x \in \{1, 2, \cdots, N\}$ is described by density operator ρ_x. The measurement of the receiver called Bob, which is a decoder performing the decoding, is given by POVM $\{M_y\}_{y=1}^{N}$. Bob knows the frequency of quantum state that Alice sends, which is called prior probability. In quantum state discrimination, Bob discriminates the quantum states of the ensemble $\{q_x, \rho_x\}_{x=1}^{N}$ using his strategy. Here, the subspace of Hilbert space used to describe the density operator or POVM satisfies the condition that the statistical mixture of the ensemble is full rank. This eliminates the trivial degree of freedom of the optimal solution.

In the minimum error discrimination(MD), Bob performs a measurement strategy that maximizes the correct probability. The maximum value of the correct probability that can be reached by Bob's measurement is called the guessing probability[5, 16, 17]. And, in general, the optimal measurement that provides a guessing probability is not unique. The general conditions under which optimal measurements are unique are not known. However, optimal measurement is known in the case of two states MD[1] or three or four qubits[16, 17]. For two quantum states, the difference between the prior probabilities multiplied by the density operator must be a full rank. Because the operator's kernel is a subspace that provides degrees of freedom in optimal measurements. The optimal measurement in three or four qubits is also determined by the geometry of the weighed vector corresponding to the product of the prior probability and the quantum states. The number of possible measurements is also determined by the geometry. It should be noted that the geometry is easily modified to a change in the prior probability, so that the optimal measurement is sensitive to prior probabilities. Because the optimal measurement easily loses optimality even for a small change of the prior probability, one needs to understand the correct probability as a function of the prior probability. And one should understand the behavior of the measurement when an error occurs in the prior probability.

We consider the MD as a two-person, zero-sum game in which the correct probability is determined by prior probability and measurement[18–20]. The optimal strategy of this game is always a minimax strategy[19]. The Minimax strategy is an ordered pair consisting of Alice and Bob's optimal strategy[21]. Here, Alice's optimal strategy is to choose the prior probability which minimizes the guessing probability obtained from the MD performed by Bob, and Bob's optimal strategy is to select the measurement which can obtain the guessing probability regardless of Alice's choice of the prior probability[19]. In particular, according to the necessary and sufficient conditions[18, 19] that the minimax strategy should satisfy, the prior probabilities that minimize the guessing

*mslab.k@gmail.com
†mslab.h@gmail.com
‡yyhkwon@hotmail.com

probability share the same optimal measurement and guessing probability.

The distribution of the prior probability, which is the probability distribution of the population, determines the frequency with which the quantum states are prepared. However, the frequency of the quantum states actually prepared in finite number of experiments assuming i.i.d may not agree with the prior probability. When the sample size N is large enough, its frequency is ϵ-convergent in the distribution of prior probabilities. However, the prior probability is only a theoretical frequency of occurrence assuming infinite experiments. Therefore, even if N is large enough, the correct probability obtained by the optimal measurement corresponding to the prior probability differs from the optimal value. This is because the frequency of occurrence is close to ϵ in the prior probability distribution, but not the prior probability.

In this paper, we investigate the quantum states in which the optimal measurement and the guessing probability ofϵ -convergent prior probability are identical to those of the prior probability when the occurrence frequency is ϵ -convergent in the prior probability. Because the trivial example of these quantum states occurs when the states of the ensemble are orthogonal to each other, we can see that those quantum states exist in all dimensions. So the states we are interested in are the quantum states which are not orthogonal but satisfy this condition. A necessary condition of these quantum states is to have the same guessing probability at different prior probabilities of the quantum states. We show that in a two-state MD which can be considered as two-person zero-sum game, a pair of prior probabilities and optimal measurement is a quantum minimax strategy if different prior probabilities can have the same optimal measurement while providing the same guessing probability. The condition to have the same optimal measurement and guessing probability in ϵ-convergent probability of occurrence is expressed using quantum minimax strategy. This allows us to determine whether the ensemble is a prior probability error tolerant ensemble when we find one minimax strategy in 2 quantum states MDs.

2 Results

First, we provide necessary and sufficient conditions that a probability distribution that is ϵ-convergent in a prior probability exists while sharing the same optimal measurement and guessing probability with the prior probability. Further, we can find the following lemma 1 from quantum minimax theorem and the necessary and sufficient conditions for minimax strategy. Here, the quantum minimax theorem and the condition provide the existence of the measurement.

Lemma 1 *When MD is performed in given prior probability, iff an optimal measurement* $\{M_x\}_{x=1}^2$ *satisfies* $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2)$*, one gets minimum guessing probability.*

Let us note that lemma 1 tells us that the prior probabilities that provide the minimum value of guessing probability share the same optimal strategy with the same guessing probability, but do not tell the opposite. Therefore, we can not be sure that all points sharing the same guessing probability and optimal measurement provide the minimum value of guessing probability. However, the lemma below shows that the inverse is hold for MD of two quantum states.

Lemma 2 *The quantum ensembles of* S_1 *and* S_2 *are given as* $\{p_x, \rho_x\}_{x=1}^2$ *and* $\{q_x, \rho_x\}_{x=1}^2$*, respectively, where* $p_1 \neq q_1$*. Suppose that in minimum error discrimination of quantum ensemble* S_x *the guessing probability is* $p_{\mathrm{guess}}^{(x)}$ *and the minimum value of guessing probability is* $p_{\mathrm{guess}}^{\star}$*. Then, when* $p_{\mathrm{guess}}^{(1)} = p_{\mathrm{guess}}^{(2)}$*, if there exists an measurement that can perform minimum error discrimination on two quantum ensembles* S_1 *and* S_2 *simultaneously, one can obtain* $p_{\mathrm{guess}}^{(1)} = p_{\mathrm{guess}}^{\star}$*.*

On the other hand, the set of prior probability that provide the minimum value of guessing probability is a convex set. It is because the guessing probability is a convex function in the prior probability domain and the sublevel set is a convex set. Thus, if $(\mathbf{q}, \mathbf{M})$ is a minimax strategy, then the conditions for existence of ϵ-convergent prior probabilities sharing the optimal measurement and the same guessing probability are given as:

Proposition 3 *The prior probability providing minimum of guessing probability is not unique if and only if* $\{M_x\}_{x=1}^2$ *satisfies following conditions:*

1. $[\rho_x, M_1] = 0 \quad \forall x \in \{1, 2\}$,
2. *For some* $x \in \{1, 2\}$*, every* $|v\rangle \in \mathrm{Supp}(M_x)$ *satisfies* $\langle v| \rho_1 |v\rangle : \langle v| \rho_2 |v\rangle \neq 1 - q : q$.

where $[A, B] = AB - BA$.

One of the requirements is that quantum states and measurements can be simultaneously diagonalized. However, since commutation relations are not generally transitive, we can not be sure that the two quantum states can be simultaneously diagonalized. In the case of a qubit, however, the two states are simultaneously diagonalized because the commutation relations of the two operators imply that the Bloch vector is parallel.

Here, we studied quantum ensembles which is error tolerant in prior probability to MD of two quantum states. An optimal strategy in a prior probability can not be optimal in different occurrence probability and guessing probability can be seen as a convex function in prior probability domain. We showed that the error-tolerant ensembles have ϵ-convergent occurrence distributions in prior probability distribution while sharing the optimal strategy and vice versa. Further, we expressed the condition, using a minimax strategy. In addition, we investigated which kind of quantum state can satisfy the condition.

References

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

[2] A. Chefles. Quantum state discrimination. *Contemp. Phys.*, 41(6):401–424, 2000.

[3] S. M. Barnett, S. Croke. Quantum state discrimination. *Adv. Opt. Photon.*, 1(2):238–278, 2009.

[4] J. A. Bergou. Discrimination of quantum states. *J. Mod. Opt.*, 57(3):160–180, 2010.

[5] J. Bae, L. Kwek. Quantum state discrimination and its applications. *J. Phys. A: Math Theor.*, 48(8):083001, 2015.

[6] I. D. Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123(6):257–259, 1987.

[7] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128(1):0375–9601, 1988.

[8] D. Dieks. Overlap and distinguishability of quantum states. *Phys. Lett. A*, 126(5):303–306, 1988.

[9] G. Jaeger, A. Shimony. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A*, 197(2):83–87, 1995.

[10] A. Chefles. Unambiguous discrimination between linearly independent quantum states. *Phys. Lett. A*, 239(6):339–347, 1998.

[11] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeers, Maximum Confidence Quantum Measurements. *Phys. Rev. Lett.*, 96(7):070401, 2006.

[12] A. Chefles, S. M. Barnett. Strategies for discriminating between non-orthogonal quantum states. *J. Mod. Opt*, 45(6):1295–1302, 1998.

[13] C.-W. Zhang, C.-F. Li, and G.-C. Guo. General strategies for discrimination of quantum states. *Phys. Lett. A*, 261(1):25–29, 1999.

[14] J. Fiurášek, M. Ježek. Optimal discrimination of mixed quantum states involving inconclusive results. *Phys. Rev. A*, 67(1):012321, 2003.

[15] Y. C. Eldar. Mixed-quantum-state detection with inconclusive results. *Phys. Rev. A*, 67(4):042309, 2003.

[16] D. Ha, Y. Kwon. Complete analysis for three-qubit mixed-state discrimination. *Phys. Rev. A*, 87(6):062302, 2013.

[17] D. Ha, Y. Kwon. Discriminating N-qudit states using geometric structure. *Phys. Rev. A*, 90(2):022330, 2014.

[18] G. M. D'Ariano, M. F. Sacchi, and J. Kahn. Minimax quantum-state discrimination. *Phys. Rev. A*, 72(3):032310, 2005.

[19] O. Hirota and S. Ikehara. Minimax Strategy in the Quantum Detection Theory and Its Application to Optical Communications. *Trans. IECE Japan*, E65(1):627–633, 1982.

[20] K. Nakahira, K. Kato, and T. S. Usuda. Minimax strategy in quantum signal detection with inconclusive results. *Phys. Rev. A*, 88(3):032314, 2013.

[21] A. Wald. Generalization of a Theorem By v. Neumann Concerning Zero Sum Two Person Games. *Annals of Math.*, 46(2):281–286, 1945.

Understanding Entanglement Survival in Hybrid Quantum System composed of Two-level Atom and Superconducting Circuit in Noisy Environment

Jeongsoo Kang[1] * Min Namkung[1] † Younghun Kwon[1] ‡

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

Abstract. In this work, we investigate the dynamics of hybrid system in noisy environment. The hybrid system consists of two-level atom and charge qubit of superconducting circuit, When the charge qubit is under a noisy environment such as relaxation and dephasing noise, we study the entanglement behavior of the hybrid system. We show that when the decoherence rate is slower than the sweeping rate, the entanglement of hybrid state is conserved. Further, we can see that if the decoherence rate is faster than the sweeping rate, the entanglement of hybrid state is diminished. Our result implies that by controling the noise rate one can construct CNOT gate, from the hybrid system in noisy environment.

Keywords: Hybrid, Qubit, Superconducting circuit, Entanglement, Open quantum system

1 Introduction

Superconducting qubits not only perform quantum computing efficiently, but also have good scalability. Therefore, superconducting qubits is very useful for implementing quantum computers in the real world[1]. However, relaxation and dephasing time of superconducting qubits are too short[2, 3]. It means that qubits consist of superconducting circuits cannot be guaranteed for their longevity. Many researchers have done research for devising hybrid systems composed of superconducting circuits and two-level atoms[4, 5, 6, 7, 8, 9, 10, 11, 12, 13]. That is because two-level atom has been believed to strengthen superconducting circuit against noise.

Recently, D. Yu *et al.*[14] proposed a hybrid system composed of a two-level atom and a charge qubit, where an alkali atom and a capacitor of charge qubit interact to each other through electric field. D. Yu. *et. al.*[14] showed that this system can perform CNOT operation. Furthermore, this system can generate entanglement. However, Ref.[14] considered charge qubit in ideal case only.

In this research, we investigate dynamics of a noisy hybrid system composed of a charge qubit and a two-level atom. Especially, we investigate entanglement in this noisy hybrid system(see Fig.1). If entanglement between two qubits is conserved, this system may perform CNOT operation very well. We assume that both relaxation and dephasing noise simultaneously occur in the charge qubit. We propose a numerical condition that hybrid system can preserves entanglement under two noises. If relaxation and dephasing rate is slower than sweeping rate, entanglement is conserved. If relaxation and dephasing rate is faster than sweeping rate, However, entanglement is diminished. Especially, if two rates are too fast, hybrid system experiences entanglement sudden death. This result implies that this hybrid system can perform CNOT operation under two noises. Since the ability to perform CNOT operation is included in DiVincenzo's criteria, This result is important for realistic quantum computing.

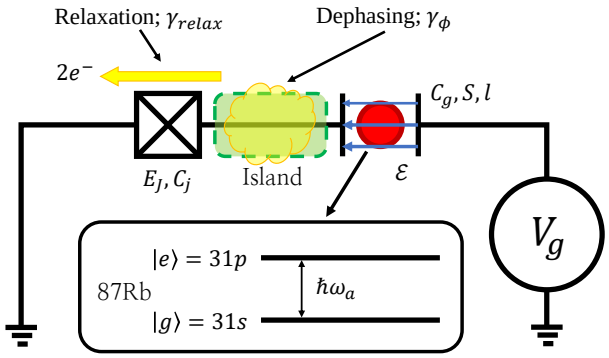


Figure 1: Two-qubit system consists of a noisy charge qubit and an atom qubit. Here, γ_{relax} is relaxation rate and γ_ϕ is dephasing rate. If two decoherence rates are slower than $10^7 \mathrm{s}^{-1}$, this system is robust under this two noises. Since $\gamma_{relax} = 2\pi \times 0.03\mathrm{MHz}$, $\gamma_\phi = 2\pi \times 0.05\mathrm{MHz}$ in the real world[20], this hybrid system can be performed in realistic situation.

This extended abstract consists of the following sections. In Section 2, we introduce a charge qubit atom hybrid system. In Section 3, we consider a Lindblad master equation of relaxation and dephasing noise. In Section 4, we analyze entanglement dynamics of hybrid system under dephasing and relaxation noise. In Section 5, we conclude this extended abstract.

2 Ideal Hybrid system

Ref.[14] proposed a two-qubit system composed of a superconducting circuit and a two-level atom(see Fig.1). Here, ^{87}Rb atom is considered as a two-level atom. The Hamiltonian $\hat{H}$ of this hybrid system is expressed as

$$\hat{H} = \hat{H}_c + \hat{H}_a. \tag{1}$$

*js.kang1202@gmail.com
†mslab.nk@gmail.com
‡yyhkwon@hotmail.com

Here, $\hat{H}_c$ is a charge qubit Hamiltonian and $\hat{H}_a$ is an atom Hamiltonian. Since a two-level atom in inside of a gate capacitor, two-level atom and charge qubit interact to each other through electric field of gate capacitor. Therefore, $\hat{H}_c(\hat{H}_a)$ from Eq.(1) affect to two-level atom(charge qubit).

Quantum state of this system is composed of product bases $\{|n\rangle \otimes |u\rangle \, | n = 0, 1 \;\; u = g, e\}$. Here, $|g\rangle(|e\rangle)$ is a ground state(excited state) of two-level atom and n is the number of Cooper-pairs in the island. Since two-qubit is considered, $n = 0, 1$ are permitted only. An eigenstate of Eq.(1) can be controlled by adiabatically changing gate voltage(V_g). Especially, when Raman process is properly performed, this hybrid model can perform CNOT operation efficiently. Therefore, this hybrid model can satisfies DiVincenzo's criteria[15] in ideal case.

3 Noise in Charge Qubit

Since a Josephson junction in charge qubit experiences various noise, we should consider a charge qubit under the noise[16, 17, 18]. We assume that relaxation and dephasing noise occurs in a charge qubit[19]. On the other hand, we assume that noise does not occur in a two-level atom. Since atom qubit is much robuster than charge qubit, this assumption is valid in realistic condition. Approximating macroscopic environment interacting with charge qubit as Markovian, time evolution of entire system is described as a following Lindblad master equation[20, 21]:

$$\frac{\partial \hat{\rho}}{\partial t} = -\frac{i}{\hbar}\left[\hat{H}, \hat{\rho}\right] + \gamma_{relax}\mathcal{D}\left[\hat{\sigma}_{-}^{(c)}\right]\hat{\rho} + \gamma_{\phi}\mathcal{D}\left[\hat{\sigma}_{z}^{(c)}\right]\hat{\rho}. \quad (2)$$

Here, $\hat{\rho}$ is a density operator of composite state between charge qubit and two-level atom, γ_{relax} is relaxation rate, γ_{ϕ} is dephasing rate. In Eq.(2), $\mathcal{D}$ is Lindblad superoperator:

$$\mathcal{D}\left[\hat{K}\right]\hat{\rho} = \hat{K}\hat{\rho}\hat{K}^{\dagger} - \frac{1}{2}\hat{K}^{\dagger}\hat{K}\hat{\rho} - \frac{1}{2}\hat{\rho}\hat{K}^{\dagger}\hat{K}. \quad (3)$$

In general, noise in charge qubit may decreases entanglement. Since entanglement is a resource of various quantum computers, we should investigate whether the hybrid system preserves entanglement under the noise.

4 Entanglement Survival

We analyze entanglement of hybrid system composed of noisy charge qubit and two-level atom. We consider concurrence[22] as an entanglement measure. In order to controll the quantum stste of hybrid system, we sweep offset charge number $N_{g0}(\propto V_{g0})$ of charge qubit from 0 to 1, where sweeping rate is considered as 1 ns^{-1}(Fig. 2)[22]. This sweeping rate is suitable for performing two-qubit gate operation[14].

Here, we investigate concurrence under the relaxation and dephasing noise. If two decoherence rates are slower than 10^7 s^{-1}, concurrence is conserved(Fig.2a). If decoherence rate is faster than 10^7, However, concurrence is diminished. Especially, if decoherence rate is too fast, concurrence becomes zero in certain region of time. This phenomenon is so called entanglement sudden death(Fig. 2b)[23]. Two decoherence rates of charge qubit is known as $\gamma_{relax} = 2\pi \times 0.03$ MHz and $\gamma_{\phi} = 2\pi \times 0.05$ MHz. This sweeping rate is almost 10,000 times slower than 10^7. Therefore, the hybrid system is robust under two noises.

5 Conclusion and Future Work

We investigated a hybrid system composed of a noisy charge qubit and ^{87}Rb atom. Here, we consider relaxation and dephasing noise. We calculate concurrence to measure entanglement between two qubits. As a result, we display that entanglement is conserved if decoherence and sweeping rates are very slow. This implies that the hybrid system in robust under relaxation and dephasing noise.

In future, we investigate how much noisy hybrid system can perform CNOT operation. Furthermore, we consider the case that $1/f$ noise occurs in superconducting circuit. Since $1/f$ noise is negatively critical for charge qubit[24, 25], investigation under the $1/f$ noise is necessary.

Acknowledgement

We thank Hyunseong Jang for his insightful discussion. This work is supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (NRF2015R1D1A1A01060795 & NRF2018R1D1A1B07049420).

References

[1] D. Castelvecchi. Quantum computers ready to leap out of the lab in 2017. Nature. p. 9-10, 2017.

[2] Y. Makhlin, G. Schön, and A. Shnirman. Quantum-state engineering with Josephson-junction devices Rev. Mod. Phys. **73**, 357, 2001.

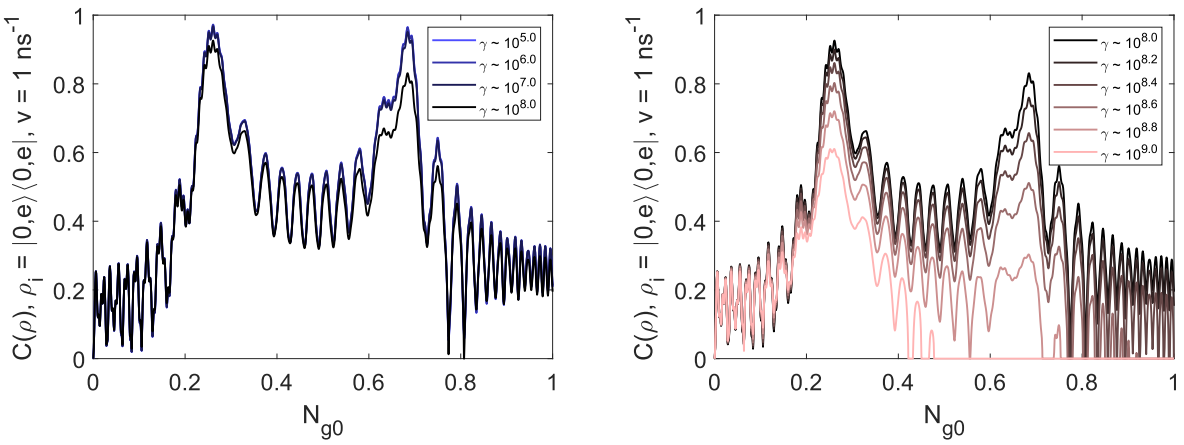
[3] Z.-L. Xiang, S. Ashhab, J. Q. You, and F. Nori. Hybrid quantum circuits: Superconducting circuits interacting with other quantum systems Rev. Mod. Phys. **85**, 623, 2013.

[4] T. Nirrengarten, A. Qarry, C. Roux, A. Emmert, G. Nogues, M. Brune, J.-M. Raimond, and S. Haroche. Realization of a Superconducting Atom Chip Phys. Rev. Lett. **97**, 200405, 2006.

[5] Y. Colombe, T. Steinmetz, G. Dubois, F. Linke, D. Hunger, and J. Reichel. Strong atom–field coupling for Bose–Einstein condensates in an optical cavity on a chip Nature(London) **450**, 272, 2007.

[6] F. Shimizu, C. Hufnagel, and T. Mukai. Stable Neutral Atom Trap with a Thin Superconducting Disc Phys. Rev. Lett. **103**, 253002, 2009.

[7] Y. Kubo, F. R. Ong, P. Bertet, D. Vion, V. Jacques, D. Zheng, A. Dréau, J.-F. Roch, A. Auffeves, F. Jelezko, J. Wrachtrup, M. F. Barthe, P. Bergonzo,



(a) (b)

Figure 2: Concurrence of two-qubit state in relaxation and dephasing noise. Here, initial condition is $\rho_i = |0, e\rangle \langle 0, e|$ and sweeping rate is given as 1 ns^{-1}. We evaluated concurrence considering two decoherence rates are assumed from 10^5 s^{-1} and 10^8 s^{-1} in (a), and from 10^8 s^{-1}and 10^9 s^{-1} in (b).

and D. Esteve. Strong Coupling of a Spin Ensemble to a Superconducting Resonator Phys. Rev. Lett. **105**, 140502, 2010.

[8] M. Siercke, K. S. Chan, B. Zhang, M. Beian, M. J. Lim, and R. Dumke. Reconfigurable self-sufficient traps for ultracold atoms based on a superconducting square Phys. Rev. A **85**, 041403(R), 2012.

[9] N. Daniilidis and H. Häffner. Quantum Interfaces Between Atomic and Solid-State Systems Annu. Rev. Condens. Matter Phys. **4**, 83, 2013.

[10] S. Bernon, H. Hattermann, D. Bothner, M. Knufinke, P. Weiss, F. Jessen, D. Cano, M. Kemmler, R. Kleiner, D. Koelle, and J. Fortägh. Manipulation and coherence of ultra-cold atoms on a superconducting atom chip Nat. Commun. **4**, 2380, 2013.

[11] Y. Qiu, W. Xiong, L. Tian, and J. Q. You. Coupling spin ensembles via superconducting flux qubits Phys. Rev. A **89**, 042321, 2014.

[12] 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. Phys. Rev. A **94**, 062301, 2016.

[13] D. Yu, A. Landra, L. C. Kwek, L. Amico, and R. Dumke. Stabilizing Rabi oscillation aof a charge qubit via the atomic clock technique. New J. Phys. **20**, 023031, 2018.

[14] D. Yu, M. M. Valado, C. Hufnagel, L. C. Kwek, L. Amico, and R. Dumke. Charge qubit-atom hybrid Phys. Rev. A **93**, 042329, 2016.

[15] D. P. DiVincenzo. The Physical Implementation of Quantum Computation. Fortschritte der Physik **48**, p.771-783, 2000.

[16] A. Rivas, and S. F. Huelga. Open Quantum Systems Berlin: Springer, 2012.

[17] M. Schlosshauer. Decoherence: And the Quantum-to-Classical Transition. Springer, 2007.

[18] A. M. Zagoskin. Quantum Engineering: Theory and Design of Quantum Coherent Structures. Cambridge University Press, 2011.

[19] L. Tian, S. Lloyd, and T. P. Orlando. Decoherence and relaxation of a superconducting quantum bit during measurement Phys. Rev. B **65**, 144516, 2002.

[20] D. Yu, L. C. Kwek, L. Amico, and R. Dumke. Superconducting Qubit-Resonator-Atom Hybrid System Quantum Sci. Technol. **2**, 035005, 2017.

[21] A. Isar, A. Sandulescu, H. Scutaru, E. Stefanescu, and W. Scheid. Open Quantum Systems Int. J. Mod. Phys. E, Vol. 3, No. 2, 635, 1994.

[22] W. K. Wootters. Entanglement of Formation of an Arbitrary State of Two Qubits. Phys. Rev. Lett. **80**, 2245, 1998.

[23] T. Yu, and J. H. Eberly. Sudden Death of Entanglement Science 323, p. 598-601, 2009.

[24] K. Bladh, T. Duty, D. Gunnarsson, and P. Delsing. The single Cooper-pair box as a charge qubit. New J. Phys. **7**, 180, 2005.

[25] M. H Devoret and R. J. Schoelkoph. Superconducting Circuits for Quantum Information: An Outlook. Science **339**, 1169, 2013.

Comparison of quantum reading in non-symmetric loss using maximum and non-maximum quasi-Bell states

Keita ISHIKAWA[1] * Tiancheng WANG[1] † Tsuyoshi Sasaki USUDA[1] ‡

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan*

Abstract. Quantum reading is one of application protocols of entanglement. This protocol uses entanglement for reading of a digital memory such as a CD or DVD. In our previous study, we assumed real settings and investigated the effect of non-symmetric loss on this protocol using a quasi-Bell state. However, we did not investigate the effect only when using a maximum quasi-Bell state. In this work, we compare the effects using maximum and non-maximum quasi-Bell states.

Keywords: entanglement, quantum reading, quasi-Bell state

1 Introduction

Entanglement is an important resource used and exploited in various quantum protocols[1]. There are protocols such as quantum teleportation[2], quantum phase estimation[3], and quantum reading[4]. In these protocols, one attempts to use the entangled state that has maximum entanglement (the strongest correlation). Among the entangled states, one may consider quasi-Bell states. Even though these states are constructed using nonorthogonal states, it is known that a quasi-Bell state with maximum entanglement (maximum quasi-Bell state) exists[5, 6].

Quantum reading is the protocol that uses entanglement for reading a bit stored in digital memory. By using entanglement, it was shown that the data rate improves[4]. Moreover, in noiseless environments, error-free reading is possible by using a maximum quasi-Bell state[7]. In [8], Kato and Hirota considered a situation where mode B was sent to memory whereas mode A was inputted to a receiver, and both were equally attenuated. Furthermore, we considered a situation where mode B was only attenuated[9].

In quantum teleportation and quantum phase estimation, quasi-Bell states that have non-maximum entanglement (non-maximum quasi-Bell states) exhibit better performance than maximum quasi-Bell states[10, 11]. It is expected that performances of these quasi-Bell states differ for each quantum protocol[12]. In our work[9], we investigated an effect of non-symmetric loss on quantum reading using a maximum quasi-Bell state. However, we did not investigate the effect using a non-maximum quasi-Bell state. In this work, we compare the effects using maximum and non-maximum quasi-Bell states.

2 Quasi-bell state by coherent states

An entangled state constructed using a nonorthogonal set of quantum states is called a quasi-Bell state[5]. Consider two modes labeled A and B, described by coherent states denoted $|\alpha\rangle$ and $|\beta\rangle$, respectively. In this paper, using these states, the quasi-Bell states are

$$|\Psi_1\rangle_{\mathrm{AB}} = h_1(|\alpha\rangle_{\mathrm{A}}|\beta\rangle_{\mathrm{B}} + |-\alpha\rangle_{\mathrm{A}}|-\beta\rangle_{\mathrm{B}}), \quad (1)$$
$$|\Psi_2\rangle_{\mathrm{AB}} = h_2(|\alpha\rangle_{\mathrm{A}}|\beta\rangle_{\mathrm{B}} - |-\alpha\rangle_{\mathrm{A}}|-\beta\rangle_{\mathrm{B}}), \quad (2)$$
$$|\Psi_3\rangle_{\mathrm{AB}} = h_3(|\alpha\rangle_{\mathrm{A}}|-\beta\rangle_{\mathrm{B}} + |-\alpha\rangle_{\mathrm{A}}|\beta\rangle_{\mathrm{B}}), \quad (3)$$
$$|\Psi_4\rangle_{\mathrm{AB}} = h_4(|\alpha\rangle_{\mathrm{A}}|-\beta\rangle_{\mathrm{B}} - |-\alpha\rangle_{\mathrm{A}}|\beta\rangle_{\mathrm{B}}), \quad (4)$$

where

$$h_1 = h_3 = 1/\sqrt{2(1+\kappa_{\mathrm{A}}\kappa_{\mathrm{B}})}, \quad (5)$$
$$h_2 = h_4 = 1/\sqrt{2(1-\kappa_{\mathrm{A}}\kappa_{\mathrm{B}})}, \quad (6)$$
$$\kappa_{\mathrm{A}} = \langle\alpha|-\alpha\rangle = \langle-\alpha|\alpha\rangle = \exp(-2|\alpha|^2), \quad (7)$$
$$\kappa_{\mathrm{B}} = \langle\beta|-\beta\rangle = \langle-\beta|\beta\rangle = \exp(-2|\beta|^2), \quad (8)$$

and α and β are amplitudes of the coherent states of modes A and B, respectively. The amplitudes are assumed to be non-negative real numbers. If $\alpha = \beta$, then $|\Psi_2\rangle$ and $|\Psi_4\rangle$ have maximum entanglement and are orthogonal[5].

3 Model of quantum reading with non-symmetric loss

3.1 Quantum reading using quasi-Bell states

Quantum reading using quasi-Bell states[7] is performed as follows. We assume that "0" or "1" is recorded on a memory cell. Here, we explain this protocol using $|\Psi_2\rangle_{\mathrm{AB}}$ in Eq. (2).

1. Mode A of $|\Psi_2\rangle_{\mathrm{AB}}$ is sent to a receiver.
2. Mode B is sent to the memory cell. If "0" is registered on the cell, the light is reflected with the same phase. Alternatively, if "1" is registered on the cell, the phase of the light is shifted by π. At the receiver, the modes A and B are inputs. When "0"("1") is registered on the cell, $|\Psi_2\rangle_{\mathrm{AB}}$ ($|\Psi_4\rangle_{\mathrm{AB}}$) is inputted to the receiver.
3. An optimum quantum measurement is performed at the receiver. It is possible to read bits using the orthogonality between $|\Psi_2\rangle_{\mathrm{AB}}$ and $|\Psi_4\rangle_{\mathrm{AB}}$.

*im181001@cis.aichi-pu.ac.jp
†id191002@cis.aichi-pu.ac.jp
‡usuda@ist.aichi-pu.ac.jp

We consider the model with non-symmetric loss. Specifically, only mode B of the quasi-Bell state $|\Psi_2\rangle_{\rm AB}$ is attenuated. In quantum reading, modes A and B reach the receiver via different paths. In particular, mode B reaches the receiver via a longer path and is reflected on the cell. Thus, mode B is exposed to a stricter environment than that of mode A.

3.2 Received quantum state using quasi-Bell states

Let us consider the received quantum state using the quasi-Bell state $|\Psi_i\rangle_{\rm AB}$ $(i = 1, 2)$ when the information recorded on a memory cell is "0". In sending to the cell, mode B is inputted in an attenuated channel. The loss incurred by this channel is expressed by the interaction with a vacuum field as an environment mode. Let $\eta(0 \leq \eta \leq 1)$ be its energy transmissivity. Then the interaction between mode B and the environment mode E is

$$\hat{U}_{\rm BE} |\beta\rangle_{\rm B} |0\rangle_{\rm E} = |\sqrt{\eta}\beta\rangle_{\rm B} |\sqrt{1-\eta}\beta\rangle_{\rm E}, \tag{9}$$

where $\hat{U}_{\rm BE}$ is a unitary operator corresponding to the interaction. Therefore, when we consider the entanglement between modes A and B, the composite system of modes A, B, and E is

$$|\Psi_i\rangle_{\rm ABE} = (\hat{I}_{\rm A} \otimes \hat{U}_{\rm BE})(|\Psi_i\rangle_{\rm AB} \otimes |0\rangle_{\rm E}), \tag{10}$$

where $\hat{I}_{\rm A}$ is the identity operator of mode A. The received quantum state $\rho_0^{(\rm A\otimes B)}$ is obtained performing the partial trace over mode E for $|\Psi_i\rangle_{\rm ABE} \langle\Psi_i|$.

$$\rho_0^{(\rm A\otimes B)} = {\rm Tr}_{\rm E} |\Psi_i\rangle_{\rm ABE} \langle\Psi_i|. \tag{11}$$

Consider the received quantum state when the information recorded on the cell is "1". The light of mode B is attenuated and reflected and is phase shifted by π.

The phase shift for mode B is

$$U(\theta) |\beta\rangle = |\beta {\rm e}^{-{\rm i}\theta}\rangle, \tag{12}$$

where $U(\theta) = {\rm e}^{-{\rm i}\theta\hat{a}^\dagger\hat{a}}$, $\hat{a}$ is the photon annihilation operator, and ${\rm i} = \sqrt{-1}$ is the imaginary unit. When the phase of mode B of $|\Psi_i\rangle_{\rm AB}$ shifts by π, $|\Psi_i\rangle_{\rm AB}$ changes into $|\Psi_{i+2}\rangle_{\rm AB}$. For example, when $i = 2$,

$$\begin{aligned}(\hat{I}_{\rm A} \otimes U(\pi)_{\rm B}) |\Psi_2\rangle_{\rm AB} &= h_2(|\alpha\rangle_{\rm A} |-\beta\rangle_{\rm B} - |-\alpha\rangle_{\rm A} |\beta\rangle_{\rm B}) \\ &= |\Psi_4\rangle_{\rm AB}. \end{aligned} \tag{13}$$

The energy loss for mode B is expressed in the same way as if the information recorded on the cell is "0". Therefore, when we consider entanglement between modes A and B, the composite system among modes A, B, and E is

$$|\Psi_{i+2}\rangle_{\rm ABE} = (\hat{I}_{\rm A} \otimes \hat{U}_{\rm BE})(|\Psi_{i+2}\rangle_{\rm AB} \otimes |0\rangle_{\rm E}). \tag{14}$$

The received quantum state $\rho_1^{(\rm A\otimes B)}$ is obtained by performing the partial trace over mode E for $|\Psi_{i+2}\rangle_{\rm ABE} \langle\Psi_{i+2}|$ and described by

$$\rho_1^{(\rm A\otimes B)} = {\rm Tr}_{\rm E} |\Psi_{i+2}\rangle_{\rm ABE} \langle\Psi_{i+2}|. \tag{15}$$

4 Property of error probability

4.1 Analytical expression of error probability

The error probability of an optimum quantum measurement[13] for quantum reading is calculated using the positive eigenvalues λ's of $\rho_0^{(\rm A\otimes B)} - \rho_1^{(\rm A\otimes B)}$. The error probability is

$$P_{\rm e} = \frac{1}{2}\left(1 - \sum_{\lambda>0} \lambda\right). \tag{16}$$

We express quasi-Bell states by matrices to calculate eigenvalues of $\rho_0^{(\rm A\otimes B)} - \rho_1^{(\rm A\otimes B)}$. To express quasi-Bell states by matrices, we use the orthonormal basis $\{|\omega_0\rangle, |\omega_1\rangle\}$ shown in [14]. Here, $|\omega_0\rangle$ and $|\omega_1\rangle$ are measurement states for the square-root measurement(SRM)[15]. Since SRM for $|\alpha\rangle$ and $|-\alpha\rangle$ is the optimum quantum measurement that minimizes the average error probability, using the measurement states, $|\alpha\rangle$ and $|-\alpha\rangle$ are written as two-dimensional vectors[16, 17]. $|\sqrt{\eta}\beta\rangle$ and $|-\sqrt{\eta}\beta\rangle$ are expressed by two-dimensional vectors in the same way. Using these vectors, we can easily obtain eigenvalues of $\rho_0^{(\rm A\otimes B)} - \rho_1^{(\rm A\otimes B)}$.

From these eigenvalues, the error probability $P_{\rm e}^{\rm max}$ using the maximum quasi-Bell state is

$$P_{\rm e}^{\rm max} = \frac{1 - \kappa_{\rm A}\kappa_{\rm B} - \sqrt{(1-\kappa_{\rm A}^2)(1-\kappa_{\rm B}'^2)}}{2(1-\kappa_{\rm A}\kappa_{\rm B})}, \tag{17}$$

and the error probability $P_{\rm e}^{\rm non-max}$ using the non-maximum quasi-Bell state is

$$P_{\rm e}^{\rm non-max} = \frac{1 + \kappa_{\rm A}\kappa_{\rm B} - \sqrt{(1-\kappa_{\rm A}^2)(1-\kappa_{\rm B}'^2)}}{2(1+\kappa_{\rm A}\kappa_{\rm B})}. \tag{18}$$

4.2 Comparison of properties using maximum and non-maximum quasi-Bell states

Figure. 1 shows the error probability when the amplitude of mode B is one and the transmissivity is 0.9; let the amplitude of mode A change from 0 to 2. The blue and red lines show the error probabilities using the non-maximum quasi-Bell state $|\Psi_1\rangle_{\rm AB}$ and using the maximum quasi-Bell state $|\Psi_2\rangle_{\rm AB}$, respectively. From this figure, in quantum reading with non-symmetric loss, the error probability using the maximum quasi-Bell state is lower than that using the non-maximum quasi-Bell state. Moreover, the more the amplitude of mode A increase, the more difference of two error probabilities decrease.

We confirm these things analytically. First, we investigate that $P_{\rm e}^{\rm non-max}$ is greater than $P_{\rm e}^{\rm max}$. From $0 \leq \kappa_{\rm A}, \kappa_{\rm B}, \kappa_{\rm B}' \leq 1$, $P_{\rm e}^{\rm non-max} - P_{\rm e}^{\rm max}$is

$$\begin{aligned} P_{\rm e}^{\rm non-max} - P_{\rm e}^{\rm max} &= \frac{\kappa_{\rm A}\kappa_{\rm B}\sqrt{(1-\kappa_{\rm A}^2)(1-\kappa_{\rm B}'^2)}}{2(1-\kappa_{\rm A}^2\kappa_{\rm B}^2)} \\ &> 0. \end{aligned} \tag{19}$$

Thus, $P_{\rm e}^{\rm non-max}$ is greater than $P_{\rm e}^{\rm max}$.

Next, we calculate $\lim_{\alpha\to\infty} P_{\rm e}^{\rm non-max}$ and $\lim_{\alpha\to\infty} P_{\rm e}^{\rm max}$. Because $\kappa_{\rm A}$ goes to 0 when α goes

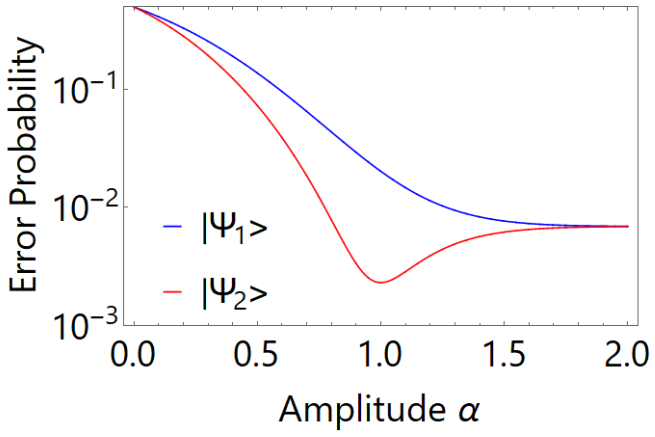


Figure 1: Error probabilities with respect to the amplitude α using $|\psi_1\rangle$ and $|\psi_2\rangle$ where the amplitude $\beta = 1$ and transmissivity $\eta = 0.9$.

to infinity, $\lim_{\alpha\to\infty} P_{\rm e}^{\rm non-max}$ and $\lim_{\alpha\to\infty} P_{\rm e}^{\rm max}$ are

$$\lim_{\alpha\to\infty} P_{\rm e}^{\rm max} = \lim_{\alpha\to\infty} P_{\rm e}^{\rm non-max} = \frac{1}{2}\left(1 - \sqrt{1-\kappa_{\rm B}'^2}\right). \tag{20}$$

Therefore, the more the amplitude of mode A increase, the more the difference decrease.

5 Conclusion

For quantum reading with non-symmetric loss, we compared the error probabilities using the maximum quasi-Bell state and using the non-maximum quasi-Bell state. As a consequence, the error probability using the maximum quasi-Bell state is lower than that using the non-maximum quasi-Bell state, and the more the amplitude of mode A increase, the more the difference of two error probabilities decrease.

Acknowledgment

This work has been supported in part by JSPS KAKENHI Grant Number JP16H04367. K. Ishikawa has been supported from Marubun Research Promotion Foundation.

References

[1] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, "Mixed state entanglement and quantum error correction," Phys. Rev. **A54**, pp.3824-3851, (1996).

[2] 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**, pp.1895-1899, (1993).

[3] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, (2000).

[4] S. Pirandola, "Quantum reading of a classical digital memory," Phys. Rev. Lett. **106**, 090504, (2011).

[5] O. Hirota and M. Sasaki, "Entangled state based on nonorthogonal state," Proc. QCM&C-Y2K, pp.359-366, (2001).

[6] S.J. van Enk and O. Hirota, "Entangled coherent states: Teleportation and decoherence," Phys. Rev. **A64**, 022313, (2001).

[7] O. Hirota, "Error free quantum reading by quasi Bell state of entangled coherent states," Quantum Measurements and Quantum Metrology **4**, pp.70-73, (2017). arXiv:quant-ph/1108.4163v2, (2011).

[8] K. Kato and O. Hirota, "Effect of decoherence in quantum reading with phase shift keying signal of entangled coherent states," Proc. SPIE **8875**, (2013).

[9] K. Ishikawa, T. Wang, and T.S. Usuda, "Effect of non-symmetric loss on quantum reading using a quasi-Bell state," Proc. of ISITA2018, pp.467-471, (2018).

[10] H. Prakash and M.K. Mishra, "Increasing average fidelity by using non-maximally entangled resource in teleportation of superposed coherent states," arXiv:quant-ph/1107.2533, (2011).

[11] J. Joo, W.J. Munro, and T.P. Spiller, "Quantum metrology with entangled coherent states," Phys. Rev. Lett. **107**, 083601, (2011).

[12] S. Yamaguchi, H. Takeuchi and T.S. Usuda, "Property of a capacity of quantum channel assisted by a non-maximum quasi-Bell state," 2012 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, O1-5, (2012). (in Japanese)

[13] C.W. Helstrom, *Quantum detection and estimation theory*, Academic Press, New York, (1976).

[14] H. Takeuchi, S. Yamaguchi, and T.S. Usuda, "Entanglement-assisted classical communication using quasi Bell states," Proc. 1st International Workshop on ECS and Its Application to QIS, T.S. Usuda and K. Kato (Eds.), Tamagawa Univ. Quant. ICT Res. Inst., pp.115-119, (2013).

[15] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, "Classical information capacity of a quantum channel," Phys. Rev. **A54**, pp.1869-1876, (1996).

[16] M. Osaki, M. Ban, and O. Hirota, "Derivation and physical interpretation of the optimum detection operators for coherent-state signals," Phys. Rev. **A54**, pp.1691-1701, (1996).

[17] M. Sasaki and O. Hirota, "Two examples of measurement processes illustrating Helstrom's optimum decision bound," Phys. Lett. **A210**, pp.21-25, (1996).

Efficient Quantum Algorithm for Solving Traveling Salesman Problem

Hyunseong Jang[1] * Jihwan Kim[1] † younghun Kwon[1] ‡

[1] *Department of applied physics, Hanyang University*

Abstract. Traveling Salesman Problem(TSP) is problem that find the optimum cycle for visiting every city and returning to starting city. In order to find the solution for TSP, there have been many approaches. Recently, Srinivasan et al. (2018) discussed a quantum algorithm for TSP, using Qunatum Phase Estimation(QPE). Their approach uses TSP database corresponding to every cycle and its cycle length. Even though the optimum cycle should be found in TSP database, they could not provide the systemtic way to construct Grover operator for it. Futhermore, they considered only a eigenvector for one cycle. In this paper, we provide a method of finding the optimum cycle state in the superposition by running quantum algorithm. Specially, by applying Quantum Counting Algorithm(QCA) we determine whether there is a cycle shorter than the given length L. If a cycle shorter than L exists, by performing a Grover Search Algorithm(GSA), we find the cycle. By considering the Symmetric 4 City TSP, we show the effectiveness of our proposal.

Keywords: Traveling Salesman Problem,Quantum Algorithm, Quantum Counting Algorithm, Grover Search Algorithm

1 Introduction

Traveling Salesman Problem(TSP) is a famous problem in computer science. TSP is to find a optimum cycle where salesman travels from a starting city, visits every city and returns to the starting city. TSP is known as a NP-hard problem in combinatorial optimization, which takes exponential time order for solving it. There are many variations of TSP and solving TSP can be widely applied to many fields. Therefore, solving TSP is important.

The classical approach for solving TSP is divided into two categories. The first is an approach to find an exact solution such as branched and bound method[2-4]. The exact solution approach can find an optimal solution, but it needs enormous time for calculation. The second approach is an approximate one such as heuristic method[5-7]. The approximate approach requires a short calculation time, but one cannot guarantee that the obtained solution is optimal.

On the other hand, there have been researches for finding a solution of TSP by using quantum physics. Martonak et al. (2004) [8] applied quantum annealing to solving TSP. They showed that quantum annealing may be better than simulated annealing. Bang et al. (2012) [9] proposed quantum heuristic algorithm by Grover Search Algorithm(GSA). However, as mentioned earlier, one cannot guarantee that the solution obtained by the Heuristic algorithm is optimal. Therefore, it is important to decide whether a cycle with a given length shorter than L exists. This is called a TSP decision problem.

Recently, Srinivasan et al. (2018) [10] discussed a method of encoding distance between cities in a phase corresponding to the eigenvector of the unitary matrix. In their method one can build TSP database corresponding to every cycle and its cycle length, by performing Quantum Phase Evaluation(QPE). The quantum state to optimum cycle can be found by Quantum Algorithm for finding minimum. In order to perform Quantum Algorithm for finding minimum, Grover operator should be constructed, but they did not discuss the method to find Grover operator. Further, even though one should consider superposed states for every cycle, they considered only an eigenvector for one city and evaluated a cycle length corresponding to the cycle.

In this paper, we explain the method to construct Grover operator and propose the way to find optimum cycle in TSP database, by considering Quantum Counting Algorithm(QCA). Even though Quantum Algorithm for finding minimum depends on GSA which does not know the rotation angle of Grover operator, by QCA we can find the rotation angle of Grover operator. Because the rotation angle is related with the number of cycle which is shorter than the given length, finding the rotation angle is important in solving TSP decision problem.

As an example, we consider symmetric 4 City TSP. By preparing superposed quantum states, we build TSP database. By GSA, we can find the optimum cycle for symmetric 4 City TSP. It should be noted that our proposal can be applied not only to the case of asymmetric distance between cities but also to the case of many cities.

2 Method

Let us construct the Grover operator G for a target state corresponding to a cycle shorter than given length L. If the rotation angle of the Grover operator G is zero, there exists a cycle shorter than L. If the rotation angle of the Grover operator G is not zero, there is no cycle shorter than L. Quantum counting algorithm tells the rotation angle θ of Grover operator G.

Here, we propose the method to solve TSP optimization. we consider a situation where the rotation angle θ obtained by a QCA is not zero. In other words, there exists a cycle shorter than a given L. Because we know the rotation angle θ of Grover operator G, we can prop-

*mslab.jang@gmail.com
†mslab.k@gmail.com
‡yyhkwon@hotmail.com

Table 1: The table of cycle, cycle length and eigenvector. QPE for each eigenvector can be performed to obtain the state corresponding to cycle length.

NO.	Cycle	Cycle length	Eigenvector
1	$0 \to 1 \to 2 \to 3 \to 0$	$\frac{9}{8}\pi$	$\|3012\rangle$
2	$0 \to 3 \to 2 \to 1 \to 0$	$\frac{9}{8}\pi$	$\|1230\rangle$
3	$0 \to 1 \to 3 \to 2 \to 0$	π	$\|2031\rangle$
4	$0 \to 2 \to 3 \to 1 \to 0$	π	$\|3012\rangle$
5	$0 \to 2 \to 1 \to 3 \to 0$	$\frac{7}{8}\pi$	$\|3201\rangle$
6	$0 \to 3 \to 1 \to 2 \to 0$	$\frac{7}{8}\pi$	$\|2310\rangle$

erly repeat Grover operator G to maximize the weight of the state corresponding to a cycle shorter than L. Therefor, Grover search algorithms can find a state that corresponds to a cycle shorter than L.

Next, we evaluate the cycle length of the newly found cycle with the GSA. The calculated cycle length can be regarded as the new L. To obtain a rotation angle of θ, we perform GSA considering new length L. If $\theta =$ is zero, the new cycle is the optimum cycle. Otherwise, with the GSA we find a cycle shorter than new L. We can find the optimum cycle by repeating this process.

3 Simulation : Symmetric 4 City TSP

Let us consider symmetric 4 City TSP. We denote the city numbers as 0, 1, 2 and 3, respectively. ϕ_{xy} means a distance from city x to city y. Let us consider the following Unitary matrix U:

$$U = U_0 \otimes U_1 \otimes U_2 \otimes U_3$$

$$U_m = e^{i\phi_{0m}} |0\rangle \langle 0| + e^{i\phi_{1m}} |1\rangle \langle 1| + e^{i\phi_{2m}} |2\rangle \langle 2| + e^{i\phi_{3m}} |3\rangle \langle 3|$$

The phase corresponding to the eigenvector of U is the sum of the distances between cities and some of these phases can be cycle lengths. That is, some eigenvector of U corresponds to a specific cycle. Further, the phase of some eigenvector corresponds to a specific cycle length.

There are six possible cycles in the 4 city TSP. Therefore, the number of eigenvectors becomes six. We consider a situation in which the distances between cities are symmetric to simplify the problem. In detail, the distances between cities are given as $\phi_{01} = \phi_{10} = \pi/2$, $\phi_{02} = \phi_{20} = \pi/8$, $\phi_{03} = \phi_{30} = \pi/4$, $\phi_{12} = \phi_{21} = \pi/4$, $\phi_{13} = \phi_{31} = \pi/4$, $\phi_{23} = \phi_{32} = \pi/8$.

Because distances between cities are symmetric, cycle 1 and 2, cycle 3 and 4, and cycle 5 and 6 have the same cycle length as shown in Table 1. In other words, there are three cycles to be considered. Our simulation prepares superposition state of cycle 1, cycle 3, cycle 4 and cycle 6. This superposition include all the cycles of 4 city symmetric TSP.

First, let us consider the following decision problem, "Is there a cycle that is shorter than $L = \pi$?" Because there are four total cycles and one cycle shorter than π (cycle 6), the rotation angle θ estimated by QCA is 60°.

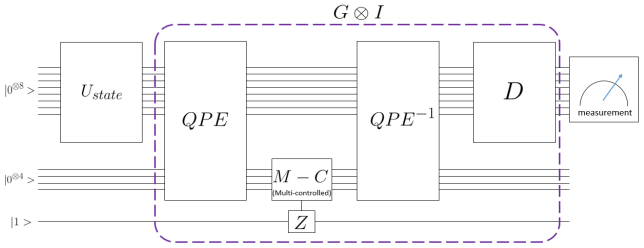


Figure 1: Algorithm for finding a cycle that is shorter than a given length of L. Through QPE, one constructs superposition corresponding to every cycle and its cycle length. Afterwards, the multiple controlled Z gate is applied to the cycle length state to change the sign. Then, Inverse QPE and Diffusion operator D are applied sequentially. This series of processes can be considered as Grover operator G applied to cycle state.

This means that the GSA, which performs the Grover operator G one time as shown in Figure 1, can find the opitmum cycle.

Even though we provide a simple example of symmetric 4 city TSP, we can see how effective our method is. The method we propose can be consistently applied even to asymetric TSP. Further, our proposal can be used for solving TSP of many cities. In addition, the proposed method may minimize costs for obtaining the optimum solution of optimization problem that can be replaced by a TSP.

References

[1] R. Matai, S. P. Singh, and M. L. Mitta. *Traveling Salesman Problem: An Overview of Applications, Formulations, and Solution Approaches.* IntechOpen, 2010.

[2] J. D. C. Little, K. G. Murty, D. W. Sweeney, and C. Karel. An Algorithm for the Traveling Salesman Problem. *Operations Res. 11*, pages 972-989, 1963.

[3] E. L. Lawler and D. E Wood. Branch-and-Bound Methods: A Survey. *Operations Res. 14*, pages 699-719, 1966.

[4] M. Padberg and G. Rinaldi. Optimization of a 532-city symmetric traveling salesman problem by branch and cut. *Operations Res. Lett. 6*, pages 1-7, 1987.

[5] R. L. Karg, and G. L. Thompson. A Heuristic Approach to Solving Travelling Salesman Problems. *Manage. Sci. 10*, pages 225-248, 1964.

[6] S. Lin and W. Kernighan. An Eective Heuristic Algorithm for the Traveling Salesman Problem. *Operations Res. 21*, pages 498-516, 1973.

[7] Z. W. Geem, J. H. Kim, and G. V. Loganathan. A new heuristic optimization algorithm: Harmony search. *Simulation 76*, pages 60-68, 2001.

[8] R. Martonak, G. E. Santoro and E. Tosatti. Quantum annealing of the traveling salesman problem. *Phy. Rev. E 70*, 057701, 2004.

[9] J. Bang, S. Yoo, J. Lim, J. Ryu, C. Lee and J. Lee. Quantum heuristic algorithm for traveling salesman problem. *J. Korean Phys. Soc. 61*, 1944-1949, 2012.

[10] K. Srinivasan, S. Satyajit, B. K. Behera and P. k. Panihrahi. Ecient quantum algorithm for solving travelling salesman problem: An IBM quantum experience. *arXiv preprint*, arXiv:1805.10928, 2018.

[11] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th ACM STOC*, pages 212–219, 1996.

[12] G. Brassard , P. Hoyer and A. Tapp. Quantum Computing. *LNCS 1443*, pages 820–831, 1998.

Performance Evaluation of Ghost Imaging with Orthogonal/Non-orthogonal Quantum States

Yuto Takahashi[1] * Keita Ishikawa[2] † Shogo Usami[1] ‡ Tsuyoshi Sasaki Usuda[2] §

[1] *Graduate School of Science and Engineering, Meijo University, 1-501 Shiogamaguchi, Tempaku-ku, Nagoya-shi, Aichi 468-8502, Japan.*
[2] *Graduate School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi 480-1198, Japan.*

Abstract. Entangled states constructed from non-orthogonal quantum states have exhibited superior performance for several application protocols. Nevertheless, the performance for each application protocol using these states differs. However, with regard to non-orthogonal states, the performance of quantum ghost imaging has not been considered. Quantum ghost imaging is an imaging technique that exploits entangled states. In this work, we compare the performances when using orthogonal quantum states and when using non-orthogonal quantum states.

Keywords: non-orthogonal quantum states, quantum ghost imaging, quantum protocol

1 Introduction

As an important resource in quantum protocols[1], entanglement is a nonlocal correlation among multiple quantum systems; quantum states with such correlations are called entangled states. Examples of protocols using entanglement are quantum teleportation[2], quantum dense coding[3], and quantum ghost imaging[4]. The Bell state, which is constructed from orthogonal quantum states, is the most famous and fundamental of the entangled states. However, there are other unique entangled states; some are constructed using non-orthogonal quantum states, and are called quasi-Bell states. Some quasi-Bell states are comparable to Bell states under ideal circumstances. For examples, some states achieve maximum entanglement although they are constructed from non-orthogonal states[5]. Furthermore, in non-ideal circumstances such as energy attenuation, some quasi-Bell states show more superior performance than Bell states.

For these reasons, we focus in this work on quantum ghost imaging as the use of non-orthogonal quantum states has yet to be considered. Moreover, we reveal the characteristics of ghost imaging using both orthogonal and non-orthogonal quantum states subject to attenuation. In addition, we reveal the characteristics when changing the average number of photons. Therefore, we analyzed the fundamental characteristics using product states to account in particular for the differences in the orthogonal and non-orthogonal states.

2 Quantum ghost imaging

2.1 Our model of quantum ghost imaging

Ghost imaging is an imaging technique using a detector without spatial resolution and another with spatial resolution. Originating with the experiment by Pittman *et al.*[4], various experiments and theories concerning ghost imaging have been published.

In this work, we consider binary imaging in the form of a slit set up on the object or in the shadow of an illuminated object. In a simplified setup of ghost imaging (Fig. 1), D_A represents the detector having no spatial resolution, D_B represents the detector that has spatial resolution, S represents the object that has a slit (or just an object), and C represents a correlator. In addition, D_B can be substituted for a detector without spatial resolution having an extremely small hole for the light-receiving part and detecting light only in that part. For an example of an object, Fig. 2 shows a filled M-letter, which is an ideal imaging output.

We use D_A to detect the light that transits the slit in the object (or not obstructed when in shadow-viewing mode; hereinafter, we assume an object with slit). However, we cannot obtain an image using only D_A because D_A does not have spatial resolution and we are unable to determine the position of the light. Similarly, we cannot obtain an image using only D_B because D_B is illuminated directly and the light does not transit the object. Nevertheless, if the light illuminating the two detectors is spatially correlated, we can determine the position of the light using D_B when the light transits the slit in the corresponding position using D_A. Hence, correlating the output from the two detectors creates the ghost image of the slit. Because we consider only binary imaging in this work, the correlation means that if both of the detectors are illuminated, we record a '1' in that position, otherwise, we record a '0'. Moreover, we consider that there is a $d \times d$-point lattice within the frame of Fig. 2 and a corresponding plane on D_B, and we are using an optimum quantum receiver. The specific procedure is to repeat the following steps for all lattice points.

1. illuminating two light beams correlated spatially to only those parts of the object with the slit and using the detector that has spatial resolution
2. detecting the light transiting the slit on D_A

*193426007@ccmailg.meijo-u.ac.jp
†im181001@cis.aichi-pu.ac.jp
‡susami@meijo-u.ac.jp
§usuda@ist.aichi-pu.ac.jp

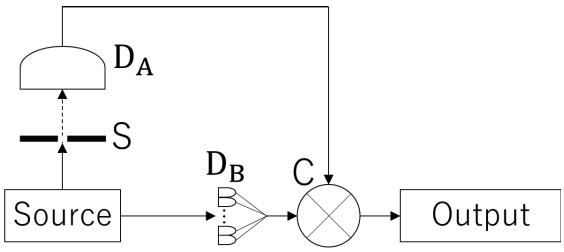


Figure 1: Schematic setup for the ghost imaging, where D_A represents the detector having no spatial resolution, D_B represents the detector that has spatial resolution, S represents the object, and C represents a correlator.

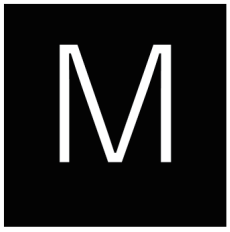


Figure 2: Object with M-shaped hole.

3. detecting the light illuminated from the source directly at each lattice point

4. correlating the outputs from the two detectors and recording the result for each lattice point of D_B

In addition, we assume there is only an attenuation for the imperfect factor of the system. Hereinafter, let η be the energy transmissivity for all systems.

3 Quantum states used in this work

Let the system illuminate the lattice point (i, j) with i, j are natural numbers, as detailed in section 2, $A_{i,j}$ $B_{i,j}$ $(1 \leq i, j \leq d)$. Moreover, we consider for spatially correlated quantum states the product states

$$|\Psi_{i,j}\rangle = |0_L\rangle_{A_{1,1}} |0_L\rangle_{B_{1,1}} \cdots |1_L\rangle_{A_{i,j}} |1_L\rangle_{B_{i,j}} \cdots |0_L\rangle_{A_{d,d}} |0_L\rangle_{B_{d,d}}, \quad (1)$$

where $|0_L\rangle$, $|1_L\rangle$ are basic quantum bits corresponding to logical bits '0' and '1'.

Taking the photon number state $|0\rangle$ for which the number of photons is 0 as the logic state $|0_L\rangle$ and the photon number state $|n\rangle$ for which the number of photons is n as logic state $|1_L\rangle$, we obtain the product states from the state in Eq. (1). In this work, we utilize these states as the orthogonal quantum states in quantum ghost imaging.

On the other hand, taking the coherent state $|0\rangle$ for which the amplitude is 0 for $|0_L\rangle$ and coherent state $|\alpha\rangle$ for which the amplitude is α for $|1_L\rangle$, we obtain the product states from the state in Eq. (1). In this work, we apply this quantum state as non-orthogonal quantum states in quantum ghost imaging. In addition, it is known that these quantum states when constructed by a non-orthogonal quantum bit show better performance such as resistance against attenuation than those constructed from the orthogonal quantum states[6].

3.1 Attenuation for quantum states

We next consider instances where all systems $A_{i,j}$ and $B_{i,j}$ are attenuated. However, the model for attenuation in a single system is fundamental. For this reason, we describe this single-system instance first. Let $\rho^{(in)}$ be the quantum state before attenuation and $\rho^{(out)}$ be the state attenuated with an energy transmissivity of η. We obtain

$$\rho^{(out)} = \sum_{k=0}^{\infty} E_k(\eta) \rho^{(in)} E_k(\eta)^\dagger, \quad (2)$$

where $E_k(\eta)$ is the Kraus operator[8] for an energy transmissivity η. The right-hand side of the Eq. (2) is called the Kraus representation[7]. The Kraus operator has expansion

$$E_k(\eta) = \sum_{n=0}^{\infty} \sqrt{\binom{n}{k}} \sqrt{\eta^{n-k}(1-\eta)^k} \, |n-k\rangle \langle n| . \quad (3)$$

Because the quantum states used in this work are product states of multiple systems, the quantum state that has attenuated $\rho^{(out)}$ is described in an extension of Eq. (2) by

$$\rho^{(out)} = \sum_{k_{1,1}=0}^{\infty} \cdots \sum_{k_{d,d}=0}^{\infty} (E_{k_{1,1}} \cdots E_{k_{d,d}}) \rho^{(in)} (E_{k_{1,1}} \cdots E_{k_{d,d}})^\dagger. \quad (4)$$

4 Result

We use two detectors for different purpose and it is necessary to obtain correct output from both detectors for ghost imaging. Therefore, if an error occurs on either D_A or D_B, imaging fails. Moreover, we consider the average error rate of ghost imaging using orthogonal and non-orthogonal quantum states. Now, let the area fractions of the slit part and the remainder of the whole object be denoted ξ_0 and ξ_1, respectively. In this case, we use the optimum quantum receiver constructed with *a priori* probabilities $|0_L\rangle$ and $|1_L\rangle$ on D_A, ξ_0 and ξ_1, at the minimum error rate. Likewise, we use the optimum quantum receiver constructed with *a priori* probabilities, $(d^2-1)/d^2$ and $1/d^2$, on D_B at the minimum error rate.

When using a binary quantum state signal with *a priori* probabilities ξ_0 and ξ_1, the error rate $P_e^{(opt)}$ is calculated using

$$P_{e-(opt)} = \xi_0 - \sum_{\lambda_+} \lambda_+, \quad (5)$$

where $\rho_0^{(out)}$ and $\rho_1^{(out)}$ are received quantum states, and λ_+ is a positive eigenvalue of $\xi_0 \rho_0^{(out)} - \xi_1 \rho_1^{(out)}$. When using orthogonal quantum states, the error from $|0\rangle$ to $|n\rangle$ does not occur because we only consider attenuation. Therefore, when light illuminates the remaining part rather than the slit part of the object, errors do not

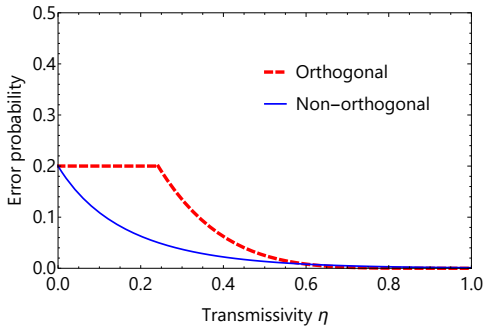


Figure 3: Error probability of ghost imaging by using the orthogonal and non-orthogonal quantum states, where $N_{\rm S} = 5$, $\xi_{\rm A1} = 0.8$.

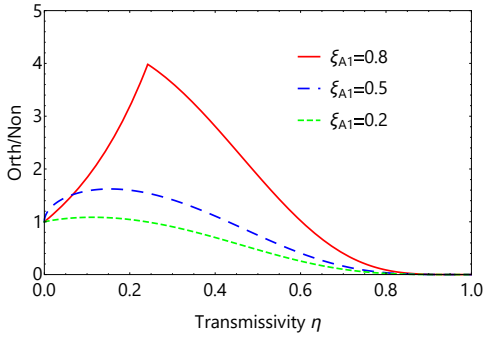


Figure 4: Ratio of error probabilities with the orthogonal to non-orthogonal quantum states, where $N_{\rm S} = 5$.

occur. For this reason, using Eq. (5), the error rate at the optimum quantum receiver becomes

$$P_{e-(\rm opt)}^{(\rm orth)} = \min\left\{\xi_1(1-\eta)^n,\ \xi_0\right\}. \tag{6}$$

Otherwise, when using non-orthogonal quantum states, using Eq. (5), the error rate at the optimum quantum receiver becomes

$$P_{e-(\rm opt)}^{(\rm non-orth)} = \frac{1}{2}\left(1-\sqrt{1-4\xi_0\xi_1 \mathrm{e}^{-\eta\alpha^2}}\right). \tag{7}$$

Using these error rate at receivers, we consider the average error probability of ghost imaging P_e. Because we should consider the probability when error does not occur at either $\rm D_A$ or $\rm D_B$, we obtain

$$P_e = 1-(1-P_{\rm A})(1-P_{\rm B}), \tag{8}$$

where $P_{\rm A}$ and $P_{\rm B}$ are the error rates at detectors $\rm D_A$ and $\rm D_B$, respectively. For these error rates, we use Eqs. (6) and (7) when using orthogonal and non-orthogonal quantum states, respectively.

The error probabilities, Eqs. (6) and (7), as functions of transmissivity η ranging from 0 to 1 where the average number of photons is $N_{\rm S} = 5$ and the area fraction for the slit part is $\xi_{\rm A1} = 0.8$ is shown in Fig. 3. In these plots, in the region where η is small, that is, the amount of attenuation is large, the error rate for ghost imaging using non-orthogonal quantum state is less than the error rate using orthogonal quantum state.

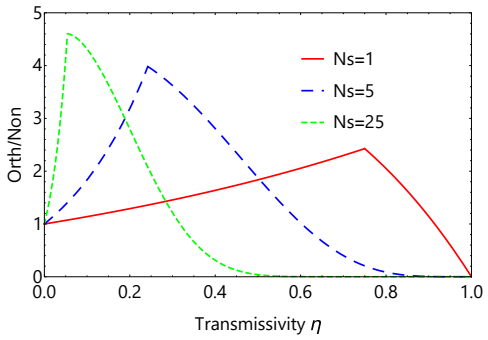


Figure 5: Ratio of error probabilities with the orthogonal to non-orthogonal quantum states, where $\xi_{\rm A1} = 0.8$.

In addition, the ratio of the error probability with the orthogonal quantum state to the error probability with non-orthogonal quantum state, where $N_{\rm S} = 5$ is shown in Fig. 4. Similarly, the ratio, where $\xi_{\rm A1} = 0.8$ is shown in Fig. 5. Also in these plots, in the region where η is small, the ratio is greater than 1, that is non-orthogonal quantum state offers better performance. Moreover, the larger slit area is and the smaller $N_{\rm S}$ is, the wider the range that non-orthogonal quantum state offers better performance is. On the other hand, when the $N_{\rm S}$ is large, the range is narrow, but the maximum of the ratio of error probabilities is large. We believe that the difference between results when using orthogonal and non-orthogonal quantum states is caused depending on how the errors occur. Specifically, the error when using the non-orthogonal quantum state occurs in all part of the object, but the error when using the orthogonal quantum state occurs in only slit part of the object.

5 Conclusion

We have applied non-orthogonal quantum states in quantum ghost imaging showing its superior robustness against attenuation. As a result, if the amount of attenuation is large, quantum ghost imaging using non-orthogonal quantum states offers a better performance. Moreover, the larger slit area or the smaller average number of photons is, the wider the range that non-orthogonal quantum state offers better performance is.

Our future work is assessing if transmissivity is different in other systems and whether optimization for quantum ghost imaging is possible by means other than the minimum error rate.

Acknowledgements: This work has been supported in part by JSPS KAKENHI Grant Number JP16H04367. We thank Richard Haase, Ph.D., from Edanz Group (www.edanzediting.com/ac) for editing a draft of our manuscript.

References

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," Phys. Rev. **A54**, pp.3824-3851, (1996).

[2] 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**, pp.1895-1899, (1993).

[3] C. H. Bennett and S. J. Wiesner, "Communication via 1- and 2-particle operators on Einstein-Podolsky-Rosen states," Phys. Rev. Lett. **69**, pp.2881-2884, (1992).

[4] 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).

[5] O. Hirota and M. Sasaki, "Entangled states based on non-orthogonal states," Proc. QCMC-Y2K, pp.359-366, (2001).

[6] R. Yamamoto, S. Hattori, T. S. Usuda, and I. Takumi, "Entanglement of formation of a quasi-Bell state with non-symmetric loss," IEEJ Transactions on Electronics, Information and Systems **126**, no.12, pp.1531-1532, (2006).

[7] K. Kraus, Lectures in Mathematical Physics at the University of Texas at Austin **190**, Springer-Verlag, (1983).

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, (2000).

Masking Quantum Information and Hyperdisks

Feng Ding[1] Xueyuan Hu[1] *

[1] *School of Information Science and Engineering, Shandong University, Qingdao 266237, China*

Abstract. Masking information protocol is a protocol that encode (mask) quantum information into bipartite entanglement while the information is completely unknown to local system. This work explicitly studies the structure of the set of maskable states and its relation to hyperdisks. We prove that maskable qubit states locate on single hyperdisk, though it is not true for higher dimension case. Our results may shed light on several research fields of quantum information theory, such as the structure of entangled states and local discrimination of bipartite states.

Keywords: masking quantum information, hyperdisk, maskable states

1 Introduction

Recently, Ref. [1] proposed a masking quantum information protocol, which encodes quantum information into non-local correlation completely. They derived a new no-go theorem called no-masking theorem, which claims that although one can encode classical information into entanglement, masking arbitrary quantum states is impossible. Still, one can go beyond classical world and mask a set of non-orthogonal quantum states into bipartite system. Furthermore, Ref. [2] generalized the protocol and prove that is possible to mask full quantum information into multipartite systems.

Although no-masking theorem has been proved, the structure of set of maskable states is still unknown. Ref. [1] proposed a masker using generalized control-NOT gate. Based on that masker, Ref. [1] conjeced that any set of maskable states must live on some disk.

In this work, we prove that the conjecture holds for qubit case, while it fails for general higher dimensional case. First, we give a clear definition of hyperdisk and introduce some related concepts. Then we study the classification of masking protocol, depending on the dimension of input space n, the Schmidt number of target states d and the degeneracy of marginal states. General methods are provided to derive the structure of maskable states in different cases. Based on those methods, we show that the maskable states may live on two or more different hyperdisks if $n \geq 3$, and we give a full characterization of maskable states for $n = 2, d \geq 2$ and $n = 3, d = 3$.

2 Hyperdisk and related concepts

Let $\mathcal{H}$ be an n-dimensional Hilbert space and $\mathcal{B} := \{|\phi_j\rangle\}_{j=0}^{m-1}$ be an orthonormal basis for some m-dimensional subspace of $\mathcal{H}$, define a real vector for a pure state $|\psi\rangle \in \mathcal{H}$:

$$\boldsymbol{r}_{\mathcal{B}}(|\psi\rangle) := \left(|\langle\phi_0|\psi\rangle|, ..., |\langle\phi_{m-1}|\psi\rangle|\right)^{\mathrm{T}}. \tag{1}$$

Notice that $\boldsymbol{r}_{\mathcal{B}}(|\Psi\rangle)$ is normalized iff $|\psi\rangle \in \mathrm{span}\{\mathcal{B}\}$.

Definition 1 (hyperdisk) *Let $\mathcal{S}$ be a set of pure states within an n-dimensional Hilbert space $\mathcal{H}$. Then $\mathcal{S}$ forms a hyperdisk if there is a complete orthonormal basis $\mathcal{B}$ for m-dimensional subspace $\mathcal{V} := \mathrm{span}\{\mathcal{S}\}$ which satisifies*

$$\boldsymbol{r}_{\mathcal{B}}(|\psi\rangle) \equiv \boldsymbol{r}, \qquad \forall\, |\psi\rangle \in \mathcal{S}, \tag{2}$$

$$\boldsymbol{r}_{\mathcal{B}}(|\xi\rangle) \neq \boldsymbol{r}, \qquad \forall\, |\xi\rangle \in \mathcal{H} \setminus \mathcal{S}. \tag{3}$$

Here $\mathcal{B}$ is called the hyperdisk basis and $m := \dim(\mathcal{V})$ is called the dimension of hyperdisk. In the simplest case $m = 1$, $\mathcal{S}$ consists of only one pure state. For the case $m = 2$, $\mathcal{S}$ can be expressed as $\left\{|\psi(\theta)\rangle = a\,|\phi_0\rangle + be^{i\theta}\,|\phi_1\rangle\,|\theta \in \mathbb{R}\right\}$, where $\{|\phi_0\rangle,|\phi_1\rangle\}$ is an orthonormal basis for $\mathcal{H}_2$. In Bloch representation, $\mathcal{S}$ can be visualized as an intersection between the sphere and some plane, which is orthogonal to crossing line of two antipodal points $|\phi_0\rangle$ and $|\phi_1\rangle$. In general case, any pure state $|\psi\rangle$ in a given m-dimensional hyperdisk $\mathcal{S}$ can be expressed as:

$$|\psi(\boldsymbol{\theta})\rangle = \sum_{j=0}^{m-1} r_j \exp(i\theta_j)\,|\phi_j\rangle\,, \tag{4}$$

where $\theta_j \in [0, 2\pi)$.

Definition 2 (Schmidt hyperdisk) *For bipartite system $\mathcal{H}_{AB}$, hyperdisk $\mathcal{S}^{AB} \subset \mathcal{H}_{AB}$ is a Schmidt hyperdisk if $\mathcal{B}$ is the Schmidt basis of $|\Psi\rangle \in \mathcal{S}^{AB}$.*

As an example, $\mathcal{S} = \{|\Psi(\boldsymbol{\theta})\rangle := |00\rangle + e^{i\theta_0}\,|11\rangle + e^{i\theta_1}\,|22\rangle\}$ is a Schmidt hyperdisk, while $\mathcal{S}' = \{|\Psi(\boldsymbol{\theta})\rangle := |00\rangle + e^{i\theta}(|11\rangle + |22\rangle)\}$ is not since $|11\rangle + |22\rangle$ is entangled. However, $\mathcal{S}'$ is vaild hyperdisk and $\mathcal{S}' \subseteq \mathcal{S}$, which leads to another concept called sub-hyperdisk.

Definition 3 (sub-hyperdisk) *Subset $\mathcal{S}' \subseteq \mathcal{S}$ is a sub-hyperdisk of hyperdisk $\mathcal{S}$ if $\mathcal{S}'$ is also a hyperdisk.*

The sub-hyperdisk is not only class of sub-structure that exists in hyperdisk. Weaker condition can be added to derive a more general structure called regular subset of hyperdisk.

Definition 4 (regular subset of hyperdisk) *A subset $\mathcal{C} \subseteq \mathcal{S}$ is a regular subset of hyperdisk $\mathcal{S}$ if $\mathcal{V}_C \cap \mathcal{S} = \mathcal{C}$, where $\mathcal{V}_C := \mathrm{span}\{\mathcal{C}\}$.*

*xyhu@sdu.edu.cn

The statement $\mathcal{V}_C \cap \mathcal{S} = \mathcal{C}$ is equivalent to that for any linear combination $|\eta\rangle$ of states in $\mathcal{C}$, the condition $|\eta\rangle \in \mathcal{S}$ leads to $|\eta\rangle \in \mathcal{C}$. Every sub-hyperdisk is a regular subset. We define the the dimension of $\mathcal{C}$ as $\dim(\mathcal{V}_C)$. Notice that $\dim(\mathcal{C}) = \dim(\mathcal{S})$ leads to $\mathcal{C} = \mathcal{S}$. To characterize the structure of regular subset $\mathcal{C}$, we define the minimal number of sub-hyperdisks that fully cover $\mathcal{C}$ as the optimal cover number. For the case $\dim(\mathcal{C}) = 2$, we have a lemma below:

Lemma 5 *The optimal cover number for 2-dimensional regular subset is at most 2.*

3 Masking information protocol

A masking information protocol involves three participants: a referee R and two players A and B. Each of them holds a space denoted as $\mathcal{H}_R$, $\mathcal{H}_A$ or $\mathcal{H}_B$. We define $\mathcal{H}_R$ as the input space. For every round of the protocol, the referee randomly chooses a pure state $|\psi\rangle$ in the set of maskable states $\mathcal{R}$ in $\mathcal{H}_R$, and referee puts the state $|\psi\rangle$ into a masking machine.

Definition 6 (masking machine) *The linear isometry*

$$V_{\text{mask}} : \mathcal{H}_R \to \mathcal{H}_A \otimes \mathcal{H}_B \tag{5}$$

is a masking machine for a set of maskable states $\mathcal{R}$ in $\mathcal{H}_R$, if for any $|\psi\rangle$ in $\mathcal{R}$, the marginal states of $|\Psi\rangle = V_{\text{mask}}|\psi\rangle$ are constant, i.e. $\text{Tr}_B(|\Psi\rangle\langle\Psi|) \equiv \rho_A$ and $\text{Tr}_A(|\Psi\rangle\langle\Psi|) \equiv \rho_B$ are independent of $|\psi\rangle$.

In this way, referee can distribute $|\psi\rangle \in \mathcal{R}$ to players without losing any quantum information. Notice that no communication is allowed between two players, so by local operation, they can not gain any information about which state referee has chosen.

The bipartite pure state $|\Psi\rangle$ is denoted by the target state. $\mathcal{T}$ is the set of target states and $\mathcal{V}_T = \text{span}\{\mathcal{T}\}$. The marginal states ρ_A and ρ_B are mixed states if $\mathcal{R}$ contains more than one state, so $|\Psi\rangle$ must be entangled.

The dimension of $\text{span}\{\mathcal{R}\}$ is denoted by n. States that do not live in $\text{span}\{\mathcal{R}\}$ can not be masked, so we set $\mathcal{H}_R = \text{span}\{\mathcal{R}\}$ without loss of generality. And V_{mask} restricts that $\mathcal{H}_R \simeq \mathcal{V}_T$, it follows that $\dim(\mathcal{V}_T) = n$.

The rank of marginal states (or the Schmidt number of target states) is denoted by d. The spectral decomposition form of two marginal states are written as $\rho_A = \sum_{j=0}^{d-1} \lambda_j |\phi_j^A\rangle\langle\phi_j^A|$ and $\rho_B = \sum_{j=0}^{d-1} \lambda_j |\phi_j^B\rangle\langle\phi_j^B|$. These marginal states may have some degrees of degeneracy, so the eigenstates usually are not fixed. By the purification process, it is neccessary for the target states to be expressed as

$$|\Psi(\boldsymbol{\theta})\rangle = \sum_{j=0}^{d-1} \sqrt{\lambda_j} \exp(i\theta_j) |\phi_j^A \phi_j^B\rangle, \tag{6}$$

where $\theta_j \in [0, 2\pi)$. However it is not a sufficient condition as these states may not live in $\mathcal{V}_T$, so we call them the legal states. The set of legal states is denoted by $\mathcal{L}$ and $\mathcal{V}_L := \text{span}\{\mathcal{L}\}$. Without loss of generality, we set $\dim(\mathcal{H}_{AB}) = d^2$.

By definition, the tuple $(V_{\text{mask}}, \rho_A, \rho_B)$ fully charactorize a masking information protocol. The set of legal target states $\mathcal{L}$ is determined by (ρ_A, ρ_B). The linear isometry V_{mask} implies $\mathcal{H}_R$ and $\mathcal{V}_T$. The set of all target states can now be expressed as

$$\mathcal{T} = \mathcal{V}_T \cap \mathcal{L}. \tag{7}$$

In order to characterize the structure of maskable states, we mainly focus on the structure of target states since $\mathcal{T}$ is isomorphic to $\mathcal{R}$.

4 Structure of the set of maskable states

The set of maskable states $\mathcal{R}$ for qubit space have simple structures without assumption on marginal states:

Theorem 7 *For $n = 2, d \geq 2$, $\mathcal{R}$ lives on a hyperdisk.*

The proof of above theorem follows both Lemma.5 and Lemma.9. Though things become more complicated for qutrit space, still we give the following theorem to characterize the set of target states $\mathcal{T}$ when $n = d = 3$:

Theorem 8 *Assuming the set of target states $\mathcal{T}$ contains at least one 2-dimensional sub-hyperdisk of some Schmidt hyperdisk, $\mathcal{T}$ has 3 possible types of structure when $n = d = 3$:*

- *Type-I: $\mathcal{T}$ is a 3-dimensional Schmidt hyperdisk.*
- *Type-II: $\mathcal{T}$ consists of two 2-dimensional sub-hyperdisk locate on different Schmidt hyperdisks.*
- *Type-III: $\mathcal{T}$ contains a 2-dimensional sub-hyperdisk plus a single state locates on different Schmidt hyperdisks.*

Because the degeneracy of the marginal states can effect the set of target state $\mathcal{L}$, not all kinds of pairs (ρ_A, ρ_B) can achieve 3 types of structure: the non-degenerate case can achieve type-I structure; the partially degenerate case can achieve type-II structure; the completely degenerate case can achieve all types of structure. So in following we divide the discussion into three parts according to the degeneracy of marginal states, in order to develop a general theory for the structure of maskable states.

4.1 non-degenerate case

In this case, ρ_A and ρ_B have fixed eigenstates. Hence the set of legal target states $\mathcal{L}_{\text{nd}}$ is a Schmidt hyperdisk $\mathcal{S}^{AB}$ as shown in Eq.(6), which leads to $\dim(\mathcal{V}_{L\text{nd}}) = d$. The set of target states for non-degenerate case is denoted by $\mathcal{T}_{\text{nd}}$ and $\mathcal{V}_{T\text{nd}} := \text{span}\{\mathcal{T}_{\text{nd}}\}$. Because $\mathcal{T}_{\text{nd}} \subseteq \mathcal{L}_{\text{nd}}$, the target states live on the d-dimensional hyperdisk $\mathcal{S}^{AB}$. From Eq.(7), we can see $\mathcal{T}_{\text{nd}}$ forms a regular subset of $\mathcal{S}^{AB}$. Then $\dim(\mathcal{V}_{T\text{nd}})$ is bounded as

$$\dim(\mathcal{V}_{T\text{nd}}) = n \leq d = \dim(\mathcal{V}_{L\text{nd}}). \tag{8}$$

The equality holds iff $\mathcal{T}_{\text{nd}} = \mathcal{S}^{AB}$, in other words, $\mathcal{T}_{\text{nd}}$ itself forms a hyperdisk.

However, there are situations when $\mathcal{T}_{\rm nd}$ does not forms a hyperdisk, an example is given below for non-degenerate masking protocol ($n=3, d=4$). Here, $\mathcal{T}_{\rm nd}$ consists of following states (unnormalized):

$$\begin{aligned}|\Psi_0(\alpha)\rangle &= |00\rangle + \sqrt{2}\,|11\rangle + e^{i\alpha}\left(\sqrt{3}\,|22\rangle + 2\,|33\rangle\right),\\ |\Psi_1(\beta)\rangle &= |00\rangle + \sqrt{3}\,|22\rangle + e^{i\beta}\left(\sqrt{2}\,|11\rangle + 2\,|33\rangle\right).\end{aligned} \tag{9}$$

It follows that $\mathcal{V}_T$ is a 3-dimensional subspace in $\mathcal{H}_{AB}$. Here we define the masking machine $V_{\rm mask}$ as $|1\rangle \to |00\rangle + \sqrt{2}\,|11\rangle$, $|1\rangle \to \sqrt{3}\,|22\rangle + 2\,|33\rangle$ and $|2\rangle \to |\Phi'\rangle$. Even though $\mathcal{T}_{\rm nd}$ is a regular subset that belongs to a 4-dimensional hyperdisk, we can not find that hyperdisk for $\mathcal{R}_{\rm nd}$ (unnormalized): $|\psi_0(\alpha)\rangle = \sqrt{3}\,|0\rangle + e^{i\alpha}\sqrt{7}\,|1\rangle$, $|\psi_1(\beta)\rangle = \sqrt{7}\,|0\rangle + 3\sqrt{3}\,|1\rangle - \sqrt{50}\,|2\rangle + e^{i\beta}\left(2\sqrt{7}\,|0\rangle + 4\sqrt{3}\,|1\rangle + \sqrt{50}\,|2\rangle\right)$. So the maskable states does not required to live on same hyperdisk, which can be achieved even for non-degerate masking protocol.

4.2 completely degenerate case

In this case, $\rho_A = \rho_B = \mathbb{I}/d$, and the set of legal states $\mathcal{L}_{\rm cd}$ is the set of all maximally entangled states in $\mathcal{H}_{AB}$. A maximally entangled state can be expressed as

$$|\Psi(U)\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} U\,|jj\rangle = U\otimes\mathbb{I}\,|\Phi_{\mathbb{I}}\rangle\,, \tag{10}$$

where $|\Phi_{\mathbb{I}}\rangle = \frac{1}{\sqrt{d}}\sum_j |jj\rangle$ and U is a unitary matrix with elements $(U)_{ij} = \langle ij|\Psi(U)\rangle$. $\{|j\rangle\}$ is defined as the computational basis for $\mathcal{H}_A$ (or $\mathcal{H}_B$). The completely degenerate set of target states is denoted by $\mathcal{T}_{\rm cd}$ and $\mathcal{V}_{T\rm cd} = {\rm span}\{\mathcal{T}_{\rm cd}\}$. A property of completely degenerate masking protocol is that $\mathcal{V}_{L\rm cd} = {\rm span}\{\mathcal{L}_{\rm cd}\} = \mathcal{H}_{AB}$. Hence $\dim(\mathcal{V}_{T\rm cd})$ is bounded as:

$$\dim(\mathcal{V}_{T\rm cd}) = n \le d^2 = \dim(\mathcal{V}_{L\rm cd}) \tag{11}$$

Unlike the non-degenerate case, $\mathcal{L}_{cd}$ is no longer a hyperdisk. Hence $\mathcal{T}_{\rm cd}$ may not belong to a hyperdisk anymore. The following example shows that $\mathcal{T}_{\rm cd}$ can consist of infinite number of hyperdisks. Here we set $n=3, d=2$ and $\mathcal{T}_{cd} = \bigcup_{\xi\eta}\mathcal{S}_{\xi\eta}$, where states in $\mathcal{S}_{\xi\eta}$ are written as:

$$|\Psi_{\xi\eta}(\theta)\rangle = \left|\phi^+_{\xi\eta}\phi^+_{\xi\eta}\right\rangle + e^{i\theta}\left|\phi^-_{\xi\eta}\phi^-_{\xi\eta}\right\rangle, \tag{12}$$

where $\left\{\left|\phi^+_{\xi\eta}\right\rangle, \left|\phi^-_{\xi\eta}\right\rangle\right\}$ is one of orthonormal basis for 2-dimensional space, defined as $\left|\phi^+_{\xi\eta}\right\rangle = \cos\frac{\xi}{2}\,|0\rangle + \sin\frac{\xi}{2}e^{i\eta}\,|1\rangle$ and $\left|\phi^-_{\xi\eta}\right\rangle = \sin\frac{\xi}{2}\,|0\rangle - \cos\frac{\xi}{2}e^{-i\eta}\,|1\rangle$. It follows that $\mathcal{V}_{T\rm cd} = {\rm span}\{|00\rangle, |11\rangle, |01\rangle + |10\rangle\}$. Notice that ξ and η are continuously chosen in $[0, 2\pi)$. Here we define masking machine $V_{\rm mask}$ as $|0\rangle \to |00\rangle$, $|1\rangle \to |11\rangle$ and $|2\rangle \to |01\rangle + |10\rangle$, then one of hyperdisk $V^\dagger_{\rm mask}\mathcal{S}_{\xi\eta}$ in $\mathcal{R}_{cd}$ can be expressed as $|\psi_{\xi\eta}(\theta)\rangle = \cos^2\frac{\xi}{2}\,|0\rangle + \sin^2\frac{\xi}{2}e^{i2\eta}\,|1\rangle + \frac{1}{\sqrt{2}}\sin\xi e^{i\eta}\,|2\rangle + e^{i\theta}(\sin^2\frac{\xi}{2}\,|0\rangle + \cos^2\frac{\xi}{2}e^{-i2\eta}\,|1\rangle - \frac{1}{\sqrt{2}}\sin\xi e^{-i\eta}\,|2\rangle)$. It is an example that the set of maskable states contains unlimited amount of hyperdisks. Hence there is a sign that degeneracy of masking protocol can enhance the masking power.

4.3 partially degenerate case

In this case, the marginal state ρ_A (or ρ_B) is partially degenerate. The jth degenerate eigenvalue for marginal state is denoted by λ_j. The dimension of jth eigenspace is $g(j)$, and the computational basis in that subspace is $\{|j,k\rangle\}_{k=0}^{g(j)-1}$. The total number of eigenspaces is t. Then the legal states can be expressed as:

$$|\Psi(U)\rangle = \sum_{j=0}^{t-1}\sqrt{\lambda_j}\sum_{k=0}^{g(j)-1} U_j\otimes\mathbb{I}\,|j,k\rangle\,|j,k\rangle \tag{13}$$

The unitary matrix for $|\Psi(U)\rangle = U\otimes\mathbb{I}\,|\Psi_{\mathbb{I}}\rangle$ can be written as $U = \bigoplus_{j=0}^{t-1}U_j$, where U_j is $g(j)$-dimensional unitary matrix act on jth degenerate subspace and $|\Psi_{\mathbb{I}}\rangle = \sum_{j=0}^{t-1}\sqrt{\lambda_j}\sum_{k=0}^{g(j)-1}|j,k\rangle\,|j,k\rangle$. The $\dim(\mathcal{V}_T)$ now is limited by $g(j)$:

$$\dim(\mathcal{V}_T) = n \le \sum_{j=0}^{t-1} g^2(j) = \dim(\mathcal{V}_L)\,, \tag{14}$$

where $\sum_{j=0}^{t-1} g(j) = d$. We have already known that $\mathcal{T}$ may not live on a fixed Schmidt hyperdisk, but the necessary and sufficient condition for target states live on same Schmidt hyperdisk is still interesting:

Lemma 9 *A set of target states $\{|\Psi(U)\rangle\}_{U\in\mathcal{U}}$ lives on same Schmidt hyperdisk iff there exists a unitary matrix U_T that satifisfies $[UU_T, U'U_T] = 0$ for all of $U, U'\in\mathcal{U}$.*

5 Conclusion

We have studied the relation between hyperdisk and masking information protocol. In this work, a clear definition of the unspeakable concept hyperdisk is introduced with related concepts called sub-hyperdisk and regular subsets of hyperdisk. Methods are given to deal with the classification of masking protocol. By using the concept hyperdisk, we fully charactorize the set of maskable states for qubit and qutrit case. Two examples are given to show that the non-degenerate masker can mask several distinct hyperdisks even for qutrit information, and the completely degenerate masker can mask unlimited amount of hyperdisks. The hyperdisk structure of target states may provide us another perspective to characterize the structure of entangled states.

References

[1] Kavan Modi, Arun Kumar Pati, Aditi Sen(De), and Ujjwal Sen. Masking quantum information is impossible. *Phys. Rev. Lett.*, 120:230501, Jun 2018.

[2] Mao-Sheng Li and Yan-Ling Wang. Masking quantum information in multipartite scenario. *Phys. Rev. A*, 98:062306, Dec 2018.

Relation of 'α-order Rényi' Subentropy and Mutual Information

Keisuke SATO[1] * Souichi TAKAHIRA[1] † Kenji NAKAHIRA[2] ‡
Tsuyoshi Sasaki USUDA[1] §

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, 1522-3, Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan*
[2] *Quantum Information Science Research Center, Quantum ICT Research Institute, 6-1-1, Tamagawagakuen, Machida-shi, Tokyo, 194-8610, Japan*

Abstract. The subentropy is defined as a lower bound on the maximum mutual information for a fixed quantum ensemble. By F. Mintert and K. Życzkowski, the subentropy was generalized to the quantity that is called the α-order Rényi subentropy. However, they did not state a relation between the quantity and the α-order mutual Rényi information. In this paper, we show a close relation between them. Furthermore, using the relation, we derive an alternative expression for the α-order Rényi subentropy.

Keywords: α-order Rényi subentropy, α-order mutual Rényi information, quantum information theory

1 Introduction

In quantum information theory, the information that may be extracted from a quantum ensemble is called the accessible information, i.e., the maximum mutual information. R. Jozsa, D. Robb, and W. K. Wootters defined the subentropy as a lower bound on the accessible information [1]. The lower bound is the best that depends only on the density operator. F. Mintert and K. Życzkowski generalized the subentropy by redefining it as the excess of the Wehrl entropy [2]. The quantity is called the α-order Rényi subentropy. They showed that this quantity is an entanglement monotone. However, they did not state a relation between the quantity and a corresponding generalization of the ordinary mutual information.

In this paper, for any integer $\alpha > 1$, we show a close relation between the α-order Rényi subentropy and the α-order mutual Rényi information [3], which is one of generalizations of the ordinary mutual information. The α-order mutual Rényi information is defined by C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer in information-theoretical context [3]. Hence, our result implies that the α-order Rényi subentropy is natural generalization also in information-theoretical context. Furthermore, using our relation, we derive an alternative expression for the α-order Rényi subentropy.

2 α-order Mutual Rényi Information I_α

Here, we recall the ordinary mutual information and the α-order mutual Rényi information in quantum information theory.

First of all, we consider a quantum ensemble, a quantum measurement, and probabilities that are obtained from them. A quantum ensemble is a set of m pure quantum states $\{|\psi_i\rangle\}_{i=0}^{m-1}$ in a d-dimensional Hilbert space $\mathcal{H}_d$ and their *a priori* probabilities $\{p_i\}_{i=0}^{m-1}$ that satisfy $\sum_{i=0}^{m-1} p_i = 1$; it is denoted by

$$\mathcal{E} := \begin{pmatrix} |\psi_0\rangle & \cdots & |\psi_{m-1}\rangle \\ p_0 & \cdots & p_{m-1} \end{pmatrix}. \tag{1}$$

For the quantum ensemble $\mathcal{E}$, the density operator $\rho = \sum_{i=0}^{m-1} p_i |\psi_i\rangle\langle\psi_i|$. We obtain information by measuring a quantum state using a quantum measurement that is described by a positive operator-valued measure (POVM). A POVM Π is a set of positive semidefinite operators $\Pi := \{\Pi_j\}_{j=0}^{n-1}$ satisfying $\sum_{j=0}^{n-1} \Pi_j = I$, where I is the identity operator. The conditional probability $P(j|i)$ that the outcome is j when a quantum state $|\psi_i\rangle$ is given as $P(j|i) := \mathrm{Tr}\,[|\psi_i\rangle\langle\psi_i|\Pi_j]$. Further, the probability $P(j)$ that we obtain the outcome j is $P(j) := \mathrm{Tr}\,[\rho\Pi_j]$.

We now introduce the mutual information.

Definition 1 (mutual information) *The mutual information $I(\Pi, \mathcal{E})$ between the POVM Π and the quantum ensemble $\mathcal{E}$ is defined as*

$$I(\Pi, \mathcal{E}) := H(\Pi) - H(\Pi|\mathcal{E}), \tag{2}$$

where

$$H(\Pi) := -\sum_{j=0}^{n-1} P(j) \ln P(j), \tag{3}$$

$$H(\Pi|\mathcal{E}) := -\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} p_i P(j|i) \ln P(j|i) \tag{4}$$

are the entropy and the conditional entropy, respectively.

The accessible information $I(\mathcal{E})$ of the quantum ensemble $\mathcal{E}$ is defined as the maximum mutual information over all possible POVMs:

$$I(\mathcal{E}) := \max_{\Pi} I(\Pi, \mathcal{E}). \tag{5}$$

Next, we introduce the α-order mutual Rényi information [3] for any positive constant $\alpha \neq 1$.

*im182006@cis.aichi-pu.ac.jp
†id171002@cis.aichi-pu.ac.jp
‡nakahira@lab.tamagawa.ac.jp
§usuda@ist.aichi-pu.ac.jp

Definition 2 (α-order mutual Rényi information) *The α-order mutual Rényi information $I_\alpha(\Pi, \mathcal{E})$ between the POVM Π and the quantum ensemble $\mathcal{E}$ is defined as*

$$I_\alpha(\Pi, \mathcal{E}) := R_\alpha(\Pi) - R_\alpha(\Pi|\mathcal{E}), \tag{6}$$

where

$$R_\alpha(\Pi) := \frac{1}{1-\alpha} \ln \left(\sum_{j=0}^{n-1} P(j)^\alpha \right), \tag{7}$$

$$R_\alpha(\Pi|\mathcal{E}) := \frac{1}{1-\alpha} \sum_{i=0}^{m-1} p_i \ln \left(\sum_{j=0}^{n-1} P(j|i)^\alpha \right) \tag{8}$$

are the α-order Rényi entropy and the α-order conditional Rényi entropy, respectively.

Eqs. (6), (7), and (8) coincide with Eqs. (2), (3), and (4) when $\alpha \to 1$. Note that, the α-order mutual Rényi information can be negative [3].

For the ordinary mutual information, a generalization using the α-order Rényi entropy is not unique. The generalizations are called the α-mutual information (see [4]).

The α-order accessible Rényi information is the maximum α-order mutual Rényi information over all possible POVMs:

$$I_\alpha(\mathcal{E}) := \max_{\Pi} I_\alpha(\Pi, \mathcal{E}). \tag{9}$$

3 α-order Rényi Subentropy Q_α

Here, we introduce the ordinary subentropy and the α-order Rényi subentropy for any positive constant $\alpha \neq 1$. We first introduce the definition of the subentropy [1].

Definition 3 (subentropy) *Let ρ be a density operator on a d-dimensional Hilbert space $\mathcal{H}_d$ and let λ_k's be eigenvalues of ρ. The subentropy $Q(\rho)$ of the density operator ρ is defined as*

$$Q(\rho) := -\sum_{k=0}^{d-1} \left(\prod_{l \neq k} \frac{\lambda_k}{\lambda_k - \lambda_l} \right) \lambda_k \ln \lambda_k. \tag{10}$$

The subentropy is known as the best lower bound that depends only on the density operator on the ordinary accessible information. Second, we introduce the definition of the α-order Rényi subentropy [2].

Definition 4 (α-order Rényi subentropy) *Let ρ be a density operator on a d-dimensional Hilbert space $\mathcal{H}_d$ and let λ_k's be eigenvalues of ρ. The α-order Rényi subentropy $Q_\alpha(\rho)$ of the density operator ρ is defined as*

$$Q_\alpha(\rho) := \frac{1}{1-\alpha} \ln \left(\sum_{k=0}^{d-1} \frac{\lambda_k^{\alpha+d-1}}{\prod_{l=0, l\neq k}^{d-1} (\lambda_k - \lambda_l)} \right). \tag{11}$$

Applying L'Hopital's rule, one demonstrates that Eq. (11) coincides with Eq. (10) when $\alpha \to 1$. It is not known whether the α-order Rényi subentropy is a lower bound on the α-order accessible Rényi information.

From the definitions, one finds that these quantities are hard to calculate when ρ is degenerate.

4 Relation Between Q_α and I_α

Here, we restrict that α is any integer such that $\alpha > 1$. We now show a close relation between the α-order Rényi subentropy and the α-order mutual Rényi information.

Proposition 5 *Let ρ be a density operator of the quantum ensemble $\mathcal{E}$ and let λ_k's be eigenvalues of ρ. Let $A = \{|a_j\rangle\langle a_j|\}_{j=0}^{d-1}$ be a complete orthogonal measurement. Then, the following equation holds:*

$$Q_\alpha(\rho) = \frac{1}{1-\alpha} \ln \left(\sum_{j=0}^{d-1} \left\langle P_A(j)^\alpha \right\rangle \right) - \frac{1}{1-\alpha} \sum_{i=0}^{m-1} p_i \ln \left(\sum_{j=0}^{d-1} \left\langle P_A(j|i)^\alpha \right\rangle \right), \tag{12}$$

where P_A describes the probability that obtains from the complete orthogonal measurement A and the quantum ensemble $\mathcal{E}$ with the density operator ρ and $\langle\cdot\rangle$ is the average over all complete orthogonal measurements.

We can prove this proposition by using a technique shown in [1].

Since the RHS of Eq. (12) is the expression that is obtained by averaging the arguments to the logarithms in the α-order mutual Renyi information, this result suggests that there is the close relation between the α-order Rényi subentropy and the α-order mutual Rényi information.

5 Alternative Expression of Q_α

Again, we restrict that α is any integer such that $\alpha > 1$. We derive an alternative expression for the α-order Rényi subentropy.

Proposition 6 *Let ρ be a density operator on a d-dimensional Hilbert space $\mathcal{H}_d$ and let λ_k's be eigenvalues of ρ. Then, the following equation holds:*

$$Q_\alpha(\rho) = \frac{1}{1-\alpha} \ln \left(\sum_{\substack{k_0,\ldots,k_{d-1}=0| \\ \sum_{l=0}^{d-1} k_l = \alpha}}^{\alpha} \lambda_0^{k_0} \cdots \lambda_{d-1}^{k_{d-1}} \right). \tag{13}$$

We can prove this proposition by using Proposition 5.

One finds that Eq. (13) is calculated easily even if the density operator is degenerate. Moreover, we may lead to a simpler expression for fixed α. As the example, we provide a simpler expression for the second-order Rényi subentropy.

Example 1 *Let ρ be a density operator on a d-dimensional Hilbert space $\mathcal{H}_d$ and let λ_k's be eigenvalues of ρ. Then, the second-order Rényi subentropy $Q_2(\rho)$ is*

$$Q_2(\rho) = \ln \left(\frac{2}{1 + \sum_{k=0}^{d-1} \lambda_k^2} \right). \tag{14}$$

In [5], using Eq. (14), it was shown the second-order Rényi subentropy is a lower bound for the minimum entropy. This fact suggests that the alternative expression is helpful expression in order to study properties of the α-order Rényi subentropy.

6 Conclusion

For any integer $\alpha > 1$, we showed the close relation between the α-order Rényi subentropy and the α-order mutual Rényi information (Proposition 5). From this relation, we think that the ordinary definition of the α-order Rényi subentropy is natural also in quantum information theory. Furthermore, using Proposition 5, we derived the simpler expression for the α-order Rényi subentropy.

Our future works are that we clarify properties of the α-order Rényi subentropy and whether the α-order Rényi subentropy is a lower bound on the α-order accessible Rényi information.

Acknowledgements: This work has been supported in part by JSPS KAKENHI Grant Number JP16H04367. We thank Richard Haase, Ph.D., from Edanz Group (www.edanzediting.com/ac) for editing a draft of our manuscript.

References

[1] R. Jozsa, D. Robb, and W. K. Wootters, "Lower bound for accessible information in quantum mechanics," Phys. Rev. **A49**, pp.668-677, (1994).

[2] F. Mintert and K. Życzkowski, "Wehrl entropy, Lieb conjecture, and entanglement monotones," Phys. Rev. **A69**, 022317, (2004).

[3] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inform. Theory **41**, pp.1915-1923, (1995).

[4] S. Verdu, "α-mutual information," 2015 Information Theory and Application Workshop (ITA), pp.1-6, (2015).

[5] H. Yuhara, K. Sato, and T. S. Usuda, "Basic property of the second-order Rényi subentropy," 2018 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, J3-5, (2018). (in Japanese)

New Quantum Algorithms for Modular Inverse and Its Application on the Elliptic Curve Discrete Logarithm Problem

Ryo Kurama[1] * Noboru Kunihiro[2] †

[1] *The Unversity of Tokyo*
[2] *University of Tsukuba*

Abstract. The elliptic curve discrete logarithm problem (ECDLP) is an important problem as the base of the security of elliptic curve cryptography. When solving the ECDLP in quantum computation, modular inverse is the bottleneck in terms of circuit size. In our research, two new quantum algorithms for computing modular inverse are proposed requiring $7n + \lfloor \log_2 n \rfloor + 5$ qubits and $32n^2 \log_2 n + O(n^2)$ Toffoli gates. By applying these to Shor's algorithm solving the ECDLP, more efficient quantum circuits can be implemented with smaller amount of quantum resources.

Keywords: Quantum computation, modular inverse, elliptic curve discrete logarithm problem, elliptic curve cryptography

1 Introduction

Cryptography has played a fundamental roll in the development of technology. It helps keeping secrets protected from malicious attacks. Some cryptosystems use elliptic curves as their buikdingblock. They are used for public key instantiation in various cryptosystems like key exchange [2] and digital signatures [3][4]. They have many application such as transport layer security and the Bitcoin digital currency system.

Elliptic curve cryptography (ECC) is superior to other cryptosystems in that it requires relatively small key sizes. For example, integer factorization cryptography like RSA [7] needs key size of 3072bits to aquire the same security strength as ECC with key size of $256 - 383$ bits according to [1]. This is because the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is the base of the security of ECC, is hard to solve classically. There is a sub-exponential time classsical algorithm for integer factorization, while the best classical algorithm currently known for the ECDLP is exponential.

However, the invention of quantum computation has endangered the security of ECC. Shor proposed two quantum algorithms in [10], one of which solves integer factorization and the other solves discrete logarithm problem in a Galois field. The latter can also be applyed to the ECDLP. This means ECC will be easily broken if a large enough general purpose computer is created. Roetteler et al. gave a concrete circuit of Shor's algorithm that solves the ECDLP, and estimated its precise quantum resources [8]. The most costly operation in their algorithm is modular inverse. Thus we propose more efficient algorithms for modular inverse with which the circuit of Shor's algorithm requires less quantum resources.

2 Algorithms for modular inverse

Our algorithms for modular inverse are based on Kaliski's algorithm [5] as in [8]. Kaliski's algorithm uses Montgomery representation [6] to represent integers to compute modular arithmetic efficiently. Let p a prime modulus and n be the length of p. An integer a is represented as $aR \mod p$ under the Montgomery representation of a radix $R > p$. The representation is often used in classical computation for its efficiency, too. We use 2^n as the radix in this paper.

Kaliski's algorithm takes an integer $x \mod p$ as an input, and outputs an integer $x^{-1}2^n \mod p$ in the Montgomery representation. Kaliski's algorithm works fine alone, but if it is applied to Shor's algorithm, one should convert convert the input from Montgomery representation to normal representation beforehand to keep the representation consistent in the whole calculation. Unfortunately the algorithm had a problem for it failed to do this.

To resolve this problem, we use another definition of modular inverse introduces by Savas and Koç [9]. In this new definition, the input is $x \mod p$ and the output is $x2^{2n} \mod p$. Taking these things into consideration, we propose two algorithms of modular inverse, modular exponentiation type and step-by-step modular doubling type.

The pseudocodes for our algorithms are shown in Algorithm 1 and Algorithm 2. The base of logarithm 2 is omitted in this paper. Though the pseudocodes are written in a classical computation style, the quantum algorithms basically do the same computation. Our main contribution is the part from Line. 21 in both algorithms. Different from Kaliski's original algorithm and Roetteler's algorithm, given a pair of integers (r, l) such that $r = -x^{-1}2^{n-l} \mod p, 0 \leq l \leq n$, this part calculates $x^{-1}2^{2n} \mod p$ by doubling r modulo p for l times. Our two algorithms calculate this in different ways.

The modular exponentiation type uses the fact that 2^l can be broken down into a product of $\lfloor \log n \rfloor + 1$ integers as $\prod_{i=0}^{\lfloor \log n \rfloor} 2^{2^i}$. The multiplication by 2^{2^i} modulo p is done in a similar way as modular multiplication, but more efficiently as the multiplier is a constant of a power of 2. The step-by-step modular doubling type is somewhat less intuitive than the previous one. The main idea of the step-by-step modular doubling type is to repeat

* r_kurama@is.s.u-tokyo.ac.jp
† kunihiro@cs.tsukuba.ac.jp

Algorithm 1 Modular exponentiation type algorithm to calculate Savas and Koç's modular inverse $x^{-1} \cdot 2^{2n} \bmod p$. l_i represents the ith bit of the variable l.

$u \leftarrow p,\ v \leftarrow x,\ r \leftarrow 0,\ s \leftarrow 1$
$l \leftarrow 0$
for $i = 0$ **to** $2n - 1$ **do**
  if $v > 0$ **then**
    if u is even **then**
      $u \leftarrow u/2,\ s \leftarrow 2s$
    else if v is even **then**
      $v \leftarrow v/2,\ r \leftarrow 2r$
    else if $u > v$ **then**
      $u \leftarrow (u - v)/2,\ r \leftarrow r + s,\ s \leftarrow 2s$
    else
      $v \leftarrow (v - u)/2,\ s \leftarrow r + s,\ r \leftarrow 2r$
    end if
  else
    $l \leftarrow l + 1$
  end if
end for
if $r \geq p$ **then**
  $r \leftarrow r - p$
end if
for $i = 0$ **to** $\lfloor \log n \rfloor$ **do**
  if $l_i = 1$ **then**
    $r \leftarrow 2^{2^i} r \bmod p$
  end if
end for
$r \leftarrow -r \bmod p$
return r

a certain subroutine l times, where if the register $|l\rangle$ is positive, the register $|r\rangle$ is multiplied by 2 and the register $|l\rangle$ is decreased by 1. Though construction of such a subroutine with reversibility may not seem obvious, it is possible by introducing another register as a counter.

3 Quantum Resource estimation for modular inverse and Shor's algorithm

We assessed the sizes of circuits by the number of qubits and Toffoli gates. We used the number of Toffoli gates as one of the measures to compare our results with [8]. Let n be the length of a modulus p of elliptic curves. Table.1, 2 show the quantum resources needed for our algorithms and the one in [8] for modular inverse and Shor's algorithm solving the ECDLP, respectively. To compare our algorithms correctly with Roetteler's, we used estimates for a modified version of their circuit to resolve their problem.

The number of qubits for modular inverse in our both algorithms was $7n + \lfloor \log n \rfloor + 6$. This is better than that of [8], but the difference is asymptotically insignificant. The number of Toffoli gates for our modular inverse was $32n^2 \log n + O(n^2)$ while Roetteler's was $48n^2 \log n + O(n^2)$. This is asymptotically about 33.3% better than that of theirs. By applying our modular inverse algorithms, Shor's eintire algorithm can be implemented with $9n + \lfloor \log n \rfloor + 7$ qubits and $832n^3 \log n + O(n^3)$ Toffoli

Algorithm 2 Step-by-step modular doubling type algorithm to calculate Savas and Koç's modular inverse $x^{-1} \cdot 2^{2n} \bmod p$. The symbols ! and $\oplus$ represent "not" and "exclusive or", respectively.

$u \leftarrow p,\ v \leftarrow x,\ r \leftarrow 0,\ s \leftarrow 1$
$l \leftarrow 0, f \leftarrow false, c \leftarrow 0$
for $i = 0$ **to** $2n - 1$ **do**
  if $v > 0$ **then**
    if u is even **then**
      $u \leftarrow u/2,\ s \leftarrow 2s$
    else if v is even **then**
      $v \leftarrow v/2,\ r \leftarrow 2r$
    else if $u > v$ **then**
      $u \leftarrow (u - v)/2,\ r \leftarrow r + s,\ s \leftarrow 2s$
    else
      $v \leftarrow (v - u)/2,\ s \leftarrow r + s,\ r \leftarrow 2r$
    end if
  else
    $l \leftarrow l + 1$
  end if
end for
if $r \geq p$ **then**
  $r \leftarrow r - p$
end if
for $i = 0$ **to** n **do**
  $f \leftarrow !(c = 0) \oplus (l = 0) \oplus f$
  if f **then**
    $c \leftarrow c + 1$
  else
    $r \leftarrow 2r \bmod p$
    $l \leftarrow l - 1$
  end if
end for
$r \leftarrow -r \bmod p$
return r

gates. When compared in Shor's algorithm, ours are asymptotically 13.3% better than [8].

In conclusion, by using our modular inverse algorithms, Shor's algorithm solving the ECDLP can be implemented efficiently with less quantum resources.

References

[1] E. Barker. Recommendation for Key Management, Part 1: General.

Table 1: Comparison in resource estimates of modular inverse between our methods and the one in [8]. "Step" and "Expo." mean the algorithms with Montgomery inverse of the Step-by-step modular doubling type and the modular exponentiation type, respectively.

Circuit	#Qubits	#Toffoli
Expo.	$7n + \lfloor \log n \rfloor + 6$	$32n^2 \log n + O(n^2)$
Step	$7n + \lfloor \log n \rfloor + 6$	$32n^2 \log n + O(n^2)$
Roetteler[8]	$7n + 2\lceil \log n \rceil + 9$	$48n^2 \log n + O(n^2)$

Table 2: Comparison in resource estimates of modular inverse between our methods and the one in [8]. "Step" and "Expo." mean the algorithms with Montgomery inverse of the Step-by-step modular doubling type and the modular exponentiation type, respectively.

Circuit	#Qubits	#Toffoli
Expo.	$9n + \lfloor \log n \rfloor + 7$	$832n^3 \log n + 2268n^3$
Step	$9n + \lfloor \log n \rfloor + 7$	$832n^3 \log n + 2252n^3$
Roetteler[8]	$9n + 2\lceil \log n \rceil + 10$	$960n^3 \log n + 4506n^3$

https://doi.org/10.6028/NIST.SP.800-57pt1r4

[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[3] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[4] D. Johnson, A. Menezes and S. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.

[5] B. S. Kaliski. The Montgomery Inverse and Its Applications. *IEEE Transaction on Computers*, 44(8):1064–1065, 1995.

[6] P. L. Montgomery. Modular multiplication without trial division. *Mathematics of Computation*, 44(170):519–521, 1985.

[7] R. L. Rivest, A. Shamir and L. Adleman A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[8] M. Roetteler, M. Naehrig, K. M. Svore and K. E. Lauter. Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms. In *Advances in Cryptology – ASIACRYPT 2017*, pages 241–270, 2017

[9] E. Savas and Ç. K. Koç. The Montgomery modular inverse-revisited. *IEEE Transactions on Computers*, 49(7):763–766, 2000.

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

Quantum Speedup Based on Classical Decision Trees

Salman Beigi[1] * Leila Taghavi[2] †

[1] *School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*
[2] *School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*

Abstract. Lin and Lin [LL16] have recently shown how starting with a classical query algorithm (decision tree) for a function, we may find upper bounds on its quantum query complexity. More precisely, they have shown that given a decision tree for a function $f : \{0,1\}^n \to [m]$ whose input can be accessed via queries to its bits, and a *guessing algorithm* that predicts answers to the queries, there is a quantum query algorithm for f which makes at most $O(\sqrt{GT})$ quantum queries where T is the depth of the decision tree and G is the maximum number of mistakes of the guessing algorithm. In this paper we give a simple proof of and generalize this result for functions $f : [\ell]^n \to [m]$ with non-binary input as well as output alphabets. Our main tool for this generalization is non-binary span program which has recently been developed for non-binary functions, as well as the dual adversary bound. As applications of our main result we present several quantum query upper bounds, some of which are new. In particular, we show that topological sorting of vertices of a directed graph $\mathcal{G}$ can be done with $O(n^{3/2})$ quantum queries in the adjacency matrix model. Also, we show that the quantum query complexity of the maximum bipartite matching is upper bounded by $O(n^{3/4}\sqrt{m}+n)$ in the adjacency list model.

Keywords: Quantum query complexity, decision trees, span program, dual adversary bound

1 Introduction

Query complexity of a function $f : [\ell]^n \to [m]$ is the minimum number of adaptive queries to its input bits required to compute the output of the function. In a quantum query algorithm we allow to make queries in superposition, which sometimes improves the query complexity, e.g., in Grover's search algorithm [Gro96].

Lin and Lin [LL16] have recently shown that surprisingly sometimes classical query algorithms may result in quantum query algorithms. They showed that having a classical query algorithm with query complexity T for some function $f : \{0,1\}^n \to [m]$, together with a *guessing algorithm* that at each step predicts the value of the queried bit and makes no more than G mistakes, the quantum query complexity of f is at most $Q(f) = O(\sqrt{GT})$. For instance, the trivial classical algorithm for the search problem which queries the input bits one by one have query complexity $T = n$, and the guessing algorithm which always predicts the output 0 makes at most $G = 1$ mistakes (because making a mistake is equivalent to finding an input bit 1 which solves the search problem). Thus the quantum query complexity of the search problem is $O(\sqrt{GT}) = O(\sqrt{n})$ recovering Grover's result.

There are two proofs of the above result in [LL16]. One of the proofs is based on the notion of *bomb query complexity* $B(f)$. Lin and Lin show that there exists a bomb query algorithm that computes f using $O(GT)$ queries, and that the bomb query complexity equals the square of the quantum query complexity, i.e., $B(f) = \Theta(Q(f)^2)$, which together give $Q(f) = O(\sqrt{GT})$. In the second proof, they build an explicit quantum query algorithm with query complexity $O(\sqrt{TG})$ for f using Grover's search; in computing the function they use the values of predicted queries instead of the real values and use a modified version of Grover's search to find mistakes of the guessing algorithm.

Our results: In this paper we give a simple proof of the above result based on the method of *non-binary span program* that has recently been development by the authors [BT18]. Then inspired by this proof, we generalize Lin and Lin's result for functions $f : [\ell]^n \to [m]$ with non-binary input as well as non-binary output alphabets. Our proof of this generalization is based on the dual adversary bound which is another equivalent characterization of the quantum query complexity [LMR+11].

As an application of our main result we show that given query access to edges of a directed and acyclic graph $\mathcal{G}$ in the *adjacency matrix model*, the vertices of $\mathcal{G}$ can be sorted with $O(n^{3/2})$ quantum queries to its edges. Moreover, we show that some existing results on the quantum query complexity of graph theoretic problems such as directed *st*-connectivity, detecting bipartite graphs, finding strongly connected components, and deciding forests can easily be derived from our results.

Our main result is also useful when dealing with graph problems in the *adjacency list model*. In this regard, we show that given query access to the adjacency list of an unweighted bipartite graph $\mathcal{G}$, the quantum query complexity of finding a maximum bipartite matching in $\mathcal{G}$ is $O(n^{3/4}\sqrt{m}+n)$, where m is the number of edges of the graph. To the authors' knowledge this is the first non-trivial upper bound for this problem.

2 From decision trees to span programs

In this section, after developing some notations we state the main result of [LL16]. In the next section we show how this result can be generalized for functions with non-binary input alphabet.

*salman.beigi@gmail.com
†ltaghavi@ipm.ir

Recall that a classical query algorithm for a function $f : D_f \to [m]$ with $D_f \subseteq \{0,1\}^n$ can be modeled by a binary decision tree $\mathcal{T}$ with internal vertices being indexed by elements of $\{1,\ldots,n\}$, edges being indexed by $\{0,1\}$, and leaves being index by elements of $[m]$. The depth of the decision tree, which we denote by T, is the classical query complexity of this decision tree. In [LL16] it is assumed that there is a further algorithm that predicts the values of the queried bits. That is, at each internal vertex of $\mathcal{T}$ makes a guess for the answer of the associated query. We can visualize the guessing algorithm in the decision tree by coloring its edges. For each internal vertex of the decision tree, there are two outgoing edges indexed by 0 and 1, one of which is chosen by the guessing algorithm. We *color* the chosen one black, and the other one red. We call such a coloring of the edges of the decision tree a *guessing-coloring (hereafter, G-coloring).* Therefore, the number of mistakes of the guessing algorithm for every $x \in D_f$ equals the number of red edges in the path from the root to the leaf of the tree associated to x. We now state the result of [LL16] based on decision trees and G-colorings.[1]

Theorem 1 (Lin and Lin [LL16]) *Assume that we have a decision tree $\mathcal{T}$ for a function $f : D_f \to [m]$ with $D_f \subseteq \{0,1\}^n$ whose depth is T. Furthermore, assume that for a G-coloring of the edges of $\mathcal{T}$, the number of red edges in each path from the root to the leaves of $\mathcal{T}$ is at most G. Then there exists a quantum query algorithm computing the function f with query complexity $O(\sqrt{GT})$.*

As mentioned before, this theorem can be proven using non-binary span programs developed in [BT18]. This proof can be found in the full paper.

3 Main result: generalization to the non-binary case

In this section we assume that the input alphabet of the function $f : D_f \to [m]$ is non-binary, i.e., $D_f \subseteq [\ell]^n$. In this case, a classical query algorithm corresponds to a decision tree whose internal vertices have out-degree ℓ (instead of 2). Moreover, a G-coloring can be defined similarly based on a guessing algorithm. Yet, we are interested in a further generalization of the notion of decision tree which we explain by an example.

Consider the following trivial algorithm for finding the minimum of a list of numbers in $[\ell]$: we keep a candidate minimum, and as we query the numbers in the list one by one, we update it once we reach a smaller number. In this algorithm, the possible numbers as answers to a query are of two types: numbers that are greater than or equal to the current candidate minimum, and those that are smaller. Now assuming that the answer to that query is of the first type, what we do next is independent of its exact value (since we simply ignore it and query the next index). Considering the associated decision tree $\mathcal{T}$, for each vertex v we have a candidate minimum, and the outgoing edges of v are labeled by different numbers in $[\ell]$. Then by the above discussion, the subtrees of $\mathcal{T}$ hanging below the outgoing edges whose labels are greater than or equal to the current candidate minimum are identical. Thus we can identify those edges and their associated subtrees. In this case the outgoing edges of v are not labeled by elements of $[\ell]$, but by its certain subsets that form a partition. Indeed, there is an outgoing edge whose label is the *subset* of numbers greater than or equal to the current candidate minimum, and an outgoing edge for any smaller number.

Motivated by the above example of minimum finding, we generalize the notion of decision tree $\mathcal{T}$ for a function $f : D_f \to [m]$ with non-binary input alphabet ($D_f \subseteq [\ell]^n$). As before each internal vertex v of $\mathcal{T}$ corresponds to a query index $1 \le J(v) \le n$. Each outgoing edge of this vertex is labeled by a subset of $[\ell]$, and we assume that these subsets form a partition of $[\ell]$. We denote this partition by

$$\bigcup_{q=0}^{\ell-1} Q_v(q) = [\ell],$$

where here $Q_v(q)$ is the subset in the partition that contains $q \in [\ell]$. Thus $Q_v(q) \subseteq [\ell]$ contains q, and for $q, q' \in [\ell]$ either $Q_v(q), Q_v(q')$ are disjoint or are equal. Moreover, the out-degree of v equals $|\{Q_v(q) : q \in [\ell]\}|$, the number of different $Q_v(q)$'s. We also denote the neighbor vertex of v connected to the edge with label $Q_v(q)$ by $N(v, Q_v(q))$.

Now given a decision tree $\mathcal{T}$ as above, the corresponding classical algorithm works as follows. We start with the root r of the tree and query $J(r)$. Then $x_{J(r)} \in [\ell]$ corresponds to the outgoing edge of v with label $Q_v(x_{J(r)})$. We take that edge and move to the next vertex $N(v, Q_v(x_{J(r)}))$. We continue until we reach a leaf of the tree which determines the value of $f(x)$.

The notation of G-coloring can also be generalized similarly. Recall that a G-coloring comes from a guessing algorithm that in each step predicts the answer to the queried index. In our generalized decision tree whose edges are labeled by subsets of $[\ell]$, we assume that the guessing algorithm chooses one of these subsets as its guess. Rephrasing this in terms of colors, we assume that for each internal vertex v of $\mathcal{T}$, one of its outgoing edges is colored in black (meaning that its label is the predicted answer) and its other outgoing edges are colored in red.

We also consider *randomized classical query algorithms.* In this case, for each value ζ of the outcomes of some coin tosses, we have a (deterministic) generalized decision tree $\mathcal{T}_\zeta$ as above. We also assume that each of these decision trees $\mathcal{T}_\zeta$ is equipped with a guessing algorithm which itself may be randomized. Nevertheless, we may assume with no loss of generality that ζ includes the randomness of the guessing algorithm as well. Therefore, for any ζ we have a generalized decision tree with a G-coloring as before. We assume that the classical randomized query algorithm outputs the correct answer $f(x)$ with high probability. The complexity of such a random-

[1] We remark that the result of [LL16] also works for randomized algorithms.

ized query algorithm is given by the *expectation* of the number of queries over the random choice of ζ.

We can now state our generalization of Theorem 1.

Theorem 2 *In the following let $f : D_f \to [m]$ be a function with $D_f \subseteq [\ell]^n$.*

(i) *Let $\mathcal{T}$ be a generalized decision tree for f equipped with a G-coloring. Let T be the depth of $\mathcal{T}$ and let G be the the maximum number of red edges in any path from the root to leaves of $\mathcal{T}$. Then the quantum query complexity of f is upper bounded by $O(\sqrt{TG})$.*

(ii) *Let $\{\mathcal{T}_\zeta : \zeta\}$ be a set of generalized decision trees corresponding to a* randomized *classical query algorithm evaluating f with bounded error. Moreover, suppose that each $\mathcal{T}_\zeta$ is equipped with a G-coloring. Let P_x^ζ be the path from the root to the leaf of $\mathcal{T}_\zeta$ associated to $x \in D_f$. Let T_x^ζ be the length of the path P_x^ζ, and let G_x^ζ be the number of red edges in this path. Define*

$$T = \max_x \mathbb{E}_\zeta[T_x^\zeta],$$
$$G = \max_x \mathbb{E}_\zeta[G_x^\zeta],$$

where the expectation is over the random choice of ζ. Then the quantum query complexity of f is $O(\sqrt{TG})$.

The span program in the proof of Theorem 1 can easily be adapted for a proof of the above theorem, yet in the complexity of the resulting span program we see an extra factor of $\sqrt{\ell - 1}$, i.e., we get the upper bound of $O(\sqrt{(\ell-1)GT})$ on the quantum query complexity. To remove this undesirable factor, getting ideas from the span program in the proof of Theorem 1, we directly construct a feasible solution of the dual adversary SDP. To prove the second part of this theorem we indeed need the dual adversary bound for the *state generation problem*.

4 Applications

We can use Theorem 2, to simplify the proof of some known quantum query complexity bounds as well as to derive new bounds. We state some of them here.

Proposition 3 *Let $x = (x_1, \ldots, x_n)$ be a list of n numbers.*

(i) [MIN] *The quantum query complexity of finding $\min_j x_j$ is bounded by $O(\sqrt{n \log n})$.*

(ii) [K-MIN] *The problem of finding a subset $S \subseteq \{1, \ldots, n\}$ of size $|S| = k$ such that for all $j \notin S$ we have $x_j \geq \max_{i \in S} x_i$ has quantum query complexity $O(\sqrt{kn \log n})$.*

Our bounds here are tight only up to a a factor of $\sqrt{\log n}$ [DH96, DHHM04]. Here we state the proof of the first part of this theorem just to present how Theorem 2 can be used in applications.

Proof. (i) Consider the randomized classical algorithm that queries all indices one by one in a random order. The algorithm keeps a candidate for minimum at each step, and updates it once it reaches a smaller number. Observe that this algorithm is ignorant of the exact answer to a query once it makes sure that it is not smaller than the current candidate for minimum. Thus in the associated decision tree (for any choice of random order ζ), at any internal vertex v we can unify outgoing edges with label in $\{q : q \geq m_v\}$ where m_v is the candidate for minimum at node v. Thus in $\mathcal{T}_\zeta$ any internal vertex v has an outgoing edge with label $\{q : q \geq m_v\}$ and an outgoing edge for any other $q < m_v$. The former edge is colored black and the latter edges are colored red. The depth of $\mathcal{T}_\zeta$ equals $T = n$ for any ζ. However, for a given x, G_x^ζ depends on ζ, so we should compute $G = \max_x \mathbb{E}_\zeta[G_x^\zeta]$. Since in the beginning of the algorithm we apply a random permutation, we can assume that $x_1 \leq \cdots \leq x_n$. Then let $y^{(m)} = (x_1, \ldots, x_m)$ and $G_m^\zeta = G_{y^{(m)}}^\zeta$. If in the random permutation $\zeta = (\zeta(1), \ldots, \zeta(n))$ the first element is n, i.e., $\zeta(1) = n$, then $G_n^\zeta = G_{n-1}^{\zeta'} + 1$ where $\zeta' = (\zeta(2), \ldots, \zeta(n))$. Otherwise, if $\zeta(1) \neq n$ then $G_n^\zeta = G_{n-1}^{\zeta''}$ where ζ'' is the same order as ζ from which n is removed. We conclude that

$$\mathbb{E}[G_n^\zeta] = \frac{1}{n}\big(\mathbb{E}\big[G_{n-1}^{\zeta'}\big] + 1\big) + \frac{n-1}{n}\mathbb{E}\big[G_{n-1}^{\zeta''}\big].$$

Therefore, letting $G_n = \mathbb{E}[G_n^\zeta]$ we have $G_n = G_{n-1} + \frac{1}{n}$. Using $G_1 = 1$ we obtain

$$G_n = \sum_{t=1}^{n} \frac{1}{t} = O(\log n).$$

As a result, $G = O(\log n)$ and by Theorem 2 the quantum query complexity of finding the minimum is bounded by $O(\sqrt{n \log n})$. □

In the following examples we use the fact that our generalization to Lin and Lin's result works for functions with non-binary input.

Proposition 4 (topological sort) *Suppose that the directed acyclic graph $\mathcal{G}$ with n vertices and m edges is given via the adjacency list model. Then the quantum query complexity of finding a vertex ordering of $\mathcal{G}$ such that for all $(u, v) \in E$, u appears before v is $O(\sqrt{mn})$.*

To the author's knowledge the above theorem gives the first non-trivial quantum query complexity upper bound for the topological sort problem.

Proposition 5 (maximum bipartite matching) *Suppose that the graph $\mathcal{G}$ with n vertices and m edges is given via the adjacency list model. Then assuming that $\mathcal{G}$ is unweighted and bipartite, the quantum query complexity of finding a maximum bipartite matching in $\mathcal{G}$ is $O(n^{3/4}\sqrt{m} + n)$.*

References

[BT18] Salman Beigi and Leila Taghavi. Span Program for Non-binary Functions. *arXiv:1805.02714*, 2018.

[DH96] Christoph Durr and Peter Høyer. A Quantum Algorithm for Finding the Minimum. *arXiv:quant- ph/9607014*, 1996.

[DHHM04] Christoph Dürr, Mark Heiligman, Peter Hoyer, and Mehdi Mhalla. Quantum query complexity of some graph problems. *arXiv:quant-ph/0401091*, 2004.

[Gro96] L K Grover. A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 212–219, 1996.

[LL16] Cedric Yen-Yu Lin and Han-Hsuan Lin. Upper bounds on quantum query complexity inspired by the Elitzur-Vaidman bomb tester. *Theory of Computing*, 12:1–35, 2016.

[LMR+11] Troy Lee, Rajat Mittal, Ben W Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Foundations of Computer Science, 2011. FOCS'11. 52nd Annual IEEE Symposium on*, pages 344–353. IEEE, 2011.

The decomposition of an MPMCT gate in consideration of NNA

Wakaki Hattori[1] * Shigeru Yamashita[1] †

[1] *Graduate School of Information Science and Engineering, Ritsumeikan University*

Keywords: quantum circuit design, Nearest Neighbor Architecture (NNA)

1 Introduction

In order to realize quantum computers, a quantum algorithm needs to be implemented. In general, a quantum algorithm includes a part to calculate logic functions. Major methods utilize ESOPs (Exclusive Sum of Products) to generate a quantum circuit calculating logic functions. A quantum circuit which is generated based on ESOPs consists of Mixed Polarity Multiple-Control Toffoli (MPMCT) gates. Due to the physical limitation, it is necessary to transform a quantum circuit consisting of MPMCT gates to the one on a Nearest Neighbor Architecture (NNA) [1]. In the following, we refer to a quantum circuit on an NNA as NNA-compliant. There have been intensive researches to transform a circuit to be NNA-compliant efficiently.

To transform a circuit consisting of MPMCT gates to be NNA-compliant, two tasks are necessary. In the first task, MPMCT gates are decomposed into elementary gates, and then, SWAP gates are inserted. Previous works address these two tasks separately. Therefore, they choose the control bits and the ancillary bits of gates when they decompose MPMCT gates without consideration of inserting SWAP gates after the decomposition. This paper proposes a totally new approach to address these two tasks simultaneously; our method can realize NNA-compliant efficiently compared with previous methods.

2 Nearest Neighbor Architecture

Currently, quantum circuits which can be realized physically such as IBM-Q and Rigetti Computing need to satisfy the following two conditions.

1. A circuit consists of only one-qubit gates and two-qubits gates.
2. Operations of all gates are performed only on adjacent qubits

In order to satisfy Condition 1, MPMCT gates need to be decomposed into elementary gates. Figure. 1 shows an example such that a four-control-bits MPMCT gate is decomposed into elementary gates. In addition, SWAP gates are inserted to swap quantum states to satisfy Condition 2. For these processes, an MPMCT gate on the left side of Figure. 1 is transformed to be NNA-compliant as show in Figure. 2.

*doyle@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp

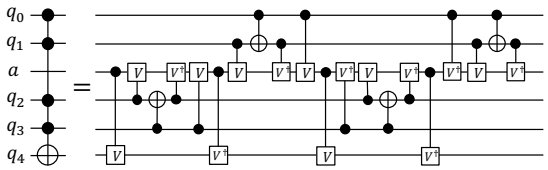


Figure 1: An example such that a four-control-bits MPMCT gate is decomposed into elementary gates.

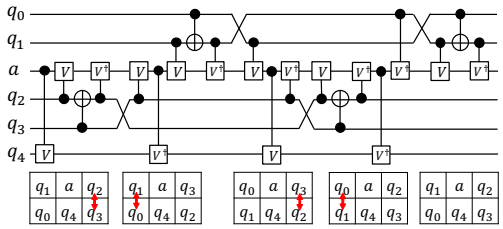


Figure 2: An NNA-compliant quantum circuit generated from the circuit in Figure. 1 by inserting SWAP gates.

3 Previous work

The previous method decomposes each MPMCT gate in a circuit into MPMCT gates with fewer control bits and two-qubits gates as shown in Figure. 3 [2]. We repeatedly apply this method to MPMCT gates until they are decomposed into only two-qubits or one-qubit gates. After the decomposition, SWAP gates are inserted so that the two qubits related to each two-qubits gate become adjacent [3]. Previous methods address these processes separately. They try to decrease the number of gates after the decomposition, but at that time they do not consider inserting SWAP gates. Therefore, the cost of a circuit may increase significantly after inserting SWAP gates.

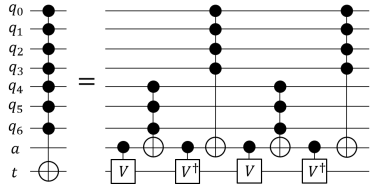


Figure 3: An example of the decomposition of an MPMCT gate by the previous method.

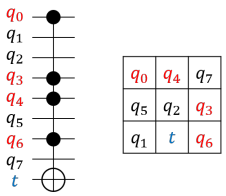


Figure 4: An example of a four-control-bits MPMCT gate and a qubit placement.

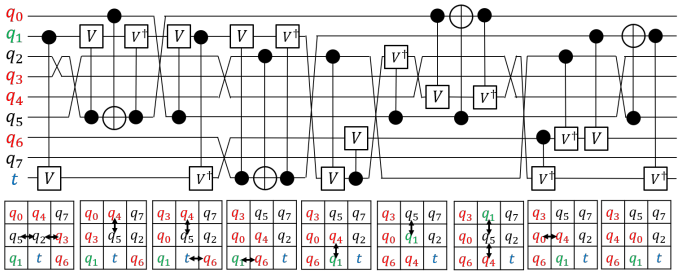


Figure 5: An example of transforming Figure. 4 to be NNA-compliant with 11 SWAP gates by the previous method.

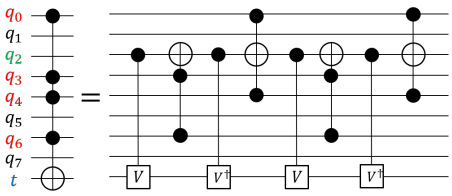


Figure 6: An example of the decomposition of Figure. 4 by our proposed method.

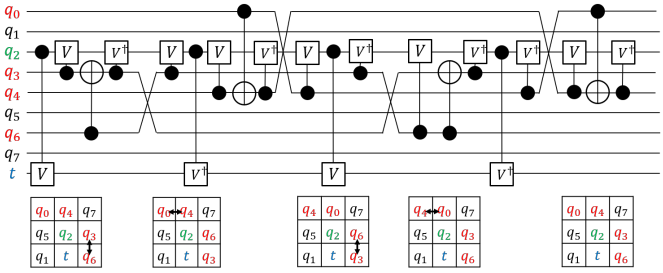


Figure 7: An example of transforming Figure. 4 to be NNA-compliant with four SWAP gates by our proposed method.

4 The proposed method

In our proposed method, we choose a combination of control bits and an ancillary bit to decrease the number of necessary inserted SWAP gates after the decomposition. We show an example of transforming an MPMCT gate on the left side of Figure. 4 to be NNA-compliant with the qubit placement on the right side of Figure. 4. As shown in Figure. 5, the number of inserted SWAP gates is 11 if we choose a combination of the control bits and the ancillary bit without considering of the qubit placement.

On the other hand, our proposed method chooses an ancillary bit in consideration of a qubit placement. In Figure. 4, qubit q_1, q_2, q_5 and q_7 are available as an ancillary bit. As shown in Figure. 3, all gates in a circuit after the decomposition use an ancillary bit. Therefore, we should choose a qubit close to control bits as an ancillary bit in order to insert SWAP gates efficiently. q_i means a control bit of an MPMCT gate, and q_j is a qubit which is available as an ancillary bit. We choose a qubit q_j which minimizes Eq. 1 as an ancillary bit.

$$\sum_i dist|q_i - q_j| \tag{1}$$

Thus, qubit q_2 is chosen as an ancillary bit by our method in the above example. Then, we divide the control bits into two groups to minimize the sum of the manhattan distance between the control bits in the group. In the qubit placement in Figure. 4, we divide control bits into $\{q_0, q_4\}$ and $\{q_3, q_6\}$. As a result, an MPMCT gate in Figure. 4 is decomposed into MPMCT gates with fewer control bits and two-qubits gates as shown in Figure. 6; after inserting SWAP gates, it is transformed to be NNA-compliant as shown in Figure. 7. Our method needs to insert only four SWAP gates, which is much fewer than the case as shown in Figure. 5. We apply this method to MPMCT gates repeatedly and realize a quantum circuit on an NNA efficiently.

5 Conclusion

In this paper, we proposed a new approach to decompose an MPMCT gate in consideration of inserting SWAP gates at the same time. Our proposed method chooses a combination of control bits and an ancillary bit to decrease the number of inserted SWAP gates. Therefore, we can transform a quantum circuit consisting of MPMCT gates to the one on an NNA more efficiently compared with previous methods.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 15H01677 and 18K19790.

References

[1] Yuichi Hirata and Masaki Nakanishi and Shigeru Yamashita and Yasuhiko Nakashima. An Efficient Conversion of Quantum Circuits to a Linear Nearest Neighbor Architecture. Quantum Info. Comput, Vol. 11, No. 1, pages 142-166, 2011.

[2] D. M. Miller, R. Wille, and Z. Sasanian. Elementary quantum gate realizations for multiple-control Toffoli gates. In Int'l Symp. on Multi-Valued Logic, pages 288-293, 2011.

[3] Shafaei, Alireza and Saeedi, Mehdi and Pedram, Massoud. Optimization of Quantum Circuits for Interaction Distance in Linear Nearest Neighbor Architectures. Proceedings of the 50th Annual Design Automation Conference, DAC '13, pages 41:1–41:6, 2013.

A BDD-based approach to the Ising partition function via Eulerian subgraphs

Ryota Yonekura[1] * Hidefumi Hiraishi[1] † Hiroshi Imai[1] ‡

[1] *Graduate School of Information Science and Technology, The University of Tokyo*

Abstract. Counting Eulerian subgraphs, which have an Eulerian circuit, has a strong relationship with the partition function in the Ising model, which is known as a #P-hard problem and necessary to evaluate the probability of spin configuration in the Gibbs distribution. From the aspect of graph theory, we give an algorithm counting Eulerian subgraphs using Binary Decision Diagram (BDD), which represents boolean function. Using path decomposition of a graph to decide the ordering of edges enabled us to give the BDD width bound of $2^{O(pw(G)\log(pw(G))}$, where $pw(G)$ denotes the pathwidth of graph G. Furthermore, implications for quantum computation are also touched upon.

Keywords: Binary Decision Diagram, Ising partition function, pathwidth, Eulerian subgraph

1 Introduction

Ising model, which is applied to Quantum Annealing [1, 2], is eagerly studied since it is coming into reality and beginning to be used to solve real optimization problems. Yet there are many "hard" problems concerning Ising model, such as calculating the Ising partition function, which we tackle in this paper. The Ising partition function, which has its origin in statistical mechanics [3], appears when we calculate the probability of spin configuration in the Gibbs distribution. This function is defined as follows [4];
Let $G = (V, E)$ be a weighted graph and J_{ij} be a weight of the edge $\{i, j\}$. The Hamiltonian for a particular state configuration $\sigma = (\sigma_1, \ldots, \sigma_{|V|})$ is

$$H(\sigma) = -\sum_{\{i,j\}\in E} J_{ij}\delta_{\sigma_i,\sigma_j} \tag{1}$$

where $\sigma_i \in \{-1, 1\}$ and $\delta_{\sigma_i,\sigma_j} = 1$ and 0 otherwise. The probability of the spin configuration σ in the Gibbs distribution is $P(\sigma) = \frac{1}{Z(\beta)}e^{-\beta H(\sigma)}$, where $\beta = 1/k_B T$, the inverse of the product of the Boltzmann constant and temperature, and $Z(\beta)$ is the partition function defined as follows.

$$Z(\beta) = \sum_{\{\sigma\}} e^{-\beta H(\sigma)} \tag{2}$$

where $\{\sigma\}$ means the full set of all possible state configurations.
From the aspect from computational complexity, this problem is known as #P-hard, so it is intractable even for a small instance. Furthermore, the difficulty of this problem in quantum device is discussed in [5].
Interestingly, also from the aspect of graph theory, van der Waerden showed this partition function is represented by the *generating function of Eulerian subgraphs* [5]. In general, an Eulerian subgraph of G is a subgraph of G which has an Eulerian circuit (a circuit which visits every edge exactly once). However, note that an Eulerian subgraph in *generating function* is defined as a subgraph the degree of whose all vertices is even, and it is not necessarily connected. In this paper, we adopt the former definition, so we consider connected subgraphs the degree of whose vertices is even, since it is easy to relax the problem using the latter definition and we expect considering this harder problem would open a new perspective on the partition function from the graphical aspect.
Let $wt(a)$ be a number of edges in the subgraph a, the *generating function* is

$$E(G, x) = \sum_a x^{wt(a)} \tag{3}$$

Via this *generating function*, the partition function is given by

$$Z(\beta) = 2^{|V|}\prod_{\{i,j\}\in E}\cosh(\beta J_{ij})E(G, \tanh(\beta J_{ij})) \tag{4}$$

So counting Eulerian subgraphs is strongly related to calculating the value of partition function. We propose an algorithm to count Eulerian subgraphs of a given graph using a binary decision diagram (BDD). BDD is a data structure which represents a boolean function. As known, a graph has an Euler circuit if and only if the degree of all vertices is even. We construct a BDD which determines whether the graph is an Eulerian graph when every edge assigned to use or not. After BDD constructed, we count Eulerian subgraphs by applying dynamic programming on BDD.
In addition, we apply path decomposition to the graph and devise the edge deciding ordering, so that we give a time complexity analysis using pathwidth of the graph.

2 Method

In this section, we show our method to count Eulerian subgraphs. We construct a BDD data structure which represents a boolean function. Assuming the edge ordering, we should judge whether a subgraph is Eulerian or not when we decide to use each edge.
Let $G = (V, E)$ be a graph and $H = (V', E')$ be a subgraph of G, there are two requirements that H should hold.

*r.yonekura@is.s.u-tokyo.ac.jp
†hiraishi1729@is.s.u-tokyo.ac.jp
‡imai@is.s.u-tokyo.ac.jp

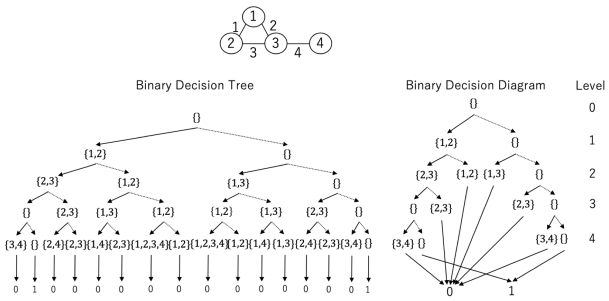


Fig 1. Comparison between BDT and BDD

1. $\forall v \in V'\ degree(v) = 0\ mod\ 2$
2. H is connected

For the first condition, we consider a binary decision tree (BDT) whose node is $Odd(H) = \{v \in V | degree(v) = 1\ mod\ 2\}$. The left side of the Fig 1 is binary decision tree on the condition of $G = (\{1,2,3,4\}, \{\{1,2\},\{2,3\},\{1,3\},\{3,4\}\})$. For simplicity, we look an empty set (the last node on the level 5 of BDT in Fig 1) as an Eulerian subgraph in this paper. Observing this BDT, you may notice that some intermediate nodes never become Eulerian, such as the second node on the level 3 since vertex 1 in this node never becomes even degree. By connecting such node to false (never becomes Eulerian), and we construct BDD such as the right side.

Formally, we should consider such $Odd(H) \cap T_k$ on level $k \geq 1$, where level k is the k-th layer of BDT and BDD, $S_k = \bigcup_{1 \leq i \leq k} e_i$ is the a set of vertices which are adjacent to at least one edge of $e_1, .., e_k$, and $T_k \subseteq S_k$ is a set of vertices such that are adjacent to at least one undecided edge and one decided edge. If there exists vertex $v \in Odd(H) \cap (S_k \setminus T_k)$, the degree of v never becomes Eulerian and we don't have to consider a subgraph H such that $Odd(H) \cap (S_k \setminus T_k) \neq \emptyset$.

Furthermore, to satisfy the second condition, we want to know which vertex in T_k is connected for each node in BDD.

Every time when we decide whether we use e_k or not, and make a subgraph $H = (V', E')$ from a subgraph which $(k-1)$-th level node represents, if there exists $v \in V' \cap (T_{k-1} \setminus T_k)$ (a vertex whose last undecided edge was decided on level k), we check following two conditions.

1. Is $degree(v) = 0\ mod\ 2$ satisfied?
2. Is v connected to any $u \in T_k$?

If the first condition is not satisfied, we connect this node to false since the subgraph this node represents never becomes Eulerian. Otherwise, and if the second condition doesn't hold, we can choose no more edges since no edge is adjacent to the connected component which includes v. Then we check whether H is a Eulerian subgraph, and connect this node to true or false due to this result. If these two condition are held, the necessity is satisfied and contienue searching.

If we finished deciding all edges, we check whether H is an Eulerian subgraph as the above case(1:true and 0:false).

Furthermore, we give the following lemma about the bound of the BDD width (the number of nodes of the BDD).

Lemma 1 *The BDD width on level k of the BDD is bounded by $2^{|T_k|}Bell(|T_k|)$, where $Bell(x)$ is x-th Bell number.*

Proof. The number of which vertex in T_k is connected on level k is bounded by the size of partition of T_k, and this equals to $Bell(|T_k|)$. If two nodes are same in both the connected components and the parity of vertices, we can merge this nodes, and the node size is bounded $2^{|T_k|}Bell(|T_k|)$. □

Then we want find a good ordering to minimize the BDD width. To do that, we introduce a path decompostion of G.

Definition 2 *A path decomposition of a graph $G = (V, E)$ is a pair $(\{B_p : p \in I\}, P)$, where P is a path, I is the node set of P and the subsets $B_p \subseteq V$ satisfies (B_p is called a bag of p)*

1. $\bigcup_{p \in I} B_p = V$
2. *For each edge $\{u, v\} \in E$, there is at least one $p \in I$ with $\{u, v\} \subseteq B_p$*
3. *For each vertex $v \in V$, a subgraph induced by $\{i \in I : v \in B_i\}$ is connected*

$pw(G)$ denotes the *pathwidth* of G, the minimum value of $(\max_{v \in V_P} |B_v|) - 1$ for all its path decompositions. A path decomposition is called *optimal* when it achieves $pw(G)$.

Theorem 3 (Theorem 2 in [6]) *The pathwidth of a graph can be computed and a corresponding path decomposition can be found in time $2^{O(k^2)}n$ for graphs of pathwidth k.*

From the above theorem, we can get an optimal path decompostion $(\{B_p : p \in I\}, P)$ of G and assume $p_1, .., p_t \in I$ forms a path in this order where $t = |I|$. Then we define W_i as follows.

$$W_i = \begin{cases} B_i \setminus B_{i+1} & (i \in [1, t-1]) \\ V \setminus \bigcup_{j \in [1,t-1]} W_j & (otherwise) \end{cases}$$

$\{W_i\}_{i \in [1,t]}$ is a partition of V and for all i, and each W_i is not an empty set since this path decomposition is optimal. We get an ordering of vertices select all vertices in W_1 at any order, and vertices in W_2, and so on. From this vertex ordering, we get an edge ordering up to lexicographical ordering of the end of edges. Then the following lemma holds.

Lemma 4 *For any edge ordering got from an optimal path decomposition of G, the following inequality holds for all levels a of the BDD.*

$$|T_a| \leq pw(G) + 1$$

Proof. Without loss of generality, define $V = [1, |V|]$ which is ordered as the above vertex ordering. Assume we are going to decide edges adjacent to $v \in W_j$, which include the a-th edge, $e_a = \{v, x\}$ on the level a of the BDD. Clearly, $v \in T_a$ holds.
For all $w \in T_a$ other than v, there exist $u \in W_i$ and $\{u, w\} \in E$ such that $u \leq v < w$ and $i \leq j \leq k$ where $w \in W_k$ due to the definition of $\{W\}$. (At least there is one edge decided to use, which should be adjacent to a vertex u less than or equal to v, and the other end w should be undecided.)
From $u \in W_i$ and its definition, u is included only less than or equal to i-th bag. Furthermore, due to $\{u, w\} \in E$, there exists a bag includes both vertices, so there exists B_l such that $\{u, v\} \subseteq B_l$, $l \leq i$. w is included by both B_l and B_k, which is a superset of W_k, and we obtain for all $l \leq m \leq k$, $w \in B_m$ from the property 3 of Definition 1.
Then, any $w \in T_a$ is included by the bag B_j, which includes v. (Note that j is included by $[l, k]$, since $l \leq i \leq j \leq k$.) This leads $T_a \subseteq B_j$, which proves the claim. □

As a result, we get following bound.

Theorem 5 *The BDD width on each level is bounded by $2^{O(pw \log pw)}$ where pw denotes the path width of G.*

Proof. From lemma 1, lemma 4, and $Bell(x) \leq x^x$,

$$\begin{aligned} 2^{|T_k|} Bell(|T_k|) &\leq 2^{pw+1} Bell(pw+1) \\ &\leq 2^{pw+1} (pw+1)^{pw+1} \\ &\leq 2^{pw+1} 2^{(pw+1)\log(pw+1)} \\ &\leq 2^{O(pw \log pw)} \end{aligned}$$

□

After constructed BDD, we can apply dynamic programming to the BDD so that each node has the number of Eulerian subgraphs. Simply adding each node number to the child node one enables us to obtain the total number of Eulerian subgraphs and the complexity of this algorithm is also $2^{O(pw \log pw)}$.
If we relax this counting problem and allow a counted subgraph $H = (V', E')$ disconnected, this algorithm becomes easier. We construct BDD which nodes are $Odd(H) \cap T_k$ and we should check that for all $v \in V' \cap (T_{k-1} \setminus T_k)$, $degree(v) = 0 \ mod\ 2$ on each level k and for all $v \in V' \cap T_{|E|}$, $degree(v) = 0 \ mod\ 2$ on the last level. After BDD constructed, we apply dynamic programming as the same way. This BDD width and time complexity is $2^{O(pw)}$. From the above discussion, we obtain the following proposition.

Proposition 6 *Given an optimal path decomposition of a graph, we have two algorithms.*

1. *If nodes of the BDD are odd-degree vertices and connected components of the elimination front, we get a $2^{O(pw \log pw)}$ algorithm to count connected subgraphs the degree of whose vertices is even.*
2. *If nodes of the BDD are odd-degree vertices of the elimination front only, we get $2^{O(pw)}$ algorithm to count subgraphs the degree of whose vertices is not necessarily even.*

where the elimination front means T_k of each level k of the BDD.

3 Concluding Remarks

We showed algorithms constructing BDD to count Eulerian subgraphs, whose motivation is calculating the partition function via the *generating function of Eulerian subgraphs*. Whether a subgraph forms Eulerian circuit or not after deciding to use each edge was regarded as a boolean function and it enabled us simple dynamic programming solution to count Eulerian subgraphs. By applying path decomposition to the edge ordering, we gave a bound of BDD width due to the path width.
In addition, approximation algorithms for the Ising partition function, including quantum algorithms, are energetically studied these days. So our exact algorithms would be useful to evaluate such approximation algorithms and make a comparison.
Graphical properties of the partition function related to the Ising model will be considered as a future work.

References

[1] Tadashi Kadowaki and Hidetoshi Nishimori. Quantum annealing in the transverse Ising model. *Phys. Rev. E*, 58(5):5355–5363, nov 1998.

[2] A B Finnila, M A Gomez, C Sebenik, C Stenson, and J D Doll. Quantum annealing: A new method for minimizing multidimensional functions. *Chemical Physics Letters*, 219(5):343–348, 1994.

[3] E T Jaynes. Information Theory and Statistical Mechanics. *Phys. Rev.*, 106(4):620–630, may 1957.

[4] Patrick J. Coles, Stephan Eidenbenz, Scott Pakin, Adetokunbo Adedoyin, John Ambrosiano, Petr Anisimov, William Casper, Gopinath Chennupati, Carleton Coffrin, Hristo Djidjev, David Gunter, Satish Karra, Nathan Lemons, Shizeng Lin, Andrey Lokhov, Alexander Malyzhenkov, David Mascarenas, Susan Mniszewski, Balu Nadiga, Dan O'Malley, Diane Oyen, Lakshman Prasad, Randy Roberts, Phil Romero, Nandakishore Santhi, Nikolai Sinitsyn, Pieter Swart, Marc Vuffray, Jim Wendelberger, Boram Yoon, Richard Zamora, and Wei Zhu. Quantum Algorithm Implementations for Beginners. 2018.

[5] Joseph Geraci. A new connection between quantum circuits, graphs and the Ising partition function. *Quantum Information Processing*, 7(5):227–242, 2008.

[6] Martin Fürer. Faster Computation of Path-Width. *International Workshop on Combinatorial Algorithms*, pages 385–396, 2016.

Efficient Mapping of the ZX calculus

Kota Asai[1] * Shigeru Yamashita[1] †

[1] *Graduate School of Information Science and Engineering, Ritsumeikan University*

Abstract. Lattice surgery performs logical operations using the error correcting code without destroying 2-dimensional nearest neighbor architecture. In lattice surgery, we use two logical operations called "merge" and "split". The representation of quantum computation called the ZX calculus can describe these operations more efficiently than quantum circuits. In this paper, we propose a method to map a procedure in the ZX calculus to a procedure in lattice surgery.

Keywords: qubit layout, circuit optimization, zx calculus, lattice surgery, surface code

1 Introduction

To realize fault-tolerant quantum computation, many efforts have been done in the research community for quantum computation. Among them, the surface code [1] has been attracting much attention recently as error correcting code performing fault-tolerant quantum computation. The surface code has a high fault-tolerant threshold [2] and it can be realized by only two-qubit quantum gates on adjacent qubits. A technique called lattice surgery can perform logical operations between two or more logical qubits encoded by the surface code [3]. In lattice surgery, we use two logical operations called "merge" and "split". These operations are non-unitary operations on the logical states, and it is difficult to describe all these operations in a quantum circuit. Therefore, it has been proposed to use the diagrammatic language called ZX calculus to describe operations in lattice surgery efficiently [4]. Thus, in this paper, we propose a method to map a procedure in the ZX calculus to a one in lattice surgery efficiently. Our method considers to parallelize the ZX calculus as much as possible, and optimize the qubit placement as well.

2 ZX calculus for lattice surgery

Lattice surgery performs operations on the planar code. The planar code encodes one logical qubit by arranging physical qubits on a two-dimensional lattice with periodic boundary conditions [5]. Figure 1 (a) shows an example such that the planar code encodes one logical qubit. The red faces in Figure 1 (a) define the two or four Z stabilizer operators. The blue faces in Figure 1 (a) define the two or four X stabilizer operators. The planar code has two types of boundaries, the X boundaries and the Z boundaries.

In lattice surgery, there are two types of operations, "split" and "merge" to perform multi-qubit operations between encoded logical qubits. Figure 1 (b) shows these operations between X boundaries. The "merge" operation generates one logical qubit from two logical qubits. The "split" operation generates two logical qubits from one logical qubit.

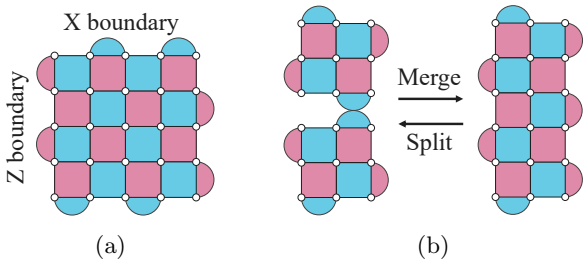


Figure 1: (a) The planar code encodes one logical qubit. The red faces define the two or four Z stabilizer operators. The blue faces define the two or four X stabilizer operators. The left and the right boundaries are called Z boundary, and the upper and the lower boundaries are called X boundary. (b) The "merge" and the "split" operations between X boundaries.

The ZX calculus is a diagrammatic language for reasoning quantum computation, similarly to quantum circuits [6]. It is consist of red nodes, green nodes and edges which connect nodes. The difference in color is associated with a choice of basis. The ZX calculus can represent initialization, measurement, single qubit gate, CNOT gate using nodes and edges as well as quantum circuits. All nodes except the initialization and measurement nodes have m (≥ 1) inputs and n (≥ 1) outputs. In particular, a red node with two inputs and an output correspond to $K = |+\rangle\langle ++| + |-\rangle\langle --|$, and it represents merge operations between Z boundaries. Then, a red node with an input and two outputs correspond to $K = |++\rangle\langle +| + |--\rangle\langle -|$, and it represents split operations between Z boundaries. Similarly, a green node with two inputs and an output correspond to $K = |0\rangle\langle 00| + |1\rangle\langle 11|$, and it represents merge operations between X boundaries. Then, a green node with an input and two outputs correspond to $K = |00\rangle\langle 0| + |11\rangle\langle 1|$, and it represents split operations between X boundaries. Therefore, the ZX calculus can describe procedures in lattice surgery more naturally than quantum circuits.

3 Mapping of ZX calculus

In our method, first, we parallelize nodes in the ZX calculus diagram before mapping a procedure in the ZX calculus to a one in lattice surgery. Next, we optimize the

*eight@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp

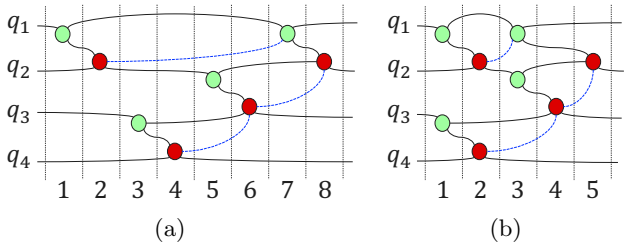


Figure 2: (a) The ZX calculus diagram converted from a quantum circuit containing only CNOT gates. (b) The ZX calculus diagram parallelized from Figure 2 (b).

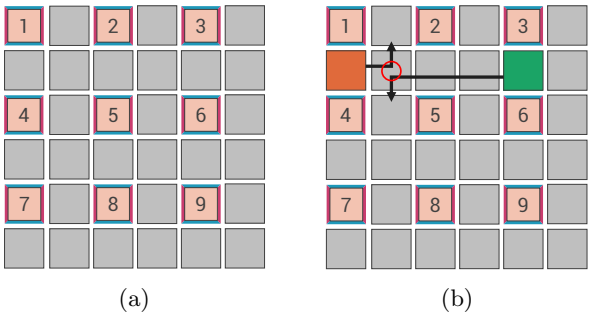


Figure 3: (a) The qubit placement used in our method. The gray qubits are ancilla qubits to perform CNOT operations. (b) An example where we cannot move qubits simultaneously.

qubit placement to increase the number of nodes that can be parallelized.

3.1 Parallelization in ZX calculus

Figure 2 (a) is the ZX calculus diagram converted from a quantum circuit containing only CNOT gates. The time axis is from left to right. The red and green nodes correspond to "merge" and "split" operations. The black edge indicates dependencies of the operations corresponding to each node. The blue edge indicates dependencies to perform error correction. When we map edges that connect a red node and a green node to a procedure of lattice surgery, we need to move qubits generated by split operations.

We can parallelize a graph converted from a quantum circuit maintaining dependency between nodes. Figure 2 (b) shows the result parallelized from Figure 2 (a). We can reduce the computational time by parallelization in the ZX calculus diagram.

3.2 Optimization of the qubit placement

To increase the number of operations that can be performed in parallel, we optimize the qubit placement. In our method, we use the qubit placement as shown in Figure 3 (a). The gray qubits are ancilla qubits to perform CNOT operations.

Figure 3 (b) shows the qubits move. The orange and green qubits are generated by splitting qubit 1 and qubit 3. The orange qubit needs to move to be adjacent to qubit 2 in order to be merged with the qubit 2. Similarly, the green qubit needs to move to be adjacent to qubit 4 in order to be merged with the qubit 4. In our method, we move qubits with only L-shaped move. Figure 3 (b) shows an example where we cannot move two qubits simultaneously. However, we can perform these move operations simultaneously by placing qubit 1 and qubit 3 appropriately. When we parallelize graphs mentioned in Section 3.1, we can consider that multiple duplications of qubit paths. Therefore, we optimize the qubit placement to minimize duplications of paths.

In our method, we formulate the problem of optimization of the qubit placement to Integer Linear Programming (ILP). We will explain the specific formulation in Appendix.

4 Conclusion

In this paper, we have proposed a method to map a procedure in the ZX calculus to a one in lattice surgery with parallelization in ZX calculus and optimization of the qubit placement. In our future work, we should perform some benchmark experiments and verify its effectiveness. In our method, we do not consider the freedom of position of each node and the complicated move of qubits. Thus, in our another future work, we need to consider these such issues to optimize circuits further.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 15H01677 and 18K19790, and by the Asahi Glass Foundation.

References

[1] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.

[2] D. S. Wang, A. G. Fowler, A. M. Stephens, and L. C. L. Hollenberg. Threshold error rates for the toric and planar codes. *Quantum Info. Comput.*, 10(5):456–469, May 2010.

[3] Clare Horsman, Austin G. Fowler, Simon Devitt, and Rodney Van Meter. Surface code quantum computing by lattice surgery. *New Journal of Physics*, 14(12):123011, 2012.

[4] Niel de Beaudrap and Dominic Horsman. The zx calculus is a language for surface code lattice surgery. *arXiv preprint arXiv:1704.08670*, 2017.

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

[6] Bob Coecke and Ross Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011.

Appendix A Formulation procedure

In our method, we formulate the problem of optimization of the qubit placement to Integer Linear Programming (ILP). Let i, j, k, l are the number of locations that qubit place. Thus, let $x_{i(j,k,l)n(o,p,q)}$ is a boolean variable that indicates whether qubit $i(j,k,l)$ is assigned to location $n(o,p,q)$ or not. Let y_{mno} is a boolean variable that indicates whether qubit n needs to move to neighbor positions of qubit o in m step or not. Let z_{ijkl} is a boolean variable that indicates whether qubit can move between location i, j and between location k, l simultaneously or not. Then, we formulate the optimization problem with the above variables in the following.

$$\begin{aligned}
\text{minimize} \quad & \sum_{m=1}^{s}\sum_{i=1}^{r}\sum_{j=1}^{r}\sum_{k=1}^{r}\sum_{l=1}^{r}\sum_{n=1}^{t}\sum_{o=1}^{t}\sum_{p=1}^{t}\sum_{q=1}^{t} \\
& z_{ijkl}y_{mno}y_{mpq}x_{in}x_{jo}x_{kp}x_{lq} \\
\text{subject to} \quad & \sum_{i=1}^{u} x_{in} = 1 \quad (n = 1, \ldots, t) \\
& \sum_{n=1}^{v} x_{in} = 1 \quad (i = 1, \ldots, r) \\
& x_{in} \in \{0, 1\} \quad (i = 1, \ldots r, n = 1, \ldots, t)
\end{aligned}$$

In our method, we use ILP solver to search a optimal solution that satisfies above constraint expression.

Design criteria for a robust quantum receiver in the presence of phase noise

Tiancheng Wang[1] * Kenji Nakahira[2] † Tsuyoshi Sasaki Usuda[1] ‡

[1] *School of Information Science and Technology, Aichi Prefectural University, 1522-3, Ibaragabasama, Nagakute, Aichi, 480-1198, Japan.*

[2] *Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, 6-1-1, Tamagawagakuen, Machida, Tokyo, 194-8610, Japan.*

Abstract. In long-distance wireless communications, the performance of quantum receiver dealing with phase noise has not been widely discussed. In this paper, we discuss the performance and design criteria of a robust quantum receiver that addresses the uncertain estimation of phase noise.

Keywords: Wireless quantum communication, Phase noise, Quantum receiver

1 Introduction

The coherent-state has been subjected to extensive research on quantum communications and information theory. For example, the coherent-state is known for its can achieve the ultimate channel capacity for a lossy bosonic channel or free-space[1, 2]. The use of coherent states encoding information in the phase angle, which we call MPSK(M-ary phase-shift keying) coherent-state signals, can increase the spectral efficiency as a typical digital modulation scheme.

Since the characteristic of MPSK signals, the transmitted signals influenced by phase noise may be hard to distinguish from the nearby signals, resulting that the performance of communication systems is affected. In a long-distance wireless quantum channel, sometimes the optimum quantum receiver is incapable of following the phase fluctuation θ caused by turbulence, atmospheric refraction, and unstable adjustment of the receiver. Therefore, θ has to be regarded as random variables Θ in general. As an example of such treatment, a study [3] focused on Θ caused by the phase diffusion, which occurs on fiber quantum channel, and assumed that Θ follows normal distribution $N(0, \sigma^2)$. In this paper, we consider that a similar phase noise caused by different cause, in the wireless quantum channel.

In fact, an optimum classical receiver, including homodyne measurement and heterodyne measurement, does not depend on the estimation in terms of phase noise. On the other hand, an optimum quantum receiver that achieves the Helstrom bound requires estimating exactly the variance of the phase noise, σ^2. Unfortunately, in long-distance communications, such as satellite-based global quantum communications, a variety of incomplete factors generate the sudden fluctuation of σ^2, resulting that σ^2 is hard to be estimated exactly. The quantum measurements that deal with such problem have not been clarified.

In our previous study[4, 5], we have focused on the performance of a quantum receiver when the estimated phase noise for an optimum quantum measurement was inconsistent with the true phase noise in the received quantum states. The analysis demonstrated that estimating an incorrect phase noise may degrade dramatically the performance of quantum receiver. In this paper, we intend to find the quantum measurements that improve the performance of quantum receiver as much as possible, in case that the performance closer to that of an optimum classical receiver within the range $R(\ni \sigma^2)$—quantum receiver estimates σ^2 including uncertainty. In addition, although we focus mainly on $M = 2$, namely BPSK(binary phase-shift keying), in this paper, we provide briefly the basics of $M > 2$ for extensibility.

2 Basics of quantum communication

Suppose the quantum density operator of a transmitted quantum state, $\rho_i^{(\mathrm{in})} (i = 0, 1, \cdots, M-1)$, is a coherent state $|\alpha\rangle$ with MPSK,

$$\rho_i^{(\mathrm{in})} = \left| \alpha \mathrm{e}^{\mathrm{j}\frac{2i\pi}{M}} \right\rangle \left\langle \alpha \mathrm{e}^{\mathrm{j}\frac{2i\pi}{M}} \right|, \tag{1}$$

where $\mathrm{j} = \sqrt{-1}$ and α is the coherent amplitude. We assume that information is transmitted from the transmitter to the receiver through the quantum channel described by a map $\mathcal{L} : \mathcal{S}(\mathcal{H}_\mathrm{A}) \to \mathcal{S}(\mathcal{H}_\mathrm{B})$, where $\mathcal{S}(\mathcal{H})$ is the set of quantum density operators over the Hilbert space $\mathcal{H}$. We make the classical input alphabet $X = \{x_0, \ldots, x_{M-1}\}$ correspond to the set of quantum states $\{\rho_0^{(\mathrm{in})}, \ldots, \rho_{M-1}^{(\mathrm{in})}\} (\in \mathcal{S}(\mathcal{H}_\mathrm{A}))$, and introduce a map of x to the received quantum states $(\in \mathcal{S}(\mathcal{H}_\mathrm{B}))$, $\Phi : x \to \Phi_x := \mathcal{L}(\rho_x^{(\mathrm{in})})$, which we call classical-quantum channel[6].

The quantum density operator of a received quantum state, $\rho_i^{(\mathrm{out})}$, is represented as

$$\rho_i^{(\mathrm{out})} = \int P(\theta) |\alpha \mathrm{e}^{\mathrm{j}(\frac{2i\pi}{M}+\theta)}\rangle\langle \alpha \mathrm{e}^{\mathrm{j}(\frac{2i\pi}{M}+\theta)}| \mathrm{d}\theta, \tag{2}$$

where $P(\theta)$ is normal distribution, $\Theta \sim N(0, \sigma^2)$. Then we consider an ensemble $\mathcal{E}_M^{\mathrm{mixed}}$ consisting of $\rho_i^{(\mathrm{out})}$ taken with equal *a priori* probabilities $\xi_i = \frac{1}{M}$. Applying a positive operator-valued measure(POVM) $\{\Pi_i\}$ that $\sum_i \Pi_i = \mathbb{I}$ (i.e. identity operator) and $\Pi_i \geq 0$ to $\rho_i^{(\mathrm{out})}$ corresponding to value i, we can calculate a conditional

*id191002@cis.aichi-pu.ac.jp
†nakahira@lab.tamagawa.ac.jp
‡usuda@ist.aichi-pu.ac.jp

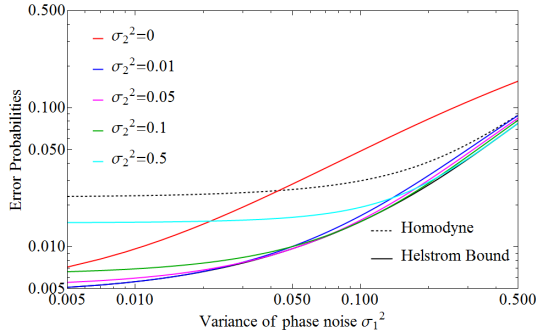


Fig. 1: The error probabilities of BPSK by the homodyne measurement and the quantum measurements optimized for σ_2^2 when $|\alpha|^2 = 1$.

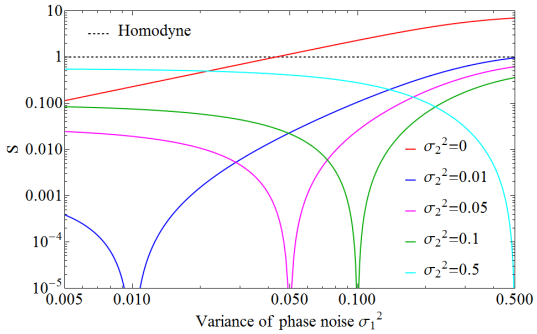


Fig. 2: The graph of S corresponding to the error probabilities of BPSK in Fig. 1 when $|\alpha|^2 = 1$.

probability $p(j|i) = \mathrm{Tr}\rho_i^{(\mathrm{out})}\Pi_j$ of detecting the value j. Thus, the error probability for the POVM to distinguish the $\mathcal{E}_M^{\mathrm{mixed}}$ is obtained by

$$P_e = 1 - \sum_i \mathrm{Tr}\xi_i\rho_i^{(\mathrm{out})}\Pi_i. \tag{3}$$

For deriving the minimum error probabilities P_e^{Opt} (i.e., Helstrom bound) for measuring BPSK signals and MPSK signals ($M > 2$), which achieved by applying optimum quantum receiver, we used a treatment given by [7] and an algorithm given by [8], respectively, to find the optimum detection operators Π_i (e.g. [5]).

The minimum error probabilities $P_e^{\mathrm{OptCla}}(\ni P_e^{\mathrm{Hom}}, P_e^{\mathrm{Het}})$ of optimum classical receiver, which achieved by the homodyne measurement for BPSK signals and the heterodyne measurement for MPSK signals(e.g., [9, 7]), are obtained by

$$P_e^{\mathrm{Hom}} = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{0} \int P(\theta) \mathrm{e}^{-2(y-|\alpha|\cos\theta)^2} \mathrm{d}\theta \mathrm{d}y, \tag{4}$$

$$P_e^{\mathrm{Het}} = \frac{1}{\pi} \int \int_{\frac{\pi}{M}}^{\frac{\pi(2M-1)}{M}} \int_0^{\infty} P(\theta) \times r\, \mathrm{e}^{-r^2-\alpha^2+2r|\alpha|\cos(\phi-\theta)} \mathrm{d}r\mathrm{d}\phi\mathrm{d}\theta, \tag{5}$$

respectively[5].

3 Error performance

An optimum quantum receiver is required to apply $\Pi := \{\Pi_i\}$ optimized for $\rho^{(\mathrm{out})} := \{\rho_i^{(\mathrm{out})}\}$. In other words, the optimum quantum receiver needs estimating $\rho^{(\mathrm{out})}$ exactly for finding the optimum Π. Because of $\rho^{(\mathrm{out})}$ that is subject to σ^2 except M and the average number of photons $|\alpha|^2$, we can rewrite $\rho^{(\mathrm{out})}$ and Π to function $\rho^{(\mathrm{out})}(\sigma^2) := \{\rho_i^{(\mathrm{out})}(\sigma^2)\}$ and $\Pi(\sigma^2) := \{\Pi_i(\sigma^2)\}$, respectively, while the optimum classical receiver does not depend on the estimation of σ^2. Estimating σ^2 for the optimum quantum receiver is not always exactly. We assume that σ_1^2 is the variance of the true phase noise and σ_2^2 is that of the estimated phase noise, instead of σ^2. As an undesirable example, [4] showed that the quantum receiver applying $\Pi(\sigma_2^2)$—the POVM optimized for $\rho^{(\mathrm{out})}(\sigma_2^2)$ measures $\rho^{(\mathrm{out})}(\sigma_1^2)$—has worse performance than an optimum classical receiver. Here, the error probability P_e exploited $\Pi(\sigma_2^2)$ is obtained by

$$P_e(\sigma_1^2, \Pi(\sigma_2^2)) = 1 - \sum_i \mathrm{Tr}\,\xi_i\rho_i^{(\mathrm{out})}(\sigma_1^2)\Pi_i(\sigma_2^2), \tag{6}$$

where $P_e = P_e^{\mathrm{Opt}}$ only for $\sigma_1^2 = \sigma_2^2$. Fig. 1 from [5] shows the error probabilities against σ_1^2 with the settings of $|\alpha|^2 = 1$ and $M = 2$. Dashed and solid black lines correspond to the optimum classical measurement and the quantum measurement; red, blue, pink, green, and cyan correspond to the estimated $\sigma_2^2 = 0, 0.01, 0.05, 0.1$, and 0.5. $\sigma_2^2 = 0$ implies the exploitation in terms of "an optimum quantum measurement only for coherent-state signals," and leads to the possibility of quantum non-superiority.

To evaluate the performance of a quantum receiver estimated σ_1^2 incorrectly, we consider a quantity S representing "how far is it from the performance of a quantum receiver to that of the optimum classical receiver," and introduce S defined in [4]:

$$S(\sigma_1^2, \Pi(\sigma_2^2)) := \frac{P_e(\sigma_1^2, \Pi(\sigma_2^2)) - P_e^{\mathrm{Opt}}(\sigma_1^2)}{P_e^{\mathrm{OptCla}}(\sigma_1^2) - P_e^{\mathrm{Opt}}(\sigma_1^2)}, \tag{7}$$

where $P_e^{\mathrm{OptCla}}(\sigma_1^2)$ and $P_e^{\mathrm{Opt}}(\sigma_1^2)$ are functions of σ_1^2. Because of $P_e(\sigma_1^2, \Pi(\sigma_2^2)) \geq P_e^{\mathrm{Opt}}(\sigma_1^2)$ and $P_e^{\mathrm{OptCla}}(\sigma_1^2) > P_e^{\mathrm{Opt}}(\sigma_1^2)$, we know that $0 \leq S$ and $S = 0$ only for $\sigma_1^2 = \sigma_2^2$. $S \geq 1$ implies that the performance of optimum classical receiver is equal to or better than that of the quantum receiver. Fig. 2 from [5] shows S corresponding to the error probabilities in Fig. 1.

4 Robust quantum measurements

We consider the range $R(\ni \sigma_1^2)$ estimated roughly instead of an unknown σ_1^2 for achieving higher performance, and introduce minimax criteria to address the problem that finds the appropriate quantum measurements described in chapter 1, in $|\alpha|^2 = 1$ and $M = 2$ settings.

4.1 Robustness

The performance of a quantum receiver which exploits $\Pi'(\in \Pi(\sigma_2^2))$, closest to that of the optimum classical receiver, is obtained by

$$S_{\max}(\Pi') := \max_{\sigma^2 \in R} S(\sigma^2, \Pi'). \tag{8}$$

In order to optimize the worst case, $S_{\max}(\Pi') \to \min(=: S^{\mathrm{Minimax}})$ (i.e., minimax value), an appropriate Π' is re-

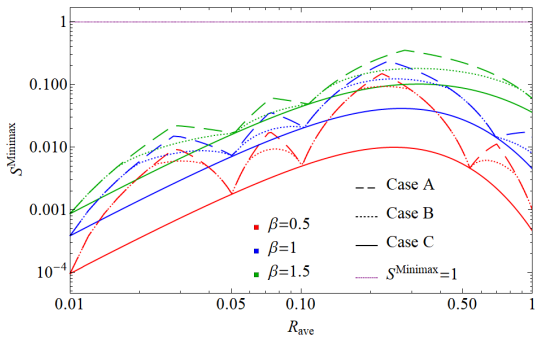


Fig. 3: The graph of robustness S^{Minimax} that applied the most robust quantum measurements when $|\alpha|^2 = 1$.

quired to find.

In this paper, we define robustness as "quantum superiority will be kept over a certain limit even if uncertainty exists in the estimation of σ_1^2." Let R_{ave} be the average of R, the amount in terms of the uncertainty is represented by a parameter β—it is taken from the width of R, $W = \beta \cdot R_{\mathrm{ave}}$, where β satisfies $0 \leq \beta \leq 2$. Then we fix R_{ave} and S^{Minimax}, and consider that the larger β, the higher the robustness. Naturally, if R_{ave} and β are fixed, it can be said that the smaller S^{Minimax}, the higher the robustness. We determine S^{Minimax} as the amount evaluated the robustness, and introduce minimax criteria to find the most robust quantum measurements under three cases.

4.2 Case A

A theorem establishes that any POVM can be realized on an extended Hilbert space[10], yet the method of realizing any quantum measurement corresponding POVM cannot necessarily be found. We assume a constraint imposed on the number n of quantum measurements we can prepare, and consider which one is the most robust, based on minimax criteria. If a set of optimum quantum measurements $\mathcal{X} = \{\Pi(\sigma_2^2)|\sigma_2^2 \in \sigma_1'^2\}$—these measure the signals including phase noise $\sigma_1'^2 = \{\varsigma_1^2, \varsigma_2^2, \ldots, \varsigma_n^2\}$ with Helstrom bound—is already realized, we can determine the most robust Π_{A} that satisfies

$$\min_{\Pi_{\mathrm{A}} \in \mathcal{X}} \max_{\sigma^2 \in R} S(\sigma^2, \Pi_{\mathrm{A}}). \tag{9}$$

4.3 Case B

The robustness exploited $\mathcal{X}$ is limited within each of $\mathcal{X}$ in Case A, because the method is that it switches between $\mathcal{X}$ depending on R. In order to surpass that, we consider a stochastic method that mixes the quantum measurements. We prepare $\mathcal{X}$ as well as Case A, and then exploit $\Pi_{\mathrm{min}}(\in \mathcal{X})$ optimized for $R_{\mathrm{min}} := \min R$ with probability c_1 and $\Pi_{\mathrm{max}}(\in \mathcal{X})$ optimized for $R_{\mathrm{max}} := \max R$ with probability c_2, where c_1 and c_2 satisfy $c_1 + c_2 = 1$. The new quantum measurement is represented as

$$\Pi_{\mathrm{B}}(\Pi_{\mathrm{min}}, \Pi_{\mathrm{max}}, c_1) := c_1 \Pi_{\mathrm{min}} + c_2 \Pi_{\mathrm{max}}. \tag{10}$$

Now, we can determine the most robust Π_{B} that satisfies

$$\min_{0 \leq c_1 \leq 1} \max_{\sigma^2 \in R} S(\sigma^2, \Pi_{\mathrm{B}}(\Pi_{\mathrm{min}}, \Pi_{\mathrm{max}}, c_1)). \tag{11}$$

The robustness of new quantum measurement will surpass or equal that of Case A, and the latter implies $\Pi_{\mathrm{min}} = \Pi_{\mathrm{max}}$. Note that since this case is on the basis of a stochastic method, the higher robustness is achieved with a large number of measuring times.

4.4 Case C

We provide an ideal case that if the constraint described in Case A is lifted in spite of uncertainty exists in the estimation of σ_1^2 yet, then a set of optimum quantum measurements $\mathcal{Y} = \{\Pi(\sigma_2^2)|\sigma_2^2 \in R\}$—these measure the signals including any $\sigma_1^2 (\in R)$ with Helstrom bound—can be prepared. The most robust Π_{C} is determined by

$$\min_{\Pi_{\mathrm{C}} \in \mathcal{Y}} \max_{\sigma^2 \in R} S(\sigma^2, \Pi_{\mathrm{C}}). \tag{12}$$

We also reduce the condition (12) to

$$S(R_{\mathrm{min}}, \Pi_{\mathrm{C}}) = S(R_{\mathrm{max}}, \Pi_{\mathrm{C}}), \ \ \Pi_{\mathrm{C}} \in \mathcal{Y}. \tag{13}$$

In addition, this case implies a solution that how an optimum quantum receiver deals with the uncertain estimation of σ_1^2 as a robust quantum receiver.

5 Conclusion

In this paper, we derived the most robust measurements that respectively correspond to three cases, based on the minimax criteria. The numerical results are shown in Fig. 3, which plot S^{Minimax} against R_{ave} in $\sigma_1'^2 = \{0.01, 0.05, 0.10, 0.50, 1.00\}$ setting. Dashed, dotted, and solid lines correspond to Case A, Case B, and Case C; red, blue, and green correspond to $\beta = 0.5, 1$, and 1.5. The dotted purple line is an exception which means a limit to the robustness.

Fig. 1 suggests the possibility that the optimum quantum receiver measuring BPSK coherent-state signals with Helstrom bound, such as Dolinar receiver[11], is not geared towards applying to the wireless quantum communications where the phase noise occurs. However, an optimum quantum receiver dealing with the phase noise has not been realized yet, as well as it is not clear whether that can be realized. This paper suggests that even if an optimum quantum receiver dealing with any σ_1^2 can not be realized, we can design a practical, robust quantum receiver by means of realizing quantum measurements optimized for some of σ_1^2 on the basis of Case A and B.

Finally, we provide a supplement in terms of when to use Case B instead of Case A. In Case B, we suppose that the use of Π_{min} and Π_{max} can be seen as a random variable followed Bernoulli distribution with parameter c_1. If we set confidence level at 95%, the confidence interval concerning the mean $\overline{c_1}$ is $\overline{c_1} \pm 1.96 \times \sqrt{c_1(1-c_1)/t}$, where t is the number of measuring times. As an example, if the error of confidence interval is required within $(\overline{c_1}) \pm 1\%$, the necessary t is $t_{\mathrm{B}} \approx 1.96^2 \times c_1(1-c_1)/0.01^2 = 9218$, in $\beta = 1$ and $R_{\mathrm{ave}} = 0.28$ settings, where the most robust $\Pi_{\mathrm{B}}(\Pi(0.5), \Pi(0.1), 60\%)$ is exploited. Case A is used in the case that the estimated $t << t_{\mathrm{B}}$.

Acknowledgment This work has been supported in part by JSPS KAKENHI Grant Number JP16H04367.

References

[1] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro and H. P. Yuen, Classical capacity of the lossy bosonic channel: the exact solution, Phys. Rev. Lett. **92**, 027902, 2004.

[2] J. H. Shapiro, S. Guha, and B. I. Erkmen, Ultimate channel capacity of free-space optical communications, J. Opt. Netw. **4**(8), pp.501-516, 2005.

[3] S. Olivares, S. Cialdi, F. Castelli, and M. G. A. Paris, Homodyne detection as a near-optimum receiver for phase-shift-keyed binary communication in the presence of phase diffusion, Phys. Rev. A**84**, 050303(R), 2013.

[4] S. Koyama and T. S. Usuda, Error performance of optimum quantum detection for BPSK signals in the presence of phase noise and its robustness, Proc. of ISITA2014, pp.259-263, 2014.

[5] T. Wang, K. Nakahira and T. S. Usuda, Error performance and robustness of optimum quantum detection for MPSK signals in the presence of phase noise, Proc. of ISITA2018, pp.344-348, 2018.

[6] A. S. Holevo, Coding theorems for quantum channels, Tamagawa University Research Review, no.**4**, 1998.

[7] C. W. Helstrom, Quantum detection and estimation theory, Academic Press, New York, 1976.

[8] C. W. Helstrom, Bayes-cost reduction algorithm in quantum hypothesis testing, IEEE Trans. Inform. Theory **28**, pp.359-366, 1982.

[9] M. Sasaki, T. S. Usuda, and O. Hirota, Physical aspect of the improvement of quantum-noise characteristics caused by unitary transformation with a nonlinear optical medium, Phys. Rev. A**51**, 1995.

[10] A. Peres, Quantum Theory: Concepts and Methods, Kluwer, Dordrecht, 1993.

[11] S. J. Dolinar, An Optimum Receiver for the Binary Coherent State Quantum Channel, MIT Res. Lab. Electron. Quart. Prog. Rep. **111**, 115, 1973.

Evaluation of quantum gain for KCQ protocol using best binary codes in high or low rate

Mana Yoshida[1] * Shogo Usami[2] † Tsuyoshi Sasaki Usuda[1] ‡

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan*
[2] *School of Science and Engineering, Meijo University, 1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi 468-8502, Japan.*

Abstract. Keyed communication in quantum noise (KCQ) is a quantum cryptographic principle that was invented by H. P. Yuen in 2000. The security of KCQ protocols is originated from different performance of optimum classical and quantum receivers, which corresponds to so-called quantum gain. In this paper, we evaluate KCQ protocols using binary codes that are the best in terms of reliable communications. We consider quantum and classical reliability functions for the evaluation. As a result, it is clarified that the best codes in reliable communications are not good for KCQ protocols.

Keywords: quantum cryptography, KCQ protocol, quantum gain, reliability function, zero rate, classical channels, classical-quantum channels.

1 Introduction

Keyed communication in quantum noise (KCQ) invented by Yuen is a quantum cryptographic principle, based on the idea of using the difference in performance of an optimum measurement by the presence of a key for security[1]. A legitimate receiver with a key can use optimum quantum measurement, whereas an eavesdropper with nothing can use only an optimum classical measurement at best. This construction is the origin of the security in KCQ protocols.

In this way, security in KCQ protocols concerns the superiority of an optimum quantum receiver compared with an optimum classical receiver, namely, the so-called "quantum gain". However, it is difficult to estimate the capabilities of a legitimate receiver and an eavesdropper. Hence, Yuen proposed surprisingly an evaluation method that virtually disclosed the key to an eavesdropper after measurement[1]. Quantum gain is by an "upper bound evaluation" the smallest difference between the capabilities of a legitimate receiver and an eavesdropper. It determines the rate that an average number of photons satisfied the same error probability in an optimum receiver of classical or quantum type.

There are two classes of KCQ protocols according to types of quantum states used: single-mode and multi-mode. The quantum gain limit is 6[dB] for the single-mode[1]. Yuen demonstrated that the quantum gain limit for the multi-mode is nothing while proposing his own cryptosystem, coherent pulse position modulation (CPPM). Kadoya et al. suggested using binary codes, as it is a generalization of CPPM in a certain sense[2]. However, there are problems in selecting the appropriate code or establishing an evaluation method.

We consider the best codes that give the smallest error probability in this study. Hence, we focus on the reliability function, which is defined as the exponential of the best error probability. We assess the quantum gain in the KCQ protocol using the difference between the classical and the quantum reliability functions by applying Kurokawa's idea[3] to quantum cryptography.

*im191813@cis.aichi-pu.ac.jp
†susami@meijo-u.ac.jp
‡usuda@ist.aichi-pu.ac.jp

2 Reliability function

2.1 Overview of reliability function

The reliability function is defined as the exponential of the decoding error probability of a very long code of block length n and coding rate R using the best code with the smallest decoding error probability (here, we call it the best error probability). Let $P_{\mathrm{e}}^{\mathrm{opt}}(n,R)$ be the best error probability for n and R. Then it is expressed by the so-called *reliability function* $E(R)$ as

$$P_{\mathrm{e}}^{\mathrm{opt}}(n,R) = e^{-nE(R)}. \tag{1}$$

$E(R)$ is also called an *error exponent*. Therefore, $E(R)$ is formally expressed as

$$E(R) = \frac{1}{n}\ln\left[\frac{1}{P_{\mathrm{e}}^{\mathrm{opt}}(n,R)}\right]. \tag{2}$$

In the theory of reliability functions, $E(R)$ is defined by considering the limit $n \to \infty$ (see [4, 5] for more details). In general, it is difficult to compute the actual minimum decoding error probability with the best code. However, because the upper and lower bounds of $E(R)$ are known, an exact value for $E(R)$ may be obtained in special cases when the upper and lower bounds coincide. When the rate R is extremely high or low, i.e., it is close to the channel capacity or almost zero, tight upper and lower bounds are known in the sense that they are close to the true values.

2.2 Quantum reliability function

Let $\mathcal{H}$ be the Hilbert space of a quantum system. We consider a classical-quantum communication that

sends M pure-state signals $|\psi_i\rangle \in \mathcal{H}$ indexed by $i (i = 1, 2, \ldots, M)$. Let ξ_i be the *a priori* probability of each classical information i. Then

$$\rho = \sum_{i=1}^{M} \xi_i |\psi_i\rangle \langle\psi_i| \tag{3}$$

is called the density operator of the quantum information source $\{|\psi_i\rangle\}$.

2.2.1 Tight bounds in high rate

Tight bounds of quantum reliability function in high rate are known as the sphere packing bound[6] and the random coding bound[5], respectively. Let $E_{\rm QU}(R)$ and $E_{\rm QL}(R)$ be the upper and lower bounds. Then,

$$E_{\rm QU}(R) = \max_{0\le s} \max_{\xi} \left[\mu(s,\xi) - sR\right], \tag{4}$$

$$E_{\rm QL}(R) = \max_{0\le s\le 1} \max_{\xi} \left[\mu(s,\xi) - sR\right], \tag{5}$$

where

$$\mu(s,\xi) = -\ln \mathrm{Tr}\, \rho^{1+s}, \tag{6}$$

and ρ is given by Eq.(3). Kato proved that the uniform $\{\xi_i\}$ maximizes $\mu(s,\xi) - sR$ in both bounds when signals are symmetric[7, 8]. Therefore, for symmetric signals, we have

$$E_{\rm QU}(R) = \max_{0\le s} \left[\mu\left(s, \left\{\frac{1}{M}\right\}\right) - sR\right], \tag{7}$$

$$E_{\rm QL}(R) = \max_{0\le s\le 1} \left[\mu\left(s, \left\{\frac{1}{M}\right\}\right) - sR\right]. \tag{8}$$

2.2.2 Quantum reliability function at zero rate

As for tight bounds of quantum reliability function in low rate, the exact value of the quantum reliability function is known at zero rate ($R = 0$)[5]. This *zero-rate quantum reliability function* is expressed as

$$E_{\rm Q}(+0) = -\min_{\{\xi\}} \sum_{i,k} \xi_i \xi_k \ln |\langle\psi_i|\psi_k\rangle|^2. \tag{9}$$

In the case of binary quantum signals,

$$E_{\rm Q}(+0) = -\ln |\langle\psi_0|\psi_1\rangle|. \tag{10}$$

2.3 Classical reliability function

Let i ($i = 1, 2, \ldots, M$) and j ($j = 1, 2, \ldots, M'$) be the input and output of the classical channel. The classical channel is represented by a conditional probability $P(j|i)$ of outputting j by inputting i.

2.3.1 Tight bounds in high rate

Tight bounds of classical reliability function in high rate are also known and called the sphere packing and random coding bounds[4]. Let $E_{\rm CU}(R)$ and $E_{\rm CL}(R)$ be the upper and lower bounds. Then,

$$E_{\rm CU}(R) = \max_{0\le s} \max_{\xi} \left[\nu(s,\xi) - sR\right], \tag{11}$$

$$E_{\rm CL}(R) = \max_{0\le s\le 1} \max_{\xi} \left[\nu(s,\xi) - sR\right], \tag{12}$$

where

$$\nu(s,\xi) = -\ln \sum_{j=1}^{M'} \left(\sum_{i=1}^{M} \xi_i P(j|i)^{\frac{1}{1+s}}\right)^{1+s}. \tag{13}$$

As same as for the quantum reliability function, the corresponding channel matrix becomes symmetric by the symmetry of the signals, so that the optimum probability distribution is uniform. It is then sufficient to perform only the optimization on s. For the classical reliability function, if the optimal s is less than or equal to 1, then $E_{\rm CL}(R) = E_{\rm CU}(R)$, which is the value of the classical reliability function itself.

2.4 Classical reliability function at zero rate

In classical theory, a tight lower bound in low rate is known as the so-called expurgated bound and is defined as[4]

$$E_{\rm C-ex}(R) = \sup_{\sigma\ge 1}[-\sigma R + \sigma\log 2 - \sigma\log(1 + a^{1/\sigma})]. \tag{14}$$

Moreover, it was proved that $E_{\rm C-ex}(R = 0)$ is the exact classical reliability function at zero rate. Therefore, the *zero-rate classical reliability function* is

$$E_{\rm C}(+0) = E_{\rm C-ex}(R = 0). \tag{15}$$

2.5 The best error probability and its bounds

For sufficiently long codes of block length n and coding rate R, the quantum version of the best error probability is written as $P_{\rm Q}^{\rm opt}(n, R)$, and the classical version as $P_{\rm C}^{\rm opt}(n, R)$. When $R = 0$,

$$P_{\rm Q}^{\rm opt}(n, R = 0) = e^{-nE_{\rm Q}(+0)}, \tag{16}$$

$$P_{\rm C}^{\rm opt}(n, R = 0) = e^{-nE_{\rm C}(+0)}. \tag{17}$$

Moreover, for any R,

$$e^{-nE_{\rm QU}(R)} \le P_{\rm Q}^{\rm opt}(n, R) \le 2e^{-nE_{\rm QL}(R)}, \tag{18}$$

$$e^{-nE_{\rm CU}(R)} \le P_{\rm C}^{\rm opt}(n, R) \le e^{-nE_{\rm CL}(R)}, \tag{19}$$

and the above inequalities are tight when R is close to the capacity. Note that the upper bound of the error probability in the quantum version takes a factor of two (see [5] for more detail).

3 Properties of quantum gain

In this study, we consider KCQ protocols using binary codes, so that we assume the BPSK (binary phase shift keying) coherent-state signals $\{|\alpha\rangle, |-\alpha\rangle\}$. The signals are characterized by their coherent amplitude α or the average number of photons $N_{\rm s} = |\alpha|^2$.

The quantum gain can be expressed using the average number of photons in the quantum and classical cases when their probabilities of error P have the same value:

$$\mathrm{Gain} = 10\log_{10} \frac{N_{\rm s}^{\rm C}(\text{When } P_{\rm C} = P)}{N_{\rm s}^{\rm Q}(\text{When } P_{\rm Q} = P)} \quad [\mathrm{dB}], \tag{20}$$

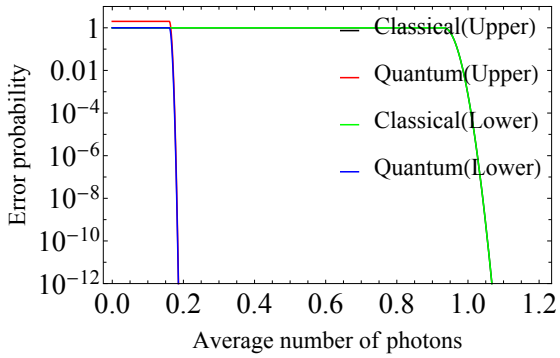


Figure 1: Upper and lower bounds of error probabilities for optimum quantum and classical measurements when $R = 0.4, n = 20000$.

where N_s^C represents the average number of photons when the error probability P_C becomes P in the classical instance and N_s^Q represents the average number of photons when the error probability P_Q becomes P in the quantum instance.

Figure 1 shows upper and lower bounds of the error probability with respect to the average number of photons when $R = 0.4$ and $n = 20000$. In this case, the bounds are tight, so that the black and green lines coincides and the red and blue lines are almost coincides. The gap between the green and blue lines represents the upper bound of the quantum gain and that between the green and red lines represents the lower bound. Table 1 shows the quantum gains [dB] for error probabilities of 10^{-12} or close to unity. In both cases, the upper and lower bounds of N_s^C match the classical case, whereas N_s^Q differs for the quantum case, as mentioned above. Hence, Table 1 lists Gain(Lower) as the lower bound and Gain(Upper) as the upper bound of the quantum gain. Both values were found to be about 7.5[dB] and there is no difference larger than 0.1[dB] even if the code of block length is doubled.

In addition, we observe the quantum gain when n is fixed and R is changed. The lower the rate is, the larger the quantum gain is. Table 2 shows the quantum gain when $R = 0$. From Table 1, 2, it seems that the smaller the rate is, the larger the quantum gain is. However, the difference is slight.

Table 1: Quantum gain [dB] when $R = 0.4$.

n	P	Gain(Lower)	Gain(Upper)
10000	10^{-12}	7.574	7.583
15000		7.581	7.583
20000		7.585	7.595
10000	1	7.499	7.645
15000		7.499	7.645
20000		7.544	7.645

Table 2: Quantum gain [dB] when $R = 0$.

n	P	Gain
20000	10^{-20}	7.9825
10^5		7.9799
10^6		7.9796
20000	10^{-12}	7.9818
10^5		7.9780
10^6		7.9780

4 Conclusion

In this paper, we use the upper and lower bounds of classical and quantum reliability functions for binary signals to evaluate the security of the KCQ protocol using binary codes. This corresponds that we consider the KCQ protocol using the best codes in reliable communications. The result of our evaluation is as the following: The quantum gain using the best codes exceeds 6[dB] which is the limit of the single-mode KCQ protocol. However, the gain seems to be almost independent of the length of codes. Therefore, we conjecture that there is limitation of the quantum gain when using the best codes. This property is completely different from the case of CPPM signals.

As a future subject, we will consider the quantum gain when using the best code for cryptographic system.

Acknowledgment This work has been supported in part by KAKENHI JP16H04367. We would like to thank E. Wada for helpful discussion. We also thank Richard Haase, Ph.D., from Edanz Group (www.edanzediting.com/ac) for editing a draft of this manuscript.

References

[1] H.P. Yuen, "KCQ: A new approach to quantum cryptography I. General principles and key generation," arXiv:quant-ph/0311061v6, (2004).

[2] A. Kadoya, Y. Umemura, S. Asano, N. Iwata, and T.S. Usuda, "KCQ using binary linear code and its performance," Proc. of AQIS2015, pp.161-162, (2015).

[3] K. Kurokawa and O. Hirota, "Properties of quantum reliability function and its applications to several quantum signals," IEICE Trans. on Fundamentals. **J83-A**, pp.57-66, (2000). (in Japanese)

[4] R.G. Gallager, "Information Theory and Reliable Communication," John Wiley & Sons, Inc., New York, (1968).

[5] M.V. Burnashev and A.S. Holevo, "On reliability function of quantum communication channel," Probl. Peredachi Inform. **34**, 2, pp.1-13, (1998).

[6] M. Dalai, "Lower bounds on the error probability for classical and classical-quantum channels," IEEE

Trans. on Inform. Theory **59**, 12, pp.8027-8056, (2013).

[7] K. Kato, "Error exponents of quantum communication system with M-ary PSK coherent state signal," Tamagawa Univ. Quant. ICT Res. Inst. Bulletin, **1**, 1, pp.33-40, (2011).

[8] K. Kato, "A note on the reliability function for M-ary PSK coherent state signal," Tamagawa Univ. Quant. ICT Res. Inst. Bulletin, **8**, 1, pp.21-25, (2018).

Quantum control with side informaiton

Ya Cao[1],* Fei Gao[1], DanDan Li[1], and QiaoYan Wen[1]†
[1] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China*

(Dated: July 10, 2019)

Protecting the state of a qubit against decoherence is an essential task in realistic quantum techniques. Recent work [Physical Review A 95(3): 032313 (2017)] shows that quantum composite control can efficiently escape from the dilemma of high fidelity and low success probability for the state protection task. Regretfully, this work just work for qubit that in special states where the priori probabilities are equal. In this paper, we consider general case where the states are in an arbitrary priori probability and present a generalized scheme. We derive its performance by both analytical and numerical optimization over parameters therein. The generalized one has advantage in two aspects. On the one hand, when priori probability is equal, this scheme outperforms than previous schemes. On the other hand, when inequal priori probability is considered, we show that the priori probability provide information for protecting and thus the performance is better than that in equal priori probability case.

Keywords: Decoherence,Quantum control, Quantum state protection

I. EXTEND ABSTRACT

Quantum information is fragile to decoherence, which heavily drags the step of Quantum technologies to practical realization. Classical control techniques shows great tolerance of noise. However, the extension from classical control technique to quantum realm is not trivial.

Unlike classical control techniques, quantum control meets two mountains. Firstly, Heisenberg's inequality limits the amount of information that measurement can obtain – information gain. Secondly, there will be an undesired phenomenon, "back-action", when quantum measurements are applied. These properties limit the performance of quantum control and make us to design control schemes with delicate.

Recent work shows that weak measurement can solve the dilemma between information gain and back-action [1] and propose a quantum feedback control (QFBC) scheme. There a weak measurement is applies after the noise and its result is fed back to a correction operator accordingly. Thereafter, Wang *et al.* presented a quantum feedforward (QFFC) control scheme[2], which improves the fidelity between output state and input state to arbitrarily close to unit. The idea therein is to drive the input state to some state almost immune to the noise before the target qubit enter the noise and then undoes the noise by partial weak measurement. However, the high fidelity can be achieved only at the price of low success probability. To solve this, Ya *et al.* nontrivially combines QFBC and QFFC, which is called quantum composite control(QCC)[3]. The authors has shown that QCC finds a better balance between fidelity and success probability by feeding the second measurement result in QFFC process to a correction unitary.

All the presented control schemes are depend on prior information, or called side information, such as the overlap, the prior probability and so on. Thus side information is essential for protection. However, the side information included in those schemes is not complete even in equal prior probability case. An optimal control scheme should taking full consideration of all given side information. In this paper, we design such kind a scheme under QCC structure. The measures or corrections therein are chosen from a family of weak measures or unitaries, respectively, which consists all given information including the overlap, the phase, the prior probability and the noise strength. By analytical and numerical optimization over all related parameters, an optimal scheme is presented.

Analysis comes from two aspects. Firstly, when equal priori probability is considered, we find the presented control schemes lacks some quantum side information. In order to show the advantage clearly, we plot figure 1.Secondly, when inequal prior probability is included, existing control schemes lack some classical side information. To find the effect bringing by classical side information, we fix the quantum side information can be included, and plot figure 2,3 and 4. Figure 2 shows the fidelity improvement, corresponding fidelity and nontrivial parameter that describing prior probability. Figure 3 gives an example to show the parameter is nontrivial in the sense that it different from that in the Helstrom basis or zero, trivially. Figure 4 plots the relation between fidelity and success probability. There we show our scheme (the triangle dots) reveals an apparent improvement in success probability when requiring the unit fidelity.

We expect our results will be helpful for suppressing decoherence in quantum computing and quantum information processing. Besides, the measurements we used here may provide a lot of candidates for developing weak

* caoshinee@126.com
†

measurements in balancing information gain and disturbance. At last, a more general family of measurements and corrections in our scheme may makes state protection less sensitive to noise and initial state, which may lead to a more realistic scheme.

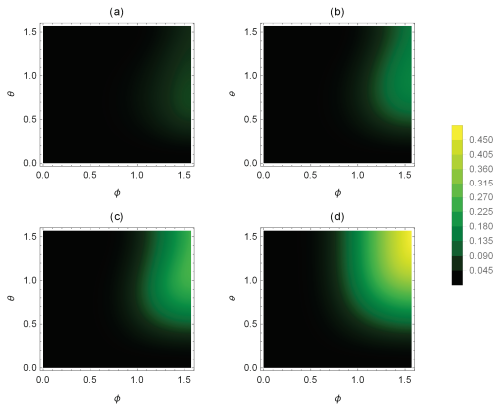


FIG. 1. Advantage of fidelity as a function of the initial angle θ and phase ϕ for different noise strength (a) r=0.25, (b) r=0.5, (c) r=0.75 and (d) r=1.

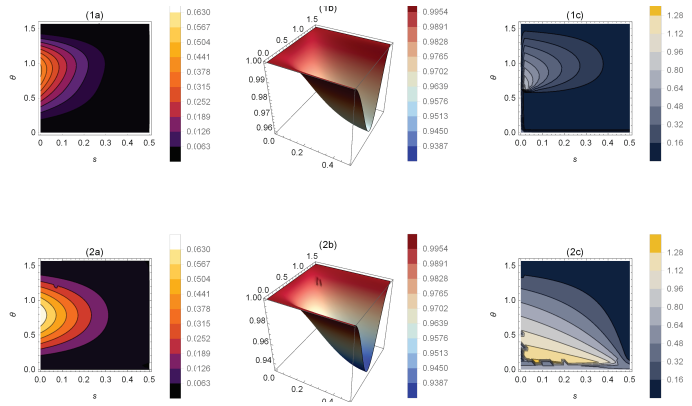


FIG. 2. Fidelity improvement, fidelity for our scheme and parameter α as a function of the initial angle θ and prior probability s when fixing ϕ=0 (fix quantum side information) for selected noise strength (1)r=0.5 and (2) r=1.

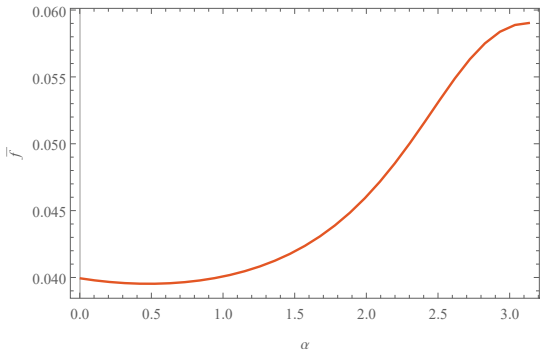


FIG. 3. Infidelity $\bar{f}$ as a function of the parameter *alpha* when s_+=1/3, $\theta = \pi/3$, $\phi = 0$ and $r = 0.8$ for schemes without fully characterization of classical side information, our scheme and Helstrom scheme(left-¿right).

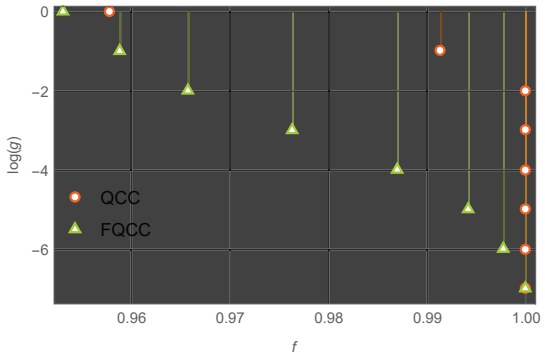


FIG. 4. Fidelity f VS. Log of success probability $log(s)$ when $\theta = \pi/3$ r=0.9 and s_+=1/3. Here dot and triangle for the scheme without and with classical side information, respectively.

[1] C. Q. Wang, B. M. Xu, J. Zou, Z. He, Y. Yan, J. G. Li, and B. Shao, Phys. Rev. A **89**, 032303 (2014).

[2] A. M. Brańczyk, P. E. M. F. Mendonça, A. Gilchrist, A. C. Doherty, and S. D. Bartlett, Phys. Rev. A **75**, 012329 (2007).

[3] Y. Cao, G. J. Tian, Z. C. Zhang, Y. H. Yang, Q. Y. Wen, and F. Gao. Physical Review A **95**, 032313 (2017).

Towards a quantum-inspired proof for IP = PSPACE

Ayal Green[1] * Yupan Liu[1] † Guy Kindler[1] ‡

[1] *School of Computer Science and Engineering, The Hebrew University, Jerusalem 91904, Israel*

Abstract. We explore quantum-inspired interactive proof systems where the prover is limited. Namely, we improve on a result by [5] showing a quantum-inspired interactive protocol (IP) for PreciseBQP where the prover is only assumed to be a PreciseBQP machine, and show that the result can be strengthened to show an IP for $\mathsf{NP}^{\mathsf{PP}}$ with a prover which is only assumed to be an $\mathsf{NP}^{\mathsf{PP}}$ machine - which was not known before. We also show how the protocol can be used to directly verify QMA computations, thus connecting the sum-check protocol by [2] with the result of [5]. Our results shed lights on a quantum-inspired proof for PSPACE = IP, since PreciseQMA captures the full PSPACE power.

Keywords: interactive proofs, verification of quantum computation

1 Introduction

The study of interactive proof systems began in the 1980's, and while initially only a few non-trivial proof systems were known [8,20], at the beginning of the 1990's it was discovered that interactive proof systems are actually extremely powerful.

In broad terms, in an interactive proof for a language L, a computationally weak *verifier* interacts with one or more *provers* which are stronger computationally. For a given input x, the provers claim that $x \in L$, but the verifier would not just take their word for it. Instead, an interactive protocol is commenced, followed by the verifier either 'accepting' the claim, or 'rejecting' it. The protocol has perfect completeness if, when x is indeed in L and the provers honestly follow the protocol, the verifier eventually accepts. The protocol has soundness-parameter s, if when x is not in L then the verifier rejects with probability at least $1 - s$, independently of whether the provers follow the protocol or not. If a protocol for L exists that has perfect completeness and soundness $1/2$, we say that it is an interactive protocol for L.

The celebrated IP = PSPACE [24, 33] result showed that any language in PSPACE has an interactive protocol with a (randomized) polynomial-time Turing machine as a verifier, and with a single prover that is computationally unbounded. The result MIP = NEXP [10] that soon followed, showed that if two provers are allowed instead of one, interactive protocols exist for any language in non-deterministic exponential space. For the languages in the smaller class NP, the celebrated PCP theorem [6,7] showed that they can be verified by a multi-prover interactive protocol with a single round: When proving that $x \in L$, the verifier sends each of two provers a 'question' string of $O(\log |x|)$ length, and gets a constant number of bits from each prover. It is important to note that in all multi-prover protocols, the provers may not communicate at all while the protocol is taking place.

Computation delegation. The PCP theorem had a huge impact for showing hardness-of-approximation for optimization problems. However the PCP theorem, as well as other interactive proofs and the techniques used to obtain them seem very relevant for another very practical application, namely computation delegation. The goal in computation delegation, introduced in [19], is for the verifier to commission the provers to perform a computational task. The provers must then supply a result of the computation, but then to also prove to the verifier, via an interactive protocol, that the result that they sent is indeed correct. Of course, this would be pointless if the proof protocol would require more resources than what the verifier needs to perform the computation herself.

For delegation, the aforementioned line of results are not useful in their original form, as they usually assume provers that are computationally unbounded. For practical applications we would like even a relatively weak honest prover to be able to follow the protocol. This brings up a natural and practical question: which classes of problems can we verify using provers that are not assumed to be all powerful?

Note that a similar question, namely of interactive *arguments* is studied in cryptography. However in arguments, it is ok if the provers can convince the verifier of a false statement, if this requires the provers to be very strong computationally. Here we want the protocol to be secure even if the provers are very strong, but we require additionally that honest provers do not need to be as strong.

Quantum delegation. The motivation of delegation of quantum computing is quite clear. Suppose we are given a box that we can feed with inputs, and then obtain from it outputs that are claimed to be the result of a quantum computation. How can we tell if the box actually performs the desired computation?

The holy grail of quantum computation-delegation would therefore be a protocol that verifies a polynomial-time quantum computation, by letting a classical polynomial-time randomized machine interact with an efficient quantum maching, namely one which is only assumed to be have the power of BQP.

There has been significant progress on interactive quantum proofs and quantum computation delegation

*ayalg@cs.huji.ac.il
†yupan.liu@gmail.com
‡gkindler@cs.huji.ac.il

in the last decade. For instance, it was shown that a polynomial-time classical machine can verify a polynomial-time quantum computation, if she is allowed to interact with a constant number of entangled polynomial-time quantum provers [13, 29–32]. Likewise, if we consider a single very restricted quantum device, namely one with a constant number of qubits, then it can verify polynomially long quantum computations [3, 4, 9, 16, 17].

Mahadev's celebrated result [25] (see also [11, 12, 21] provides a protocol by which a strictly classical verifier can verify quantum computation using a single quantum prover. However Mahadev's protocol relies on a computational-hardness assumption for soundness (a standard post-quantum cryptographic assumption). A protocol that is unconditionally sound is still unknown.

Towards unconditional quantum delegation. As an intermediate step in the search for information-theoretic soundness for verifying polynomial quantum computation with only classical interactions, a more general question arises: which classes of problems can be verified using a single prover which is only assumed to have the computational power of the same class?

Definition 1 (In-class IP - informal) *Let* $\mathsf{IP}[\mathcal{P}, \mathcal{V}]$ *be the set of all languages* $\mathcal{L}$ *for which there exists an efficient interactive proof protocol between a* $\mathcal{V}$*-power verifier and a prover, such that a prover in class* $\mathcal{P}$ *can follow the protocol for an input in* $\mathcal{L}$*, and the protocol is sound against* any *prover when the input is not in* $\mathcal{L}$*.*

A recent attempt by Aharonov and Green [5] provides an interactive proof protocol verifying *precise* polynomial-time quantum computations (PreciseBQP), showing that PreciseBQP $\subseteq$ IP[PreciseBQP, BPP]. Let us remind the reader of the definition of PreciseBQP: Recall that in normal polynomial-time quantum computation (BQP), the gap between the acceptance probability of *yes*-cases and *no*-cases is inverse-polynomial[1]. In the precise case, however, this gap is inverse exponential. This change in the precision gives a much stronger class – in fact it captures the full power of PP [1, 18, 23]. We note that it immediately follows from [5], that the same protocol can be extended to work for languages in $\mathsf{P}^{\mathsf{PreciseBQP}} = \mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\#\mathsf{P}}$. Thus it gives a quantum analogue of [24], which showed an interactive protocol for $\mathsf{P}^{\#\mathsf{P}}$.

We eventually would like a protocol with a BQP prover, but it is also natural to try to extend the protocol of [5] to larger complexity classes – we do know that such a protocol exists for PSPACE = BQPSPACE, but even getting direct quantum-inspired protocol for BQPSPACE would be interesting. A potential way to answer this question is by considering PreciseQMA (informally, a variant of QMA where the gap between the acceptance probabilities of *yes* and *no* cases is inverse exponential), which has been shown to be equal to PSPACE [14, 15].

[1]This gap can be amplified to a constant using standard gap amplification techniques.

2 Main Results

An in-class interactive proof for PreciseQCMA. We make a step towards a direct BQPSPACE $\subseteq$ IP result: we show that PreciseQCMA, a sub-class of PreciseQMA = BQPSPACE in which the witness is restricted to being classical , can be verified by a classical interaction with a PreciseQCMA prover. This is stated in the following:

Theorem 2 PreciseQCMA $\subseteq$ IP[PreciseQCMA, BPP].

Noting that PreciseQCMA is equivalent to the classical complexity class $\mathsf{NP}^{\mathsf{PP}}$ [18, 27], we get the immediate corollary.

Corollary 3 $\mathsf{NP}^{\mathsf{PP}} \subseteq \mathsf{IP}[\mathsf{NP}^{\mathsf{PP}}, \mathsf{BPP}]$.

This result is an improvement on [5, 24], and was not known before.

3 Proof Techniques

In our proof we make crucial use of the following protocol from [5] (see Theorem 2 and 4).

The AG protocol: An in-class interactive proof for PreciseBQP. Using the terminology of Definition 1), the protocol in [5] shows that as

$$\mathsf{PreciseBQP} \subseteq \mathsf{IP}[\mathsf{PreciseBQP}, \mathsf{BPP}].$$

Namely, they show a protocol by which a polynomial probabilistic classical machine can verify the acceptance probability of a polynomial quantum circuit[2], to within inverse-exponential accuracy, by interacting with a PreciseBQP prover.

A naive attempt of an in-class interactive proof for PreciseQCMA. In order to verify a language $\mathcal{L} \in$ PreciseQCMA, given an instance x one's first attempt would be to have the verifier ask the prover for a witness w for x, and then use an in-class interactive proof for PreciseBQP, such as AG protocol, to verify the acceptance probability of w. Since $\mathcal{L} \in$ PreciseQCMA we indeed know that if $x \in L$ there really is a classical witness that could be sent to the verifier, and that given the witness, the process of verifying it is a computation in the class PreciseBQP, which can be verified via that AG protocol. However there is a caveat in this approach: while we allow the prover to be a PreciseQCMA machine, this only means that for a language $\mathcal{L} \in$ PreciseQCMA and an instance x of $\mathcal{L}$, the prover can distinguish whether x is a *yes* or a *no* instance. However this does not a-priori mean that the prover can actually find the witness, even if it knows that $x \in L$.

[2]i.e. a quantum circuit consisting of a polynomial number of sequential local gates on n qubits

Adaptive Search. For languages in NP, we know how to adapt an NP oracle into a witness-finding algorithm: We use consecutive accesses to the oracle, to adaptively find one bit of the witness at a time. For example, to find the first bit of the witness the verifier asks the prover if the following NP claim, denoted S_0, is true "there exists a witness for the instance x where the first bit is 0". If the answer is "no", the verifier can ask about the statement S_0, where the value of the bit is flipped. Once the first bit b of the witness is found in this way, the verifier can continue by asking about the statements S_b0 and S_b1, etc. .

The previous process indeed works for any instances of any language in NP $\subseteq$ PreciseQCMA, but does it extend to all of PreciseQCMA? Let $\mathcal{L}$ be a language in PreciseQCMA and $x \in \mathcal{L}$ be a yes input. Consider the statement S_0 for x as described above. Is this really a PreciseQCMA statement, namely can a PreciseQCMA oracle answer it? Recall that such an oracle can verify the acceptance probability up to an inverse-exponential additive factor. However, if x is a yes instance but there is no witness that begins with the zero bit, we do not know that the best witness that begins with 0 has acceptance probability that is inverse exponentially separated from the actual best witness: it could perhaps be that the separation is much smaller – there is no upper bound on the acceptance probability of x given a wrong witness! So it is not clear that a PreciseQCMA machine can decide if the statement S_0 is true, as we are not guaranteed an inverse-exponential separation between the acceptance probability in the *yes* case and in the *no* case. We solve this issue by observing that we can assume, without loss of generality, a certain structure of the PreciseQCMA verification circuit, which ensures that its acceptance probability for any witness lies on an inverse-exponentially-separated grid.

4 Discussion and Open Problems

Below we observe that combining the AG protocol with the result in [26], which showed that QMA $\subseteq$ PP, we obtain an interactive protocol for QMA with a PreciseBQP prover.

An interactive proof for QMA. Using the witness-preserving gap amplification for QMA [26, 28], we can compute the acceptance probability of a correct QMA witness using precise efficient quantum computations. Specifically, invoking the AG protocol with gap-amplified circuits and the circuit for preparing random-guess witness, we conclude the following.

Theorem 4 QMA $\subseteq$ IP[PreciseBQP, BPP].

The main idea in the proof of Theorem 4 is that once one amplifies enough the gap between the acceptance probability in the no case, and the acceptance probability in the yes case with a correct witness, a PreciseBQP algorithm can distinguish between the yes and no case simply by choosing a 'random' witness. We leave the details for the full version of the paper.

The protocol of 4 improves the previous result in [2], which provides an interactive proof protocol for QMA by computing the polynomial power of the local Hamiltonian, since the computational power of the prover in their protocol is not explicitly bounded from above (although it is clearly bounded by PSPACE).

Towards an interactive proof for PreciseQMA. It is natural to ask if the protocols from Theorem 2 or from Theorem 4 can be extended to PreciseQMA. Indeed, such quantum-inspired interactive protocols might provide a direct proof for BQPSPACE $\subseteq$ IP, which could provide a interesting quantum analogue of the sum-check primitive from the original proof of PSPACE $\subseteq$ IP.

However, if we try to apply the protocol from Theorem 2, even allowing quantum messages, it is not clear how a BQP verifier would be able to obtain exponential accuracy without needing exponentially many copies of the witness.

Likewise, applying the protocol from Theorem 4 does not work for PreciseQMA in an obvious way, as amplifying an exponentially-small gap using the witness-preserving gap amplification technique used in Theorem 4 requires exponentially many rounds.

PostQMA. We note that PostQMA = PSPACE (see [27] for definition) seemingly does not have the problems mentioned above for PreciseQMA, as the gap between the yes and no case accept probabilities is constant. However, due to the use of conditioned probability, we do not know of witness-preserving amplification techniques for PostQMA.

References

[1] S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proc. R. Soc. A*, volume 461, pages 3473–3482, 2005.

[2] D. Aharonov, I. Arad, and T. Vidick. Guest column: the quantum PCP conjecture. *ACM SIGACT News*, 44(2):47–79, 2013.

[3] D. Aharonov, M. Ben-Or, and E. Eban. Interactive proofs for quantum computations. *Proc. of ITCS*, 2010.

[4] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev. Interactive proofs for quantum computations. *arXiv:1704.04487*.

[5] D. Aharonov and A. Green. A quantum inspired proof of $\mathsf{P}^{\#\mathsf{P}} \subseteq$ IP. *arXiv:1710.09078*.

[6] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *JACM*, 45(3):501–555, 1998.

[7] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *JACM*, 45(1):70–122, 1998.

[8] L. Babai. Trading group theory for randomness. *Proc. of the 17th STOC*, 421–429, 1985.

[9] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proc. of 50th FOCS*, pages 517–526. IEEE, 2009.

[10] L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocols. *Comput. complexity*, 1(1):3–40, 1991.

[11] A. Cojocaru, L. Colisson, E. Kashefi, P. Wallden. On the possibility of classical client blind quantum computing. *arXiv:1802.08759*.

[12] A. Cojocaru, L. Colisson, E. Kashefi, P. Wallden. QFactory: classically-instructed remote secret qubits preparation. *arXiv:1904.06303*.

[13] A. Coladangelo, A. Grilo, S. Jeffery, T. Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. *EUROCRYPT*, 2019.

[14] B. Fefferman and C. Lin. Quantum merlin arthur with exponentially small gap. *arXiv:1601.01975*.

[15] B. Fefferman and C. Y. Lin. A complete characterization of unitary quantum space. In *9th ITCS*, 2018.

[16] T. Morimae, M. Hajdušek and J. F Fitzsimons. Post hoc verification of quantum computation. *Phys. Rev. Lett.*, 120(4):040501, 2018.

[17] J. F Fitzsimons and E. Kashefi. Unconditionally verifiable blind quantum computation. *Phys. Rev. A*, 96(1):012303, 2017.

[18] S. Gharibian, M. Santha, J. Sikora, A. Sundaram, and J. Yirka. Quantum generalizations of the polynomial hierarchy with applications to QMA(2). In *43rd MFCS*, 2018.

[19] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum. Delegating computation: interactive proofs for muggles. In *Proc. of 40th STOC*, pages 113–122. ACM, 2008.

[20] S. Goldwasser, S. Micali, C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. on Comp.*, 18(1):186–208, 1989.

[21] A. Gheorghiu and T. Vidick. Computationally-secure and composable remote state preparation. *arXiv:1904.06320*.

[22] A. Y. Kitaev, A. Shen, and M. N. Vyalyi. *Classical and quantum computation*. Number 47. American Mathematical Soc., 2002.

[23] G. Kuperberg. How hard is it to approximate the jones polynomial? *Theory of Comput.*, 11(6):183–219, 2015.

[24] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. In *Proc. of the 31st FOCS*, pages 2–10. IEEE, 1990.

[25] U. Mahadev. Classical verification of quantum computations. In *Proc. of the 59th FOCS*, pages 259–267. IEEE, 2018.

[26] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Comput. Complexity*, 14(2):122–152, 2005.

[27] T. Morimae and H. Nishimura. Merlinization of complexity classes above BQP. *Quantum Inf. & Comput.*, 17(11-12):959–972, 2017.

[28] D. Nagaj, P. Wocjan, and Y. Zhang. Fast amplification of QMA. *Quantum Inf. & Comput.*, 9(11):1053–1068, 2009.

[29] Z. Ji. Classical verification of quantum proofs In *Proc. of 48th STOC*, pages 885–898, ACM, 2016.

[30] A. Natarajan, T. Vidick. A quantum linearity test for robustly verifying entanglement In *Proc. of 49th STOC*, pages 1003–1015, ACM, 2017.

[31] A. Natarajan, T. Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA In *Proc. of 59th FOCS*, pages 731–742, ACM, 2018.

[32] B. W Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456, 2013.

[33] A. Shamir. IP=PSPACE. In *Proc. of the 31st IEEE FOCS*, pages 11–15, 1990.

Optimizing quantum heuristics with machine learning

Max Wilson[1 2 6 *] Sam Stromswold[1] Filip Wudarski[1 5] Thomas Vandal[3]
Walter Vinci[1] Norm Tubman[1] Alejandro Perdomo-Ortiz[3 4] Eleanor Rieffel[1]

[1] *Quantum Artificial Intelligence Lab., NASA Ames Research Center, Moffett Field, CA 94035, USA*
[2] *Bristol University, Quantum Engineering Center for Doctoral Training, Centre for Nanoscience and Quantum Information, 4 Tyndall Avenue, BS8 1DF, United Kingdom*
[2] *NASA Ames Research Center / Bay Area Environmental Research Institute, Moffett Field, CA 94035, USA*
[3] *Zapata Computing Inc., 439 University Avenue, Office 535, Toronto, ON, M5G 1Y8, Canada*
[4] *Department of Computer Science, University College London, WC1E 6BT London, United Kingdom*
[5] *USRA Research Institute for Advanced Computer Science (RIACS), Mountain View,CA 94035, USA*
[6] *Stinger Ghaffarian Technologies Inc., Greenbelt, MD 20770, USA*

Abstract. We compare a broad set of optimization algorithms for parameter setting in quantum heuristics, where the parameters define gate operations. The work will provide evidence to whether machine learning approaches to optimization will be integral to useful quantum heuristics implemented on NISQ devices. THIS PAPER IS ELIGIBLE FOR BEST STUDENT POSTER AWARD

1 Introduction

It is unclear what will be the first useful application of quantum computers. Computations beyond what can be run on even the world's largest supercomputers will likely be successfully performed on next generation quantum hardware. However, these computations do not solve a problem of practical interest. Examples with theoretically proven advantages for quantum computation cannot be run on problems with practical application in the near-term. A recently developed class of algorithms, variational quantum algorithms [1,2], show some promise for advancing our understanding of where near-term quantum computers might be useful. With applications in combinatorial optimization and quantum simulation they provide a sandbox for testing quantum devices, as they do not require error-correction and can be applied to small (and interesting) problems.

Variational algorithms involve a quantum and a classical subroutine, where the classical step optimizes the parameters of the quantum circuit to improve the solution found by the quantum subroutine, guided by some cost function. Here, we focus on benchmarking different methods for the classical optimization of parameters in quantum circuits for variational quantum algorithms on specific families of problems. The field of optimization methods is rich and diverse; many methods are available to choose from when building techniques to optimize parameters of quantum heuristics.

In this work, we explore a set of optimization methods coming from Bayesian, gradient-based, gradient-free, machine learning, genetic and reinforcement learning approaches. We compare their performance Quantum Alternating Operator Ansatz (QAOA) on MAX-2-SAT and Graph Bisection optimization problems, and Variational Quantum Eigensolver (VQE) for estimating the ground state of Fermi Hubbard models.

*aw16952@bristol.ac.uk

This investigation provides a base to understand how parameter setting of these quantum heuristics respond to a broad range of methods. Initially, we investigate the performance on classical simulations of quantum circuits with comparatively little uncertainty in the evaluation of the cost function (limited only by the standard error on the expectation), and then on simulations with noise models representative of hardware.

We expect that recent advances in optimizer design from machine learning will continue to improve optimizer performance [3–7], and that machine learning techniques will eventually become a standard tool for optimizing quantum circuits. To realize the potential of machine learning based optimizers for parameter setting in quantum heuristics, a critical step is the early adaption and adoption of these tools and the evaluation of their effectiveness.

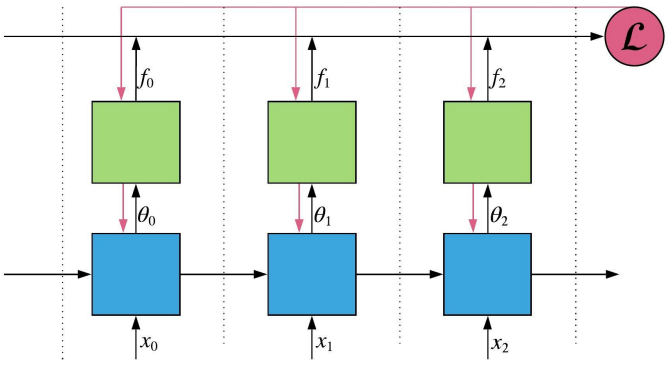


Figure 1: Recurrent neural network of LSTMs (blue) optimizing and learning from a quantum circuit (green) via the loss function (pink).

A number of researchers have investigated reinforcement learning for the control of quantum gates [9–11], and in some cases found orders of magnitude improve-

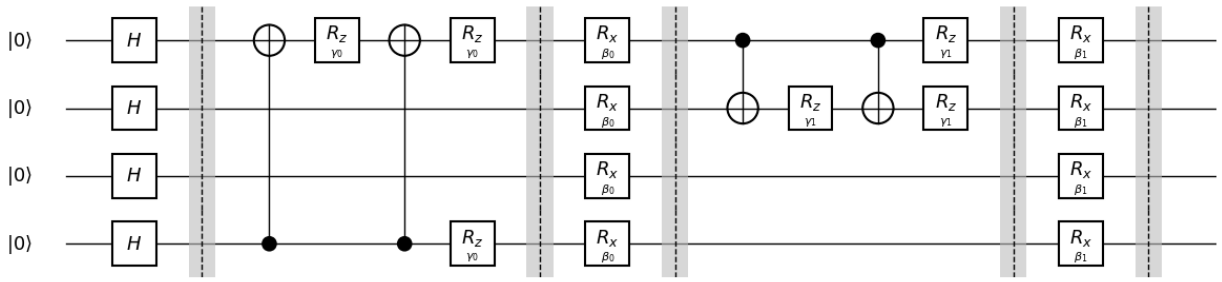


Figure 2: Example QAOA quantum circuit, for finding optimal configuration of variables in the max-2-sat problm with 2 clauses, where p, the number of phases, is 2. Image generated with Qiskit [8]

ment in performance over stochastic gradient descent methods. These successes inspire us to apply machine learning to the parameter setting problem.

2 Parameter setting of quantum heuristics

We evaluate these methods on two types of problem classes, QAOA and VQE.

2.1 Quantum Alternating Operator Ansätz

Prior work on parameter setting in QAOA includes comparison of analytical and finite difference methods [12], a method for learning a model for a good schedule [13], and comparison of standard methods over problem classes [14].

We evaluate parameter setting approaches for QAOA on MAX-2-SAT and Graph Partitioning problems [15], both NP-complete combinatorial optimization problems. We use standard [2] and extended QAOA methods [16], respectively.

2.2 Variational Quantum Eigensolver

The initial demonstration of VQE used Nelder-Mead, a standard derivative-free approach, for parameter setting after observing that gradient descent methods did not converge. Since then, examples include the use of Simultaneous Perturbation Stochastic Approximation (SPSA) in [17], where they argue that while simultaneous perturbation methods can be very useful in the optimization of fermionic problems, for classical problems, such as instances of MaxCut, the ease of evaluating the cost function may favor standard gradient-descent or derivative-free routines". Other routines used include COBLYA, L-BFGS-B, Nelder-Mead and Powell in [18]. Finally, in [19] they explore the use of Bayesian optimisation in VQE optimisation.

2.3 Gradients

Analytical expressions for the gradient of a cost function with respect to the parameters in variational quantum algorithms allow computation of the gradient efficiently on a quantum computer, and finite differences is an acceptable method for computing the gradient when this is unavailable. If we are working with devices that are outside our ability to simulate, however, as may happen within the next 5 years, and given the complications due to noise on quantum hardware, optimization procedures from noisy black-box optimization, or models trained with reinforcement learning algorithms, may be a better choice: The optimizer developed for a noisy simulation may not be appropriate for useful application of early quantum devices. Finally, initialization strategies developed to avoid the barren plateau [20] and work into the effect of circuit depth on the gradient evaluations [21] provide more evidence that gradient computation for optimization of these circuits is a non-trivial task.

2.4 Designing an optimiser

In the last few years, machine learning researchers have developed techniques in 'learning to learn', a model makes decisions about how to optimize parameters given a problem. Early research explored Guided Policy Search [3], which has been superceded by Recurrent Neural Networks (RNN)s of LSTM cells [4–7]. They achieve better performance than ADAM, a common optimizer used in machine learning. In a black-box setting, where we do not have access to the gradient, these models will have to be trained with reinforcement learning. Though these techniques are not yet mainstream, optimized models of optimization will be an important tool in the development of useful quantum heuristics.

3 Outlook

While optimizing quantum heuristics is recognized as an important problem, best practises have not yet been established for parameter setting in quantum algorithms. The method chosen depends in part on the metric used to evaluate its performance and the type of problem. In this work, we evaluate both time to solution and optimality of solution.

This comparison will serve as a reference whenever people need to choose an optimizer for parameter setting of quantum heuristics. Further, it introduces machine learning based methods for optimization to the field, and provides evidence that these approaches are promising enough to merit further research. It is likely that the first useful application of quantum computers will be augmented by machine learning methods, whether that be in parameter setting or gate control. Demonstrating how these methods perform in practice is an important task.

There are other areas that naturally follow from this

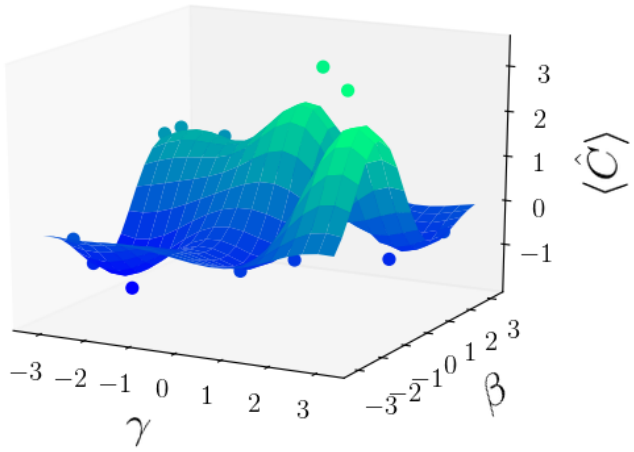


Figure 3: Mean of posterior distribution from Gaussian process after training with 20 random points of the noisy objective function of QAOA applied to an example MAX-2-SAT problem with 6 variables and 2 clauses.

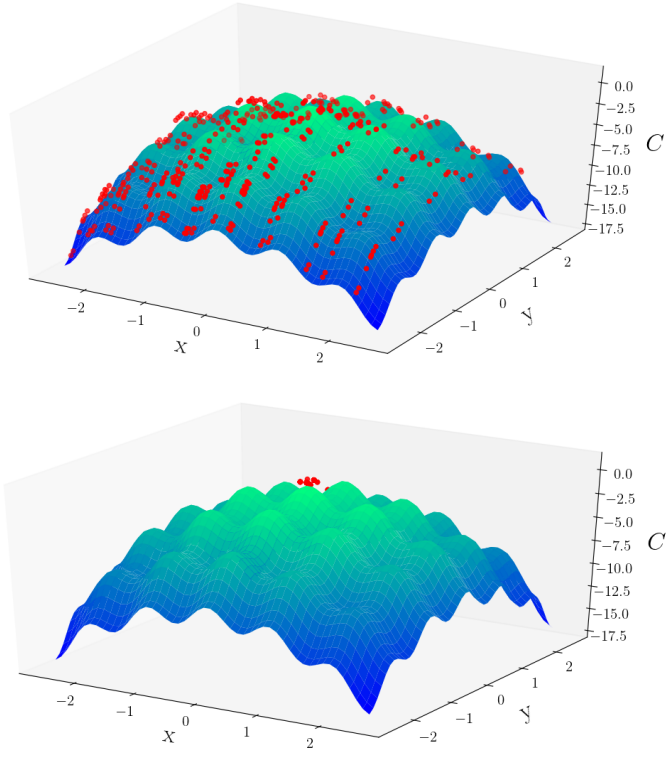


Figure 4: Top: A random initialization used by a genetic algorithm. Bottom: The resulting population after 100 iterations of the genetic algorithm. The fitness function (negative cost function) depicted is a modified version of the 2D-Rastrigin function with more gentle peaks for visual clarity.

work. Given systematic biases in near-term quantum devices that are not captured by calibration, machine learning based approached to optimization could improve device-specific optimization by learning systematic errors as features in the model. For this reason, it will be important to compare these methods on quantum hardware.

There are limits to precision of parameter setting on near-term quantum processors. Some research questions include how much precision is need to solve the quantum optimization problem, and how this available precision will influence the performance of the parameter setting optimizer.

A machine learning driven approach to optimization of these algorithms improves with exposure to training examples. We investigate whether this learning transfers across problem classes. Additionally, there will be differences in optimization procedure performance across problem classes, dependent on the structure of the problem. These investigations will point to good problem specific procedures. It is also unclear how the structure of the parameter space will affect the choice of optimizer; for each problem tested, the parameter space will have different properties such as ruggedness and varying depths of local minima. The properties will also determine the choice of optimizer, though we believe machine learning approaches here will learn to exploit parameter space structure within a problem class.

To summarize, in this work we benchmark a set of classical optimizers for the parameter setting subroutine in variational quantum algorithms. We expect machine learning based approaches to be competitive and to continue to improve in the near-term, such that useful near-term implementations of quantum heuristics on noisy devices will use these methods going forward.

References

[1] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. Obrien, "A variational eigenvalue solver on a photonic quantum processor," *Nature communications*, vol. 5, p. 4213, 2014.

[2] E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm," *arXiv preprint arXiv:1411.4028*, 2014.

[3] K. Li and J. Malik, "Learning to optimize," *arXiv preprint arXiv:1606.01885*, 2016.

[4] M. Andrychowicz, M. Denil, S. Gomez, M. W. Hoffman, D. Pfau, T. Schaul, B. Shillingford, and N. De Freitas, "Learning to learn by gradient descent by gradient descent," in *Advances in Neural Information Processing Systems*, pp. 3981–3989, 2016.

[5] Y. Chen, M. W. Hoffman, S. G. Colmenarejo, M. Denil, T. P. Lillicrap, M. Botvinick, and N. de Freitas, "Learning to learn without gradient descent by gradient descent," in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pp. 748–756, JMLR. org, 2017.

[6] I. Bello, B. Zoph, V. Vasudevan, and Q. V. Le, "Neural optimizer search with reinforcement learning," in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pp. 459–468, JMLR. org, 2017.

[7] O. Wichrowska, N. Maheswaranathan, M. W. Hoffman, S. G. Colmenarejo, M. Denil, N. de Freitas, and J. Sohl-Dickstein, "Learned optimizers that scale and generalize," in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pp. 3751–3760, JMLR. org, 2017.

[8] N. authors, "Qiskit: An open-source framework for quantum computing," 2019.

[9] M. Bukov, A. G. Day, D. Sels, P. Weinberg, A. Polkovnikov, and P. Mehta, "Reinforcement learning in different phases of quantum control," *Physical Review X*, vol. 8, no. 3, p. 031086, 2018.

[10] C. Chen, D. Dong, H.-X. Li, J. Chu, and T.-J. Tarn, "Fidelity-based probabilistic q-learning for control of quantum systems," *IEEE transactions on neural networks and learning systems*, vol. 25, no. 5, pp. 920–933, 2013.

[11] M. Y. Niu, S. Boixo, V. N. Smelyanskiy, and H. Neven, "Universal quantum control through deep reinforcement learning," in *AIAA Scitech 2019 Forum*, p. 0954, 2019.

[12] G. G. Guerreschi and M. Smelyanskiy, "Practical optimization for hybrid quantum-classical algorithms," *arXiv preprint arXiv:1701.01450*, 2017.

[13] D. Wecker, M. B. Hastings, and M. Troyer, "Training a quantum optimizer," *Physical Review A*, vol. 94, no. 2, p. 022309, 2016.

[14] G. Nannicini, "Performance of hybrid quantum-classical variational heuristics for combinatorial optimization," *Physical Review E*, vol. 99, no. 1, p. 013304, 2019.

[15] S. Hadfield, Z. Wang, B. O'Gorman, E. G. Rieffel, D. Venturelli, and R. Biswas, "From the quantum approximate optimization algorithm to a quantum alternating operator ansatz," *Algorithms*, vol. 12, no. 2, p. 34, 2019.

[16] S. Hadfield, Z. Wang, E. G. Rieffel, B. O'Gorman, D. Venturelli, and R. Biswas, "Quantum approximate optimization with hard and soft constraints," in *Proceedings of the Second International Workshop on Post Moores Era Supercomputing*, pp. 15–21, ACM, 2017.

[17] N. Moll, P. Barkoutsos, L. S. Bishop, J. M. Chow, A. Cross, D. J. Egger, S. Filipp, A. Fuhrer, J. M. Gambetta, M. Ganzhorn, *et al.*, "Quantum optimization using variational algorithms on near-term quantum devices," *Quantum Science and Technology*, vol. 3, no. 3, p. 030503, 2018.

[18] J. Romero, R. Babbush, J. R. McClean, C. Hempel, P. J. Love, and A. Aspuru-Guzik, "Strategies for quantum computing molecular energies using the unitary coupled cluster ansatz," *Quantum Science and Technology*, vol. 4, no. 1, p. 014008, 2018.

[19] B. Moseley, M. Osborne, and S. Benjamin, "Bayesian optimisation for variational quantum eigensolvers,"

[20] E. Grant, L. Wossnig, M. Ostaszewski, and M. Benedetti, "An initialization strategy for addressing barren plateaus in parametrized quantum circuits," *arXiv preprint arXiv:1903.05076*, 2019.

[21] A. Harrow and J. Napp, "Low-depth gradient measurements can improve convergence in variational hybrid quantum-classical algorithms," *arXiv preprint arXiv:1901.05374*, 2019.

Finite-key analysis for differential phase encoded measurement-device-independent quantum key distribution

Shashank Kumar Ranu[1] * Anil Prabhakar[1] † Prabha Mandayam[2] ‡

[1] *Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India*
[2] *Department of Physics, Indian Institute of Technology Madras Chennai, India*

Abstract. This paper presents a novel measurement-device-independent quantum key distribution (MDI-QKD) protocol based on phase encoding. Our protocol uses a differential-phase-shifted (DPS) keying scheme wherein a single photon is realized as a linear superposition of three orthogonal paths. We carry out the asymptotic key rate analysis of the proposed protocol and demonstrate its superior performance compared to the existing protocols. We also show that our DPS-MDI-QKD protocol is unconditionally secure by mapping it to an entanglement-based scheme. Finally, we also perform finite-key analysis for the proposed scheme and estimate the secure key rate.

Keywords: Measurement-device-independent quantum key distribution, differential-phase-shift, entanglement-based, finite-key.

1 Introduction

Quantum key distribution (QKD) allows secure communication between two parties with absolute secrecy [1, 2]. However, this theoretical security does not translate to practical security due to the non-ideal nature of devices used in the practical implementations. This has led to the emergence of various side-channel attacks [3, 4, 5], most of which target the detectors used in the implementation. Measurement-device-independent (MDI) QKD was proposed as a means to counteract these detector side-channel attacks [6].

While the original MDI-QKD proposals involved polarization-based encodings, more recently, phase-based MDI-QKD protocols have been discussed in the literature [7, 8, 9, 10]. The MDI protocol presented in [8] uses a path and phase encoding technique, starting with a single-photon source. The scheme uses four different phase values $(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2})$ to generate two pairs of orthogonal states needed to implement BB84. The other phase-based MDI schemes discussed in [9, 7, 10] propose to implement BB84 or B92 protocol (using two phase values, namely, 0 and π), using a weak coherent source (WCS) for key generation. The use of WCS makes such an implementation vulnerable to attacks which target multi-photon pulses.

In a departure from existing work, we present a differential-phase-shifted (DPS) MDI protocol using only two phases $(0, \pi)$ and employing single-photon sources for key generation. The proposed scheme combines the best of both differential-phase-shifted (DPS) QKD and MDI-QKD. It is more robust to phase fluctuations, and also ensures protection against detector side-channel attacks. Use of single-photon source makes the proposed protocol immune against eavesdropping attacks that make use of multi-photon pulses for gaining key information.

*ee16s300@ee.iitm.ac.in
†anilpr@ee.iitm.ac.in
‡prabhamd@physics.iitm.ac.in

2 DPS-MDI-QKD protocol

Fig. 1 gives a schematic description of the proposed protocol. Our protocol is broadly based on the differential-phase-based QKD scheme using a single-photon source, proposed in [11].

Alice and Bob use single-photon sources. They both employ *identical* delay lines with three different path lengths each, and thus realise their single photons in superpositions of three distinct time-bins corresponding to the three distinct paths. They encode their random key bits $\{0, 1\}$ as a random phase $\{0, \pi\}$ between successive pulses in their respective 3-pulse trains. Alice and Bob thus generate encoded single-photon states corresponding to one of the four non-orthogonal quantum states given below, depending on their random key bits.

$$|\psi(\pm,\pm)\rangle = \frac{1}{\sqrt{3}}\left(|1\rangle_1|0\rangle_2|0\rangle_3 \pm |0\rangle_1|1\rangle_2|0\rangle_3 \pm |0\rangle_1|0\rangle_2|1\rangle_3\right).$$

Here, $|1\rangle$ and $|0\rangle$ indicate the presence and absence of a photon respectively, in each of the paths labeled $1, 2, 3$. The photons have an equal probability of traversing each of the paths in each setup. Alice and Bob send their encoded signals to the untrusted third party, Charles.

The key information is now encoded in the relative phase between corresponding paths in Alice and Bob's setup. Charles simply uses a beam-splitter and two single-photon detectors, labeled c and d respectively in Fig. 1). Let t_i denote the time at which the photon traversing through path i of either source set-up reaches Charles. Then, for every signal received by Charles, he publicly announces as to which detector clicked (D_c or D_d), as well as the associated time, namely, t_1, t_2, or, t_3.

The complete two-photon state after the action of the beam splitter is written down in the appendix. We first note that when Charles announces a detection in only one of the three times (t_1, t_2 or t_3), Alice and Bob discard the corresponding key bit. Detection in a single time-slot implies that either the photons coming from Alice and Bob

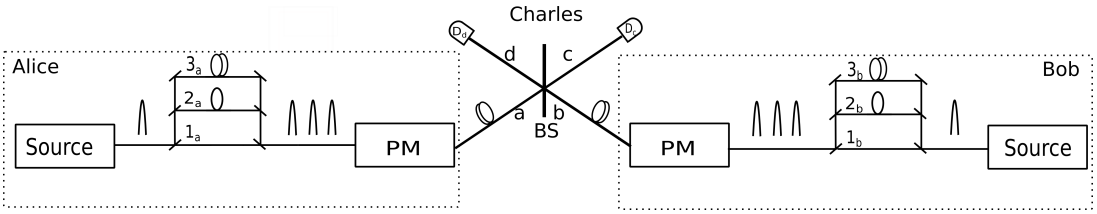


Figure 1: Schematic of 3-pulse differential-phase-shifted QKD.

bunched together because of Hong-Ou-Mandel interference or that one of the photons got lost in the channel. Such a detection does not convey any information about the relative phase between the pair of arriving photons.

Whenever Charles announces detection at two different time instances, Alice and Bob may treat the detection as a valid one, and extract the corresponding raw key information. Table I shows the key reconciliation scheme in detail, where, $\Delta\phi_1$ ($\Delta\phi_2$) is the phase difference between the photons traversing through the second (third) arm of Alice and Bob's interferometers respectively. Notice that even when Charles announces two valid time-instances, there are cases where Alice and Bob may have to discard their key-bits; this follows from a detailed analysis of the final two-photon state presented in the technical appendix.

We see that a third of the incoming photons have to be discarded due to Hong-Ou Mandel interference. This leads to the first factor of $\frac{2}{3}$. Next, we observe from the key-reconciliation table that two-thirds of Charles' measurements contribute to the raw key, thus leading to a sifted key rate of $\frac{4}{9}$:

$$R_{\text{sift}} = \frac{2}{3} \times \frac{2}{3} = \frac{4}{9}. \tag{1}$$

Alice and Bob perform classical post-processing, including classical error correction and privacy amplification, on the sifted key to extract the final secure key from it. We may now follow the standard analysis in [12] to obtain the asymptotic secure key rate for our DPS-MDI protocol. The plot shown in Fig. 2 compares the secure key rate obtained for our DPS-MDI-QKD with that obtained for the standard 3-pulse DPS and the BB84 protocols.

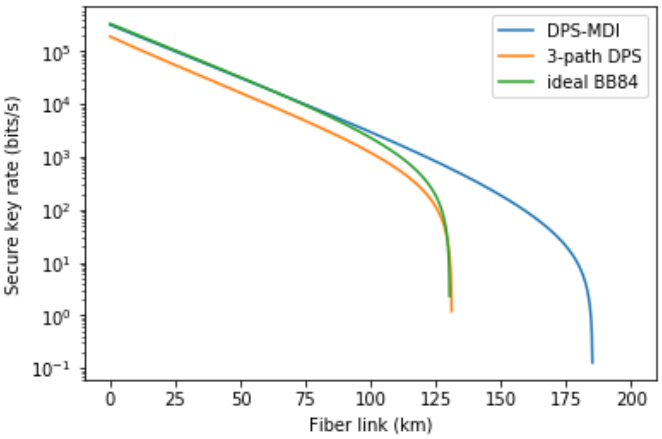


Figure 2: Secure key rate as a function of channel length in the asymptotic case.

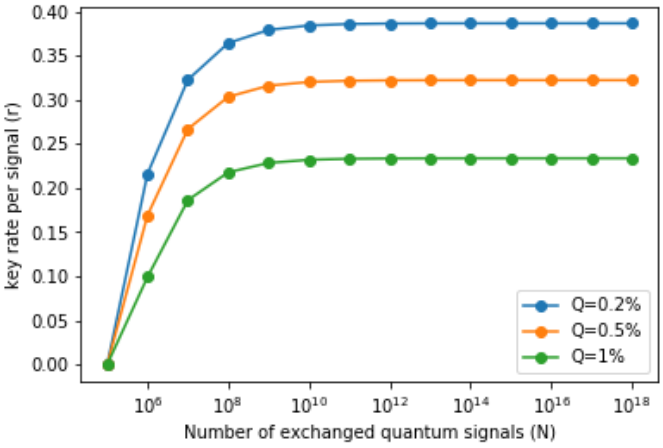


Figure 3: Key rate r as a function of the number of exchanged quantum signals for different values of error rate (Q).

We see that the DPS-MDI protocol yields a non-zero secure key rate for much longer channel lengths, in comparison with the standard 3-pulse DPS protocol. This enhanced security can be achieved due to the fact that the MDI protocols are immune to individual attacks such as intercept and resend attack. Hence, Eve has lesser information about the key bits, which in turn translates to longer distances over which secure key transmission is possible.

3 Finite-key analysis

Finally, we establish the security of our protocol in a finite-key regime, against general attacks. As the resources of Alice and Bob are limited in practice, it becomes important to show that a QKD protocol is secure in the finite-key regime. We use the method outlined in [13] to calculate the finite-key rate corresponding to our scheme, as a function of the number of signals generated at the source. This analysis first requires mapping of the QKD protocol to an equivalent entanglement-based protocol. As explained in the appendix, it is possible to rewrite our DPS-MDI protocol such that after sifting and reconciliation, Alice and Bob are left with a pair of entangled qubits.

Table I : Key reconciliation scheme for the proposed protocol.

Measurement outcome of Charles	Action of Alice and Bob	Requirement of bit flip
Det c clicks at both t_1 and t_2	Extract key using $\Delta\phi_1$	No
Det c clicks at both t_2 and t_3	Discard the bits	-
Det c clicks at both t_1 and t_3	Extract key using $\Delta\phi_2$	No
Det d clicks at both t_1 and t_2	Extract key using $\Delta\phi_1$	No
Det d clicks at both t_2 and t_3	Discard the bits	-
Det d clicks at both t_1 and t_3	Extract key using $\Delta\phi_2$	No
Det c clicks at t_1 and det d at t_2	Extract key using $\Delta\phi_1$	Yes
Det c clicks at t_2 and det d at t_1	Extract key using $\Delta\phi_1$	Yes
Det c clicks at t_1 and det d at t_3	Extract key using $\Delta\phi_2$	Yes
Det c clicks at t_3 and det d at t_1	Extract key using $\Delta\phi_2$	Yes
Det c clicks at t_2 and det d at t_3	Discard the bits	-
Det c clicks at t_3 and det d at t_2	Discard the bits	-

Finally, we make use of the modified Devetak-Winter formula based on the smooth min-entropy [13] to numerically estimate the secure key-rates obtained using our protocol (see Fig. 3). We refer to the appendix for a detailed analysis. The key rate per signal (r) tends to the sifted key rate of $\frac{4}{9}$ in the asymptotic limit, as expected. This is a reflection of the fact that only $\frac{4}{9}$ of the raw key bits can be used for key generation and rest is used for parameter estimation.

4 Conclusion

In summary, we have demonstrated a differential-phase-encoded measurement-device independent QKD protocol, which is robust against phase fluctuations and offers a high asymptotic key rate at long distances. We have establish unconditional security using an equivalent, entanglement-based protocol. Finally, we provide a finite-key analysis, thus bridging the gap between theory and practice.

References

[1] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[2] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, 48(3):351–406, 2001.

[3] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *arXiv preprint quant-ph/0512080*, 2005.

[4] Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo. Phase-remapping attack in practical quantum-key-distribution systems. *Physical Review A*, 75(3):032314, 2007.

[5] Antía Lamas-Linares and Christian Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Optics express*, 15(15):9388–9393, 2007.

[6] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[7] Agnes Ferenczi. *Security proof methods for quantum key distribution protocols*. University of Waterloo, 2013.

[8] Xiongfeng Ma and Mohsen Razavi. Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A*, 86(6):062319, 2012.

[9] Kiyoshi Tamaki, Hoi-Kwong Lo, Chi-Hang Fred Fung, and Bing Qi. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Physical Review A*, 85(4):042307, 2012.

[10] Jie Lin and Norbert Lütkenhaus. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Physical Review A*, 98(4):042332, 2018.

[11] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. *Physical Review Letters*, 89(3):037902, 2002.

[12] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE, 2004.

[13] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical review letters*, 100(20):200501, 2008.

Ground state entanglement in an extended Hubbard model with Ising-like interactions

Robertson C. Esperanza[1] * Francis N. C. Paraan[1] †

[1] *National Institute of Physics, University of the Philippines Diliman, Philippines*

Abstract. We probe the half-block von Neumann entanglement entropy along with the ground state properties of a 1D extended Hubbard model as its intrasite and intersite interaction parameters are varied. The half-block entanglement entropy was calculated using the density matrix renormalization group (DMRG) for a periodic chain. We demonstrate that the half-block entanglement entropy provides a sketch of the changes in the ground state of the system and that it can be used to locate the quantum critical lines in the model.

Keywords: Entanglement, DMRG, Extended Hubbard models

1 Introduction

It is hoped that quantum information theory may lead to novel ways to characterize many-body ground state properties of a condensed matter system. One such approach is to probe the entanglement behavior of the ground state as the driving parameters of the model system are varied across quantum phase transitions (QPTs) [1, 2]. QPTs are qualitative changes in the ground state properties of the system at zero temperature [3], and entanglement is said to be connected to the long-range correlations that develop at the quantum critical point [4, 5]. It is proposed that for QPTs resulting from analyticities in the energy, ordering is signalled by a discontinuity in the ground state concurrence [6]. However, it was shown that for some spin models, a discontinuity of the concurrence appears in the absence of QPT [7]. It is a possibility that other entanglement measures might bridge a connection between QPTs and entanglement.

The Hubbard model simplifies the physics of strongly correlated fermions into an itinerant model with hopping and intrasite interactions. Experimentally, manipulable Hubbard dimers at half-filling have been realized using two ultracold fermionic atoms that are optically trapped in a double well [8]. Furthermore, entanglement measurements on Hubbard dimer states have been demonstrated in localized impurities in silicon [9]. This model may also be generalized to include additional interactions in what are called extended Hubbard models [10].

We consider a particular extended Hubbard Hamiltonian by introducing Ising-like interactions at half-filling (i.e. number of fermions is the same as the number of lattice sites L)

$$H = -t \sum_{\langle i,j \rangle} \sum_{\sigma} (c^{\dagger}_{i\sigma} c_{j\sigma} + c^{\dagger}_{j\sigma} c_{i\sigma}) + U \sum_{i} n_{i\uparrow} n_{i\downarrow} + V \sum_{\langle i,j \rangle} \sum_{\sigma} n_{i\sigma} n_{j\sigma} - V \sum_{\langle i,j \rangle} \sum_{\sigma} n_{i\sigma} n_{j(-\sigma)}, \quad (1)$$

where $c_{i\sigma}$ ($c^{\dagger}_{i\sigma}$) is the fermionic annihilation (creation) operator for a fermion at site i with spin $\sigma =\uparrow$ or $\downarrow$, and $n_{i\sigma} = c^{\dagger}_{i\sigma} c_{i\sigma}$ is the number operator. The angular brackets in the summation indicates that we only look into nearest-neighbor interactions. The first term in the Hamiltonian (1) accounts for the fermion hopping to adjacent sites. The second term describes the Coulombic interaction between two fermions occupying the same lattice site. The last two terms introduce a nearest-neighbor intersite interaction between fermions having the same (opposite) spins, with energy V ($-V$). This model has no known exact solution—except for the case of one-dimensional chain of length $L = 2$.

In this work, we carried out numerical calculations of the ground state entanglement for an extended Hubbard model on a periodic chain of length $L = 100$ at half-filling. We used the half-block von Neumann entropy (detailed in Sec. 2) as the entanglement measure since it is readily obtainable in density matrix renormalization group (DMRG) [11] calculations. When compared to a phase diagram constructed from order parameters–such as local operator expectation values and two-point correlators of fermionic density and magnetization–the half-block entropy qualitatively captures the ground state properties of the system.

2 Density matrix renormalization group

One of the common numerical methods used for low-dimensional quantum systems is DMRG. However, a physical hurdle is the exponential increase in the Hilbert space dimension as the system size increases.

DMRG employs a truncation of the Hilbert space by selecting the most probable states–described by the eigenvalues of the reduced density matrix–as the system gradually grows. Since the least probable states are discarded, the size of the matrices we work on is constrained as the system grows. It is known that the ground states of one-dimensional lattice models—near or away from criticality—satisfy the condition that the entanglement of a subsystem with respect to the whole system is bounded, which makes a simulation of the system using DMRG possible [12].

Using this numerical technique, we can calculate operator expectation values and also the block entanglement

*rcesperanza@up.edu.ph
†fparaan@nip.upd.edu.ph

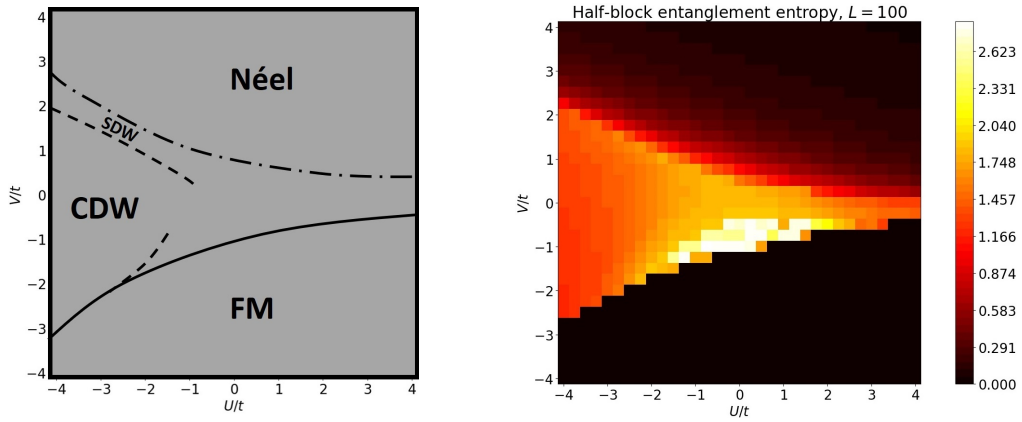


Figure 1: The schematic phase diagram for the Hamiltonian (1) is obtained by superimposing the ground state variations of various order parameters–local expectation values and two-point correlators involving fermionic density and magnetization (Left). The main features of the ground state phase diagram for large $|U|$ and $|V|$ are also mirrored in the half-block entanglement entropy (Right).

entropy. Suppose we divide a linear chain of length L into two blocks–one with length l and another with length $(L-l)$. For a pure ground state $|\mathrm{GS}\rangle$, we can define the block von Neumann entanglement entropy as

$$S_{\mathrm{vN}}(l) = -\mathrm{Tr}\ \rho_l \ln \rho_l, \tag{2}$$

where $\rho_l = \mathrm{Tr}_{l+1,\ldots,L} |\mathrm{GS}\rangle \langle \mathrm{GS}|$ is the reduced density matrix describing the block of length l. Specifically, we calculated the half–block entanglement entropy where $l = L/2$.

Numerical calculations in this work are performed using a DMRG implementation [13, 14] based on matrix product states from the Algorithms and Libraries for Physics Simulations (ALPS) project [15].

3 Ground state entanglement and QPTs

A crude phase diagram in the parameter space of the extended Hubbard Hamiltonian (1) is shown on the left of Figure 1, and it is strikingly similar to the features of the entanglement entropy profile shown on the right pf Figure 1. The most prominent aspect of the half-block entropy surface is its sudden discontinuity from zero to a non-zero value as the ground state undergoes transition from ferromagnetic (FM) to non-ferromagnetic state. For the case of $L = 2$ the ground state of Eq. (1) is exactly solvable, in which a level crossing exists such that there is a discontinuity in the ground state energy as the ground state transition from FM to a non-FM state—which possibly extends for longer chains.

While the FM state configuration involves alignment of spins along the lattice (since at $V < 0$, the third term of Eq. (1) that favors spin alignment is dominant), the Néel phase has antiferromagnetic ordering characterized by spatial alternation of spins along the lattice (since at $V > 0$, the fourth term of Eq. (1) that favors spin anti-alignment dominates). These are known to be product states hence they are unentangled and have zero half-block entropy, consistent with the DMRG results shown on the right of Figure 1.

For a charge density wave (CDW), the ground state has spatial modulation of fermionic occupation along the lattice (since for $U < 0$, double occupancy of a site is favored), described by an integrated density-density correlator. While in the spin density wave (SDW) phase, the ground state has alternation of magnetic moment along the lattice, described by an integrated spin-spin correlator. Both of these ground state properties are not highlighted by the half-block entropy–as there is continuous change in the entanglement measure on the region in the parameter space corresponding to these states. It should also be noted that while we qualitatively identified some ground state properties of this particular extended Hubbard model in terms of the half-block entropy, they are mostly in the limit of strong interactions.

Since QPTs are defined in the thermodynamic limit, a finite-size scaling analysis could be done to extrapolate the ground state behavior at criticality (and obtain the critical points and critical exponents), which is the subject of a future work.

4 Conclusion

Upon addition of an Ising-like nearest-neighbor interaction to the 1D Hubbard model, the ground state at half-filling exhibits ferromagnetic/antiferromagnetic ordering, and spatial modulation of either fermionic density or net magnetic moment along the lattice. These are reflected in the half-block von Neumann entanglement entropy at large $|U|$ and $|V|$. Other entanglement measures might be able to highlight the ground state properties for small $|U|$ and $|V|$. While there is no established fundamental relationship between quantum phase transitions and entanglement, entanglement entropy—calculated using DMRG—provides a qualitative description of the ground state for a non-integrable 1D model with no exact solution.

References

[1] F. Iemini, T. O. Maciel, R. O. Vianna. Entanglement of indistinguishable particles as a probe for quantum phase transitions in the extended Hubbard model. *Phys. Rev. B* **92**(7), 075423, 2015.

[2] S.-J. Gu, S.-S. Deng, Y.-Q. Li, H.-Q. Lin. Entanglement and quantum phase transition in the extended Hubbard Model. *Phys. Rev. Lett.* **93**(8), 086402, 2004.

[3] S. Sachdev. *Quantum Phase Transitions*, 2nd. ed. Cambridge University Press, 2011.

[4] T. J. Osborne, M. A. Nielsen. Entanglement in a simple quantum phase transition. *Phys. Rev. A* **66**, 032110, 2002

[5] Entanglement, quantum phase transitions, and density matrix renormalization. *Quant. Inf. Proc.* 1, 45, 2002. quant-ph/0109024.

[6] L.-A. Wu, M. S. Sarandy, D. A. Lidar. Quantum Phase Transitions and Bipartite Entanglement. *Phys. Rev. Lett.* **93**(25), 250404, 2004.

[7] M.-F. Yang. Reexamination of entanglement and the quantum phase transition. *Phys. Rev. A* **71**(3), 030302(R), 2005.

[8] S. Murmann, A. Bergschneider, V. M. Klinkhamer, G. Zürn, T. Lompe, and S. Jochim. Two fermions in a double well: Exploring a fundamental building block of the Hubbard model. *Phys. Rev. Lett.* **114**(8), 080402, 2015.

[9] J. Salfi, J. A. Mol, R. Rahman, G. Klimeck, M. Y. Simmons, L. C. L. Hollenberg, and S. Rogge. Quantum simulation of the Hubbard model with dopant atoms in silicon. *Nature Comm.* **7**, 11342, 2016.

[10] F. H. Essler, H. Frahm, F. Göhmann, A. Klümper, V. E. Korepin. *The one-dimensional Hubbard model*. Cambridge University Press, 2005.

[11] S. R. White. Density-matrix algorithms for quantum renormalization groups. *Phys. Rev. B*, **48**(14), 10345, 1993.

[12] G. De Chiara, M. Rizzi, D. Rossini, S. Montangero. Density Matrix Renormalization Group for Dummies. *J. Comput. Theor. Nanosci.* 5, 1277-1288, 2008. cond-mat/0603842.

[13] M. Dolfi, B. Bauer, S. Keller, A. Kosenkova, T. Ewart, A. Kantian, T. Giamarchi, and M. Troyer. Matrix product state applications for the ALPS project. *Comput. Phys. Commun.*, 185(2014), 3430-3440.

[14] U. Schollwöck. The density-matrix renormalization group in the age of matrix product states. *Ann. Phys.*, 326 (2011) 96-192.

[15] B. Bauer, L. D. Carr, H. G. Evertz, A. Feiguin, J. Freire, S. Fuchs, L. Gamper, J. Gukelberger, E. Gull, S. Guertler, et al. The ALPS project release 2.0: Open source software for strongly correlated systems, *J. Stat. Mech.*, P05001, 2011.

A study on the encoding function for the binary classification problem via quantum support vector machine

Yudai Suzuki[1] * Hiroshi Yano[2] † Sho Sasaki[3] ‡ Naoki Yamamoto[3] § Qi Gao[4 5] ¶

[1] *Department of Mechanical Engineering, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*
[2] *Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*
[3] *Department of Applied Physics and Physico-Informatics, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*
[4] *Quantum Computing Center, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*
[5] *Mitsubishi Chemical Corporation & innovation center, 1000, Kamoshida-cho, Aoba-ku, Yokohama 227-8502, Japan*

Abstract. Support Vector Machine (SVM) is a powerful method for classification or regression. Recently, the SVM-type classifier implemented on a quantum computer was proposed, which successfully obtains high accuracy for binary classification problems. However, the performance of that proposed method depends on the form of functions that encode the data onto a quantum computer. In this paper, we give a new encoding function that shows better classification result over the existing method, for a special type of data. Also, we provide a reasonable visualization method that gives a characterization of the classifying ability of the encoding function.

Keywords: Quantum machine learning, Support Vector Machine, Encoding functions, Pauli decomposition

1 Introduction

Thanks to the drastic progress in computing speed as well as the cost-effectiveness ratio, machine learning is now widely applied in a variety of field. In particular, Support Vector Machine (SVM) is a powerful method used for classification or regression; the key technique involved in SVM is the Kernel method, which is typically useful for pattern analysis [2]. To further extend the scope of their applicability, quantum computation is expected to be a promising tool that could enhance the performance of machine learning by exploiting the intrinsic characteristics of quantum mechanics. In fact, recently, Havlíček et al. [1] proposed two SVM-type classifiers implemented on a real quantum computer, which demonstrated the potential to make machine learning further capable to deal with bigger size of data. The proposed quantum SVM methods, however, have a difficulty in finding the encoding function, i.e., a function that encodes the input data into the quantum device. In this paper, we actually show that the classification performance of a quantum kernel estimator, one of the SVM methods proposed in [1], depends on the choice of encoding functions. More precisely, we give a new encoding function such that, for four types of example data, it classifies all those datasets very well while the (quadratic type) encoding function taken in [1] does not. Also, we provide a reasonable visualization method that gives a characterization of the classifying ability of the encoding function, which in fact explains why the chosen encoding function work well.

*baseball1212@keio.jp
†hiroshi.yano.gongon@keio.jp
‡sho_sasaki@keio.jp
§yamamoto@appi.keio.ac.jp
¶caoch@user.keio.ac.jp

2 Method

The success of SVM lies in the use of kernel trick, which enables us to classify even highly complicated dataset with high accuracy; more precisely the kernel is a function that involves a transformation of the input dataset to a linearly separable dataset in a higher dimensional space. The quantum kernel estimator proposed in [1] is a quantum device that computes an estimate of the kernel, with the use of quantum intrinsic properties such as a superposition. A similar work has been done by Schuld et al. [3]. Through the approach, one has to define a set of encoding functions, which transforms the input classical data $\boldsymbol{x}$ to the quantum state $|\Phi(\boldsymbol{x})\rangle$; for more details, see Appendix A.

In this paper we study the four types of dataset shown in Fig.1. Each dataset is composed of 100 two-dimensional data, which are classified to two subgroups with blue or orange colors. All the elements range from -1 to 1; note that the data range studied in [1] is $[0, 2\pi]$.

To encode those classical dataset onto the quantum state $|\Phi(\boldsymbol{x})\rangle$, here we take the following set of encoding functions:

$$\phi_{\{1\}} = x_1, \quad \phi_{\{2\}} = x_2, \quad \phi_{\{1,2\}} = \frac{\pi}{3\cos x_1 \cos x_2}, \quad (1)$$

where x_i is the element of the input data. For comparison, we also perform the same numerical simulation using the following encoding functions:

$$\phi_{\{1\}} = x_1, \quad \phi_{\{2\}} = x_2, \quad \phi_{\{1,2\}} = \pi x_1 x_2. \quad (2)$$

These are a modified version of the encoding functions used in [1], where the range of variables is changed to $[-1, 1]$ from the original one $[0, 2\pi]$.

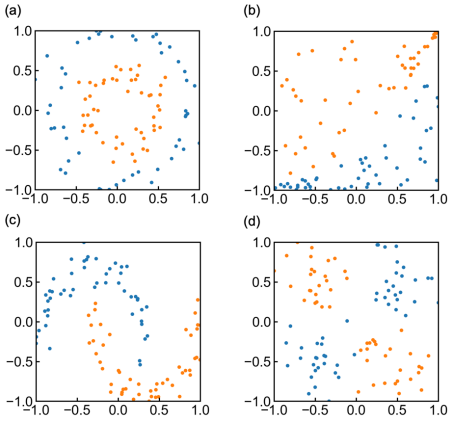


Figure 1: Classification datasets, (a) Circle, (b) Exp, (c) Moon, and (d) XOR.

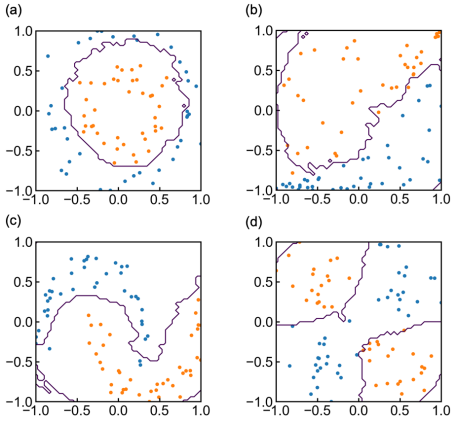


Figure 2: Decision boundaries for the dataset (a) Circle, (b) Exp, (c) Moon, and (d) XOR drawn by learning the training set using the encoding functions (1).

Table 1: Accuracy of training and test sets for four datasets through 5-fold cross validation.

		XOR	Circle	Moon	Exp
(1)	Training	0.97	0.99	0.97	0.97
	Test	0.95	0.97	0.95	0.95
(2)	Training	0.98	0.96	0.81	0.85
	Test	0.96	0.96	0.77	0.85

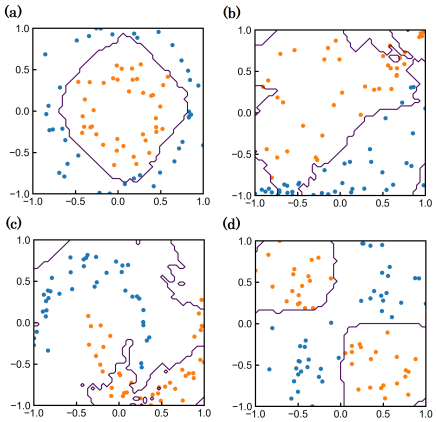


Figure 3: Decision boundaries for the dataset (a) Circle, (b) Exp, (c) Moon, and (d) XOR drawn by learning the training set using the encoding functions (2).

3 Result

To carry out the classification task, each dataset is divided into 5 groups (i.e., each group has 20 data), 4 out of which are used for the training and the remaining for the test. Then we performed the classification for all combination of training and test sets, i.e., the 5-cross validation [2]. In this work we use the QASM simulator provided by IBM to execute the quantum kernel estimator. The decision boundaries for the classification are obtained by examining the training dataset; Fig.2 depicts the boundaries for the proposed encoding function (1), and Fig.3 for the function (2). Moreover, the classification accuracy is shown in Table.1. The decision boundaries for each dataset with the encoding functions (1) appear to be drawn so that two labels are appropriately classified. As for the classification accuracy, the score is bigger than 0.95 for every dataset. On the other hand, the decision boundaries made with the use of the encoding functions (2) also works well, except for the dataset 'Moon' and 'Exp' in Fig.3. In fact, Table.1 shows that the classification accuracy for the dataset 'Moon' and 'Exp', for the case of the encoding function (2), are clearly less than that for the case (1).

4 A characterization for the encoding function

We implemented a classification task with aforementioned two sets of encoding functions to see and compare the classification accuracies for four datasets; as a result, we observe that the accuracy depends on the encoding functions. Hence an important question is as follows; why the functions (1) achieves a much better classification performance particularly for the dataset 'Moon', compared to (2)? Here we focus on a higher dimensional space associated with the quantum state $|\Phi(\boldsymbol{x})\rangle$ to which the input data $\boldsymbol{x}$ is mapped through the encoding function and in which SVM is actually working. That is, we consider the space corresponding to the coefficients of the Pauli decomposition of the density matrix $|\Phi(\boldsymbol{x})\rangle\langle\Phi(\boldsymbol{x})|$; if a n qubits quantum computer is used, the coefficients constitute a 4^n-dimensional real vector $\boldsymbol{a}(\boldsymbol{x})$ whose element $a_i(\boldsymbol{x})$ is the function of the input data $\boldsymbol{x}$; see Appendix B for details.

Here we use a $n = 2$ qubits machine with specific structured quantum circuit. Figure 4 illustrates $a_i(\boldsymbol{x})$ for $i = 1, \ldots 16$ as a function of the two-dimensional input data $\boldsymbol{x}$, for each encoding function (1) and (2). The striking point of this visualization is that there seems to exist one or more vector(s) that is (are) similar to each dataset for encoding functions (1). For example, ZZ, ZI and ZZ components have similar tendency of dataset Circle. Similarly, IY and YI resemble dataset Moon, whereas XI and IX have a partial tendency of dataset XOR. In the case

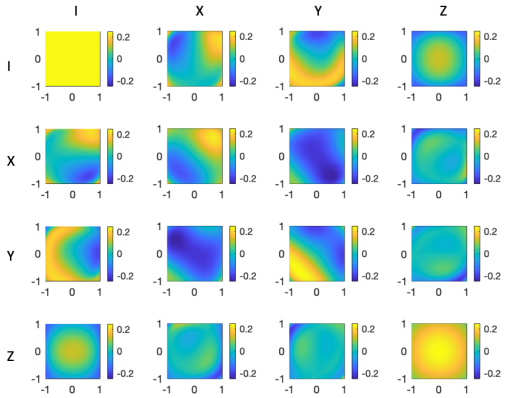


Figure 4: Colormap representation of the vector elements $\{a_i(\boldsymbol{x})\}$, for the case of encoding functions (1).

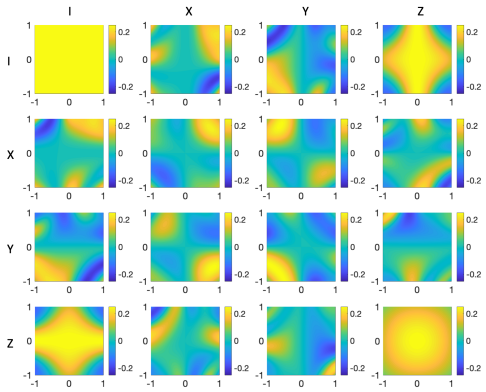


Figure 5: Colormap representation of the vector elements $\{a_i(\boldsymbol{x})\}$, for the case of encoding functions (2).

of encoding functions (2), the information of the dataset Moon appears to be lacking in the vectors. Namely, there is a possibility that a quantum kernel estimator with the encoding functions (1) succeed in separating two labels, because the encoding functions (1) can generate vectors that contains the characteristics of all datasets, while the encoding functions (2) cannot.

5 Conclusion

We demonstrated that the quantum kernel estimator proposed by Havlíček et al. [1] is able to classify several type of nonlinearly separable datasets. In this method, we have to customize the encoding functions that are essential for properly mapping the input data to a quantum space, so that SVM can linearly separate the two labels. To understand the classification accuracy in terms of the encoding functions, we investigate the vectors obtained by Pauli decomposition of the quantum state. Consequently, we observed that the vectors derived by this visualization procedure seem to have the feature of prepared input datasets, that might contribute to successful separations. However, it is difficult to properly set the encoding functions that has a desirable feature map in the quantum space and eventually enables us to get a linearly separable higher dimensional space. We hope

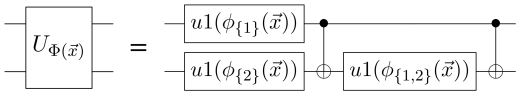


Figure 6: Quantum circuit realizing $U_{\Phi(\boldsymbol{x})}$.

that the analysis of the vectors will help to understand the relationship between the encoding functions and the transformed higher dimensional space, and will also give an insight into development of quantum machine learning.

This work was supported by MEXT, Q-LEAP.

References

[1] V. Havlíček et al.. Supervised learning with quantum-enhanced feature spaces. *Nature* **567**, pages 209–212, 2019.

[2] M. Bishop. Pattern recognition and machine learning (information science and statistics). Springer-Verlag New York, Inc., Secaucus, NJ, 2006.

[3] M. Schuld and N. Killoran. Quantum Machine Learning in Feature Hilbert Spaces. *Phys. Rev. Lett.* **122**, 040504, 2019.

A The quantum kernel estimator

In the quantum kernel estimator [1], only a kernel is estimated on a quantum computer, while the remaining SVM parts are performed on a classical one. The kernel $K(\boldsymbol{x}, \boldsymbol{z}) = |\langle\Phi(\boldsymbol{x})|\Phi(\boldsymbol{z})\rangle|^2$ for the input data $\boldsymbol{x}$ and $\boldsymbol{z}$, is calculated on a quantum computer in the following way. Firstly, the unitary $\mathcal{U}_{\Phi(\boldsymbol{x})}$ is applied to the initial state $|0\rangle^n$, followed by the unitary $\mathcal{U}^\dagger_{\Phi(\boldsymbol{z})}$, where n is the dimension of the input data. Afterwards, the final state in the Z-basis is measured repeatedly to get the number of zero strings 0^n. In this way, the procedure transforms the input data to a quantum state $|\Phi(\boldsymbol{x})\rangle$ and $|\Phi(\boldsymbol{z})\rangle$, and calculate the inner product of them. The unitary $\mathcal{U}_{\Phi(\boldsymbol{x})}$ is composed of two layers of Hadamard gate H^n and the unitary $U_{\Phi(\boldsymbol{x})}$, which means

$$\mathcal{U}_{\Phi(\boldsymbol{x})} = U_{\Phi(\boldsymbol{x})} H^n U_{\Phi(\boldsymbol{x})} H^n, \tag{3}$$

where

$$U_{\Phi(\boldsymbol{x})} = \exp\left(i \sum_{S \subseteq [n]} \phi_{\{S\}}(\boldsymbol{x}) \prod_{i \in S} Z_i \right). \tag{4}$$

In the case $n = 2$, the detail of $U_{\Phi(\boldsymbol{x})}$ is represented as a quantum circuit in Fig. 6. Here, the unitary $U_{\Phi(\boldsymbol{x})}$ contains three user-defined functions $\phi_{\{S\}}$, what we call encoding functions, that nonlinearly transform input data.

B Pauli Decomposition

As explained in Appendix A, the kernel obtained by a quantum kernel estimator is the inner product between two quantum states $\langle\Phi(\boldsymbol{x})|\Phi(\boldsymbol{z})\rangle|^2$. This can be understood in terms of a density operator as follows. Let $\rho(\boldsymbol{x}) = |\Phi(\boldsymbol{x})\rangle\langle\Phi(\boldsymbol{x})|$ be a density operator of the quantum state $|\Phi(\boldsymbol{x})\rangle$. Then, the kernel can be expressed as

$$K(\boldsymbol{x}, \boldsymbol{z}) = \mathrm{tr}\rho(\boldsymbol{x})\rho(\boldsymbol{z}). \tag{5}$$

Furthermore, a density operator $\rho(\boldsymbol{x})$ can be expanded by a set of a Pauli operators, that is,

$$\rho(\boldsymbol{x}) = \sum_{i=1}^{4^n} a_i(\boldsymbol{x})\sigma_i, \tag{6}$$

where,

$$\sigma_i \in \{I, X, Y, Z\}^n. \tag{7}$$

Here, note that $a_i(\boldsymbol{x}) \in \mathbb{R}$. Then, by substituting Eq. 6 into Eq. 5, we get

$$K(\boldsymbol{x}, \boldsymbol{z}) = \sum_{i=1}^{4^n} a_i(\boldsymbol{x})a_i(\boldsymbol{z}), \tag{8}$$

where the trace relation $\mathrm{tr}[\sigma_i\sigma_j] = 2^n\delta_{i,j}$ has been used. Since the kernel is a linear combination of product of Pauli decomposition coefficients according to the Eq.8, the coefficients $\boldsymbol{a}(\boldsymbol{x})$ can be considered as the vectors of the transformed real space by the kernel.

Breakout Local Search for Finding Graph Minors

Kanto Teranishi[1] * Hidefumi Hiraishi[1] † Hiroshi Imai[1 2] ‡

[1] *Graduate School of Information Science and Technology, The University of Tokyo*
[2] *NanoQuine, The University of Tokyo*

Abstract. Quantum Annealing (QA), a framework of finding the ground state of Ising model with using quantum fluctuation, has attracted much attention from researchers. Today, QA machine which has thousands of variables is developed by D-wave Systems. But it is still difficult to solve Ising model whose size is over hundreds because of the engineering constraints of D-wave machine. For the constraints, we need to determine the graph of Ising model is graph minor of the hardware graph implemented in QA machine.

In this paper, we propesed to use Breakout Local Search (BLS), one of the-state-of-the-art classical metaheuristics, for finding graph minor and experimented for measuring its computing power. We ran BLS in the following setting; The hardware graph is a Chimera graph, implemented in D-wave machine, and the input graphs is (a) random graphs, (b) random cubic graphs or (c) random scale-free graphs. Our experimental results imply BLS is better than previous heuristics in embedding random graphs to a Chimera graph. But the results also indicate our implementation could stand improvement in embedding random cubic graphs.

Keywords: Quantum Annealing, graph minor, metaheuristics, Breakout Local Search

1 Introduction

Quantum Computing has attracted attention from many researchers since Peter Shor showed exponentially speedup for integer factoring algorithm by leveraging quantum mechanics [1]. One of the well-researched quantum algorithm is Quantum Annealing (QA), introduced by Nishimori and Kadowaki [2]. QA is approximate algorithm specialized in finding ground state of Ising model and also regarded as a metaheuristic for combinatorial optimization problems. Finding ground state of Ising model minimize the below energy function subject to $\sigma \in \{-1, 1\}^N$ when given $h \in \mathbb{R}^N$ and $J \in \mathbb{R}^{N \times N}$.

$$E(\sigma) = h^\top \sigma + \sigma^\top J \sigma$$

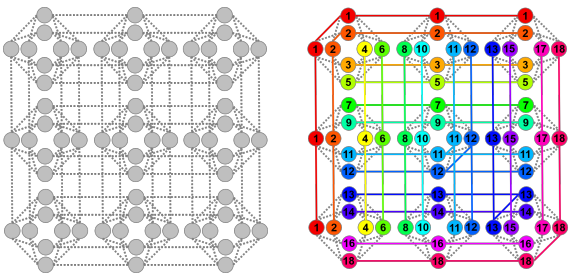
Today, the QA machine is realized by D-wave Systems and we are able to handle thousands of variables in the machine. However it is still difficult to solve Ising model which has hundreds of variables. As one of the factor, the machine restricts interactions between variables to edges of the hardware graph, for example, Chimera graph (Figure 1 (a)) implemented in the D-wave machine. The embedding problem is indicated by Choi [3]. When we would like to solve Ising model, we have to map each variable of Ising model to variables of the D-wave machine. The mapping exists if and only if the graph of Ising model is a minor of the hardware graph.

Let $I = (V(I), E(I))$ denote an input graph, which we want to embed, and $H = (V(H), E(H))$ denote a hardware graph. We figure that an input graph is a graph minor of a hardware graph, when we find $\phi : V(I) \to 2^{V(H)}$ such that

- $\forall i \in V(I), \phi(i) \subset V(H)$, the subgraph induced by $\phi(i)$ is connected in H.
- $\forall i \in V(I), \phi(i) \neq \emptyset$.
- $\forall i, j \in V(I), \phi(i) \cap \phi(j) = \emptyset$ when $i \neq j$.

$$\begin{aligned} \mathcal{E}(\phi) &= |\{(i,j) \in E(I) | \exists u \in \phi(i), \exists v \in \phi(j), (u,v) \in E(H)\}| \\ &= |E(I)| \end{aligned}$$

Finding graph minors is NP-hard problem and exact algorithm for the problem require exponnential time. As heuristical approach, there exist the heuristic introduced by Cai, Macready and Roy (CMR) [7] and probabilistic-swap-shift-annealing (PSSA), Simulated Annealing for finding graph minors by Sugie et al. [8] These heuristics are contrast; while searching graph minors, CMR tolerate a hardware vertex represents multiple input variables, but keeps $\mathcal{E}(\phi) = |E(I)|$, on the other hand, PSSA keeps a hardware vertex represents an input variable, but tolerate $\mathcal{E}(\phi) \leq |E(I)|$ These heuristics enabled us to embed cubic graphs with a certain size, but embedding random graphs is still difficult.



(a) (b)

Figure 1: (a) A Chimera graph, which is implemented in the QA machine developed by D-wave Systems. (b) Generating initial solutions ϕ following grid-line of a Chimera graph based on PSSA counterpart.

*teranishi@is.s.u-tokyo.ac.jp
†hiraishi1729@is.s.u-tokyo.ac.jp
‡imai@is.s.u-tokyo.ac.jp

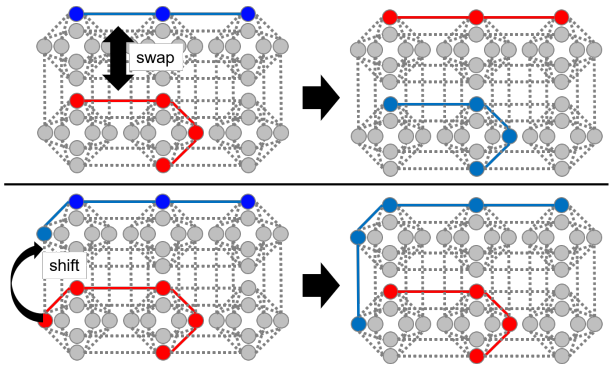


Figure 2: Move operations, swap and shift based on PSSA counterpart.

In this paper, we proposed to use Breakout Local Search (BLS), one of the-state-of-the-art classical metaheuristics, applied to finding graph minors. Our implementation is inspired by PSSA. BLS is proposed by Benlic and Hao, and they experimentally showed BLS exhibits high performance in several NP-hard problems [4][5][6]. Generating initial solutions and move operations, swap and shift (Figure 2), are based on PSSA counterpart.

We describe below briefly our implementation of BLS for a Chimera graph.

1. Generate initial solutions ϕ following grid-line of a Chimera graph (Figure 1 (b)).
2. Move to a local optimum from the current solutions with using best-first search. Firstly apply best-first search with swap move, then with shift move.
3. Adjusts the jump magnitude. If the current solutions is equal to the previous local optimum, increase the jump magnitude, else set the jump magnitude at the initial jump magnitude.
4. Decide a perturbation type with probability depending on the current search stagnation. If BLS assesses the search is stagnate, decide applying strong perturbation, else applying weak perturbation.
5. Reconstruct initial solutions with probability in strong perturbation, else apply shift move chosen randomly.
6. In weak perturbation, chose swap or shift move with probability, then apply the chosen move and search better solutions near the current solutions. BLS has tabu list and prevent repeat same move in short time.

Repeat 2.∼6. while the stopping condition not reached. We ran our BLS in the following situations. The input graphs is (a) random graphs, (b) random cubic graphs or (c) random scale-free graphs and the hardware graph is a Chimera graph.

2 Outline of our experiments

The machine environment is as shown below: CPU: Intel(R) Core(TM) i5-7200U CPU @2.50GHz, Memory: 8.00GBytes. The parameter of BLS is in Table 1.

The hardware graph is a fixed Chimera graph ($|V| = 2048$) and the maximum number of iterations is 40000. We ran BLS 10 times for each input graph, and counted the number of success to finding graph minors. We prepared three graph types for input graphs.

(a) random graphs: We generated random graphs with `rudy` [9], a graph generator which is frequently used. We set graph density 20% for comparing results of [8]. Hence, the number of edges of generated graphs is about $|V| * (|V| - 1) * 0.2$.

(b) random cubic graphs: Degree of each vertex of cubic graphs is 3. We generated random cubic graph in according to [10]. The number of edges of cubic graphs is $1.5 * |V|$.

(c) random scale-free graphs: Degree distribution of scale-free graphs follows a power law. We used Barabasi-Albert model [11]. The number of edges of generated graphs is almost $|V|$.

3 Results and Discussion

Experimental results are given in Table 2. In random graph ($|V| \leq 76$), BLS could find graph minor with high probability only applying best-first search. We assessed initial solutions are exceedingly good.

In [8], CMR running repeatedly (CMRR) and PSSA could embed random cubic graphs ($|V| \geq 200$), however they fail in embedding random graphs ($|V| \geq 68$). Our implemented BLS could only embed random cubic graphs ($|V| \leq 150$), but embed random graphs ($|V| \leq 80$). The results imply BLS is better than PSSA and CMRR in embedding random graphs and our implementation could stand improvement in embedding random cubic graphs.

4 Future Work

Generating initial solutions of our implementation is hold up on the assumption that the hardware graph has no missing edge nor vertex. For applying the existing D-wave machine, we have to implement generating initial solutions dealing with dead edges and vertices.

Acknowledgement

This work was supported by JSPS KAKENHI Grant Numbers 15H01677, 16K12392, 17K12639.

References

[1] 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.

Table 1: The parameter of BLS.

Param.	Description	Value
L_0	Initial jump magnitude	$0.1\|V(I)\|$
T	Maximum number of local optimum visited before applying strong perturb	1000
t	Tabu tenure	$2\|V(I)\|$
P_0	Minimum probability for applying weak perturb	0.8
Q	Probability for applying swap move in weak perturb	0.3
R	Probability for applying restart in strong perturb	0.1

Table 2: Success ratio of finding graph minors by BLS in running 10 times for each instance. In random cubic and random graph instances, We gathered success ratio for instances whose number of vertices and edges are same. There are (a) Random cubic graphs in upper row, (b) Random graphs in middle row, and (c) Random scale-free graphs in lower low.

Graph type	$\|V(I)\|$	$\|E(I)\|$	Succ. ratio
Random cubic	110	165	50/50
	120	180	50/50
	130	195	50/50
	140	210	41/50
	150	225	1/50
Random graph	68	456	50/50
	72	511	50/50
	76	570	50/50
	80	632	50/50
	80	632	50/50
	84	697	0/20
Random scale-free	150	155	10/10
	160	165	6/10
	160	169	6/10
	170	178	4/10
	180	186	4/10
	180	187	1/10
	180	190	2/10

[2] T. Kadowaki and H. Nishimori. Quantum annealing in the transverse Ising model. Physical Review E, 58(5355), 1998.

[3] V. Choi. Minor-embedding in adiabatic quantum computation: I. The parameter setting problem. Quantum Information Processing, 7.5: 193-209, 2008.

[4] U. Benlic and J-K. Hao. Breakout local search for the vertex separator problem. In: Twenty-Third International Joint Conference on Artificial Intelligence, 2013.

[5] U. Benlic and J-K. Hao. Breakout local search for maximum clique problems. Computers and Operations Research, 40(1):192–206, 2013.

[6] U. Benlic and J-K. Hao. Breakout local search for the max-cutproblem. Engineering Applications of Artifcial Intelligence, 26(3):1162–1173, 2013.

[7] J. Cai, W. G. Macready and A. Roy. A practical heuristic for finding graph minors. arXiv preprint arXiv:1406.2741, 2014.

[8] Y. Sugie, Y. Yoshida, N. Mertig, T. Takemoto, H. Teramoto, A. Nakamura, I. Takigawa, S. Minato, M. Yamaoka and T. Komatsuzaki. Graph Minors from Simulated Annealing for Annealing Machines with Sparse Connectivity. In: International Conference on Theory and Practice of Natural Computing. (TPNC 2018), LNCS, Vol. 11324, pp. 111–123, 2018.

[9] G. Rinaldi. Rudy. http://www-user.tu-chemnitz.de/˜helmberg/rudy.tar.gz, 1998.

[10] A. Steger and N. C. Wormald. Generating random regular graphs quickly. Combinatorics, Probability and Computing, 8.4, 377-396, 1999.

[11] A-L. Barabasi and R. Albert. Emergence of scaling in random networks. Science, 286.5439: 509-512, 1999.

Quantum phase transitions and Schmidt gap closing in a Kitaev chain with long-ranged interactions

Cleofe Dennielle P. Ayang-ang[1] * Francis N. C. Paraan[1] †

[1] *National Institute of Physics, University of the Philippines Diliman, Philippines*

Abstract. The quantum phase diagram of a generalized Kitaev chain that exhibits long-ranged hopping and pairing is mapped out by looking for sharp changes in the Schmidt gap of a ground state bipartition. Finite-size scaling analysis reveals that the Schmidt gap exhibits universal scaling behavior about the quantum critical lines. The critical exponents found shows that the model displays different properties at the long- and short-range limits of the interaction.

Keywords: entanglement, critical exponents, quantum phase transition

1 Background and motivations

The past few decades saw an increase of interest in quantum information theory considering its wide range of possible applications (e.g. quantum computers). Much of the study of quantum information theory revolves around the concept of entanglement which leads to further investigation of strongly correlated many-body systems. The entanglement in these systems manifests in the different quantum phases driven by changes in ground state parameters. In this study, the quantum phases of a fermionic chain model with long-range interactions were identified by numerically calculating the Schmidt gap in a finite bipartition of the system prepared in the ground state. The Schmidt gap is the difference between the first two largest eigenvalues of the reduced density matrix of the subsystem under study. In [1], the Schmidt gap is shown to be an acceptable order parameter to signal the symmetry protected topological phase in spin models even if it does not lie under the standard Ginzburg-Landau theory of phase transitions.

Moreover, from the quantum phases mapped, the critical points were located. The Schmidt gap in the vicinity of these points was scaled using finite-size methods. The universal scaling lead to the numerical calculation of the quantum critical exponents associated to the phase transition within the model.

2 Model and methods

The model, which is a generalization of the Kitaev chain model, is defined by the Hamiltonian

$$H = \sin\theta \sum_{i,j=1}^{L} \frac{a_i^\dagger a_j + a_i^\dagger a_j^\dagger + h.c.}{|i-j|^\alpha} + 2\cos\theta \sum_{i=1}^{L} a_i^\dagger a_i. \quad (1)$$

The pairing and coupling interactions decay with site distance by a power law decay with exponent α. The site indices (i, j) run from 1 to the chain length L. Additionally there is a relative chemical potential controlled by the parameter θ. The model can be diagonalized by a Bogoliubov transformation in k-space. The exactly diagonalized Hamiltonian in quasi-fermionic modes is,

$$H = \sum_k \gamma_\alpha(k)(\eta_k^\dagger \eta_k - 1/2). \quad (2)$$

where $\gamma_\alpha(k)$ is the excitation spectrum.

The reduced density matrix (RDM) was derived analytically for a subsystem with 30 sites. All calculations were done in the thermodynamic limit of an infinite chain. Numerical calculations yielded the eigenvalues of the RDM for $0 \leq \alpha \leq 3$ and $0 \leq \theta \leq \pi$. The Schmidt gap, $\Delta\lambda = \lambda_1 - \lambda_2$, showed the different phases of the Kitaev chain. Finite-size analysis was applied to the Schmidt gap near the critical points of the phase transition.

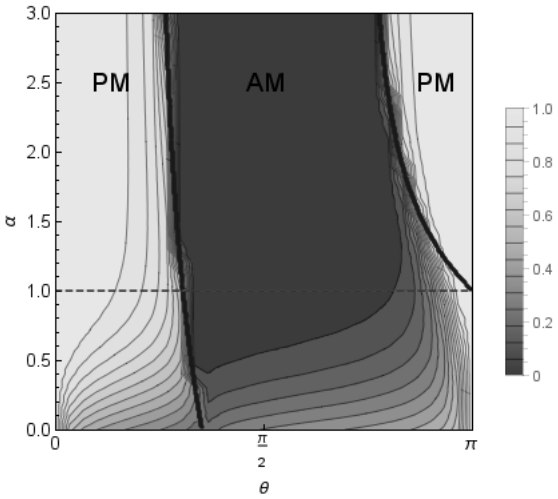


Figure 1: The Schmidt gap shows the 2 different phases of the model with the anti-ferromagnetic phase with vanishing Schmidt gap and the paramagnetic phase with nonzero gap. $\alpha < 1$ denotes the region with long-range interactions while $\alpha \geq 1$ are for short-range.

3 Phase diagram and scaling

In Ref. [2], phases of this model were mapped using the effective central charge of an underlying conformal field theory. Here we show that the same phases can be

*cleofedennielleayangang@gmail.com
†fparaan@nip.upd.edu.ph

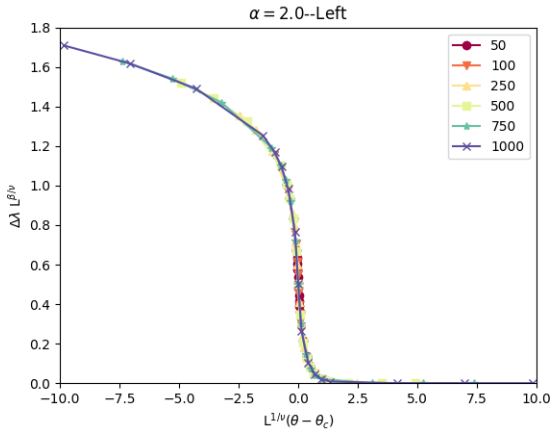


Figure 2: Finite-size analysis near the critical point of $\alpha = 2.0$ on the left critical line obtains curve collapse for all lengths

located using the Schmidt gap as the parameter. Non-zero Schmidt gap shows the area for the paramagnetic phase. This phase is characterized by the disorder of spins caused by the presence of strong interactions. A transition to the anti-ferromagnetic phase is indicated by the abrupt change in the Schmidt gap to zero. The absence of entanglement restores the system in a ordered phase in this region. This also indicates a double degeneracy in the low level entanglement spectrum. The transition lines between these phases also correspond to the gapless regions (broad solid black lines, Fig. 1). The limiting case, $\alpha \to \infty$, the phase diagram simplifies to three regions and the vertical critical lines lie at $\theta = \pi/4$ and $\theta = 3\pi/4$. The paramagnetic phases corresponds to the non-topological phase at $\theta < \pi/4$ and $\theta > 3\pi/4$. The anti-ferromagnetic phase reduces to the topological phase at $\pi/4 < \theta < 3\pi/4$ where unpaired Majoranas are localized at the boundaries [3].

The Schmidt gap for five critical points was scaled for finite block lengths, $\ell = 50, 100, 250, 500, 750, 1000$ using finite-size scaling analysis. The following universal scaling ansatz [4] was used to calculate the exponents β and ν:

$$\mathcal{O}(g, L) = L^{\beta/\nu} f(|g - g_c|L^{-\nu}). \tag{3}$$

The critical exponents (Table 1) were chosen when an optimal curve collapse was achieved such as shown in Fig. 2. In [4], the exponents of the Schmidt gap scaling in the spin-1/2 Ising model showed close correspondence to the critical exponents when using the magnetization as the order parameter, $\beta = 1/8$ and $\nu = 1.0$. A similar observation can be made with the values extracted from α values in the short-range region. Eq. 3 was derived under the assumption that the correlation function decays exponentially with ν when approaching the critical point. Since the correlation is preserved over longer distances in the long-range region, the scaling anzats may not apply accurately as seen in the relatively larger discrepancy in β for $\alpha = 0.5$. This raises the possibility that there is an α dependence in the scaling of long-range interactions, a problem for a presently ongoing work.

Table 1: Numerical values of the critical exponents for each critical point

α	β	ν
0.5	0.1883	0.9916
2.0 (Left)	0.1670	1.0025
2.5 (Left)	0.1699	0.9999
2.0 (Right)	0.1511	1.1428
2.5 (Right)	0.1734	0.9968

4 Summary and conclusions

The Schmidt gap was shown to behave like an order parameter so that its value delineates the quantum phases of a Kitaev chain model with power law decaying interactions. The quantum phase transition occurs at the closing of the Schmidt gap, indicating a degeneracy in the first two levels of the entanglement spectrum. The Schmidt gap also exhibits associated critical behavior resulting in universal critical exponents. Finite-size analysis showed that the scaling of this parameter is consistent with the Ising class of phase transitions when the interactions are sufficiently short-ranged.

References

[1] F. Pollman, A. M. Turner, E. Berg, and M. Oshikawa, Entanglement spectrum of a topological phase in one dimension, *Phys. Rev. B*, 81, 064439, 2010.

[2] D. Vodola, L. Lepori, E. Ercolessi, and G. Pupillo, Long-range Ising and Kitaev models: phases, correlations and edge modes, *New J. Phys.*, 18, 015001, 2015.

[3] A. Yu Kitaev Unpaired Majorana fermions in quantum wires *Physics-Uspekhi* 131, 44.10S, 2001.

[4] G. de Chiara, L. Lepori, M. Lewenstein, and A. Sanpera, Entanglement spectrum, critical exponents, and order parameters in quantum spin chains *Phys. Rev. Lett.*, 109, 237208, 2012.

Minimizing Quantum Circuits for Simultaneous Two-Qubit Measurement by Single-Qubit Measurements

Risa Segawa[1] * Shigeru Yamashita[1] † Rudy Raymond[2]

[1] *Graduate School of Information Science and Engineering, Ritsumeikan University*
[2] *IBM Research - Tokyo*

Abstract. $(3, 2)$-Quantum Random Access Coding (QRAC) is one of the examples of measuring two qubits simultaneously. Although IBM Q system allows only single-qubits measurement at a time, an example shows that a method of decoding $(3, 2)$-QRAC is implemented by IBM Q System. The method performs simultaneous measurement of two-qubit by single-qubit measurement. However, the quantum circuit which is used for the method contains a large number of Controlled-NOT (CNOT) gates. This paper shows a method to minimize the number of CNOT gates used in a quantum circuit to perform simultaneous measurement of two-qubits by single-qubit measurement. The proposed method generates a quantum circuit consisting of only one CNOT gate. Our method generates a circuit which maps an arbitrary orthogonal basis to the initial states. We determine parameters of one-qubit gates in the circuit by approximation. We found that the optimal initial states is different depending on the orthogonal basis used in the quantum circuit generated by the proposed method. We also show that our method can construct a circuit for $(3, 2)$-QRAC decoding with the minimal number of CNOT gates.

Keywords: two-qubit measurement, circuit optimization, IBM Q System

1 Introduction

(3, 2)-Quantum Random Access Coding (QRAC) is an example of performing two-qubit simultaneous measurement [1]. IBM Q system is a system of quantum computing developed by IBM. The system allows only measuring single-qubits at a time. Therefore, we need to consider a special way to perform two-qubit measurements on IBM Q System. Measurement is performed in the example of implementation of (3, 2)-QRAC on Quantum Information Software Kit (QISKit) [2] by IBM as follows [3]. First, we decode a quantum state using a quantum circuit that maps each orthogonal basis used for measurement to $|00\rangle$ and $|01\rangle$. Then, we can measure the two qubits simultaneously by measuring the second qubit only. Three circuits are constructed so that each of three bits can be decoded. These circuits contain at least two CNOT gates.

A Controlled-NOT (CNOT) gate is more costly than a one-qubit gate [4]. Therefore, we need to reduce the number of CNOT gates in a quantum circuit. KAK decomposition [5] can automatically design a quantum circuit that maps a pair of orthogonal basis states to $|00\rangle$ and $|01\rangle$, so it is also useful technique. However, we cannot reduce the number of CNOT gates in the circuit designed by KAK decomposition compared to [3]. This is because KAK decomposition construct a circuit using three CNOT gates.

By considering the above, this paper proposes a method for minimizing a quantum circuit to perform two-qubit simultaneous measurement with single-qubit measurements. We propose to construct a quantum circuit consisting of four ry gates which are one-qubit gates and one CNOT gate. The circuit maps an arbitrary orthogonal basis to the initial states which can be expressed as a tensor product of $|0\rangle$ and $|1\rangle$. We approximate parameters of ry gates in the circuit.

We found that the optimal initial states differ depending on the orthogonal basis in the circuit of the proposed method. We also show the result of applying the proposed method to (3, 2)-QRAC. In this case, the success probability of (3, 2)-QRAC can be maintained and the number of CNOT gates can be reduced compared to the quantum circuit of [3].

*hotaru@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp

2 Simultaneous two-qubit mesurement with single-qubit measurements

We propose a method of measuring two-qubit simultaneously with single-qubit measurements. Figure 1 (a) shows a quantum circuit used in our work. The circuit contains one CNOT gate and four ry gates which are one-qubit gates and it maps the orthogonal basis to the initial states. Initial states mean orthogonal quantum states which are expressed as a tensor product of $|0\rangle$ and $|1\rangle$. In the following, we determine the parameters of ry gates in the circuit; we express those four parameters as $a,\ b,\ c,\ d \in \mathbb{R}$. In this way, we use approximation to determine the parameters. Namely, we minimize the error between the coefficients in the state vectors of actually mapped and those of the initial states.

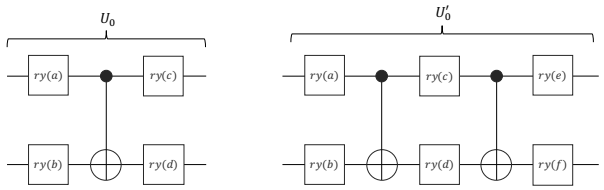
We explain the procedure to derive an expression about a quantum circuit as shown in Fig. 1 (a). First, we prepare the orthogonal basis and the initial states. K_1 and K_2 are the orthogonal basis (Eq. (1)) . S_1 and S_2 are the initial states (Eq. (2)) .

$$K_1 = \begin{pmatrix} K_1[0] \\ K_1[1] \\ K_1[2] \\ K_1[3] \end{pmatrix} \qquad K_2 = \begin{pmatrix} K_2[0] \\ K_2[1] \\ K_2[2] \\ K_2[3] \end{pmatrix} \tag{1}$$

$$S_1 = \begin{pmatrix} S_1[0] \\ S_1[1] \\ S_1[2] \\ S_1[3] \end{pmatrix} \qquad S_2 = \begin{pmatrix} S_2[0] \\ S_2[1] \\ S_2[2] \\ S_2[3] \end{pmatrix} \tag{2}$$

We calculate a matrix to express the linear transformation corresponding to the quantum circuit as shown in Fig. 1 (a). Equation (3) shows the calculation result.

$$U_0 = (ry(c) \otimes ry(d)) \cdot CNOT \cdot (ry(a) \otimes ry(b)) \tag{3}$$



(a) (b)

Figure 1: (a) A quantum circuit with one CNOT gate (b) A quantum circuit with two CNOT gates

Arbitrary orthogonal basis K_1 and K_2 are inputs of Fig. 1 (a). Equation (4) shows the calculation result. M_1 and M_2 in Eq. (4) are state vectors of calculation results corresponding to inputs K_1 and K_2 respectively.

$$U_0K_1 = \begin{pmatrix} M_1[0] \\ M_1[1] \\ M_1[2] \\ M_1[3] \end{pmatrix} \qquad U_0K_2 = \begin{pmatrix} M_2[0] \\ M_2[1] \\ M_2[2] \\ M_2[3] \end{pmatrix} \tag{4}$$

We compare the state vectors of Eq. (4) to that of the initial states. In Eq. (5), we sum up all the squared differences of the corresponding coefficients between the initial and the state vectors expressed as Eq. (4). When we consider only the part where the coefficients in the initial sates are 0 (or 1), we do not sum up all the squared differences in Eq. (5) but we sum up only the squared differences corresponding to the part where the coefficients of initial sates are 0 (or 1).

$$\begin{aligned} &\{S_1[0] - M_1[0]\}^2 + \{S_1[1] - M_1[1]\}^2 \\ &+ \{S_1[2] - M_1[2]\}^2 + \{S_1[3] - M_1[3]\}^2 \\ &+ \{S_2[0] - M_2[0]\}^2 + \{S_2[1] - M_2[1]\}^2 \\ &+ \{S_2[2] - M_2[2]\}^2 + \{S_2[3] - M_2[3]\}^2 \end{aligned} \tag{5}$$

To obtain failure probability, we calculate the square of the amplitude coefficients of the state created by the circuit as shown in Fig. 1 (a) and sum up all of them. Note that, we use the basis excluding we want to obtain by measurement.

In addition, we can determine the parameters in Fig. 1 (b) by the same method for Fig. 1 (a). We calculate a matrix to express the linear transformation corresponding to the quantum circuit of Fig. 1 (b). Eq. (6) shows the calculation result.

$$U_0^{'} = (ry(e) \otimes ry(f)) \cdot CNOT \cdot U_0 \tag{6}$$

After that, we calculate the matrix in the same method as Eq. (5).

3 Experimental results

In order to create quantum circuit with only one CNOT gate, we used Eq. (5) and determined parameters of one-qubit gates in this circuit. We measured of $(3, 2)$-QRAC with QISKit and used a simulator called local_qasm_simulator as a backend to execute quantum programs.

In our work, three orthogonal basis are used as inputs of quantum circuit. M1-M4, M5-M8 and M9-M12 are test cases using different basis. The initial states in each test case are as follows. M1, M5, M9 is $|00\rangle, |11\rangle$, M2, M6, M10 is $|00\rangle, |10\rangle$, M3, M7, M11 is $|11\rangle, |01\rangle$ and M4, M8, M12 is $|11\rangle, |10\rangle$. Failure probabilities of M5-M8 are higher than those of other test cases. M5-M8 use second basis. For example, the failure probability of M1 is 2.4×10^{-28}, but that of M5 is 0.9. We found that the failure probability changes by the initial states; the failure probabilities of M5 and M8 are very high especially. For example, the failure probability of M5 is 0.9 but the failure probability of M6 is 0.1. M6 differs from M5 only in the initial states.

We also constructed a circuit for $(3, 2)$-QRAC decoding keeping success probability of this method (errors of less than 0.6). More than two CNOT gates are used in the circuit for $(3, 2)$-QRAC decoding by [3]. With the proposed method, one CNOT gate is used in the circuit decoding the first bit and the third bit. Two CNOT gates are used in the circuit decoding the second bit.

4 Conclusion

We proposed a method for minimizing a quantum circuit to perform two-qubit simultaneous measurement with single-qubit measurement.

As a result, we found that optimal initial states differ from orthogonal basis in the circuit for mapping the two-qubit states which can be expected original states by measuring single-qubit. With maintaining the success probability, we can reduce CNOT gates used in the circuit for $(3, 2)$-QRAC decoding of proposed method as compared with that of [3].

We will analyze the regularity for mapping arbitrary initial states to orthogonal basis in the circuit used one CNOT gate, and consider application to QRAC.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 15H01677 and 18K19790.

References

[1] Takashi Imamichi and Rudy Raymond. Constructions of Quantum Random Access Codes. Asian Quantum Information Science Conference, 2018.

[2] Quantum Information Software Kit. `https://www.qiskit.org/`. Accessed: 2018.12.17.

[3] $(3, 2, 1/2 + 1/\sqrt{6})$-QRAC - github repository. `https://github.com/rraymondhp/qrac/blob/master/32QRAC.ipynb`. Accessed: 2018.12.17.

[4] The IBM Q provider - Jupyter Notebook Viewer. `https://nbviewer.jupyter.org/github/Qiskit/qiskit-tutorial/blob/master/qiskit/basics/the_ibmq_provider.ipynb`. Accessed: 2018.12.29.

[5] Vidal, Guifre and Dawson, Christopher M. Universal quantum circuit for two-qubit transformations with three controlled-NOT gates. Physical Review A, vol.69, no.1, pp.010301, 2004.

Generalized nonlocality criteria under the correlation symmetry

Kwangil Bae[1] Wonmin Son[1] *

[1] *Department of Physics, Sogang University, Mapo-gu, Shinsu-dong, Seoul 121-742, Korea*

Abstract. The class of correlation for the most generalized Bell scenario considering N-partite d-chotomic system with k number of measurements is derived under the constraint of measurement symmetries. The nonlocality criteria for the generalized scenario is obtained using the correlation function, which is derived from Fourier analysis of probability spectrum. The condition under which the local hidden variable model is violated by the multipartite quantum state is found in analytic manner. It is shown that the various types of known Bell inequalities can be derived in our class of correlation.

Keywords: Non-locality, Bell inequality, quantum correlation

1 Introduction

Bell inequality is the correlation inequality satisfied by any local-realistic theory. Since the seminal work of J. S. Bell showing the violation of local hidden-variable model by quantum mechanical expectation [1], various type of the Bell inequalities has been derived under generalized Bell scenarios [2–10]. Although there has been many contributions to the problem of the characterization of so-called all-the-Bell inequalities [11], many problems has still remained [12, 13]. The difficulty of characterizing nonlocality in generalized scenario arises from the fact that the dimension of the correlation space increases geometrically when the system becomes complex. In this work [10], we present the nonlocality criteria in the fully generalized Bell scenario using generic correlation with the symmetries on the choice of the measurement settings [10, 14]. The local-realistic [15] and quantum [16] optimization of our class of Bell inequalities [7] has been studied in our previous work. The symmetrization method to efficiently characterize generalized Bell inequality has been introduced independently in the papers [7, 10, 14, 17, 18]. Although with the constraint on the choice of measurement settings, it is found that the various types of known Bell inequalities can be derived from our class of correlation. The application of our class of Bell inequalities to entanglement measure [19] and quantum cryptography [20] has been recently introduced based on [7]. In the following sections, the general class of correlation is defined and the nonlocality criteria is derived from it with the quantum violation condition.

2 General class of Bell correlation

The correlation for the fully generalized Bell scenario for N-partite d-chotomic system with k-number of measurement settings is given below.

$$G^c_{N,k,d} = \sum_{\bar{n}=1}^{d-1} f(\bar{n}_c) \left\langle \prod_{j=1}^{N} \left[\sum_{m_j=0}^{k-1} \omega^{c_j n_j m_j/k} A_j^{c_j n_j}(\lambda, m_j) \right] \right\rangle + \text{c.c.} \quad (1)$$

where *c.c.* denotes the complex conjugate. The complex weighting function of the correlation, $f(\bar{n}_c)$, determines the specific form of correlation in the class $G^c_{N,k,d}$. The joint-probabilistic representation is derived as

$$G^c_{N,k,d} = \sum_{\{\alpha_j\}=1}^{d} \sum_{\{m_j\}=0}^{k-1} g^c_{\vec{\alpha},\vec{m}} p(\vec{\alpha}|\vec{m}). \quad (2)$$

The real coefficient $g^c_{\vec{\alpha},\vec{m}}$ is derived from the Fourier transform relation of correlation function such that

$$g^c_{\vec{\alpha},\vec{m}} = 2\text{Re}\left[\sum_{\vec{n}} f(\bar{n}_c) \omega^{\bar{n}_c \cdot (\vec{\alpha} + \vec{m}/k)} \right]. \quad (3)$$

Then the bound by the local hidden-variable theory can be obtained from the weighting function g such that

$$G^c_{N,k,d} \leq B_{LR} = \max_{\vec{\alpha}} \left[\sum_{\vec{m}} g^c_{\vec{\alpha},\vec{m}} \right] \quad (4)$$

In [10], it is shown that the known Bell inequalities; CHSH [2], Mermin [3], CGLMP [4], Zukowski-Brukner [5], Epping-Kampermann-Bruss [8] can be derived in our class. The weighting functions f and g for each Bell correlations are listed in [10].

3 Quantum violation by maximally entangled state

Using the concurrent observables defined in [10], the Bell operator corresponding to (1) reduce to the sum of ladder operators whose dimensional weighting is given as the fucntion f. The violation of the local-realistic bound with the maximally entangled state can be evaluated from the bound obtained,

$$B_{LR} \leq Q_M = 2k^N \sum_{n=1}^{d-1} \left(1 - \frac{n}{d}\right) |f(n)| \quad (5)$$

when assuming the high-order powers for the correlation functions is homogeneous. For example, the CGLMP violation can be derived from the weighting function of CGLMP as a not-closed(open) but analytic formula (6).

$$Q_M^{CGLMP} = 2k^N \sum_{n=1}^{d-1} \left(1 - \frac{n}{d}\right) \left| \sec\left[\frac{n\pi}{2d}\right] \right| \quad (6)$$

* sonwm@physics.org

4 Conclusion

In this work, a class of correlation for fully generalized Bell scenario is presented under correlation symmetry which reduces the complexity embedded in the derivation of generalized Bell inequalities. Although with the constraints on correlation, we could derive various type of known Bell type correlations from the correlation. The criteria for deriving LHV bound and quantum violation for the suggested correlation is obtained as the functions of weighting parameter which is given when the specific correlation is determined in our class of correlation.

References

[1] J. S. Bell On the Einstein Podolsky Rosen paradox *Physics*, 1:195, 1964.

[2] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable(LHV) theories *Phys. Rev. Lett.*, 23:880-4, 1969.

[3] N. David Mermin Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States. *Phys. Rev. Lett.*, 65:1838, 1990.

[4] D. Collins. et al. Bell inequalities for arbitrarily high dimensional systems *Phys. Rev. Lett.*, 88:170405, 2002.

[5] M. Zukowski and C. Brukner. *Phys. Rev. Lett.* 88:210401, 2002.

[6] D. Collins. et al. Bell inequalities for arbitrarily high dimensional systems *J. Phys. A: Math. Gen.*, 37:1775, 2004.

[7] W. Son, J. Lee and M. Kim Generic Bell Inequalities for Multipartite Arbitrary Dimensional Systems *Phys. Rev. Lett.*, 96:060406, 2006.

[8] M. Epping, H Kampermann and D. Bruss. Designing Bell Inequalities from a Tsirelson Bound. *Phys. Rev. Lett.* 111: 240404, 2013.

[9] A. Salavrakos et al. Bell Inequalities Tailored to Maximally Entangled States *Phys. Rev. Lett.*, 119:040402, 2017.

[10] K. Bae and W. Son. Generalized nonlocality criteria under the correlation symmetry. *Phys. Rev. A* 98: 022116, 2018.

[11] A. Peres All the Bell Inequalities. *Foundations of Physics* 29:589, 1999.

[12] N. Gisin Bell inequalities: many questions, a few answers. aXiv:quant-ph/0702021, 2007.

[13] N. Gisin Bell nonlocality. *Rev. Mod. Phys.* 86:419, 2014

[14] W. Son, J. Lee and M. S. Kim d-outcome measurement for a nonlocality test *J. Phys. A: Math. Gen.*, 37:11897, 2004.

[15] G. Bae and W. Son Axiomatic approach for the functional bound of generic Bell's inequality. *Curr. Appl. Phys.*, 16:378-386, 2016.

[16] G. Bae and W. Son Analytic Evaluation of the High-Order Quantum Correlation for Non-Locality. *J. Kor. Phys. Soc.*, 69:11, 2016.

[17] J. D. Bancal et al. 2010 **43** 385303 Looking for symmetric Bell inequalities. *J. Phys. A: Math. Theor.*, 43:385303, 2010.

[18] V. U. Gunery and M. Hillery Bell inequalities from group actions: Three parties and non-Abelian groups. *Phys. Rev. A*, 80:010103, 2009.

[19] C. Datta, P. Agrawal, and S. K. Choudhary Measuring higher-dimensional entanglement. *Phys. Rev. A*, 95:042323, 2017.

[20] S. Roy and S. Mukhopadhyay Device Independent Quantum Secret Sharing in Arbitrary Even Dimension. arXiv:1903.11836 [quant-ph], 2019.

A handy condition of bridge compression for topological quantum circuits

Yohei Wakabayashi[1] * Shigeru Yamashita[1] †

[1] *Graduate School of Science and Engineering, Ritsumeikan University*

Abstract.
TQC (Topological Quantum Computation) has been proposed because it has fault tolerance to quantum decoherence. In TQC, we can perform quantum computation by using 3D cluster states. We can optimize a topological quantum circuit by some transformation rules. In 2019, a variety of transformation rules have been proposed. However, we can optimize circuits by utilizing these rules only manually. This paper studies the condition that a transformation called bridge does not destroy the topology of circuits. We then propose an optimization method of quantum circuits by focusing the number of intersections of the torus.

1 Introduction

The quantum decoherence is a phenomenon that the quantum superposition is destroyed by the effect of outside factors such as heat and electromagnetism, etc. TQC has been proposed because it has the fault tolerance to quantum decoherence [1]. In TQC, we can perform quantum computation by using topological cluster states and a logical operation called braiding [2, 3, 4]. The topological cluster state consists of surface codes [1]. Circuits can be represented by the tracks of braiding.

Topological rules are to transform an original circuit into an equivalent circuit by only expansion and contraction. Another rule is a transformation called bridge [5]. Bridge is one of the transformations for preserving the equivalence of a calculation.

We need to reduce the cost of a topological quantum circuit because it uses many quantum bits. Fowler and Devitt proposed a method that reduces the cost of a topological quantum circuit by using the topological rules and bridge [5]. Their method spends bags of time to optimize a topological quantum circuit because they optimize a circuit manually. Adam and Fowler also proposed a method to optimize a topological quantum circuit by only using topological rules [6].

In this paper, we propose to reduce the cost of circuits by using bridge, which is called bridge compression. We study an automatic optimization method based on the condition such that bridge compression does not destroy the topology of circuits. Then we can generate an optimized circuit which has a minimal number of intersections of the toruses. We can reduce the cost of circuits by only using topological rules. Subsequently, we can further reduce the cost of circuits by applying bridge compression to the reduced circuits.

2 Optimization of Topological Quantum Circuits

All topological quantum circuits can be considered as a set of toruses where each torus corresponds to a pair of defects. Fig. 1 (a) shows a topological quantum circuit represented by a set of toruses. A topological quantum circuit consists of red and blue toruses as shown in Fig. 1 (a). Red and blue toruses are referred to as primal and dual toruses, respectively. We can reduce the cost of circuits by considering a set of toruses. In this paper, the cost of circuits is the number of intersections of toruses. The presence or absence of intersections of toruses corresponds to the presence or absence of braiding between the corresponding defects, respectively.

Our proposed condition of bridge compression:
Fig. 1 (b) shows bridge which is a transformation to connect toruses of the same type. We can reduce the cost of circuits by using bridge, which is called bridge compression. Bridge compression integrates primal (dual) edges which intersect with a shared dual (primal) torus, respectively. We can transform the circuit shown in Fig. 1 (b) to the circuit shown in Fig. 1 (c) by applying bridge compression. In this paper, we introduce the concept of what we call an integrated edge. By applying bridge compression, we can integrate dual (primal) edges into one edge, which we call an integrated edge. The formula (1) represents an integrated edge shown in Fig. 1 (c).

$$P_2[D_1, D_2] \tag{1}$$

First and second dual torus intersects with the second primal torus. Therefore, the formula (1) indicates that these edges of dual toruses are integrated. We show two conditions of integrated edges that destroy the topology of circuits in the following.

(i) The integrated edges are not adjacent in Fig. 2 (a)

(ii) We can not apply bridge compression to each edge of all toruses that a concave torus shown in Fig. 2 (b) intersects with. (Fig. 2 (c))

We can optimize circuits by applying bridge compression if bridge compression satisfies some condition.

*jonathan@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp

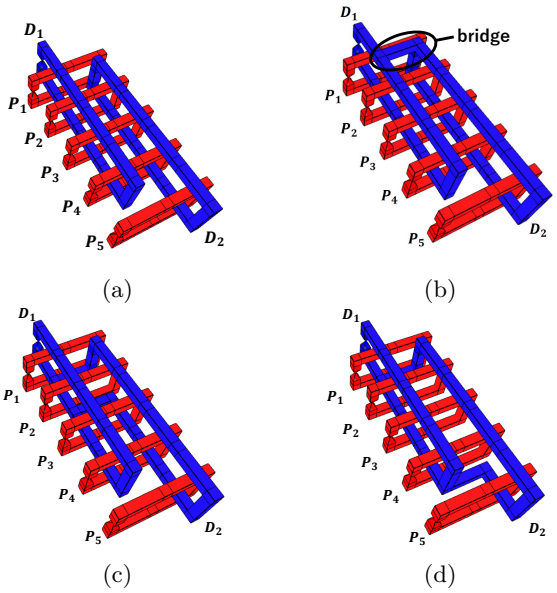


Figure 1: (a)A topological quantum circuit represented by toruses. (b)A topological quantum circuit can be obtained by applying bridge to Fig. 1 (a). (c)A topological quantum circuit can be obtained by applying bridge compression to P_2. (d)A topological quantum circuit can be obtained by applying bridge compression to P_3 and P_4

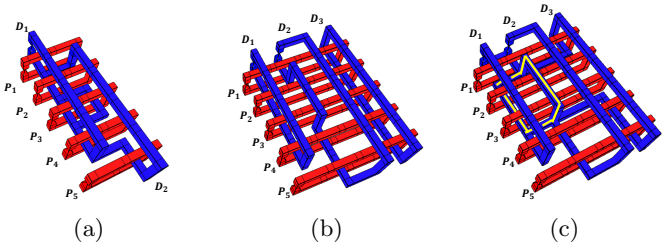


Figure 2: (a)A topological quantum circuit whose integrated edges are not adjacent. (b)A concave torus form a part of a topological quantum circuit. (c)A topological quantum circuit whose genus is distinct from Fig. 2 (b).

3 Experimental results

We have compared our method with the method by Fowler and Devitte. For our comparison, we used $|Y\rangle$ state distillation circuit as shown in Fig. 3 (a). Fig. 3 (b) shows an initial topological quantum circuit to perform the quantum circuit shown in Fig. 3 (a). The initial cost of Fig.3(b) is 22. The cost of Fig. 3 (b) has decreased to 4 by our method. We can obtain the same cost as the method by Fowler and Devitte. Therefore, we can confirm that the method by Fowler and Devitte is thought to be best for $|Y\rangle$ state distillation circuit.

4 Conclusion

In this paper, we have proposed a new scheme to optimize a topological quantum circuit automatically with a bridge. We can treat a topological quantum circuit entirely as a set of toruses and optimize topological quantum circuits by using transformation rules. In 2019, a variety of transformation rules have been proposed. However, the condition of bridge compression has not been defined precisely. Therefore, we define two conditions of bridge compression. Consequently, we can optimize topological quantum circuits automatically with our scheme.

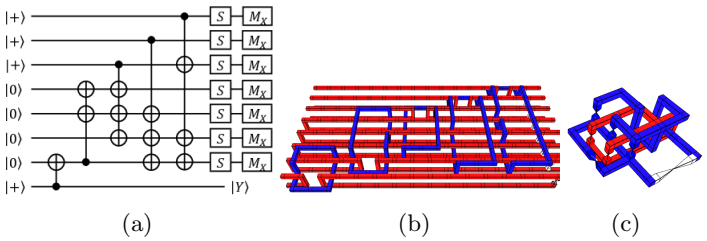


Figure 3: (a)$|Y\rangle$ state distillation circuit (b)A topological quantum circuit performing the computation of Fig. 3 (a) (c)A topological quantum circuit obtained by the method by Folwer and Devitte from Fig. 3 (b)

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 15H01677 and 18K19790, and by the Asahi Glass Foundation.

References

[1] Austin G Fowler, Matteo Mariantoni, John M Martinis, and Andrew N Cleland. Surface codes: Towards practical large-scale quantum computation. Physical Review A, Vol. 86, No. 3, p. 032324, 2012.

[2] Raussendorf, R. and Harrington, J. and Goyal, K. Topological fault-tolerance in cluster state quantum computation. New Journal of Physics, vol.9, p.199, 2007.

[3] Austin G Fowler and Kevid Goyal. Topoogical cluster state quantum computing. arXiv preprint arXiv:0805.3202, 2008.

[4] Michael Freedman, Alex Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. Bulletin of the American Mathematical Society, Vol. 40, No. 1, pp. 33-38, 2003.

[5] Fowler, A. G. and Devitt, S. J. A bridge to lower overhead quantum computation. quant-ph/1209.0510, 2012.

[6] Paetznick, A. and Fowler, A. G. Quantum circuit optimization by topological compaction in the surface code. quant-ph/1304.2807, 2013.

Self-testing of unsharp measurements

Nikolai Miklin,[1] Jakub J. Borkała,[1] and Marcin Pawłowski[1]
[1] *University of Gdansk, Poland*

Unsharp, or generalized, measurements are known to provide an advantage in certain Quantum Information Processing tasks. Examples include quantum tomography, state discrimination, randomness certification, to name a few. However, there is one important property of generalized measurements that is discussed less often than the others in the literature. It is the trade-off between information gain and the disturbance that this type of measurements allows for. In fact, unsharp measurements can be seen as a resource in sequential scenarios, as compared to projective ones and their probabilistic mixtures.

In this work we consider the case of binary qubit unsharp measurements. All these measurements can be simulated by probabilistic mixture of projective measurements. However, as we show in our work, there exist sequential scenarios, in which unsharp measurements provide a strict advantage over their probabilistic realizations. The key fact, which allows for such discrimination, is that the set of quantum instruments realizing a given Positive-Operator Valued Measure (POVM) is much larger than the set of instruments, corresponding to simulation of that POVM with projective measurements. Moreover, as shown later in the text, the proposed scheme allows for semi-device-independent self-testing of essentially all binary qubit measurements.

Semi-device-independent (SDI) framework, introduced in [1], is an analogy of device-independent approach for the scenarios with communication. In this framework the single assumption is made on the dimension of the Hilbert space, associated with the degree of freedom, used for encoding of quantum information. We would like to point out that the assumption on the dimension is natural for both cryptographic schemes with quantum communication and for studying generalized measurements.

Since in the SDI framework the bases of measurements are not fixed, the only parameters that we will be interested in are the eigenvalues of the effects of POVMs. However, we will concentrate on the case when all the effects are trace-1. This case is the most relevant one, as it studies the trade-off between an unbiased random assignment and a projective measurement. The "biased case" corresponds to the same picture, but with random assignment being biased.

Let us now introduce our scenario for self-testing. This scenario is a direct generalization of $2^2 \to 1$ Quantum Random Access Code (QRAC) [2]. Consider three parties, Alice, Bob, and Charlie, communicating in a sequential way as shown on Fig. 1. Alice receives two random bits, $\vec{x} = (x_0, x_1),\ x_0, x_1 \in \{0, 1\}$. Bob and Charlie each receives a random bit, y and z respectively, which indicates which bit of Alice they are interested in. Depending on $\vec{x}$, Alice prepares a qubit state $\varrho_{\vec{x}}$, which she sends to Bob, who then performs some quantum operation on it, depending on his input y. Afterwards, Bob sends the post-operation state $\varrho^y_{\vec{x},b}$ to Charlie, who performs a measurement, depending on z. The instruments of Bob and the respective POVMs are the ones that we are self-testing in this scheme.

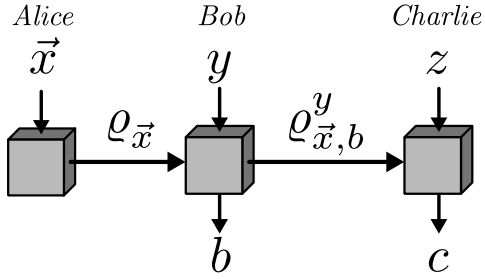


FIG. 1: Scenario. $\vec{x}$ – input data of Alice. y, b – input and output of Bob, z, c – input and output of Charlie. $\varrho_{\vec{x}}$ – states that Alice sends to Bob. $\varrho^y_{b,\vec{x}}$ – states that Bob sends to Charlie.

A figure of merit that we consider, is the following average success probability

$$\bar{P}_{\text{succ}} = \frac{\alpha}{8}\sum_{\vec{x},y}\Pr(b = x_y|\vec{x}, y) + \frac{1-\alpha}{8}\sum_{\vec{x},z}\Pr(c = x_z|\vec{x}, z), \tag{1}$$

with $\alpha \in [0, 1]$. The parameter α is announced prior to the game and remains unchanged. It dictates the parties whose guess will contribute more to the overall success probability.

Now we are ready to present our main results.

Proposition 1. *Average success probability $\bar{P}_{succ}$ for strategies, involving projective measurements and their probabilistic mixtures, is bounded by the following expression*

$$\bar{P}^{PVM}_{succ}(\alpha) = \begin{cases} \frac{1}{2} + \frac{1-\alpha}{2\sqrt{2}}, & 0 \le \alpha \le 1 - \frac{2}{\sqrt{7}}, \\ \frac{1}{2} + \frac{1}{8}\sqrt{4 + (1-\alpha)^2}, & 1 - \frac{2}{\sqrt{7}} < \alpha \le \frac{1}{3}, \\ \frac{1}{2} + \frac{1}{4}\sqrt{1 + \alpha^2}, & \frac{1}{3} < \alpha \le 1. \end{cases}$$

Proposition 2. *The bound on the average success probability $\bar{P}_{succ}$ for the general strategy is the following*

$$\bar{P}^{POVM}_{succ}(\alpha) = \frac{1}{2} + \frac{1-\alpha}{4\sqrt{2}} + \frac{1}{4\sqrt{2}}\sqrt{(1-\alpha)^2 + 4\alpha^2}. \tag{2}$$

The operator norm of the effects of the optimal POVMs of Bob is the following

$$\| B^y_b \| = \frac{1}{2} + \frac{\alpha}{\sqrt{(1-\alpha)^2 + 4\alpha^2}},\ b = 0, 1,\ y = 0, 1. \tag{3}$$

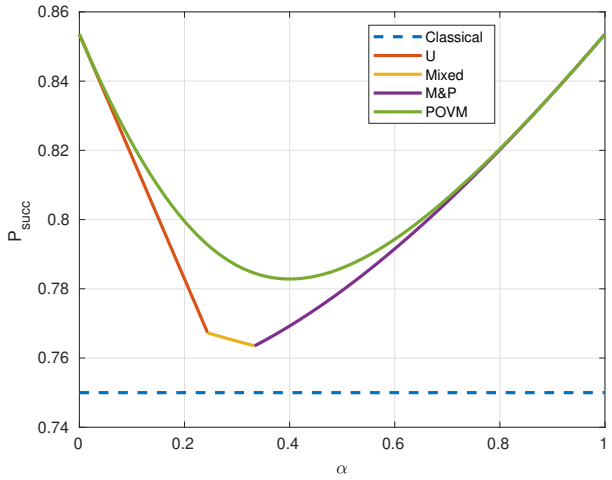


FIG. 2: Bounds on average success probability. Blue dashed line corresponds to the classical strategy, orange yellow and purple to the "unitary", "mixed" and "measure and prepare" projective strategies respectively. Green line corresponds to the general strategy with unsharp measurements.

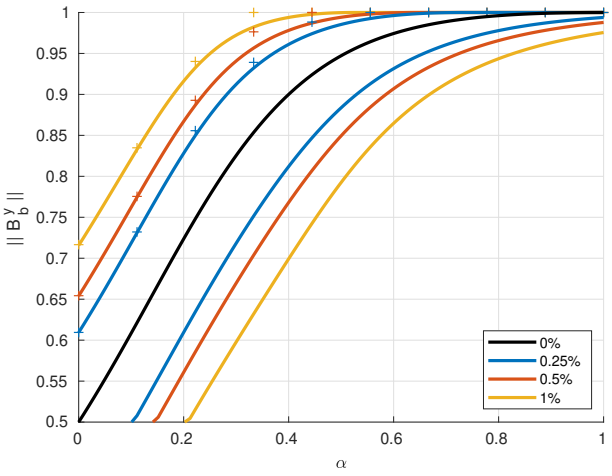


FIG. 3: Optimal operator norm (black line) and bounds (colour lines) on the norm for different drops in observed average success probability, with respect to the optimal one.

As a part of the proof of this Proposition, we have proposed a modification of the Semi-Definite Programming (SDP) techniques of Ref. [3] that approximate the set of correlations, that can be observed in our scenario.

The results of both Propositions 1, 2 are shown on Figure 2. On this plot we have also shown the classical bound of $\frac{3}{4}$ for this game, which does not require a proof. We should point out that all the bounds are tight, in the sense that there exist states and measurement reaching these average success probabilities.

On Figure 3 (black line) we plot the optimal norm $\| B_b^y \|$ from Eq. (3), which is, as we can see, a monotonically increasing function of α. It also takes all possible values from 0.5 to 1. This fact suggests that we can, in principle, self-test any unsharp "unbiased" POVM by picking the corresponding value of α.

The next main result is the robustness of our tests. In particular, we can ask what can be inferred about the norm of the POVM effects, if our experimental value of the average success probability is somewhere between $\bar{P}_{\text{succ}}^{\text{PVM}}(\alpha)$ and $\bar{P}_{\text{succ}}^{\text{POVM}}(\alpha)$. Our results on the robustness are shown on Figure 3 (colour lines).

In Ref. [1] the authors proposed a semi-device-independent one-way quantum key distributions scheme which is based on QRAC protocol. It was shown that one can prove a security against individual attacks if the average success probability of the $2^2 \to 1$ QRAC is greater than $\frac{5+\sqrt{3}}{8} \approx 0.8415$.

As one of the main results of this paper (Proposition 2) we have derived the following family of monogamy relations

$$\alpha \bar{P}_{\text{QRAC}}^{\text{Bob}} + (1-\alpha)\bar{P}_{\text{QRAC}}^{\text{Charlie}} \leq \bar{P}_{\text{succ}}^{\text{POVM}}(\alpha), \ \alpha \in [0,1]. \quad (4)$$

We can now naturally think about Bob as an eavesdropper, and Alice and Charlie trying to establish a secret key, as described in Ref. [1]. From Eq. (4) we can immediately derive the bound on Bob's success probability as a function of Charlie's success probability by optimizing over α. Setting $\bar{P}_{\text{QRAC}}^{\text{Bob}} = \bar{P}_{\text{QRAC}}^{\text{Charlie}}$, and taking the optimal $\alpha = \frac{2}{5}$, we find the value of the critical success probability $\frac{1}{2} + \frac{\sqrt{2}}{5} \approx 0.7828$, which is a significant improvement, in comparison to 0.8415.

From the monogamy relations (4) one could also calculate the secret key rates corresponding to a particular success probability of Charlie. For Charlie's success probability equal to $\frac{1}{2} + \frac{1}{2\sqrt{2}}$, we can see that Bob's success probability has to be $\frac{1}{2}$, which results in the secret key rate of approximately 0.5835. This is also a significant improvement to the results of Ref. [1], where the maximal key rate was reported to be 0.0581.

[1] M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," *Physical Review A*, vol. 84, no. 1, p. 010302, 2011.

[2] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," *arXiv preprint arXiv:0810.2937*, 2008.

[3] M. Navascués and T. Vértesi, "Bounding the set of finite dimensional quantum correlations," *Physical review letters*, vol. 115, no. 2, p. 020501, 2015.

Quantum Generative Adversarial Networks for Discrete Data

Haozhen Situ[1,3] , **Zhimin He**[2] , **Yuyi Wang**[4] , **Lvzhou Li**[3,5] , **Shenggen Zheng**[3,6]
[1] College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China
[2] School of Electronic and Information Engineering, Foshan University, Foshan 528000, China
[3] Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518055, China
[4] Distributed Computing Group, ETH Zurich
[5] School of Data and Computer Science, Sun Yat-Sen University, Guangzhou 510006, China
[6]Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China

Abstract

We propose quantum generative adversarial networks (quantum-GANs) for discrete data generation, which complements classical GANs that are not suitable for this task due to the problem of indifferentiability. Our quantum GAN is composed of a parameterized quantum circuit as the generator and a classical feedforward neural network as the discriminator. Two families of quantum circuits, both consist of simple one-qubit rotation and two-qubit controlled-phase gates, are considered. The analytic gradient of the quantum generator can be estimated by sampling the same quantum generator, and thus gradient-based methods can be used in the training. The results of a small-scale numerical simulation demonstrate the effectiveness of our scheme.

1 Introduction

Generative models aim to emulate the distribution of training data and generate new instances accordingly, and a number of deep generative models have been proposed that are capable to create novel human-level art. Have you ever imagined that you could paint like da Vinci or Picasso? That's out of question today and generative adversarial networks (GANs [Goodfellow et al., 2014]) can help you producing images which look like paintings by the artist you choose.

The idea of GANs is to introduce a discriminator to play the role of the generator's adversary, forming a two-player game. The objective of the discriminator is to distinguish real from generated ones, *e.g.,* fake images, while the objective of the generator is to produce new instances resembling training instances, *e.g.,* real images.

Apart from images, language data also plays an important role in artificial intelligence. As Denis Diderot said, "If they find a parrot who could answer to everything, I would claim it to be an intelligent being without hesitation ..." You may wonder whether GANs can help with such dialogue generators, or generate other language and text data, *e.g.,* poetry, stories and jokes. Indeed, GANs could potentially become powerful tools for natural language processing, but the first condition is that the indifferentiability problem of GANs can be resolved, since language data is much more discrete than data in the visual domain.

The indifferentiability problem of GANs is in the training process: The generator produces some fake samples. Not only is the discriminator trained to distinguish between the generated and real data, but also the discriminator tells the generator how to tweak so that generated instances become more realistic. Technically, the gradients of the discriminator's output with respect to the generated data is further back-propagated to all the generator's parameters. In order to do this, the loss function should be differentiable w.r.t. the instance, which requires that the data space is continuous.

We propose a novel method based on quantum computing techniques, which shows that quantum computation naturally has this merit to equip GANs with the ability of dealing with discrete data.

The era of quantum computing is around the corner. In 2016, IBM provided access to its quantum computer to the community through a cloud platform called IBM Quantum Experience. A quantum computing competition among IT giants including Microsoft, Google, Intel is under way. Because quantum computing has the admirable capability of processing exponentially high-dimensional data, quantum machine learning [Biamonte et al., 2017] is expected to be one of the most intriguing future applications of quantum computers. Many researches on machine learning problems with the help of quantum computing have been taken in the last decade [Wiebe et al., 2012; Rebentrost et al., 2014; Yu et al., 2016; Dunjko et al., 2016; Monràs et al., 2017; Duan et al., 2017; Du et al., 2018; Yu et al., 2019].

In this paper, we present a quantum GAN in which the generator is a parameterized quantum circuit and the discriminator is a classical feedforward neural network. Two families of quantum circuits, both consist of simple one-qubit rotation and two-qubit controlled-phase gates, are considered. This quantum GAN can be trained by a hybrid quantum-classical gradient descent approach, as the analytic gradient of the quantum generator can be estimated by sampling the same quantum generator. We also use a small-scale numerical sim-

ulation to demonstrate the effectiveness of our scheme.

2 Related Work

Recently, some efforts have been devoted to how to improve the generative models with the help of quantum computing. [Benedetti et al., 2018a] trained shallow parameterized quantum circuits to generate GHZ states, coherent thermal states and Bars and Stripes images. [Liu and Wang, 2018] developed a gradient-based learning scheme to train deep parameterized quantum circuits for generation of Bars and Stripes images and mixture of Gaussian distributions. These quantum generative models are also known as Born machines as the output probabilities are determined by Born's rule. In addition, the idea of quantum generative adversarial learning was recently explored theoretically by [Lloyd and Weedbrook, 2018]. A quantum GAN consists of a quantum generator and a quantum discriminator was numerically implemented to generate simple quantum states [Dallaire-Demers and Killoran, 2018]. [Benedetti et al., 2018b] derived an adversarial algorithm for the problem of approximating an unknown quantum pure state. [Hu et al., 2019] demonstrated that a superconducting quantum circuit can be adversarially trained to replicate the statistics of the quantum data output from a digital qubit channel simulator. Compared with these researches on quantum GANs that focused on generating quantum data, our work centers on the generation of classical discrete data. We emphasize the fact that the outputs of quantum generators can be either quantum states, or classical discrete measurement outcomes. But there is no way to produce classical continuous data for a quantum circuit.

Parameterized quantum circuits are also used in other machine learning parameterized models [Wan et al., 2017; Romero et al., 2017; Mitarai et al., 2018; Cincio et al., 2018; Lamata et al., 2018]. One of the possible reasons for adopting parameterized quantum circuits is that sampling from output distributions of random quantum circuits must take exponential time in a classical computer [Boixo et al., 2018], which suggests that quantum circuits exhibit stronger representational power than neural networks.

Besides GANs, there is another commonly used generative model, called variational autoencoders (VAE [Kingma and Welling, 2013]), which can also be improved with quantum techniques. [Khoshaman et al., 2018] introduced quantum VAEs and used quantum Monte Carlo simulations to train and evaluate the performance of quantum VAEs.

Several ways have been proposed to make classical GANs capable to output discrete data, in particular language and text data. For example, by combining with policy gradient, GANs use a discriminative model to guide the training as a reinforcement learning policy [Guo et al., 2018].

3 Model Architecture

In this section, we present the architecture of our generative quantum circuits built with simple one-qubit rotation and two-qubit controlled-phase gates, and the adversarial training scheme.

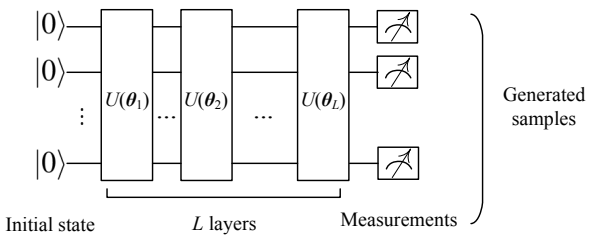


Figure 1: The generative quantum circuit with L layers

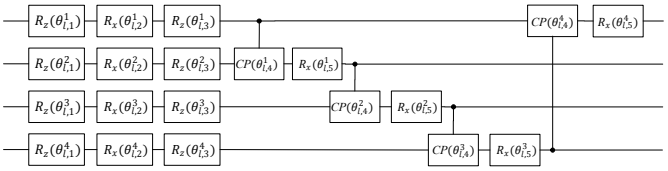


Figure 2: A layer of the quantum circuit for four qubits

3.1 Generative Quantum Circuit

Our quantum circuit for generation of N-bit samples involves N qubits, the layout of which is described in Fig. 1. The input quantum state is initialized to $|0\rangle^{\otimes N}$, and then passed through L layers of unitary operations. At the end of the circuit, all the qubits are measured in the computational basis. The measurement outcomes are gathered to form an N-bit sample x. Each layer is composed of several one-qubit rotation gates and two-qubit controlled-phase gates. Fig. 2 shows the arrangement of these gates in one layer. Three rotation operations are first applied to each qubit. This process can be written as

$$\prod_{i=1}^{N} R_z^i(\theta_{l,3}^i) R_x^i(\theta_{l,2}^i) R_z^i(\theta_{l,1}^i),$$

where the superscript i denotes the ith qubit, and the subscript l denotes the lth layer. $R_x(\theta)$ and $R_z(\theta)$ are rotation gates, *i.e.,*

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

The number of parameters/gates in this process is $3N$ per layer. The choice of these operators is because any one-qubit unitary can be decomposed into this sequence of rotation operators.

We also need to entangle the qubits by performing controlled-U gates between the qubits. This process can be written as

$$\prod_{i=1}^{N} CU_{(i \bmod N)+1}^{i},$$

where the superscript i denotes the control qubit, and the subscript $(i \bmod N)+1$ denotes the target qubit. Each unitary is characterized by three parameters, so the number of parameters in this process is $3N$ per layer. However, [Schuld et al., 2018] has pointed out that this process can be simplified to

$$\prod_{i=1}^{N} R_x^{(i \bmod N)+1}(\theta_{l,5}^i) CP_{(i \bmod N)+1}^{i}(\theta_{l,4}^i),$$

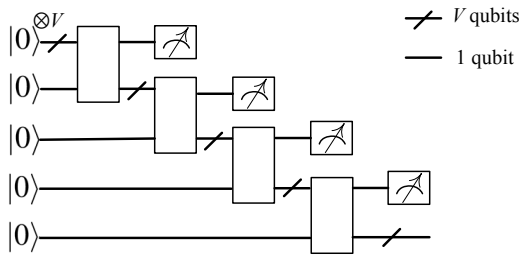


Figure 3: The generative MPS quantum circuit with $N = 4$ nodes

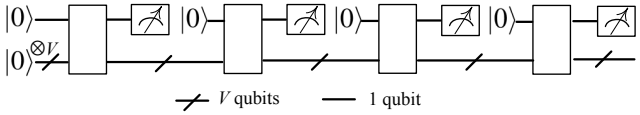


Figure 4: The generative MPS quantum circuit with reused qubits

where

$$CP(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

is the controlled-phase gate. Now the entangling process only has $2N$ parameters/gates per layer. The total number of parameters/gates in the quantum circuit is $5NL$. The set of all parameters can be denoted as a vector $\vec{\theta} = \{\theta_1, \ldots, \theta_{5NL}\}$ for convenience of expression.

3.2 Generative MPS Quantum Circuit

Besides the aforementioned family of quantum circuits, we also consider another family of quantum circuits, which are called "MPS quantum circuits" [Huggins et al., 2018]. Fig. 3 illustrates the structure of the MPS quantum circuit, which looks like a maximally unbalanced tree with N nodes. Each node is a quantum ansatz which inputs and outputs $V + 1$ qubits. The uppermost output qubit of each node is measured in the computational basis and the other V qubits flow to the next node. The N measurement outcomes comprise the N-bit generated sample x. Each node can contain $L \geqslant 1$ layers which have the same gates and layouts as the layers depicted in Fig. 2. The number of parameters/gates in one node is $5L(V + 1)$, so the number of parameters/gates in an MPS quantum circuit is $5NL(V + 1)$. The input qubits are all initialized to $|0\rangle$ in our numerical experiment.

If the MPS quantum circuit is implemented using quantum devices, each qubit that has been measured can be set to $|0\rangle$ and reused as the input of the next node. So only $V+1$ qubits are actually needed in the circuit evaluation process. The sample dimension N is only related to the depth of the circuit. Fig. 4 gives an equivalent form of the MPS circuit in order to illustrate the idea of qubit recycling. This quantum circuit has advantage in physical implementation because near-term quantum devices have limited number of qubits.

3.3 Discriminator

A discriminator D is introduced to distinguish between real samples and generated samples. The discriminator we use is a shallow feedforward neural network. The input layer has the same dimension as the samples. Only one hidden layer is employed. The output layer has only one output value in $[0, 1]$, which represents the discriminator's prediction about the probability of the input sample being real. An output $D(x) = 1$ means the discriminator believes the input sample x is definitely real, while an output $D(x) = 0$ means it believes the input sample x is definitely fake.

The loss function of the discriminator we adopt here is the binary cross entropy function commonly used in binary classification tasks:

$$J_D = -\frac{1}{2}\Big(\mathbb{E}_{x\sim P_d(x)} \log D(x) + \mathbb{E}_{x\sim P_{\vec{\theta}}(x)} \log\big(1 - D(x)\big)\Big), \tag{1}$$

where $P_d(x)$ is the real data distribution and $P_{\vec{\theta}}(x)$ is the generated distribution. In every epoch of the training process, we sample one mini-batch of samples from the training data and the generator, respectively, to calculate the average loss

$$J_D(\mathbf{x}, \mathbf{y}) = -\frac{1}{2 \cdot \mathbf{batch\_D}} \sum_i y_i \log D(x_i) + (1 - y_i) \log(1 - D(x_i)), \tag{2}$$

where $\mathbf{batch\_D}$ denotes the number of samples in one mini-batch, $(x_i, y_i) \in (\mathbf{x}, \mathbf{y})$ denotes the ith sample and its label, $y_i = 1(0)$ for real (fake) labels. The loss function evaluates how close are the predictions $D(x_i)$ and the desired labels y_i. $J_D(\mathbf{x}, \mathbf{y})$ achieves minimum zero if $D(x_i) = y_i$ for every (x_i, y_i).

Let $\mathbf{w}$ be the set of all the parameters of the discriminator. The gradient of $J_D(\mathbf{x}, \mathbf{y})$ with respect to $\mathbf{w}$ can be obtained by the backpropagation algorithm. A variety of gradient-based optimization algorithms can be used to train the discriminator. For example, the vanilla gradient descent method updates $\mathbf{w}$ in the following way:

$$\mathbf{w} \leftarrow \mathbf{w} - \alpha_D \cdot \frac{\partial J_D(\mathbf{x}, \mathbf{y})}{\partial \mathbf{w}},$$

where α_D is the learning rate.

3.4 Optimization of the generator parameters

The goal of the generator is to generate samples that can fool the discriminator. The training process of the generator only uses generated samples, which are paired with true labels, so Eq. (1) reduces to

$$J_G = -\mathbb{E}_{x\sim P_{\vec{\theta}}(x)} \log D(x),$$

where $P_{\vec{\theta}}(x)$ is the probability of getting measurement outcome x from the quantum circuit parameterized with $\vec{\theta} = \{\theta_1, \theta_2, \ldots\}$. The gradient of J_G with respect to θ_i is

$$\frac{\partial J_G}{\partial \theta_i} = -\sum_{x\in\{0,1\}^N} \log D(x) \frac{\partial P_{\vec{\theta}}(x)}{\partial \theta_i}. \tag{3}$$

Using the techniques in [Mitarai et al., 2018] we have

$$\frac{\partial P_{\vec{\theta}}(x)}{\partial \theta_i} = \frac{1}{2}\big(P_{\vec{\theta}^+}(x) - P_{\vec{\theta}^-}(x)\big), \tag{4}$$

where $\vec{\theta}^{\pm} = \vec{\theta} \pm \frac{\pi}{2}\mathbf{e}^i$, $\mathbf{e}^i$ is the ith unit vector in the parameter space (i.e., $\theta_i \leftarrow \theta_i \pm \frac{\pi}{2}$, with other angles unchanged). The proof is given in the appendix. By substituting Eq. (4) into Eq. (3), we have

$$\frac{\partial J_G}{\partial \theta_i} = \frac{1}{2}\mathbb{E}_{x\sim P_{\vec{\theta}^-}(x)} \log D(x) - \frac{1}{2}\mathbb{E}_{x\sim P_{\vec{\theta}^+}(x)} \log D(x).$$

In order to estimate the gradient with respect to each θ_i, we have to sample two mini-batches $\mathbf{x}_\mathbf{i}^+$ and $\mathbf{x}_\mathbf{i}^-$ from the circuits with parameters $\vec{\theta}^+$ and $\vec{\theta}^-$, respectively, then the gradient is estimated by

$$\frac{1}{2 \cdot \mathbf{batch\_G}}\Big(\sum_{x\in\mathbf{x}_\mathbf{i}^-} \log D(x) - \sum_{x\in\mathbf{x}_\mathbf{i}^+} \log D(x)\Big), \tag{5}$$

where $\mathbf{batch\_G}$ denotes the number of samples in one mini-batch.

The generator's parameters $\vec{\theta}$ can be optimized by gradient-based optimization algorithms. For example, the vanilla gradient descent method updates $\vec{\theta}$ in the following way:

$$\vec{\theta} \leftarrow \vec{\theta} - \alpha_G \cdot \frac{\partial J_G}{\partial \vec{\theta}}, \tag{6}$$

where α_G is the learning rate.

3.5 Adversarial Training

The adversarial training algorithm of our quantum GAN is described in Algorithm 1. The training process iterates for a fixed number of epochs, or until some stopping criterion is reached, *e.g.,* convergence on the loss function. At each epoch, the parameters of the discriminator and the generator are updated $\mathbf{d\_step}$ and $\mathbf{g\_step}$ times, respectively.

Algorithm 1 Adversarial training algorithm of our quantum GAN

Input: L: number of layers; V: number of ancilla qubits (only for MPS circuits); $\mathbf{batch\_D}, \mathbf{batch\_G}$: mini-batch size; $\mathbf{d\_step}$: times of updating $\mathbf{w}$ in one epoch; $\mathbf{g\_step}$: times of updating $\vec{\theta}$ in one epoch;
Output: $\vec{\theta}$: the parameters of the generator

```
Initialize the generator and the discriminator with random parameters
for number of training epochs do
    for d_step steps do
        Sample a mini-batch of batch_D samples from the training dataset. Label them as "real".
        Sample a mini-batch of batch_D samples from the quantum circuit. Label them as "fake".
        Use these samples and labels to calculate the gradient of the loss according to Eq. (2).
        Update the discriminator's parameters w according to the gradient.
    end for
    for g_step steps do
        For each θ_i, sample a mini-batch of batch_G samples from the quantum circuit with parameters θ⃗+.
        For each θ_i, sample a mini-batch of batch_G samples from the quantum circuit with parameters θ⃗−.
        Use these samples to calculate the gradient of the loss according to Eq. (5).
        Update the generator's parameters θ⃗ according to the gradient.
    end for
end for
```

4 Numerical Simulation

We verify our proposal using a synthetic dataset known as Bars and Stripes (BAS), which is also used in [Benedetti et al., 2018a; Liu and Wang, 2018] to test quantum generative models. The dataset contains $m \times m$ binary images with only bar patterns or stripe patterns. There are 2^m different vertical bar patterns and 2^m different horizontal stripe patterns. The all-black and all-white patterns are counted in both bar patterns and stripe patterns. So there are $2^{m+1} - 2$ possible BAS patterns for an $m \times m$ image. We assume all BAS patterns appear with equal probability. Obviously each pixel can be encoded in one qubit, so an $m \times m$ image can be encoded in m^2 qubits. We restrict our experiments to the case of $m = 2$, because it's difficult to simulate more qubits efficiently using an ordinary PC. Experiments for larger m will be done in the future if an intermediate-scale near-term quantum device is available.

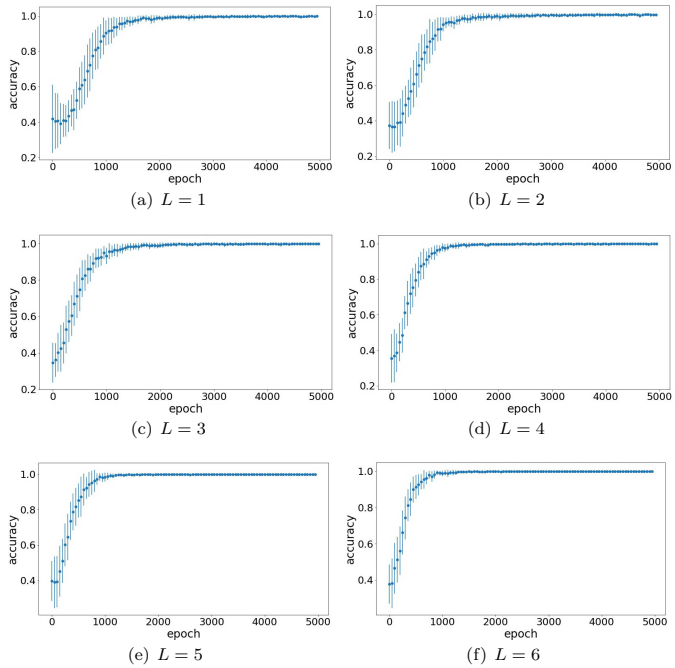
The simulation code is written in Python language. The discriminator is classical so it's implemented using the widely used deep learning framework PyTorch. The discriminator has one input layer with dimension $m \times m$, one hidden layer made up of 50 neurons with the ReLU activation function $f(x) = \max(0, x)$, and one output neuron using the Sigmoid activation function $f(x) = 1/(1+e^{-x})$. The stochastic gradient optimizer Adam (Adaptive Moment Estimation) [Kingma and Ba, 2014] is used to update the discriminator's parameters. The initial learning rate for Adam is 10^{-3}.

The generative quantum circuit is simulated directly by calculating the evolution of the wavefunction. An N-qubit wavefunction is encoded in a 2^N-dimensional complex vector. After performing a single-qubit operation $u_{11}|0\rangle\langle 0| + u_{12}|0\rangle\langle 1| + u_{21}|1\rangle\langle 0| + u_{22}|1\rangle\langle 1|$ on the ith qubit, the wavefunction is transformed to

$$\alpha'_{*\ldots*0_i*\ldots*} = u_{11} \cdot \alpha_{*\ldots*0_i*\ldots*} + u_{12} \cdot \alpha_{*\ldots*1_i*\ldots*},$$
$$\alpha'_{*\ldots*1_i*\ldots*} = u_{21} \cdot \alpha_{*\ldots*0_i*\ldots*} + u_{22} \cdot \alpha_{*\ldots*1_i*\ldots*},$$

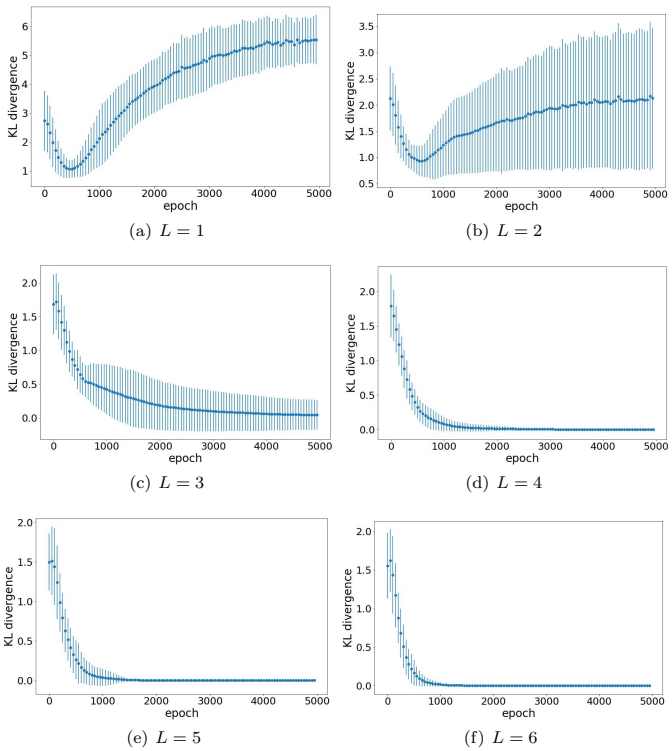
where α and α' are amplitudes before and after transformation. The case of two-qubit operation can be deduced analogously. The parameters of the quantum circuit is updated according to Eq. (6) with a constant learning rate $\alpha_G = 2 \times 10^{-2}$. The gradient is estimated according to Eq. (5).

The two numerical experiments we perform differ in the structure of the quantum generator. The first experiment uses the general quantum circuit described in section 3.1, while the



(a) $L = 1$ (b) $L = 2$ (c) $L = 3$ (d) $L = 4$ (e) $L = 5$ (f) $L = 6$

Figure 5: Averages and standard deviations of the accuracy w.r.t. the number of epochs



(a) $L = 1$ (b) $L = 2$ (c) $L = 3$ (d) $L = 4$ (e) $L = 5$ (f) $L = 6$

Figure 6: Averages and standard deviations of the KL divergence w.r.t. the number of epochs

second experiment uses the MPS quantum circuit described in section 3.2.

4.1 Generative Quantum Circuit

In the first numerical experiment, the quantum generator is the general quantum circuit presented in Section 3.1. We choose hyper-parameters $\mathbf{batch\_D} = 64$, $\mathbf{batch\_G} = 100$, $\mathbf{d\_step} = 1$, $\mathbf{g\_step} = 1$. The learnable parameters of the quantum circuit are randomly initialized in the interval $(-\pi, \pi)$. Unlike the training of classification models, the stopping criterion of training GANs is very tricky, so we simply run the training algorithm for 5000 epochs. For each $L = 1, 2, 3, 4, 5, 6$, we repeat the experiment 30 times. The averages and standard deviations of three indicators (i.e., accuracy, KL divergence and loss) are reported every 50 epochs.

We first examine the accuracy of the generator. The accuracy in some epoch is defined as the ratio of the number of valid samples (*i.e.,* BAS patterns) in one mini-batch to $\mathbf{batch\_D}$. The generator accuracy w.r.t. the number of epochs is depicted in Fig. 5. We can see that for each L from 1 to 6, the accuracy increases very quickly and achieves nearly 100% in 1000 epochs, which means that it's not difficult for the generator to learn to avoid producing non-BAS patterns.

But our goal is not merely producing correct BAS patterns. The distribution of the generated patterns is expected to be the same as that of the training dataset, i.e., uniform distribution in our case. KL divergence is usually used to measure how one probability distribution diverges from a second, expected probability distribution, which is defined by

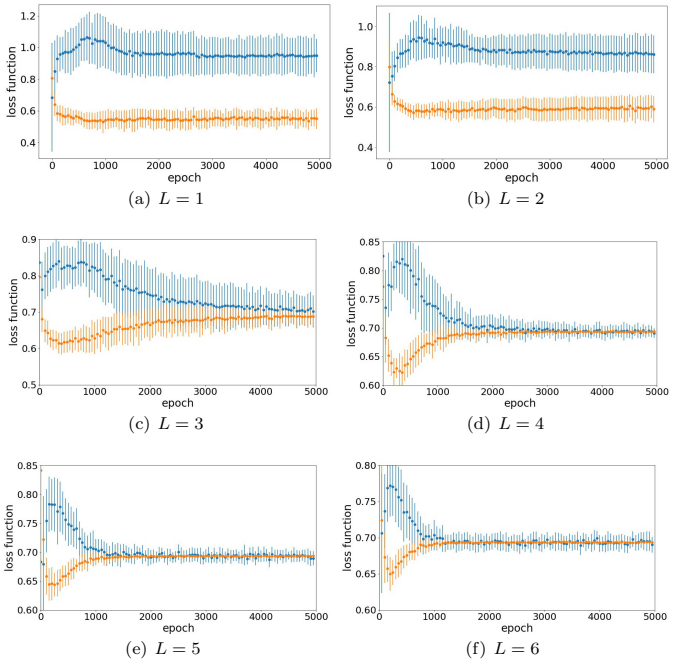
$$\mathrm{KLD}(P_d \| P_{\vec{\theta}}) = -\sum_x P_d(x) \log \frac{P_{\vec{\theta}}(x)}{P_d(x)},$$

where P_d and $P_{\vec{\theta}}$ are the real data distribution and the generated distribution, respectively. $\mathrm{KLD}(P_d \| P_{\vec{\theta}})$ is non-negative and equals zero if and only if $P_d = P_{\vec{\theta}}$ almost everywhere. The distribution of the generated samples can be estimated by their frequency of occurrences. In numerical simulation, the exact distribution can be obtained from the wave function. We draw the variation of the KL divergence w.r.t. the number of epochs in Fig. 6. For $L = 1, 2$, the capacity of the generator is not enough for generating the target distribution. A large standard deviation means in some runs the generator can produce the target distribution, but in other runs it can generate only part of the valid BAS patterns. For $L = 3$, the trained generator can generate the target distribution in most of the 30 runs. For $L = 4, 5, 6$, the KL divergence always converges to zero, which demonstrates the representation power of deeper quantum circuits.

We also plot the loss functions of both the generator and the discriminator w.r.t. the number of epochs in Fig. 7. When the adversarial game reaches equilibrium, the output of the discriminator is 1/2 for both real and generated samples. By substituting $D(x_i) = 1/2$ into Eq. (2), we have $J_{final} = -\log \frac{1}{2} \approx 0.693$. According to Fig. 7 we can see that for $L = 1, 2$, the averages of two loss functions are separated. With the increase of L, they gradually converge to J_{final}.

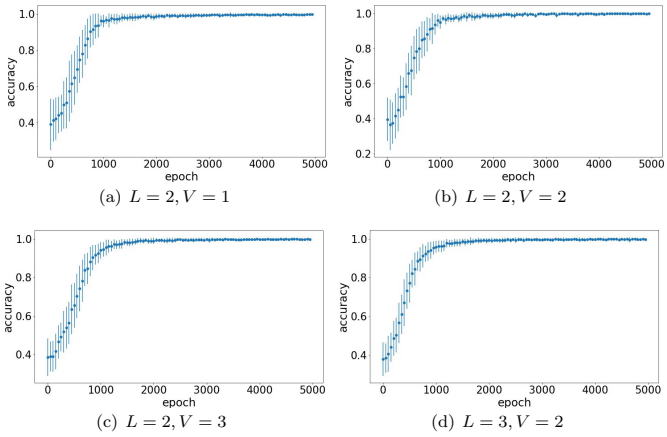
4.2 Generative MPS Quantum Circuit

In the second numerical experiment, the quantum generator is the MPS quantum circuit presented in section 3.2. After a lot of trials, we choose the hyper-parameters $\mathbf{batch\_D} = 64$,



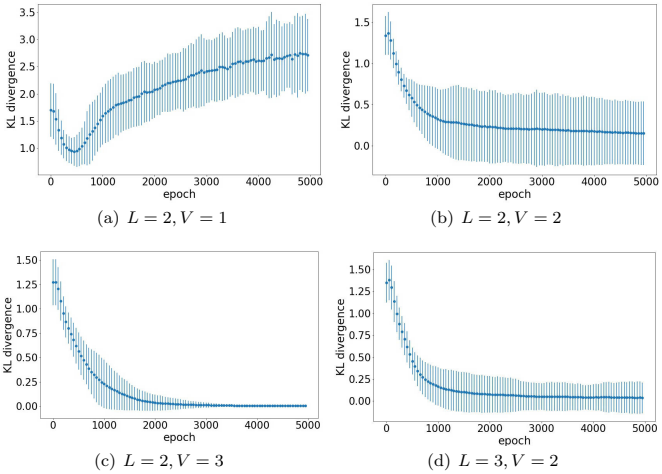
(a) $L = 1$ (b) $L = 2$ (c) $L = 3$ (d) $L = 4$ (e) $L = 5$ (f) $L = 6$

Figure 7: Averages and standard deviations of the loss functions of the generator (in blue) and the discriminator (in orange) w.r.t. the number of epochs



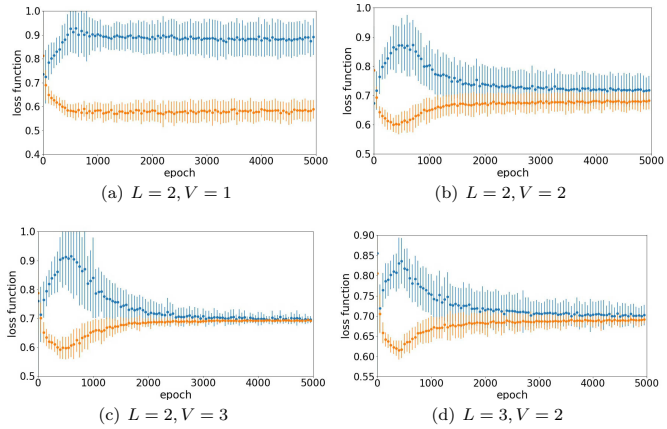
(a) $L = 2, V = 1$ (b) $L = 2, V = 2$ (c) $L = 2, V = 3$ (d) $L = 3, V = 2$

Figure 8: Averages and standard deviations of the accuracy w.r.t. the number of epochs



(a) $L = 2, V = 1$ (b) $L = 2, V = 2$ (c) $L = 2, V = 3$ (d) $L = 3, V = 2$

Figure 9: Averages and standard deviations of the KL divergence w.r.t. the number of epochs



(a) $L = 2, V = 1$ (b) $L = 2, V = 2$ (c) $L = 2, V = 3$ (d) $L = 3, V = 2$

Figure 10: Averages and standard deviations of the loss functions of the generator (in blue) and the discriminator (in orange) w.r.t. the number of epochs

$\mathbf{batch\_G} = 100$, $\mathbf{d\_step} = 1$, $\mathbf{g\_step} = 1$. The learnable parameters of the quantum circuit are randomly initialized in the interval $(-\pi, \pi)$. We report 4 cases with L and V set to: (a) $L = 2, V = 1$, (b) $L = 2, V = 2$, (c) $L = 2, V = 3$, (d) $L = 3, V = 2$. Because the amount of learnable parameters in the MPS circuit is $5NL(V + 1)$, the number of parameters in these four cases is 80, 120, 160 and 180, respectively. A model with more parameters can be regarded as having larger capacity. For each case, we repeat the experiment 30 times and report the averages and standard deviations every 50 epochs.

The generator accuracy w.r.t. the number of epochs is depicted in Fig. 8, which shows that the accuracy increases very quickly and achieves nearly 100% after 1000 epochs. The variation of the KL divergence is depicted in Fig. 9. We can see that the generated distribution gradually approaches the real data distribution with the increase of the capacity of the generator. The variation of the loss functions of both the generator and the discriminator w.r.t. the number of epochs is plotted in Fig. 10. We can see that both loss functions converge to J_{final} when the KL divergence approaches zero.

5 Conclusion

We propose quantum GANs for classical discrete data generation, which can be regarded as a complement to classical GANs and deserve further research.

Interesting future research directions include 1) generating discrete data with higher dimension, 2) choosing the layout of the generative quantum circuit, 3) modelling the generator with non-unitary quantum dynamics, 4) employing variants

of GAN framework, using more heuristics to guide the training, and 5) in-depth theoretical analysis of quantum GANs.

References

[Benedetti et al., 2018a] Benedetti, M., Garcia-Pintos, D., Perdomo, O., Leyton-Ortega, V., Nam, Y., and Perdomo-Ortiz, A. (2018a). A generative modeling approach for benchmarking and training shallow quantum circuits. *arXiv:1801.07686*.

[Benedetti et al., 2018b] Benedetti, M., Grant, E., Wossnig, L., and Severini, S. (2018b). Adversarial quantum circuit learning for pure state approximation. *arXiv:1806.00463*.

[Biamonte et al., 2017] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., and Lloyd, S. (2017). Quantum machine learning. *Nature*, 549(7671):195.

[Boixo et al., 2018] Boixo, S., Isakov, S. V., Smelyanskiy, V. N., Babbush, R., Ding, N., Jiang, Z., Bremner, M. J., Martinis, J. M., and Neven, H. (2018). Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595.

[Cincio et al., 2018] Cincio, L., Subaşı, Y., Sornborger, A. T., and Coles, P. J. (2018). Learning the quantum algorithm for state overlap. *New Journal of Physics*, 20(11):113022.

[Dallaire-Demers and Killoran, 2018] Dallaire-Demers, P.-L. and Killoran, N. (2018). Quantum generative adversarial networks. *Physical Review A*, 98(1):012324.

[Du et al., 2018] Du, Y., Liu, T., Li, Y., Duan, R., and Tao, D. (2018). Quantum divide-and-conquer anchoring for separable non-negative matrix factorization. In *Proceedings of the 27th International Joint Conference on Artificial Intelligence*, pages 2093–2099. AAAI Press.

[Duan et al., 2017] Duan, B., Yuan, J., Liu, Y., and Li, D. (2017). Quantum algorithm for support matrix machines. *Physical Review A*, 96(3):032301.

[Dunjko et al., 2016] Dunjko, V., Taylor, J. M., and Briegel, H. J. (2016). Quantum-enhanced machine learning. *Physical review letters*, 117(13):130501.

[Goodfellow et al., 2014] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. (2014). Generative adversarial nets. In *Advances in neural information processing systems*, pages 2672–2680.

[Guo et al., 2018] Guo, J., Lu, S., Cai, H., Zhang, W., Yu, Y., and Wang, J. (2018). Long text generation via adversarial training with leaked information. In *Thirty-Second AAAI Conference on Artificial Intelligence*, pages 5141–5148.

[Hu et al., 2019] Hu, L., Wu, S.-H., Cai, W., Ma, Y., Mu, X., Xu, Y., Wang, H., Song, Y., Deng, D.-L., Zou, C.-L., et al. (2019). Quantum generative adversarial learning in a superconducting quantum circuit. *Science Advances*, 5(1):eaav2761.

[Huggins et al., 2018] Huggins, W. J., Patil, P., Mitchell, B., Whaley, K. B., and Stoudenmire, M. (2018). Towards quantum machine learning with tensor networks. *Quantum Science and Technology*.

[Khoshaman et al., 2018] Khoshaman, A., Vinci, W., Denis, B., Andriyash, E., and Amin, M. H. (2018). Quantum variational autoencoder. *Quantum Science and Technology*, 4(1):014001.

[Kingma and Ba, 2014] Kingma, D. P. and Ba, J. (2014). Adam: A method for stochastic optimization. *arXiv:1412.6980*.

[Kingma and Welling, 2013] Kingma, D. P. and Welling, M. (2013). Auto-encoding variational bayes. *arXiv:1312.6114*.

[Lamata et al., 2018] Lamata, L., Alvarez-Rodriguez, U., Martín-Guerrero, J. D., Sanz, M., and Solano, E. (2018). Quantum autoencoders via quantum adders with genetic algorithms. *Quantum Science and Technology*, 4(1):014007.

[Liu and Wang, 2018] Liu, J.-G. and Wang, L. (2018). Differentiable learning of quantum circuit born machines. *Physical Review A*, 98(6):062324.

[Lloyd and Weedbrook, 2018] Lloyd, S. and Weedbrook, C. (2018). Quantum generative adversarial learning. *Physical review letters*, 121(4):040502.

[Mitarai et al., 2018] Mitarai, K., Negoro, M., Kitagawa, M., and Fujii, K. (2018). Quantum circuit learning. *Physical Review A*, 98(3):032309.

[Monràs et al., 2017] Monràs, A., Sentís, G., and Wittek, P. (2017). Inductive supervised quantum learning. *Physical review letters*, 118(19):190503.

[Rebentrost et al., 2014] Rebentrost, P., Mohseni, M., and Lloyd, S. (2014). Quantum support vector machine for big data classification. *Physical review letters*, 113(13):130503.

[Romero et al., 2017] Romero, J., Olson, J. P., and Aspuru-Guzik, A. (2017). Quantum autoencoders for efficient compression of quantum data. *Quantum Science and Technology*, 2(4):045001.

[Schuld et al., 2018] Schuld, M., Bocharov, A., Svore, K., and Wiebe, N. (2018). Circuit-centric quantum classifiers. *arXiv:1804.00633*.

[Wan et al., 2017] Wan, K. H., Dahlsten, O., Kristjánsson, H., Gardner, R., and Kim, M. (2017). Quantum generalisation of feedforward neural networks. *npj Quantum Information*, 3(1):36.

[Wiebe et al., 2012] Wiebe, N., Braun, D., and Lloyd, S. (2012). Quantum algorithm for data fitting. *Physical review letters*, 109(5):050505.

[Yu et al., 2019] Yu, C.-H., Gao, F., Liu, C., Huynh, D., Reynolds, M., and Wang, J. (2019). Quantum algorithm for visual tracking. *Physical Review A*, 99(2):022301.

[Yu et al., 2016] Yu, C.-H., Gao, F., Wang, Q.-L., and Wen, Q.-Y. (2016). Quantum algorithm for association rules mining. *Physical Review A*, 94(4):042311.

Distributed Encoding and Decoding of Quantum Information over Networks

Hayata Yamasaki[1] * Mio Murao[2] †

[1]*Photon Science Center, Graduate School of Engineering, The University of Tokyo, 7–3–1 Hongo, Bunkyo-ku, Tokyo 113–8656, Japan*

[2]*Department of Physics, Graduate School of Science, The University of Tokyo, 7–3–1 Hongo, Bunkyo-ku, Tokyo 113–0033, Japan*

Abstract. We analyze entanglement costs of encoding and decoding quantum information in a multipartite quantum system distributed among spatially separated parties connected by a network, aiming at quantitatively characterizing nonlocal properties of the encoding and decoding. We identify conditions for parties being able to encode or decode quantum information in the distributed quantum system deterministically and exactly, when inter-party quantum communication is restricted to a tree-topology network. While encoding and decoding are inverse of each other, our results suggest that a quantitative difference in entanglement cost between encoding and decoding arises due to the difference between quantum state merging and splitting.

Keywords: distributed quantum information processing, quantum network, quantum encoding and decoding, multipartite entanglement transformation, entanglement cost

1 Motivation and setting

Encoding and decoding quantum information in a multipartite quantum system are fundamental building blocks in quantum information processing. In particular, quantum error correcting codes [2–5] require such encoding and decoding between a logical state and an entangled physical state of a multipartite system. Quantum information is represented by this logical state, and these encoding and decoding are the inverse transformation of each other, mathematically represented by isometries. These encoding and decoding have to be performed so that coherence of these states is kept; that is, an arbitrary superposition of the logical state should be preserved without revealing the classical description of the logical state. In addition to quantum information processing, the concept of encoding and decoding nowadays has interdisciplinary roles in analyzing many-body quantum systems exhibiting nonlocal features, such as topological order in quantum phase of matter [6, 7], holographic principle in quantum gravity [8, 9], and eigenstate thermalization hypothesis in statistical physics [10].

These encoding and decoding are also indispensable when we aim to perform distributed quantum information processing, where spatially separated parties connected by a network for quantum communication cooperate in achieving an information processing task. Distributed quantum information processing is considered to be a promising candidate for realizing large-scale quantum computation, since there exists technical difficulty in increasing the number of low-noise qubits in one quantum device. Moreover, encoding and decoding are especially crucial for some multiparty cryptographic tasks such as quantum secret sharing [11–13]. In these distributed settings, a multipartite system encoding a logical state is distributed among these spatially separated parties. Thus, encoding and decoding are nonlocal transformations over all the parties, and the nonlocal properties of transformations for encoding and decoding lead to cost in implementations of the encoding and decoding.

This submission with the technical version [1] aims to quantitatively characterize nonlocal properties of transformations for the encoding and decoding in the distributed settings, adopting an entanglement theoretical approach. In the entanglement theory, operations beyond the restriction of local operations and classical communication (LOCC) can be performed with assistance of nonlocal resource states, such as bipartite maximally entangled states. Under LOCC, a single use of a noiseless quantum channel and that of a maximally entangled state are at equivalent cost by means of quantum teleportation achieving quantum communication [14]. For a bipartite state, the minimal amount of quantum communication required for preparing the state provides a well-established entanglement measure

*yamasaki@qi.t.u-tokyo.ac.jp

†murao@phys.s.u-tokyo.ac.jp

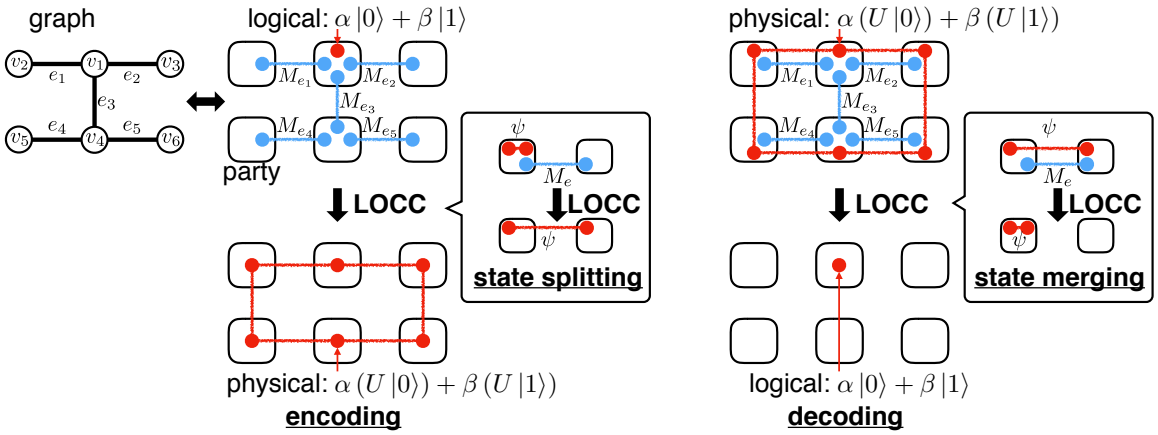


Figure 1: Encoding and decoding quantum information in a multipartite quantum system shared among spatially separated parties, where the quantum information is represented by *unknown* states illustrated by red circles. The parties are connected by a network of noiseless quantum channels represented by a graph, so that the parties can sequentially apply exact state splitting to spread quantum information for encoding, and exact state merging to concentrate quantum information for decoding. Under LOCC, a single use of each noiseless quantum channel represented by an edge e of the graph is equivalent to that of a maximally entangled state $\left|\Phi^+_{M_e}\right\rangle$ of the Schmidt rank M_e illustrated by a pair of blue circles connected by a line.

quantifying a nonlocal property of the state, called the *entanglement cost* of the state [15–17]. The entanglement cost of a bipartite *state* also generalizes to that required for spatially separated parties implementing a given nonlocal *transformation*, such as nonlocal unitaries [18–37] and nonlocal measurements [38–40], although this generalization usually accompanies challenging optimization and has been analyzed only in special cases to date. Another direction is generalization of a *bipartite* state to a *multipartite* state [41–43] while analysis of multipartite entanglement is also challenging [44–46]. Regarding a multipartite generalization in terms of quantum communication, Ref. [41] formulates a cost required for preparing a multipartite state shared among parties using a network [47] of the noiseless quantum channels.

Progressing beyond these previous works, we formalize entanglement costs characterizing the nonlocal properties of multipartite transformations for encoding and decoding. In our setting, as illustrated in Fig. 1, N parties are connected by a network of the noiseless quantum channels. The network topology is represented by a graph $G=(V,E)$, where each vertex $v_k\in V=\{v_1,\ldots,v_N\}$ represents one of the N parties, and each edge $e=\{v_k,v_{k'}\}\in E$ represents the channel between two parties v_k and $v_{k'}$. Any connected network of N parties requires at least $N-1$ channels. If an N-vertex connected graph has exactly $N-1$ edges, the graph is called a tree, denoted by $T=(V,E)$. Given any connected graph, there exist trees spanning all the vertices which can be obtained by removing some of the edges of the given graph. We consider tasks where using quantum communication over a given network, the parties spread and concentrate quantum information of arbitrary *unknown* state so as to encode and decode the quantum information in a distributed system. In other words, for any unknown state, these tasks aim to implement a given nonlocal isometry $U:\mathcal{H}^{v_1}\to\bigotimes_{k=1}^N\mathcal{H}^{v_k}$ and $U^\dagger:\bigotimes_{k=1}^N\mathcal{H}^{v_k}\to\mathcal{H}^{v_1}$ representing the encoding and decoding, respectively, where $\mathcal{H}^{v_k}$ represents a local system for each party $v_k\in V$, and without loss of generality, we always assign $v_1\in V$ as the party where logical states of these encoding and decoding are input and output. These tasks are performed deterministically and exactly.

The amount of quantum communication required for spreading and concentrating quantum information over the network characterizes nonlocal properties of the isometries. In our setting, we assume that LOCC is free, and consider a collection of *bipartite* entanglement as an initial resource state that is motivated by quantum communication on networks, while more general states exhibiting *multipartite* entanglement could also be candidates for resources. Since quantum communication of a state of an M_e-dimensional system is achieved by LOCC assisted by a maximally entangled state $\left|\Phi^+_{M_e}\right\rangle^e:=\frac{1}{\sqrt{M_e}}\sum_{l=0}^{M_e-1}|l\rangle^{v_k}\otimes|l\rangle^{v_{k'}}$ of the Schmidt rank M_e shared between v_k and $v_{k'}$ connected by an edge $e=\{v_k,v_{k'}\}$, we consider the initial resource state

$\bigotimes_{e\in E}\left|\Phi^+_{M_e}\right\rangle^e$ consisting of bipartite maximally entangled states distributed according to a given network topology $G=(V,E)$, which serves as a resource for quantum communication on the network. The minimal total amount of quantum communication for spreading and concentrating quantum information is evaluated by the entanglement entropy $\log_2 M_e$ of the maximally entangled state for each edge $e\in E$, which we call the *entanglement costs of spreading and concentrating quantum information*. The entanglement cost of spreading quantum information characterizes the encoding represented by a given isometry U, and that of concentrating characterizes the decoding represented by $U^\dagger$.

2 Results and implications

We evaluate the entanglement costs of spreading and concentrating quantum information over any given tree-topology network for an *arbitrarily* given isometry, which differs from the works presented in Ref. [48, 49] for implementing *particular* isometries in the context of quantum secret sharing. During spreading and concentrating *quantum* information, coherence has to be kept, and this point contrasts with encoding and decoding *classical* information in a distributed quantum system which have been investigated in the context of a type of quantum secret sharing based on LOCC state distinguishability [50–55]. To analyze the entanglement costs, we consider multiparty transformations between *particular* fixed states that are proven to be equivalent to spreading and concentrating quantum information represented by *arbitrary* unknown states. Then, we achieve these multiparty transformations by reducing them to sequential applications of exact quantum state merging and splitting for two parties that we have established in Ref. [56] (See also Fig. 1).

Regarding spreading quantum information, we use exact state splitting to provide an algorithm that achieves the *optimal* entanglement cost of spreading quantum information for any encoding. Note that we show this optimality using the LOCC monotonicity of the Schmidt rank.

Theorem 1 Entanglement cost of spreading quantum information. *Given any tree T representing network topology and any isometry $U:\mathcal{H}^{v_1}\to\bigotimes_{k=1}^N\mathcal{H}^{v_k}$ representing encoding, the* minimal *entanglement cost of spreading quantum information according to the encoding U over the network T is given in terms of the rank of quantum states that can be defined with respect to each edge of T.*

We also provide another algorithm achieving concentrating quantum information using exact state merging, and show that the entanglement cost of concentrating quantum information can be reduced compared to that of spreading.

Theorem 2 Entanglement cost of concentrating quantum information. *Given any tree T representing network topology and any isometry $U^\dagger:\bigotimes_{k=1}^N\mathcal{H}^{v_k}\to\mathcal{H}^{v_1}$ representing decoding, there exists an algorithm for concentrating quantum information according to the decoding $U^\dagger$ over the network T whose entanglement cost, given by an explicitly calculable formula, is always* smaller *or equal to that for the corresponding encoding U over T.*

Applications of our algorithms for spreading and concentrating quantum information are wide-range because these algorithms are applicable to any isometry representing encoding and decoding. Given any tree-topology network, the algorithm for concentrating quantum information achieves zero entanglement cost in decoding quantum error correcting codes such as the 5-qubit and 7-qubit codes, while the algorithm for spreading quantum information is optimal for any encoding. Using these algorithms, we show an algorithm for one-shot distributed source compression [57–59] that is applicable to arbitrarily small-dimensional systems unlike the previously known algorithms. We also provide a general algorithm for LOCC-assisted decoding of shared quantum information that have been studied in the context of quantum secret sharing for special classes of encoding [60].

Consequently, while the multipartite entanglement transformations $U:\mathcal{H}\to\bigotimes_{k=1}^N\mathcal{H}^{v_k}$ for encoding and $U^\dagger:\bigotimes_{k=1}^N\mathcal{H}^{v_k}\to\mathcal{H}$ for decoding are inverse of each other, our results yield bounds that quantitative differentiate between nonlocal properties of U and $U^\dagger$ in terms of entanglement cost. Further analyses of these tasks over other network topologies than trees may lead to another characterization of nonlocal properties of the multipartite transformations in terms of changes of network topologies, while our algorithms for trees also provide bounds of the entanglement costs over general-topology networks by considering their spanning trees. The concept of encoding and the decoding represented by isometries has essential roles not only in quantum information science, and we leave investigation of further applications within and beyond quantum information science for future works.

References

[1] H. Yamasaki and M. Murao, *Adv. Quantum Technol.* **2019**, 2, 1800066, arXiv:1807.11483.

[2] D. Gottesman, arXiv:0904.2557.

[3] S. J. Devitt, W. J. Munro, K. Nemoto, *Rep. Prog. Phys.* **2013**, *76*, 076001.

[4] B. M. Terhal, *Rev. Mod. Phys.* **2015**, *87*, 307.

[5] B. J. Brown, D. Loss, J. K. Pachos, C. N. Self, J. R. Wootton, *Rev. Mod. Phys.* **2016**, *88*, 045005.

[6] A. Y. Kitaev, *Ann. Phys.* **2003**, *303*, 2.

[7] A. Y. Kitaev, *Ann. Phys.* **2006**, *321*, 2.

[8] A. Almheiri, X. Dong, D. Harlow, *J. High Energy Phys.* **2015**, *04*, 163.

[9] F. Pastawski, B. Yoshida, D. Harlow, J. Preskill, *J. High Energy Phys.* **2015**, *06*, 149.

[10] F. G. S. L. Brandão, E. Crosson, M. B. Şahinoğlu, J. Bowen, arXiv:1710.04631.

[11] M. Hillery, V. Bužek, A. Berthiaume, *Phys. Rev. A* **1999**, *59*, 1829.

[12] R. Cleve, D. Gottesman, H.-K. Lo, *Phys. Rev. Lett.* **1999**, *83*, 648.

[13] D. Gottesman, *Phys. Rev. A* **2000**, *61*, 042311.

[14] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, *Phys. Rev. Lett.* **1993**, *70*, 1895.

[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, *Phys. Rev. A* **1996**, *54*, 3824.

[16] P. M. Hayden, M. Horodecki, B. M. Terhal, *J. Phys. A* **2001**, *34*, 6891.

[17] B. M. Terhal, P. Horodecki, *Phys. Rev. A* **2000**, *61*, 040301.

[18] X. Zhou, D. W. Leung, I. L. Chuang, *Phys. Rev. A* **2000**, *62*, 052316.

[19] J. Eisert, K. Jacobs, P. Papadopoulos, M. B. Plenio, *Phys. Rev. A* **2000**, *62* 052317.

[20] A. Chefles, C. R. Gilson, S. M. Barnett, *Phys. Rev. A* **2001**, *63*, 032314.

[21] D. Collins, N. Linden, S. Popescu, *Phys. Rev. A* **2001**, *64*, 032302.

[22] M. A. Nielsen, C. M. Dawson, J, L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, A. Hines, *Phys. Rev. A* **2003**, *67*, 052301.

[23] C.-P. Yang, *Phys. Lett. A* **2008**, *372*, 9, 25, 1380.

[24] S. M. Cohen, *Phys. Rev. A* **2010**, *81*, 062316.

[25] L. Yu, R. B. Griffiths, S. M. Cohen, *Phys. Rev. A* **2010**, *81*, 062315.

[26] D. Stahlke, R. B. Griffiths, *Phys. Rev. A* **2011**, *84*, 032316.

[27] A. Soeda, P. S. Turner, M. Murao, *Phys. Rev. Lett.* **2011**, *107*, 180501.

[28] L. Chen, L. Yu, *Phys. Rev. A* **2014**, *89*, 062326.

[29] L. Chen, L. Yu, *Ann. Phys.* **2014**, *351*, 682.

[30] D. Saha, S. Nandan, P. K. Panigrahi, J. *Quantum Inf. Sci.* **2014**, *4*, 2, 46117.

[31] L.-P. Xue, M. Jiang, *2015 34th Chinese Control Conference (CCC)* **2015**, *6636*.

[32] L. Chen, L. Yu, *Phys. Rev. A* **2016**, *93*, 042331.

[33] N. Vyas, D. Saha, P. K. Panigrahi, *Quantum Inf. Processing* **2016**, *15*, 3855.

[34] L. Yu, K. Nemoto, *Phys. Rev. A* **2016**, *94*, 022320.

[35] E. Wakakuwa, A. Soeda, M. Murao, *IEEE Trans. Inf. Theory* **2017**, *63*, 5372.

[36] E. Wakakuwa, A. Soeda, M. Murao, arXiv:1608.07461.

[37] E. Wakakuwa, A. Soeda, M. Murao, arXiv:1810.08447.

[38] R. Jozsa, M. Koashi, N. Linden, S. Popescu, S. Presnell, D. Shepherd, A. Winter, *Quantum Inf. Comput.* **2003**, *3*, 5, 405.

[39] S. Bandyopadhyay, G. Brassard, S. Kimmel, W. K. Wootters, *Phys. Rev. A* **2009**, *80*, 012313.

[40] S. Bandyopadhyay, R. Rahaman, W. K. Wootters, *J. Phys. A* **2010**, *43*, 45.

[41] H. Yamasaki, A. Soeda, M. Murao, *Phys. Rev. A* **2017**, *96*, 032330.

[42] E. F. Galvão, L. Hardy, *Phys. Rev. A* **2000**, *62*, 012309.

[43] S. Yang, H. Jeong, *Phys. Rev. A* **2015**, *92*, 022322.

[44] J. Eisert, D. Gross, in *Lectures on Quantum Information*, (Eds: D. Bruß, G. Leuchs), Wiley, Weinheim **2007**, Ch. 13.

[45] M. Walter, D. Gross, J. Eisert, arXiv:1612.02437.

[46] I. Bengtsson, K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, Cambridge University Press, New York **2017**, Ch. 17.

[47] H. J. Kimble, *Nature* **2008**, *453*, 1023.

[48] B. Fortescue, G. Gour, *IEEE Trans. Inf. Theory* **2012**, *58*, 6659.

[49] K. Senthoor, P. K. Sarvepalli, arXiv:1801.09500.

[50] R. H. Choi, B. Fortescue, G. Gour, B. C. Sanders, *Phys. Rev. A* **2013**, *87*, 032319.

[51] R. Rahaman, M. G. Parker, *Phys. Rev. A* **2015**, *91*, 022330.

[52] Y.-H. Yang, F. Gao, X. Wu, S.-J. Qin, H.-J. Zuo, Q.-Y. Wen, *Sci. Rep.* **2015**, *5*, 16967.

[53] J. Wang, L. Li, H. Peng, Y. Yang, *Phys. Rev. A* **2017**, *95*, 022320.

[54] C.-M. Bai, Z.-H. Li, C.-J. Liu, Y.-M. Li, *Quantum Inf. Processing* **2017**, *16*, 304.

[55] C.-J. Liu, Z.-H. Li, C.-M. Bai, M.-M. Si, *Int. J. Theor. Phys.* **2018**, *57* 428.

[56] H. Yamasaki, M. Murao, *IEEE Trans. Inf. Theory* **2019**, *65*, 6, 3950.

[57] N. Dutil, P. Hayden, arXiv:1011.1974.

[58] N. Dutil, *PhD Thesis*, McGill University, May, **2011**.

[59] A. Anshu, R. Jain, N. A. Warsi, *IEEE Trans. Inf. Theory* **2018**, *64*, 3, 1436.

[60] V. Gheorghiu, B. C. Sanders, *Phys. Rev. A* **2013**, *88*, 022340.

Extended Abstract: Experimental Cryptographic Verification for Near-Term Quantum Cloud Computing

Xi Chen,[1,2,3,*] Bin Cheng,[4,*] Zhaokai Li,[1,2,3] Xinfang Nie,[1,2,3] Nengkun Yu,[5,†] Man-Hong Yung,[4,6,7,‡] and Xinhua Peng[1,2,3,§]

[1]*Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China (USTC), Hefei 230026, China*
[2]*CAS Key Laboratory of Microscale Magnetic Resonance, USTC, Hefei 230026, China*
[3]*Synergetic Innovation Center of Quantum Information and Quantum Physics, USTC, Hefei 230026, China*
[4]*Institute for Quantum Science and Engineering, and Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China*
[5]*Centre for Quantum Software and Information, School of Software, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW, Australia*
[6]*Shenzhen Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China*
[7]*Central Research Institute, Huawei Technologies, Shenzhen, 518129, P. R. China*

We explore the applicability of a cryptographic verification scheme for quantum cloud computing, where the clients are completely classical. We provided a theoretical extension and implemented the scheme on a 5-qubit NMR quantum processor in the laboratory and a 5-qubit and 16-qubit processors of the IBM quantum cloud. We found that the experimental results of the NMR processor can be verified by the scheme with about 2.5% error, after noise compensation by standard techniques. However, the fidelity of the IBM quantum cloud is currently too low to pass the test (about 42% error). This verification scheme shall become practical when servers claim to offer quantum-computing resources that can achieve quantum supremacy. (The long version of the present work is available on arXiv [1])

Introduction.— Quantum computation promises a regime with unprecedented computational power over classical devices, offering numerous interesting applications, such as factorization [2], quantum simulation [3, 4], and quantum machine learning [5, 6]. However, before quantum computers become prevalent to the public, one might expect that only organizations with sufficient resources could operate a full-scale quantum computer, analogous to today's supercomputers. Furthermore, individuals who have demands for quantum computation could access the service through the internet, i.e., quantum cloud computing. In fact, several small-scale quantum cloud services have already been launched [7–9], which can be operated by remote clients through the internet. As a result, many simulations performed from quantum cloud servers have been reported (see Ref. [10] for a summary).

In the near future, it is not impossible that these clouds may claim to offer 100 or more working qubits and many layers of quantum gates, where quantum supremacy [11–14] could be achieved. However, one may naturally ask, is there a real quantum computer behind the cloud? Or, would it just be a classical computer simulating quantum computation? For ordinary clients who only have control and access of classical computer, a natural task is to verify whether these cloud servers are truly quantum.

Alternatively, the question can be formalized as follows: *is it possible for a purely-classical client to verify the output of a quantum prover?* This question has been extensively explored for more than ten years. In 2004, Gottesman initialized this question, which Aaronson wrote down in his blog [15]. A straight-forward idea is to run a quantum algorithm solving certain NP problems, for example, Shor's algorithm for integer factorization [2]. Such problems might be hard for classical computation, but are easy for *classical verification* once the result is known. However, the challenge is that a full quantum algorithm typically requires thousands of qubits and quantum error correction to be implemented, which is out of question in the NISQ [16] (Noisy Intermediate-Scale Quantum) era.

Note that the verification problem have different variants. For example, one may assume that the supposedly "classical" client may actually have a limited ability to perform quantum operations on a small number of qubits. This line of research has already attracted much attention [17–23]. Without any quantum power, the client might still be able to verify delegated quantum computation which is spatially separated and entanglement can be shared [24, 25]. Currently, this approach does not seem to fit the setting of the available quantum cloud services, but it does reveal the outstanding challenge for establishing a rigorous verification scheme based on a classical client interacting with a single server using only classical communication [26].

Until recently, Mahadev has made important progresses [27, 28], assuming that the learning-with-errors problem [29] is computationally hard even for quantum computer. The protocol allows a classical computer to *interactively* verify the results of an efficient quantum computation, achieving a fully-homomorphic encryption scheme for quantum circuits with classical keys. Despite these great efforts, we are still facing the problems of "non-interactively" verifying *near-term* quantum clouds, which would be too noisy for implementing full quantum algorithms but may be capable of demonstrating quantum supremacy.

Here we report an experimental demonstration of a simple but powerful cryptographic verification protocol, originally

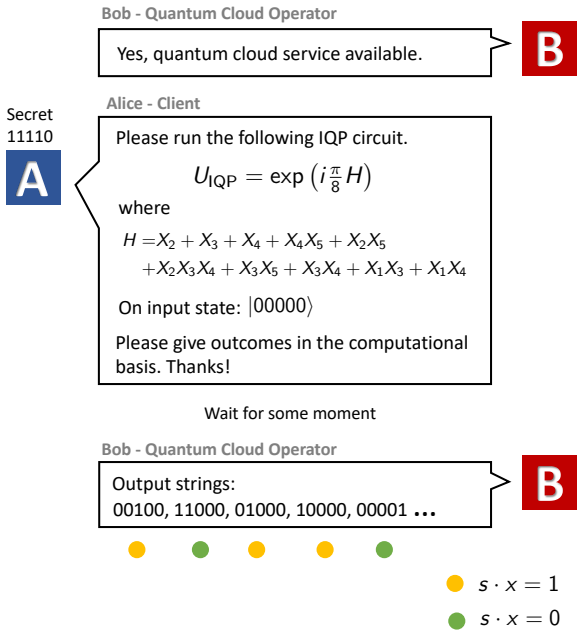


FIG. 1. Schematic representation of the protocol. Alice generates an IQP circuit and an associating secret vector s, using the method described in Ref. [30]. Bob runs this circuit, measures and sends back the measurement data to Alice. From Bob's data, Alice computes the probability bias $\mathcal{P}_{s\perp}$, with respect to the secret vector s, and sees whether it is close to 0.854, to decide whether Bob has a true quantum device or not.

proposed by Bremner and Shepherd [30] in 2008. We further extended the theoretical construction in terms of n-point correlation. The implementation was first performed with a 5-qubit NMR quantum processor in the laboratory. Additionally, we also benchmarked the performance of the verification scheme by actually implementing the protocol with the IBM quantum cloud processors [7].

The verification protocol implemented is based on a simplified circuit model of quantum computation, called IQP (instantaneous quantum polynomial) model [30]; the qubits are always initialized in the '0' state. The IQP circuits contain three parts. In the first and the last part, single-qubit Hadamard gates are applied to every qubit. The middle part of an IQP circuit does not contain an explicit temporal structure, in the sense that diagonal (and hence commuting) gates acting on single or multiple qubits are applied. On one hand, the IQP model represents a relatively resource-friendly computational model to be tested with near-term quantum devices. On the other hand, the IQP model has been proven to be hard for classical simulation [31, 32], under certain computational assumptions, similar to Boson sampling [33].

Verification protocol.— In the cryptographic verification protocol [30], there are two parties labeled as Alice (the client) and Bob (the server). Alice is assumed to be *completely classical*; she can only communicate with others through classical communication (e.g., internet). Suppose Bob claims to own a quantum computer and Alice is going to test it. In reality, of course, there is no need for Alice to inform Bob about her intention; she may just pretend to run a normal quantum program. The protocol can be succinctly summarized as follows (depicted by Fig. 1).

Step 1: Alice first generates an IQP circuit U_{IQP} associated with a secret string $s \in \{0,1\}^n$, which is only kept by Alice. Then she sends the information about the circuit to Bob.

Step 2: Bob returns the outputs to Alice in terms of the bit strings $x \in \{0,1\}^n$, which should follow the distribution of the IQP circuit, i.e., $\Pr(x) = |\langle x| U_{\mathrm{IQP}} |0^n\rangle|^2$, if Bob is honest.

Step 3: Ideally, Alice should be able to determine if the probability distributions $\Pr(x)$ for a subset of strings orthogonal to the secret string, where $x \cdot s \equiv x_1 s_1 + x_2 s_2 + \cdots + x_n s_n = 0 \mod 2$, add up to an expected value 0.854. Otherwise, Bob fails to pass the test.

More specifically, the key quantity of interest is the following probability bias defined by,

$$\mathcal{P}_{s\perp} \equiv \sum_{x\in\{0,1\}^n} |\langle x|U_{\mathrm{IQP}}|0^n\rangle|^2 \, \delta_{x\cdot s=0} \,, \tag{1}$$

where $\delta_{x\cdot s=0} = 1$ if it is true that $x \cdot s = 0$, and $\delta_{x\cdot s=0} = 0$ otherwise. For a perfect quantum computation, the value of the probability bias should be $\mathcal{P}_{s\perp} = 0.854$. The best known classical algorithm [30] would instead produce a value of 0.75, which is relevant when n is sufficiently large. This quantum-classical gap in the probability bias makes it possible to apply such a resource-friendly cryptographic verification scheme for testing quantum cloud computing in the regime where quantum supremacy would be achieved.

The IQP circuit used in the protocol is of the form $\exp(i\theta H)$, where the effective Hamiltonian H is a sum of tensor products of Pauli-X (see Fig. 1 for an example). Each term in the Hamiltonian can be represented as an n-bit binary vector, with the positions of 1 indicating the qubits that this term non-trivially acts on; for example, $X_1X_3X_4$ corresponds to $(1,0,1,1,0)$.

Here the IQP circuit has a layer of security for protecting the knowledge of the secret string s from Bob. Explicitly, there are two parts in the Hamiltonian (and hence the circuit), (i) the main part and (ii) a redundant part. Those vectors representing terms in the main part are not orthogonal to the secret vector s, i.e., $x \cdot s = 1$, while vectors for the redundant part are, i.e., $x \cdot s = 0$. Both parts have to be changed if the secret string is changed.

However, an important property of the IQP circuit is that the probability bias $\mathcal{P}_{s\perp}$ depends only on the main part. So Alice can append as many redundant vectors that are orthogonal to s to this Hamiltonian as she wishes, which corresponds to adding gates to the circuit. Of course, later she would need to scramble the Hamiltonian, in order to hide the secret s from Bob. See the long version for a description [1].

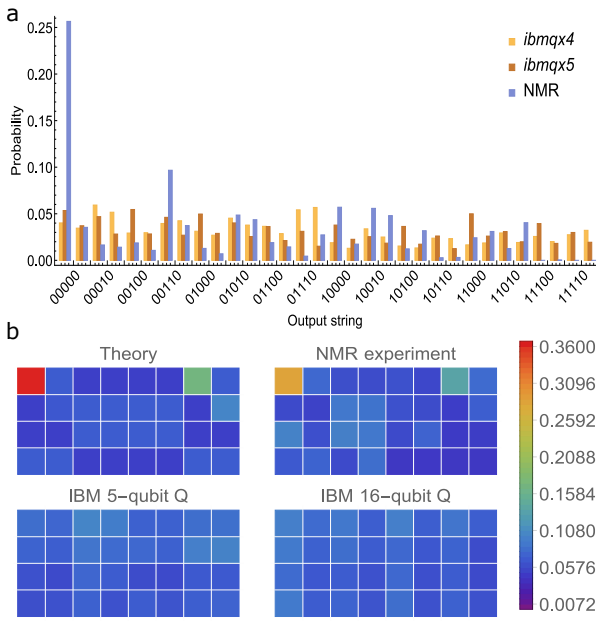


FIG. 2. **(a)** Probability distributions from IBM quantum processors and the NMR processor. *ibmqx4* is the 5-qubit processor and *ibmqx5* is the 16-qubit one. **(b)** The probabilities are put into grids and the colors indicate their values according to the color scale on the right.

Theoretical extension.— We provide a theoretical extension of the original work [30], transforming it into a form more familiar to the physics community. Specifically, we connect the probability bias in Eq. (1) with the Fourier coefficient of the probability $\Pr(x)$ of the output strings. As a result, we can express the probability bias through the n-point correlation function (see the long version [1]):

$$\mathcal{P}_{s\perp} = \frac{1}{2}\left(1 + \langle Z^{s_1} Z^{s_2} \cdots Z^{s_n} \rangle\right) . \tag{2}$$

Since the string $s = s_1 s_2 \cdots s_n$ is not known to Bob, the verification protocol can be regarded as a game where Alice tests the outcomes in terms of a particular correlation function unknown to Bob.

In addition, the representation of Eq. (2) provides a straightforward way to understand why the redundant part of the IQP circuit does not affect the probability bias—they commute with the n-point correlation function.

Our theoretical extension in Eq. (2) allows us to take into account the effect of noises. More precisely, if one models [34, 35] the decoherence by a dephasing channel (with an error rate ϵ) applied for each qubit at each time step, then the probability bias becomes $\mathcal{P}_{s\perp} \to \frac{1}{2}\left(1 + (1-2\epsilon)^{|s|} \langle Z^{s_1} Z^{s_2} \cdots Z^{s_n} \rangle\right)$, where $|s|$ is the Hamming weight of s, that is the number of 1's in s.

Experimental results.— Experimentally, our data were taken separately from two different sources, namely a five-qubit NMR processor in the laboratory, and the IBM cloud services, aiming to benchmark the performances of the IQP circuit implementation under the laboratory conditions and that from the quantum-cloud service.

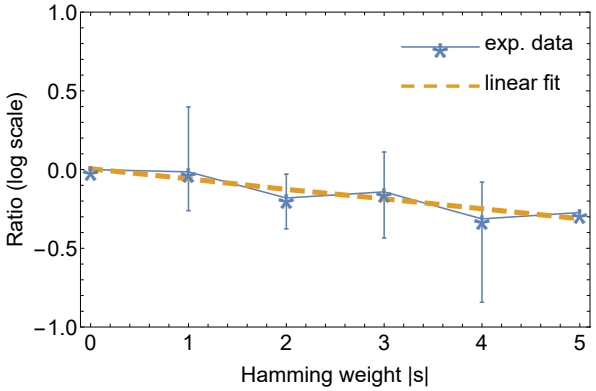


FIG. 3. The ratio of the experimental value to the theoretical value of the n-point correlation function $\langle Z^{s_1} Z^{s_2} \cdots Z^{s_n} \rangle$ in log scale, versus Hamming weights.

Our results show that the laboratory NMR quantum processor can be employed to verify the IQP circuit after noise compensation by standard techniques, but the IBM quantum cloud was too noisy. The probability bias obtained from the IBM's processors are close to 0.5, which is the result of uniform distribution. The main reason is that IBM's system has many constraints on the connectivity between the physical qubits; we had to include many extra SWAP gates to complete the circuit, causing a severe decoherence problem.

Specifically, the blue histogram in Fig. 2 (a) gives the output distribution from the NMR processor, which is the raw data. The probability bias from this raw distribution is 0.755. After noise compensation, the probability bias obtained from the NMR processor is 0.866 ± 0.016 (comparable to the theoretical value: 0.854).

The other two histograms in Fig. 2 (a) show the distribution from two IBM quantum devices. However, the probability bias from the two distributions is 0.488 and 0.492, respectively, which are all close to that from a completely mixed state, indicating that the final states of the IBM devices are highly corrupted by noise. Fig. 2 (b) shows the comparison of experimental data. The probabilities are put into a grid, and the color indicates the corresponding values, according to the color scale on the right.

As we mentioned, we can use the relation between probability bias and n-point correlation function to study the effect of noise. If there is single-qubit dephasing noise on every qubits at each step, the n-point correlation function will decay by a factor $(1-2\epsilon)^{|s|}$ [34, 35]. Thus the ratio of the experimental n-point correlation (which is from the raw distribution) to the theoretical value is $(1-2\epsilon)^{|s|}$. Fig. (3) shows this ratio in log scale, versus Hamming weights of all possible s. The slope of the linear fit is $\log(1-2\epsilon)$, from which we obtain an effective noise rate $\epsilon = 6.79\%$ of the NMR processor.

* These two authors contributed equally
† nengkunyu@gmail.com
‡ yung@sustech.edu.cn
§ xhpeng@ustc.edu.cn

[1] X. Chen, B. Cheng, X. Nie, N. Yu, M.-H. Yung, and X. Peng, "Experimental cryptographic verification for near-term quantum cloud computing," (2018), arXiv:1808.07375.
[2] P. Shor, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press).
[3] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[4] S. Lloyd, Science **273**, 1073 (1996).
[5] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009).
[6] S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum algorithms for supervised and unsupervised machine learning," (2013), arXiv:1307.0411.
[7] IBM QX team, "IBM Quantum Experience," https://github.com/QISKit/qiskit-backend-information, *ibmqx4* V1.1.0 accessed Dec 2017; *ibmqx5* V1.1.0 accessed May 2018.
[8] Rigetti Computing, devices specification http://docs.rigetti.com/en/latest/qpu.html.
[9] "Quantum in the Cloud," University of Bristol, http://www.bristol.ac.uk/physics/research/quantum/engagement/qcloud/.
[10] P. J. Coles, S. Eidenbenz, S. Pakin, A. Adedoyin, J. Ambrosiano, P. Anisimov, W. Casper, G. Chennupati, C. Coffrin, H. Djidjev, D. Gunter, S. Karra, N. Lemons, S. Lin, A. Lokhov, A. Malyzhenkov, D. Mascarenas, S. Mniszewski, B. Nadiga, D. O'Malley, D. Oyen, L. Prasad, R. Roberts, P. Romero, N. Santhi, N. Sinitsyn, P. Swart, M. Vuffray, J. Wendelberger, B. Yoon, R. Zamora, and W. Zhu, (2018), arXiv:1804.03719.
[11] J. Preskill, "Quantum computing and the entanglement frontier," (2012), arXiv:1203.5813.
[12] A. P. Lund, M. J. Bremner, and T. C. Ralph, npj Quantum Inf. **3**, 15 (2017).
[13] B. M. Terhal, Nat. Phys. **14**, 530 (2018).
[14] M.-H. Yung, Natl. Sci. Rev. , nwy072 (2018).
[15] At first sight, this seems a simple question. One may ask the quantum cloud to run a classical intractable task which is feasible for a quantum computer. This idea is not practical as it is equivalent to separating BQP (bounded-error quantum polynomial time) and P (polynomial time), one of the most important open problem in quantum complexity theory. See https://www.scottaaronson.com/blog/?p=284 for more detail..
[16] J. Preskill, "Quantum Computing in the NISQ era and beyond," (2018), arXiv:1801.00862.
[17] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (2009) pp. 517–526.
[18] A. Broadbent, J. Fitzsimons, and E. Kashefi, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **6154 LNCS**, 43 (2010).
[19] D. Aharonov, M. Ben-Or, and E. Eban, (2008), arXiv:0810.5375.
[20] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, (2008), arXiv:1704.04487.
[21] J. F. Fitzsimons and E. Kashefi, Phys. Rev. A **96**, 012303 (2017).
[22] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, Phys. Rev. Lett. **120**, 040501 (2018).
[23] D. Mills, A. Pappa, T. Kapourniotis, and E. Kashefi, Electronic Proceedings in Theoretical Computer Science **266**, 209 (2018).
[24] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).
[25] H.-L. Huang, Q. Zhao, X. Ma, C. Liu, Z.-E. Su, X.-L. Wang, L. Li, N.-L. Liu, B. C. Sanders, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **119**, 050503 (2017).
[26] S. Aaronson, A. Cojocaru, A. Gheorghiu, and E. Kashefi, (2017), arXiv:1704.08482.
[27] U. Mahadev, (2017), arXiv:1708.02130.
[28] U. Mahadev, (2018), arXiv:1804.01082.
[29] O. Regev, in *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05 (ACM, 2005) pp. 84–93.
[30] D. Shepherd and M. J. Bremner, Proc. R. Soc. A **465**, 1413 (2009).
[31] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A **467**, 459 (2011).
[32] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).
[33] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).
[34] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Quantum **1**, 8 (2017).
[35] M.-H. Yung and X. Gao, (2017), arXiv:1706.08913.

Quantifying the magic of quantum channels

Xin Wang[1] Mark M. Wilde[2] Yuan Su[1]

[1] *Joint Center for Quantum Information and Computer Science, University of Maryland, Maryland 20742, USA*
[2] *Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Louisiana 70803, USA*

Abstract. To achieve universal quantum computation via general fault-tolerant schemes, stabilizer operations must be supplemented with other non-stabilizer quantum resources. Motivated by this necessity, we develop a resource theory for magic quantum channels to characterize and quantify the quantum "magic" or non-stabilizerness of noisy quantum circuits. For qudit quantum computing with odd dimension d, it is known that quantum states with non-negative Wigner function can be efficiently simulated classically. First, inspired by this observation, we introduce a resource theory based on completely positive-Wigner-preserving quantum operations as free operations, and we show that they can be efficiently simulated via a classical algorithm. Second, we introduce two efficiently computable magic measures for quantum channels, called the mana and thauma of a quantum channel. As applications, we show that these measures not only provide fundamental limits on the distillable magic of quantum channels, but they also lead to lower bounds for the task of synthesizing non-Clifford gates. Third, we propose a classical algorithm for simulating noisy quantum circuits, whose sample complexity can be quantified by the mana of a quantum channel. We further show that this algorithm can outperform another approach for simulating noisy quantum circuits, based on channel robustness. Finally, we explore the threshold of non-stabilizerness for basic quantum circuits under depolarizing noise.

Keywords: Non-stabilizer state, fault-tolerant quantum computing, resource theory, gate synthesis

1 Introduction

One of the main obstacles to physical realizations of quantum computation is decoherence that occurs during the execution of quantum algorithms. Fault-tolerant quantum computation (FTQC) [1, 2] provides a framework to overcome this difficulty by encoding quantum information into quantum error-correcting codes, and it allows reliable quantum computation when the physical error rate is below a certain threshold value.

The fault-tolerant approach to quantum computation allows for a limited set of transversal, or manifestly fault-tolerant, operations, which are usually taken to be the stabilizer operations. However, the stabilizer operations alone do not enable universality because they can be simulated efficiently on a classical computer, a result known as the Gottesman–Knill theorem [3, 4]. The addition of non-stabilizer quantum resources, such as *non-stabilizer operations*, can lead to universal quantum computation [5]. With this perspective, it is natural to consider the resource-theoretic approach [6] to quantify and characterize non-stabilizer quantum resources, including both quantum states and channels.

One solution for the above scenario is to implement a non-stabilizer operation via state injection of so-called "magic states," which are costly to prepare via magic-state distillation [5] (see also [7, 8, 9, 10, 11, 12, 13]). The usefulness of such magic states also motivates the resource theory of magic states [14, 15, 16, 17, 18, 19], where the free operations are the stabilizer operations and the free states are the stabilizer states (abbreviated as "Stab"). Moreover, since a key step of fault-tolerant quantum computing is to implement non-stabilizer operations, a natural and fundamental problem is to quantify the non-stabilizerness or "magic" of quantum operations. As we are at the stage of Noisy Intermediate-Scale Quantum (NISQ) technology, a resource theory of magic for noisy quantum operations is desirable both to exploit the power and to identify the limitations of NISQ devices in fault-tolerant quantum computation.

This submission is based on arXiv:1903.04483.

2 Overview of results

In this paper, we develop a framework for the resource theory of magic quantum channels, based on qudit systems with odd prime dimension d. Related work on this topic has appeared recently [20], but the set of free operations that we take in our resource theory is larger, given by the completely positive-Wigner-preserving operations as we detail below. We note here that d-level fault-tolerant quantum computation based on qudits with prime d is of considerable interest for both theoretical and practical purposes [21, 22, 23, 24, 25]. In particular, we establish the following:

(i) We introduce and characterize the completely positive-Wigner-preserving (CPWP) operations. We then introduce two efficiently computable magic measures for quantum channels. The first is the mana of quantum channels, whose state version was introduced in [16]. The second is the max-thauma of quantum channels, inspired by the magic state measure from [19]. We prove several desirable properties of these two measures, including reduction to states, faithfulness, additivity for tensor products of channels, subadditivity for serial composition of channels, an amortization inequality, and monotonicity under CPWP superchannels.

(ii) We explore the ability of quantum channels to generate magic states. We first introduce the amortized

magic of a quantum channel as the largest amount of magic that can be generated via a quantum channel. Furthermore, we introduce an information-theoretic notion of the distillable magic of a quantum channel. In particular, we show that distillable magic of a quantum channel can be bounded by its max-thauma.

(iii) We apply our magic measures for quantum channels in order to evaluate the magic cost of quantum channels, and we explore further applications in quantum gate synthesis. In particular, we show that at least four T gates are required to perfectly implement a controlled-controlled-NOT gate.

(iv) We propose a classical algorithm, inspired by [26], for simulating quantum circuits, which is relevant for the broad class of noisy quantum circuits that are currently being run on NISQ devices. This algorithm has sample complexity that scales with respect to the mana of a quantum channel. We further show by concrete examples that the new algorithm can outperform a previous approach for simulating noisy quantum circuits [20].

3 Resource theory of magic quantum channels

For most known fault-tolerant schemes, the restricted set of quantum operations is the set of stabilizer operations, consisting of preparation and measurement in the computational basis and a restricted set of unitary operations. Here we review the basic elements of the stabilizer states and operations for systems with a dimension that is a product of odd primes. Let $\mathcal{H}_d$ denote a Hilbert space of dimension d, and let $\{|j\rangle\}_{j=0,\cdots,d-1}$ denote the standard computational basis. For a prime number d, we define the unitary boost and shift operators $X, Z \in \mathcal{L}(\mathcal{H}_d)$ in terms of their action on the computational basis. We define the Heisenberg–Weyl operators as $T_{\mathbf{u}} = \tau^{-a_1 a_2} Z^{a_1} X^{a_2}$, where $\tau = e^{(d+1)\pi i/d}$, $\mathbf{u} = (a_1, a_2) \in \mathbb{Z}_d \times \mathbb{Z}_d$. For each point $\mathbf{u} \in \mathbb{Z}_d \times \mathbb{Z}_d$ in the discrete phase space, there is a corresponding operator $A_{\mathbf{u}}$, and the value of the discrete Wigner representation [27, 28, 29] of a state ρ at this point is given by

$$W_\rho(\mathbf{u}) \coloneqq \frac{1}{d} \operatorname{Tr}[A_{\mathbf{u}} \rho], \tag{1}$$

where d is the dimension of the Hilbert space and $\{A_{\mathbf{u}}\}_{\mathbf{u}}$ are the phase-space point operators: $A_0 = \frac{1}{d} \sum_{\mathbf{u}} T_{\mathbf{u}}$ and $A_{\mathbf{u}} = T_{\mathbf{u}} A_0 T_{\mathbf{u}}^\dagger$.

Our *first main contribution* is to introduce a resource theory with the free operations being those that completely preserve the positivity of the Wigner function. This is motivated by the fact that any quantum circuit consisting of an initial quantum state, unitary evolutions, and measurements, each having non-negative Wigner functions, can be classically simulated [26].

Specifically, a Hermiticity-preserving linear map Π is called completely positive-Wigner-preserving (CPWP) if for any system R with odd dimension, the following holds

$$\forall \rho_{RA} \in \mathcal{W}_+, \quad (\mathrm{id}_R \otimes \Pi_{A\to B})(\rho_{RA}) \in \mathcal{W}_+, \tag{2}$$

where $\mathcal{W}_+$ denotes the set of quantum states with non-negative Wigner function. Indeed, any such free quantum operation can be efficiently simulated via a classical algorithm introduced in our paper and thus become reasonable free operations for the resource theory of magic. We further show that the following statements about CPWP operations are equivalent:

1. The quantum channel $\mathcal{N}$ is CPWP;
2. The discrete Wigner function of the Choi–Jamiołkowski matrix of $\mathcal{N}$ is non-negative;
3. The Wigner function of the channel $W_{\mathcal{N}}(\mathbf{v}|\mathbf{u}) \coloneqq \frac{1}{d_B} \operatorname{Tr}[A_B^{\mathbf{v}} \mathcal{N}(A_A^{\mathbf{u}})]$ is non-negative for all $\mathbf{u}$ and $\mathbf{v}$ (i.e., $W_{\mathcal{N}}(\mathbf{v}|\mathbf{u})$ is a conditional probability distribution or classical channel).

We then introduce two magic measures for channels:

$$\text{Mana of } \mathcal{N}: \ \mathcal{M}(\mathcal{N}) \coloneqq \log \max_{\mathbf{v}} \sum_{\mathbf{u}} |\operatorname{Tr} \mathcal{N}(A_{\mathbf{v}}) A_{\mathbf{u}}|/d,$$

$$\text{Max-thauma of } \mathcal{N}: \ \theta_{\max}(\mathcal{N}) \coloneqq \min_{\mathcal{E}: \mathcal{M}(\mathcal{E}) \le 0} D_{\max}(\mathcal{N} \| \mathcal{E}),$$

where $D_{\max}(\mathcal{N}\|\mathcal{E}) \coloneqq \log \min\{t : J_{AB}^{\mathcal{N}} \le t J_{AB}^{\mathcal{E}}\}$ and $J_{AB}^{\mathcal{N}}, J_{AB}^{\mathcal{E}}$ are Choi operators. Here, the mana of a channel $\mathcal{N}$ can be understood as the maximal mana that can be generated via $\mathcal{N}$ and it is generalized from the state version in [16]. Meanwhile, the max-thauma of a channel $\mathcal{N}$ is defined in terms of the channel divergence between $\mathcal{N}$ and the set of free operations.

We show that these measures have desirable properties, including faithfulness, additivity, monotonicity, and non-increase under amortization. In particular, we show the subadditivity of these measures under serial composition of channels: $\mathcal{M}(\mathcal{N}_2 \circ \mathcal{N}_1) \le \mathcal{M}(\mathcal{N}_1) + \mathcal{M}(\mathcal{N}_2)$, $\theta_{\max}(\mathcal{N}_2 \circ \mathcal{N}_1) \le \theta_{\max}(\mathcal{N}_1) + \theta_{\max}(\mathcal{N}_2)$, which can be applied to analyze operational tasks in FTQC.

4 Distilling magic from channels

Since many physical tasks relate to quantum channels and time evolution rather than directly to quantum states, it is of interest to consider the non-stabilizer properties of quantum channels. Now having established suitable measures to quantify the magic of quantum channels, it is natural to figure out the ability of a quantum channel to generate magic from input quantum states.

Our second contribution is to establish fundamental limits on the capability of the channel $\mathcal{N}$ to *generate magic states*. A common choice for a non-Clifford gate is the T-gate. The qutrit T gate [30] is given by $T = \operatorname{diag}(\xi, 1, \xi^{-1})$, where $\xi = e^{2\pi i/9}$ is a primitive ninth root of unity. The T gate leads to the T magic state $|T\rangle \coloneqq T|+\rangle$. Furthermore, by the method of state injection [31, 32], one can generate a T gate by acting with stabilizer operations on the T state $|T\rangle$.

The most general protocol for distilling some resource by means of a quantum channel $\mathcal{N}$ employs n invocations of the channel $\mathcal{N}$ interleaved by free channels [33, Section 7]. In our case, the resource of interest is magic, and

here we take the free channels to be the CPWP channels. In such a protocol, the instances of the channel $\mathcal{N}$ are invoked one at a time, and we can integrate all CPWP channels between one use of $\mathcal{N}$ and the next into a single CPWP channel, since the CPWP channels are closed under composition. The goal of such a protocol is to distill magic states from the channel.

In particular, we establish the limits for the T-gate generating capacity of a channel $\mathcal{N}$: the rate R of distilling T states via n uses of $\mathcal{N}$ with infidelity tolerance ε is upper bounded by

$$R \leq \frac{1}{\log(1+2\sin(\pi/18))}\left(\theta_{\max}(\mathcal{N}) + \frac{\log(1/[1-\varepsilon])}{n}\right).$$

Consequently, the T-gate generating capacity of a channel $\mathcal{N}$ (the rate of generating T gates via $\mathcal{N}$ with vanishing error in the asymptotic limit) is bounded by

$$C_T(\mathcal{N}) \leq \frac{\theta_{\max}(\mathcal{N})}{\log(1+2\sin(\pi/18))}.$$

The main idea here is to utilize the sub-additivity of $\theta_{\max}$ as well as the stabilizer hypothesis testing [19].

5 Magic cost of a quantum channel

Beyond magic distillation via quantum channels, the magic measures of quantum channels can also help us investigate the magic cost in quantum gate synthesis. In the past two decades, tremendous progress has been accomplished in the area of gate synthesis for qubits (e.g., [34, 35, 36, 37, 38, 39, 40, 41]) and qudits (e.g., [42, 43, 44, 45, 46]). Elementary two-qudit gates include the controlled-increment gate [43] and the generalized controlled-X gate [45, 46]. More recently, the synthesis of single-qutrit gates was studied in [47, 48].

Our third contribution is to establish lower bounds for the task of *synthesizing noiseless or noisy non-Clifford gates*. For a given channel $\mathcal{N}$, let $S_T(\mathcal{N})$ denote the number of qutrit T gates required to implement it. Then

$$S_T(\mathcal{N}) \geq \max\left\{\mathcal{M}(\mathcal{N})/\mathcal{M}(T), \theta_{\max}(\mathcal{N})/\theta_{\max}(T)\right\}.$$

The proof utilizes monotonicity of the channel measures.

As applications, we investigate gate synthesis of elementary gates. In particular, for the controlled-controlled-X qutrit gate, we find that

$$S_T(CCX) \geq \frac{\mathcal{M}(CCX)}{\mathcal{M}(|T\rangle\langle T|)} \geq \frac{2.1876}{0.6657} \geq 3.2861, \quad (3)$$

which means that four qutrit T gates are necessary to implement a qutrit CCX gate.

For NISQ devices, it is natural to consider gate synthesis under realistic quantum noise. One common noise model in quantum information processing is the depolarizing channel $\mathcal{D}_p(\rho) = (1-p)\rho + \frac{p}{d^2-1}\sum_{\substack{0\leq i,j\leq d-1 \\ (i,j)\neq(0,0)}} X^i Z^j \rho (X^i Z^j)^\dagger$. Suppose that a T gate is not available, but instead only a noisy version $\mathcal{D}_p \circ T$ of it is. Then it is reasonable to consider the number

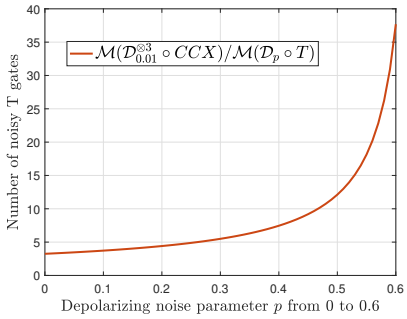


Figure 1: Number of noisy T gates required to implement a low-noise CCX gate.

of noisy T gates required to implement a low-noise CCX gate, and the resulting lower bound is depicted in Figure 1. Considering the depolarizing noise ($p = 0.01$), our lower bound gives the magic resource cost:

$$\mathcal{M}(\mathcal{D}_{0.01}^{\otimes 3} \circ CCX)/\mathcal{M}(\mathcal{D}_p \circ T).$$

6 Classical simulation of noisy circuits

An operational meaning associated with mana is that it quantifies the rate at which a quantum circuit can be simulated on a classical computer. Our fourth contribution is to propose a classical algorithm for simulating quantum channels, inspired by [26], whose sample complexity scales with the mana of quantum channels. We show that the complexity of this algorithm scales with the mana (the logarithmic negativity) of quantum channels, establishing mana as a useful measure for measuring the cost of classical simulation of a noisy quantum circuit.

Consider a noisy circuit consisting of channels $\{\mathcal{N}_l\}_{l=1}^L$ acting on the initial state $|0^n\rangle$, after which a computational basis measurement is performed. The goal is to estimate the value $\mathrm{Tr}\left[E(\mathcal{N}_L \circ \cdots \circ \mathcal{N}_1)(\rho)\right]$ for a stabilizer measurement operator E. With our algorithm, it suffices to take

$$\frac{2}{\epsilon^2}\mathcal{M}_{\rightarrow}^2 \log\left(\frac{2}{\delta}\right) \quad (4)$$

samples to estimate the probability of a fixed measurement outcome with accuracy ϵ and success probability $1-\delta$, where $\mathcal{M}_{\rightarrow} = 2^{\sum_{j=1}^L \mathcal{M}(\mathcal{N}_j)}$. Note that for a series of CPWP operations $\{\mathcal{N}_l\}_{l=1}^L$, it holds that $\mathcal{M}_{\rightarrow} = 2^{\sum_{j=1}^L \mathcal{M}(\mathcal{N}_j)} = 1$. This indicates that CPWP operations can be classically simulated efficiently and thus are reasonable free operations for the resource theory of magic quantum resources.

We further show via concrete examples that our algorithm can outperform previous approaches in simulating noisy quantum circuits. For an n-qudit system with odd prime dimension, the sample complexity of our algorithm is never worse than the algorithm of [20] based on channel robustness. Furthermore, our approach can be strictly faster than the simulation approaches based on channel robustness and magic capcaity [20] for certain quantum circuits.

References

[1] Peter W. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65. IEEE Comput. Soc. Press, 1996.

[2] Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, sep 2017.

[3] Daniel Gottesman. Stabilizer codes and quantum error correction. *PhD thesis*, may 1997.

[4] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, nov 2004.

[5] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, feb 2005.

[6] Eric Chitambar and Gilad Gour. Quantum resource theories. jun 2018.

[7] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, nov 2012.

[8] Cody Jones. Multilevel distillation of magic states for quantum computing. *Physical Review A*, 87(4):042305, apr 2013.

[9] Jeongwan Haah, Matthew B. Hastings, D. Poulin, and D. Wecker. Magic state distillation with low space overhead and optimal asymptotic input count. *Quantum*, 1:31, oct 2017.

[10] Earl T. Campbell and Mark Howard. Magic state parity-checker with pre-distilled components. *Quantum*, 2:56, mar 2018.

[11] Matthew B. Hastings and Jeongwan Haah. Distillation with sublogarithmic overhead. *Physical Review Letters*, 120(5):050504, jan 2018.

[12] Anirudh Krishna and Jean-Pierre Tillich. Towards low overhead magic state distillation. *arXiv:1811.08461*, pages 1–7, nov 2018.

[13] Christopher Chamberland and Andrew W. Cross. Fault-tolerant magic state preparation with flag qubits. *arXiv:1811.00566*, nov 2018.

[14] Victor Veitch, Christopher Ferrie, David Gross, and Joseph Emerson. Negative quasi-probability as a resource for quantum computation. *New Journal of Physics*, 14(11):113011, nov 2012.

[15] Andrea Mari and Jens Eisert. Positive Wigner functions render classical simulation of quantum computation efficient. *Physical Review Letters*, 109(23):230503, dec 2012.

[16] Victor Veitch, S. A. Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. The resource theory of stabilizer quantum computation. *New Journal of Physics*, 16(1):013009, jan 2014.

[17] Mark Howard and Earl Campbell. Application of a resource theory for magic states to fault-tolerant quantum computing. *Physical Review Letters*, 118(9):090501, mar 2017.

[18] Sergey Bravyi, Graeme Smith, and John Smolin. Trading classical and quantum computational resources. *Physical Review X*, 6(2):021043, jun 2015.

[19] Xin Wang, Mark M. Wilde, and Yuan Su. Efficiently computable bounds for magic state distillation. *arXiv:1812.10145*, dec 2018.

[20] James R. Seddon and Earl Campbell. Quantifying magic for multi-qubit operations. *arXiv:1901.03322*, pages 1–35, jan 2019.

[21] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos, Solitons & Fractals*, 10(10):1749–1758, sep 1999.

[22] Mark Howard, Joel J. Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the magic for quantum computation. *Nature*, 510:351–355, June 2014.

[23] Earl T. Campbell. Enhanced fault-tolerant quantum computing in d-level systems. *Physical Review Letters*, 113(23):230501, dec 2014.

[24] Hussain Anwar, Earl T. Campbell, and Dan E. Browne. Qutrit magic state distillation. *New Journal of Physics*, 14(6):063006, feb 2012.

[25] Hillary Dawkins and Mark Howard. Qutrit magic state distillation tight in some directions. *Physical Review Letters*, 115(3):030501, jul 2015.

[26] Hakop Pashayan, Joel J. Wallman, and Stephen D. Bartlett. Estimating outcome probabilities of quantum circuits using quasiprobabilities. *Physical Review Letters*, 115(7):070501, mar 2015.

[27] William K. Wootters. A Wigner-function formulation of finite-state quantum mechanics. *Annals of Physics*, 176(1):1–21, may 1987.

[28] David Gross. Hudson's theorem for finite-dimensional quantum systems. *Journal of Mathematical Physics*, 47(12):122107, dec 2006.

[29] David Gross. Non-negative Wigner functions in prime dimensions. *Applied Physics B*, 86(3):367–370, feb 2007.

[30] Mark Howard and Jiri Vala. Qudit versions of the qubit pi/8 gate. *Physical Review A*, 86(2):022316, aug 2012.

[31] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, nov 1999.

[32] Xinlan Zhou, Debbie W. Leung, and Isaac L. Chuang. Methodology for quantum logic gate construction. *Physical Review A*, 62(5):052316, oct 2000.

[33] Eneet Kaur and Mark M. Wilde. Amortized entanglement of a quantum channel and approximately teleportation-simulable channels. *Journal of Physics A*, 51(3):035303, January 2018.

[34] Michael J. Bremner, Christopher M. Dawson, Jennifer L. Dodd, Alexei Gilchrist, Aram W. Harrow, Duncan Mortimer, Michael A. Nielsen, and Tobias J. Osborne. Practical scheme for quantum computation with any two-qubit entangling gate. *Physical Review Letters*, 89(24):247902, nov 2002.

[35] Matthew Amy, Dmitri Maslov, and Michele Mosca. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(10):1476–1489, oct 2014.

[36] Cody Jones. Low-overhead constructions for the fault-tolerant Toffoli gate. *Physical Review A*, 87(2):022328, feb 2013.

[37] Peter Selinger. Quantum circuits of T-depth one. *Physical Review A*, 87(4):042302, oct 2012.

[38] Neil J. Ross and Peter Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information and Computation*, 11-12:901–953, mar 2016.

[39] David Gosset, Vadym Kliuchnikov, Michele Mosca, and Vincent Russo. An algorithm for the T-count. *Quantum Information and Computation*, 14(15-16):1261–1276, aug 2014.

[40] Alex Bocharov, Martin Roetteler, and Krysta M Svore. Efficient synthesis of universal repeat-until-success quantum circuits. *Physical Review Letters*, 114(8):080502, feb 2015.

[41] Nathan Wiebe and Martin Roetteler. Quantum arithmetic and numerical analysis using repeat-until-success circuits. *Quantum Information & Computation*, 16:134–178, 2016.

[42] Ashok Muthukrishnan and C. R. Stroud. Multivalued logic gates for quantum computation. *Physical Review A*, 62(5):052309, feb 2000.

[43] Gavin K. Brennen, Stephen S. Bullock, and Dianne P. O'Leary. Efficient circuits for exact-universal computations with qudits. *Quantum Information and Computation*, 6:436, sep 2006.

[44] Stephen S. Bullock, Dianne P. O'Leary, and Gavin K. Brennen. Asymptotically optimal quantum circuits for d-level systems. *Physical Review Letters*, 94(23):230502, oct 2004.

[45] Yao-Min Di and Hai-Rui Wei. Synthesis of multivalued quantum logic circuits by elementary gates. *Physical Review A*, 87(1):012325, jan 2013.

[46] Yao-Min Di and Hai-Rui Wei. Optimal synthesis of multivalued quantum circuits. *Physical Review A*, 92(6):062317, dec 2015.

[47] Shiroman Prakash, Akalank Jain, Bhakti Kapur, and Shubhangi Seth. Normal form for single-qutrit Clifford+T operators and synthesis of single-qutrit gates. *Physical Review A*, 98(3):032304, mar 2018.

[48] Andrew N. Glaudell, Neil J. Ross, and Jacob M. Taylor. Canonical forms for single-qutrit Clifford+T operators. *arXiv preprint arXiv:1803.05047*, pages 1–19, mar 2018.